N O R M A I T A L I A N A C E I

Norma Italiana

CEI 0-16;V2

Data Pubblicazione

2023-05

Titolo

Regola tecnica di riferimento per la connessione di Utenti attivi e passivi alle reti AT ed MT delle imprese distributrici di energia elettrica

Title

Reference technical rules for the connection of active and passive consumers to the HV and MV electrical networks of distribution Company

VARIANTE

Sommario

Questa Norma costituisce la Variante V2 della Norma CEI 0-16:2022-03, ed è costituita dal solo Allegato T "Scambio informativo basato su standard IEC 61850" in versione consolidata come risultante dell'Allegato T della Norma CEI 0-16:2022-03, delle successive modifiche introdotte con la CEI 0-16/V1:2022-11 e delle modifiche ora introdotte, che sono evidenziate con una riga verticale a lato del testo.

DATI IDENTIFICATIVI CEI

Norma italiana	CEI 0-16;V2
Classificazione	CEI 0-16;V2
Edizione	

COLLEGAMENTI/RELAZIONI TRA DOCUMENTI

Nazionali	
Europei	
Internazionali	
Legislativi	
Legenda	

INFORMAZIONI EDITORIALI

Pubblicazione	Variante
Stato Edizione	In vigore
Data validità	01-06-2023
Ambito validità	Nazionale
Fascicolo	19498
Ed. Prec. Fasc.	Nessuna
Comitato Tecnico	CT 316-Connessioni alle reti elettriche Alta, Media e Bassa Tensione

Approvata da	Presidente del CEI	*In data*	15-05-2023
		In data	
Sottoposta a	Inchiesta pubblica come Progetto C.1318	*Chiusura in data*	04-05-2023
ICS	29.240.01;		

PREMESSA

Questa Norma costituisce la variante V2 della Norma CEI 0-16:2022-03, ed è costituita dal solo Allegato T “Scambio informativo basato su standard IEC 61850” in versione consolidata come risultante dell’Allegato T della Norma CEI 0-16:2022-03, delle successive modifiche introdotte con la CEI 0-16/V1:2022-11 e delle modifiche ora introdotte, che sono evidenziate con una riga verticale a lato del testo.

I contenuti tecnici modificati sono relativi alle seguenti sezioni del documento:

Funzione di Regolazione - cosϕ = f(P)

Modifica editoriale della tabella di descrizione dei DO, spostando FctOpSt nella sezione corretta degli Status Information senza modificarne natura, struttura e semantica.

Modello dei dati del CCI e privilegi di accesso ai fini della sicurezza

Specifica del concetto di privilegio di accesso ai dati gestiti dal CCI in relazione al riconoscimento esclusivo dell’identità degli attori abilitati (i.e. DSO e Aggregatore).

Gestione dei ruoli nelle comunicazioni IEC 61850/MMS

Specifica del criterio di identificazione e gestione dei ruoli del protocollo di comunicazione 61850/MMS in relazione al riconoscimento esclusivo dell’identità degli attori abilitati (i.e. DSO e Aggregatore).

Utente

Parziale rielaborazione del testo volta a chiarire i requisiti di sicurezza delle comunicazioni Utente. In particolare, si specifica la necessità di utilizzare protocolli standard dotati di servizi di sicurezza che abilitano mutua autenticazione delle parti. Si introduce il criterio di gestione dei permessi degli Utenti.

Log delle comunicazioni MMS con profilo di sicurezza Applicativo

Corretto il titolo del capitolo.

Configurazione del dispositivo

Rielaborazione del contenuto informativo in formato tabellare atto a favorirne la comprensione. La tabella, salvo alcune revisioni terminologiche, ripropone il contenuto già originariamente presente nell'allegato T.

Trust Anchor

Introduzione, tra i Trust Anchor necessari, della CA associata univocamente al DSO. Introduzione, tra i Trust Anchor facoltativi, della CA dell’Aggregatore. Estensione del criterio di Trust Anchor dalle Root CA alle Sub-CA secondo discrezione degli attori coinvolti. Allineamento della nomenclatura dei Trust Anchor degli attori abilitati (i.e. Dominio Amministrativo sostituisce Dominio Operativo).

Allegato T
(normativo)

Scambio informativo basato su standard IEC 61850(237)

T.1 Introduzione

Nella prospettiva di evoluzione delle reti di distribuzione verso il paradigma delle smart grid, risulta necessario definire un insieme di scambi informativi finalizzati al governo della rete elettrica in presenza di una consistente quantità di Generazione Diffusa (nel seguito GD) al punto di connessione con la rete di distribuzione.

Il modello considerato per la definizione dell'interfaccia del Controllore Centrale di Impianto (nel seguito CCI) prevede che la GD comunichi con il Distributore (nel seguito DSO), con l'Aggregatore e con l'operatore di GD (o Utente) e non definisce la comunicazione verso gli elementi costituenti l'impianto.

L'implementazione e l'utilizzo dello standard IEC 61850 secondo quanto prescritto nel presente Allegato è obbligatorio per le comunicazioni con il DSO. Tale soluzione può essere adottata anche per le comunicazioni verso altri attori abilitati, nel rispetto dei rispettivi ruoli, ma questo approccio non è richiesto dal presente Allegato.

Per quanto riguarda la sicurezza delle comunicazioni, le prescrizioni contenute in questo documento fanno riferimento alle interfacce di rete per gli accessi remoti al dispositivo. L'accesso remoto è previsto sia per funzioni di monitoraggio e controllo, sia per esigenze di gestione dell'impianto.

Verranno fornite le indicazioni da rispettare per assicurare un adeguato livello di sicurezza, applicabili a protocolli normati da enti o organismi internazionali (IEC, ITU-T, IETF, ecc). Quando non diversamente specificato, il riferimento ad uno standard è inteso all'ultima versione pubblicata.

Verranno quindi presentati i meccanismi di base per la sicurezza degli scambi informativi basati sui protocolli IEC 61850, le prescrizioni di sicurezza per i servizi di supporto, i processi relativi alla gestione dei certificati elettronici.

La modalità di integrazione del CCI nell'architettura di sistema esula dal contesto del presente documento, che si limita a specificare l'interfaccia IEC 61850 del CCI.

T.2 Struttura dell'allegato

La struttura dell'allegato prevede una prima sezione che definisce i requisiti tecnici/funzionali (in ottemperanza all'Allegato O) ed una seconda sezione che specifica la conseguente soluzione tecnologica per l'implementazione delle interfacce di comunicazione del dispositivo CCI.

Più nello specifico, la prima sezione definisce i requisiti funzionali, il conseguente scambio informativo ed i relativi requisiti tecnici.

La seconda sezione definisce la soluzione tecnologica da adottare in termini di Modello Dati, Servizi di comunicazione, mappatura su specifico protocollo, requisiti, algoritmi e processi di cyber security, ai fini dell'implementazione delle funzionalità definite nella precedente sezione.

(237) Per i volumi dello standard già recepiti da CEI ed in forza, si può equivalentemente fare riferimento agli omologhi CEI EN.

T.3 Specifiche associate al CCI – interfaccia IEC 61850

Sulla base dei requisiti funzionali e tecnici associati sia alla gestione della rete di distribuzione che alla fornitura di servizi di rete da parte della GD, la presente specifica ha individuato gli scambi informativi e la conseguente interfaccia conforme allo standard IEC 61850 che la GD deve esporre verso gli attori del sistema elettrico previsti.

Al fine di risultare interoperabile con gli attori previsti, l'interfaccia IEC 61850 della GD è stata dettagliatamente specificata in termini di Modello Dati, Servizi ACSI, mappatura su specifico protocollo di comunicazione e relative specifiche di cyber security.

L'interfaccia del CCI prevede l'implementazione di un server IEC 61850 con un unico punto di accesso logico concretamente rappresentato da un indirizzo IP reso accessibile agli attori interessati.

Nei seguenti paragrafi, le tabelle che definiscono il contenuto informativo da scambiare tramite l'interfaccia IEC 61850 del CCI contengono un campo "Presenza": esso identifica la finalità del dato (Osservabilità/Controllabilità) ed il vincolo di implementazione (Mandatorio/Opzionale).

Per la specifica realizzazione della modalità di comunicazione del CCI si può fare riferimento al Technical Report "Esempio di file SCL per la comunicazione IEC 61850 del CCI".

T.3.1 Definizione dei requisiti funzionali associati al CCI

Gli scambi informativi associati al CCI dovranno consentire di supportare le funzionalità definite nell'Allegato O

- Erogare i servizi di rete attraverso una modulazione apposita di potenza attiva e reattiva secondo quanto richiesto;
- Fornire le misure delle grandezze elettriche come previsto in Articolo O.8;
- Lo stato dell'organo DG e dei Singoli Gruppi di Generazione come previsto in Articolo O.8.

La comunicazione verso gli elementi di impianto è fuori dallo scopo.

Le informazioni sono concettualmente raggruppate nelle seguenti categorie funzionali.

Tabella 79 – Organizzazione funzionale delle informazioni relative al CCI

Informazioni relative alle caratteristiche dell'impianto	Informazioni relative alla configurazione, caratteristiche e capacità nominali degli elementi costituenti l'impianto. Queste informazioni derivano dall'impianto e non sono oggetto di modifica da parte di processi remoti
Informazioni relative allo stato operativo dell'impianto	Informazioni riguardo lo stato operativo dell'impianto e degli apparati fisici presenti in impianto, quali la posizione dell'interruttore DG e l'operatività dei Singoli Gruppi di Generazione. Lo stato può modificarsi a seguito di eventi in impianto o a seguito di comandi remoti
Informazioni relative alle misure dell'impianto	Valori analogici misurati direttamente o determinati tramite elaborazione di grandezze misurate, quali tensioni, correnti, potenze, ecc.
Informazioni relative ai valori dei parametri operativi	Valori di riferimento necessari per l'operatività delle funzioni e degli algoritmi. I parametri sono impostati in fase di inizializzazione dell'apparato e possono successivamente essere modificati da remoto

Per maggior sintesi, le informazioni relative alle caratteristiche di potenza degli elementi costituenti l'impianto, previste nei "Messaggi relativi alle caratteristiche dell'impianto" sono espresse mediante un vettore unificato contenente le grandezze di Tabella 80. Tutte le grandezze elettriche si intendono ai morsetti degli elementi costituenti l'impianto, salvo dove diversamente specificato.

Tabella 80 – Definizione del vettore delle potenze caratteristiche

Informazione	Descrizione	Unità di misura
Potenza attiva massima in immissione	Potenza attiva massima che l'unità di generazione o di accumulo può generare	kW
Potenza attiva massima in assorbimento	Potenza attiva massima che l'unità di consumo o di accumulo può assorbire	kW
Potenza apparente massima dell'impianto Smax	Potenza apparente massima dell'impianto Smax delle unità di generazione o di accumolo	kVA
Potenza reattiva induttiva massima	Massima potenza reattiva induttiva che il generico componente può scambiare con continuità	kVAr
Potenza reattiva capacitiva massima	Massima potenza reattiva capacitiva che il generico componente può scambiare con continuità	kVAr

Dove richiesto dall'allegato O verrà inoltre specificata l'origine delle azioni di configurazione e comando verso il CCI, come specificato nella seguente tabella.

Tabella 81 – Identità degli attori abilitati

Origine	Categoria	Identità
Distributore	automatic-station Operazione di controllo/comando remoto da funzione automatica a livello di Stazione	DSO
Aggregatore	remote-control Operazione di controllo/comando da operatore remoto al di fuori dell'impianto (ad es. un network control center)	AGGREGATORE

T.3.1.1 Informazioni relative alle caratteristiche di impianto

Le informazioni relative alle caratteristiche degli elementi dell'impianto sono informazioni "statiche" da definire in fase di prima configurazione sul CCI o in caso di modifiche rilevanti ai suoi componenti e "dinamiche" come risultato delle condizioni di esercizio. In particolare, le informazioni previste sono indicate in Tabella 82 come specificato nei paragrafi dedicati dei Articolo O.9 ed O.10. Qualora una o più sezioni non dovessero essere presenti in impianto, le relative caratteristiche non dovranno essere compilate.

Tabella 82 – Informazioni relative alle caratteristiche dell'impianto

Informazione	Descrizione	Tipo informazione / Unità di misura	Presenza
Informazioni Statiche (Configurazione)			
Costruttore dell'apparato di Monitoraggio Impianto	Testo descrittivo: costruttore dell'impianto	Stringa di testo	Osservabilità Mandatorio
Versione del software dell'apparato di Monitoraggio Impianto	Testo descrittivo: versione SW del Controllore Centrale di Impianto	Stringa di testo	Osservabilità Mandatorio
Identificativo punto di connessione (POD)	Identificativo del punto di connessione dell'impianto alla rete elettrica definito dal DSO	Stringa di testo	Osservabilità Mandatorio
Potenza sul punto di connessione	Definisce il vettore della potenza riferito al punto di connessione con la rete. È rappresentato dalla Tabella 80 Il valore della Potenza apparente massima dell'impianto Smaxcostituisce il riferimento per tutti i valori di potenza attiva e reattiva espressi percentualmente.	Vedi vettore delle potenze caratteristiche (Tabella 80)	Osservabilità Opzionale
Informazioni Dinamiche (Esercizio)			
Funzioni di regolazione disponibili nell'impianto	Elenca le funzioni di regolazione che il CCI può attuare in relazione alle capacità tecniche dell'impianto: Limitazione della potenza attiva, Modulazione della potenza attiva, Regolazione di tensione con erogazione di potenza reattiva, Set-point PF, Regolazione Q(V), Regolazione cosφ(P)	Stato della funzione (lista dei possibili valori): Non disponibile/ Autonoma / Asservita La priorità delle funzioni di regolazione disponibili nell'impianto è definita alle tabelle di dettaglio	Controllabilità Opzionale
	Elenca le funzioni di regolazione che il CCI può attuare in relazione alle capacità tecniche dell'impianto: Set-point potenza attiva, Set-point potenza reattiva	Stato della funzione (lista dei possibili valori): Non disponibile / Asservita	Partecipazione all'MSD Facoltativo

T.3.1.2 Informazioni relative allo stato dell'impianto

Tale tipologia di informazioni permette di rilevare le modalità operative dell'impianto. In Tabella 83 sono specificate secondo 3 categorie che fanno riferimento a quanto previsto nel Paragrafo O.8.6:

Tabella 83 – Informazioni relative allo stato dell'impianto

Informazione	Descrizione	Tipo informazione / Unità di misura	Presenza
Generali d'impianto			
Disponibilità ad operare le funzioni di regolazione presenti	Disponibilità a regolare perImpianto completo Macroblocco di Generazione, Macroblocco di Accumulo	Disponibilità: Non disponibile / Disponibile	Osservabilità Mandatorio
Modalità di funzionamento dell'impianto	Indica il modo operativo nel quale si trova l'impianto: Limitazione della potenza attiva, Modulazione della potenza attiva, Regolazione di tensione con erogazione di potenza reattiva, Set-point PF, Regolazione Q(V), Regolazione cosφ (P)	Stato (per singola funzione): Operativo/Non operativo	Controllabilità Opzionale
	Indica il modo operativo nel quale si trova l'impianto: Set-point potenza attiva, Set-point potenza reattiva Ulteriori modi operativi potranno essere definiti in successive versioni della presente specifica	Stato (per singola funzione): Operativo/Non operativo	Partecipazione all'MSD Facoltativo
Disponibilità alla regolazione dell'Impianto	Disponibilità dell'impianto ad operare le funzioni di regolazione	Stato: Disponibile/Non Disponibile	Osservabilità Mandatorio
Stato del Dispositivo Generale	Indica la posizione dell'interruttore generale dell'impianto	Stato: Aperto/Chiuso	Osservabilità Mandatorio
Macro-blocco generazione			
Disponibilità alla regolazione del macro-blocco	Disponibilità del macro-blocco di generazione ad operare le funzioni di regolazione	Stato: Disponibile/ Non Disponibile	Osservabilità Mandatorio
Stato operativo del singolo gruppo di generazione	Indica se il singolo gruppo di generazione è operativo o meno	Stato: Operativo/ Non Operativo	Osservabilità Mandatorio
Identificatore del singolo gruppo di generazione	Numero Identificativo del singolo gruppo di generazione di cui si osserva l'operatività	Codice numerico	Osservabilità Mandatorio
Macro-blocco sistemi di accumulo			
Disponibilità alla regolazione del macro-blocco	Disponibilità del sistema di accumulo ad operare le funzioni di regolazione	Stato: Disponibile/Non Disponibile	Osservabilità Mandatorio
Stato operativo del sistema di accumulo	Indica se il sistema di accumulo, equivalente ad un singolo gruppo di generazione, è in condizioni operative o fuori servizio	Stato: Operativo/ Non operativo	Osservabilità Mandatorio

T.3.1.3 Informazioni relative alle misure di grandezze elettriche dell'impianto

Il CCI acquisisce le misure dagli apparati di campo, se questi le rendono disponibili, oppure tramite propri sensori.

Nel seguito, in Tabella 84, vengono elencate le misure che il CCI dovrà gestire. Per maggior sintesi, le informazioni relative alla misura della potenza sono espresse mediante un vettore unificato contenente le grandezze di Tabella 80

Tabella 84 – Misure

Informazione	Descrizione	Unità di misura	Presenza
Punto di Connessione			
Potenza attiva	Valore con segno della potenza attiva	kW	Osservabilità Mandatorio, Partecipazione MSD Facoltativo
Potenza reattiva	Valore con segno della potenza reattiva	kVAr	Osservabilità Mandatorio, Partecipazione MSD Facoltativo
Tensioni	Valore delle tensioni fase-fase	kV	Osservabilità Mandatorio
Correnti di fase	Valore della tensione fase-fase	A	Osservabilità Opzionale
Aggregati di generazione (Fotovoltaico/Eolico/Termoelettrico/Idroelettrico)			
Potenza attiva	Valore con segno della potenza attiva Valore complessivo della potenza attiva prodotta dai generatori con stessa fonte primaria di energia (Fotovoltaico/Eolico/Termoelettrico/Idroelettrico). Deve essere fornito un valore distinto in base alla fonte primaria.	kW	Osservabilità Mandatorio
Sistemi di accumulo (equivalenti ad Aggregati di generazione)			
Potenza attiva	Valore con segno della potenza attiva	kW	Osservabilità Mandatorio
Singolo gruppo di generazione (Fotovoltaico/Eolico/Termoelettrico/Idroelettrico)			
Potenza attiva	Valore con segno della potenza attiva	kW	Osservabilità Mandatorio
Sistema di Accumulo (equivalenti a Singolo gruppo di generazione)			
Potenza attiva	Valore con segno della potenza attiva	kW	Osservabilità Mandatorio

T.3.1.4 Informazioni relative ai parametri operativi dell'impianto

Tale tipologia di informazioni permette di impostare i parametri associati alle modalità operative dell'impianto. L'attivazione di una modalità operativa dovrà avvenire soltanto qualora le condizioni operative dell'impianto consentano il soddisfacimento dei parametri di funzionamento imposti. I modi operativi potenzialmente attivabili possono essere più di uno, purché gli stessi siano funzionalmente compatibili.

Se il modo di funzionamento è già attivo, la modifica di un suo parametro causa la variazione della regolazione per uniformarsi alla nuova taratura.

T.3.1.4.1 Funzione di regolazione - limitazione di potenza attiva

Nella seguente Tabella 85 si specificano le informazioni relative alla configurazione e allo stato della funzione che attua la limitazione della potenza attiva che è possibile immettere in rete.

Tabella 85 – Parametri della funzione "Limite di potenza attiva"

Parametro	Unità di misura	Range	Riferimento	Valore di default	Presenza
Stato operativo	-	1 = Operativa/ 5 = Non-Operativa	-	5	Controllabilità Opzionale
Limite di potenza attiva in generazione	%	0..100	Potenza apparente massima dell'impianto Smax	0	Controllabilità Opzionale
Comando di attivazione	–	5 = Inattiva, 1 = Attiva	–	5	Controllabilità Opzionale
Stato della funzione Set-Point da DSO	–	0= Non disponibile / 1 = Autonoma/ 2 = Asservita (Prioritario)	–	1	Controllabilità Opzionale
Stato della funzione limite di P 110%	–	0=Non Disponibile / 1=Autonoma;	–	2	Controllabilità Opzionale

T.3.1.4.2 Funzione di regolazione – Modulazione della potenza attiva

Nella seguente Tabella 86 si specificano le informazioni relative alla configurazione e allo stato della funzione che, su comando del DSO, attua la modulazione della potenza attiva che è possibile scambiare con la rete.

Tabella 86 – Parametri della funzione "Modulazione della Potenza attiva"

Parametro	Unità di misura	Range	Riferimento	Valore di default	Presenza
Stato operativo	–	1 = Operativa/ 5 = Non-Operativa	–	5	Controllabilità Opzionale
Setpoint di potenza attiva in Immissione e Assorbimento	%	0..100 (+ = Immissione, - = Assorbimento)	Potenza apparente massima dell'impianto Smax	100 / 0	Controllabilità Opzionale
Comando di attivazione	–	5 = Inattiva, 1 = Attiva	-	5	Controllabilità Opzionale
Stato della funzione	–	0= Non disponibile / 2 = Asservita (Prioritario)	–	2	Controllabilità Opzionale
Per potenza attiva in immissione si intende la potenza che l'impianto immette in rete. Per potenza attiva in assorbimento si intende la potenza che l'impianto assorbe dalla rete.					

T.3.1.4.3 Funzione di regolazione – Set-point della potenza attiva

Nella seguente Tabella 87 si specificano le informazioni relative alla configurazione e allo stato della funzione che, sulla base di segnali di mercato, attua il set-point della potenza attiva che è possibile scambiare con la rete.

Tabella 87 – Parametri della funzione "Set-point della Potenza attiva"

Parametro	Unità di misura	Range	Riferimento	Valore di default	Presenza
Stato operativo	–	1 = Operativa/ 5 = Non-Operativa	–	5	Partecipazione all'MSD Facoltativo
Setpoint di potenza attiva in Immissione e Assorbimento	%	0..100 (+ = Immissione, - = Assorbimento)	Potenza apparente massima dell'impianto Smax	100 / 0	Partecipazione all'MSD Facoltativo
Comando di attivazione	–	5 = Inattiva, 1 = Attiva	–	5	Partecipazione all'MSD Facoltativo
Stato della funzione	–	0= Non disponibile/ 2 = Asservita (Prioritario)	–	2	Partecipazione all'MSD Facoltativo
Per potenza attiva in immissione si intende la potenza che l'impianto immette in rete. Per potenza attiva in assorbimento si intende la potenza che l'impianto assorbe dalla rete.					

T.3.1.4.4 Funzione di regolazione – regolazione di tensione con erogazione di potenza reattiva

Nella seguente Tabella 88 si specificano le informazioni relative alla configurazione e allo stato della funzione che, su comando del Distributore, attua la regolazione di tensione con erogazione di potenza reattiva Capacitiva o Induttiva che è possibile scambiare con la rete.

Tabella 88 – Parametri della funzione "regolazione di tensione con erogazione di potenza reattiva"

Parametro	Unità di misura	Range	Riferimento	Valore di default	Presenza
Stato operativo	–	1 = Operativa/ 5 = Non-Operativa	–	5	Controllabilità Opzionale,
Setpoint di potenza reattiva in immissione o assorbimento	%	0..100 (+ = Capacitiva, - = Induttiva)	Potenza apparente massima dell'impianto Smax	0 / 0	Controllabilità Opzionale
Comando di attivazione	-	5 = Inattiva, 1 = Attiva	–	5	Controllabilità Opzionale
Stato della funzione	–	0= Non disponibile / 2 = Asservita (Prioritario)	–	2	Controllabilità Opzionale
Per potenza reattiva in immissione si intende la potenza che l'impianto immette in rete attraverso il funzionamento in sovreccitazione dei generatori (comportamento dell'impianto da condensatore). Per potenza reattiva in assorbimento si intende la potenza che l'impianto assorbe dalla rete attraverso il funzionamento in sottoeccitazione dei generatori (comportamento dell'impianto da induttore).					

T.3.1.4.5 Funzione di regolazione – Set-Point di potenza reattiva

Nella seguente Tabella 89 si specificano le informazioni relative alla configurazione e allo stato della funzione che, sulla base di segnali di mercato, attua il set-point della potenza reattiva Capacitiva ed Induttiva che è possibile scambiare con la rete.

Tabella 89 – Parametri della funzione "Set-Point potenza reattiva"

Parametro		Unità di misura	Range	Riferimento	Valore di default	Presenza
Stato operativo		–	1 = Operativa/ 5 = Non-Operativa	–	5	Partecipazione MSD Facoltativa
Setpoint di potenza reattiva in immissione o assorbimento		%	0..100 (+ = Capacitiva, - = Induttiva)	Potenza apparente massima dell'impianto Smax	0 / 0	Partecipazione MSD Facoltativa
Comando di attivazione		–	5 = Inattiva, 1 = Attiva	–	5	Partecipazione MSD Facoltativa
Stato della funzione		–	0= Non disponibile/ 2 = Asservita (Prioritario)	–	2	Partecipazione MSD Facoltativa
Per potenza reattiva in immissione si intende la potenza che l'impianto immette in rete attraverso il funzionamento in sovreccitazione dei generatori (comportamento dell'impianto da condensatore). Per potenza reattiva in assorbimento si intende la potenza che l'impianto assorbe dalla rete attraverso il funzionamento in sottoeccitazione dei generatori (comportamento dell'impianto da induttore).						

T.3.1.4.6 Funzione di regolazione – Set-Point del fattore di potenza

Nella seguente Tabella 90si specificano le informazioni relative alla configurazione e allo stato della funzione che attua il set-point del fattore di potenza che deve caratterizzare la potenza scambiata con la rete.

Tabella 90 – Parametri della funzione "Set-Point Fattore di Potenza"

Parametro		Unità di misura	Range	Riferimento	Valore di default	Presenza
Stato operativo		–	1 = Operativa / 5 = Non-Operativa	–	5	Controllabilità Opzionale
Setpoint di cosϕ in caso di generazione di potenza attiva		P.U.	-1.00..+1.00 (+ = Capacitiva, - = Induttiva)	–	-0.95	Controllabilità Opzionale
Setpoint di cosϕ in caso di assorbimento di potenza attiva		P.U.	-1.00..1.00 (+ = Capacitiva, - = Induttiva)	–	0.95	Controllabilità Opzionale
Comando di attivazione		–	5 = Inattiva, 1 = Attiva	–	5	Controllabilità Opzionale
Stato della funzione		–	0= Non disponibile / 1 = Autonoma / 2 = Asservita (Prioritario)	-	1	Controllabilità Opzionale
Il valore di potenza reattiva che deve essere scambiato con la rete deve essere determinato considerando il valore assoluto del fattore di potenza imposto. Il segno associato al fattore di potenza determina se la potenza reattiva è immessa attraverso il funzionamento in sovreccitazione dei generatori (comportamento dell'impianto da condensatore) oppure assorbita dalla rete attraverso il funzionamento in sottoeccitazione dei generatori (comportamento dell'impianto da induttore).						

T.3.1.4.7 Funzione di regolazione – Q(V)

Nella seguente Tabella 92 si specificano le informazioni relative alla configurazione e allo stato della funzione che attua la regolazione della potenza reattiva rispetto al valore della tensione sul punto di connessione.

Tabella 91 – Parametri della funzione "Q(V)"

Parametro	Unità di misura	Range	Riferimento	Valore di default	Presenza
Stato operativo	–	1 = Operativa / 5 = Non-Operativa	–	5	Controllabilità Opzionale
Comando di attivazione	-	5 = Inattiva, 1 = Attiva	–	5	Controllabilità Opzionale
Stato della funzione	–	0= Non disponibile / 1 = Autonoma / 2 = Asservita (Prioritario)	–	1	Controllabilità Opzionale
K	–	-1.00..1.00	–	0	Controllabilità Opzionale
Potenza attiva di lock-in	P.U.	0.00..max	Potenza Attiva Nominale	0.20	Controllabilità Opzionale
Potenza attiva di lock-out	P.U.	0.00..max	Potenza Attiva Nominale	0.05	Controllabilità Opzionale
V superiore 1	P.U.	0.00..max	Tensione Nominale al PdC	1.08	Controllabilità Opzionale
V inferiore 1	P.U.	0.00..max	Tensione Nominale al PdC	0.92	Controllabilità Opzionale
V superiore 2	P.U.	0.00..max	Tensione Nominale al PdC	1.10	Controllabilità Opzionale
V inferiore 2	P.U.	0.00..max	Tensione Nominale al PdC	0.90	Controllabilità Opzionale

T.3.1.4.8 Funzione di regolazione – cosϕ (P)

Nella seguente Tabella 92 si specificano le informazioni relative alla configurazione e allo stato della funzione che attua la regolazione del fattore di potenza rispetto al valore della potenza attiva sul punto di connessione.

Tabella 92 – Parametri della funzione "cosφ (P)"

Parametro	Unità di misura	Range	Riferimento	Valore di default	Presenza
Stato operativo	–	1 = Operativa/ 5 = Non-Operativa	–	5	Controllabilità Opzionale
Comando di attivazione	–	5 = Inattiva, 1 = Attiva	–	5	Controllabilità Opzionale
Stato della funzione	–	0= Non disponibile/ 1 = Autonoma/ 2 = Asservita (Prioritario)	–	1	Controllabilità Opzionale
Valore P (punto A)	P.U	0.00..max	Potenza Attiva Nominale	0.20	Controllabilità Opzionale

Parametro	Unità di misura	Range	Riferimento	Valore di default	Presenza
Valore cosϕ (punto A)	P.U.	-1.00..-0.1 +0.1..1.00 (+ = Capacitiva, - = Induttiva)	–	1.00	Controllabilità Opzionale
Valore P (punto B)	P.U	0.00..max	Potenza Attiva Nominale	0.50	Controllabilità Opzionale
Valore cosϕ (punto B)	P.U.	-1.00..-0.1 +0.1..1.00 (+ = Capacitiva, - = Induttiva)	–	1.00	Controllabilità Opzionale
Valore P (punto C)	P.U	0.00..max	Potenza Attiva Nominale	1.00	Controllabilità Opzionale
Valore cosϕ (punto C)	P.U.	-1.00..-0.1 +0.1..1.00 (+ = Capacitiva, - = Induttiva)	–	0.95	Controllabilità Opzionale
V di Lock-in	P.U.	1.00..1.10	Tensione Nominale al PdC	1.05	Controllabilità Opzionale
V di Lock-out	P.U.	0.90..1.00	Tensione Nominale al PdC	0.98	Controllabilità Opzionale

T.3.2 Definizione dei requisiti tecnici associati all'interfaccia del CCI

T.3.2.1 Modalità di comunicazione

L'insieme completo delle informazioni associate ai requisiti funzionali del CCI riportate nell'Allegato O, devono essere rese disponibili al DSO.

L'attore che agirà da Aggregatore avrà viceversa accesso alle sole informazioni funzionali alla partecipazione all'MSD.

Lo scambio delle informazioni può avvenire su richiesta, oppure su base periodica o per variazione del valore di un parametro, prevedendo eventualmente una fascia di tolleranza. Le informazioni possono essere richieste o inviate singolarmente o per gruppi omogenei.

Dove non diversamente specificato, considerare le indicazioni di T.1.

Per la valutazione delle performance della comunicazione, trattate

- all'interno della sottostazione dalla CEI EN 61850-5 "Communication networks and systems for power utility automation - Part 5: Communication requirements for functions and device models" e
- tra sottostazioni dalla IEC 61850-90-1 Ed.2.0 "Communication networks and systems for power utility automation - Part 90-1: Use of IEC 61850 for the communication between substations",

si consideri che le informazioni sono essenzialmente scambiate tra un dispositivo Client (ad es. SCADA o sistema centrale di valutazione della rete) e Server (CCI); per questo genere di flussi informativi le performance attese sono di tipo "Low speed messages" con tempi di transito tra gli end-point dell'ordine dei 500 ms quando all'interno della sottostazione. All'esterno della sottostazione, invece, questo tipo di scambi non sono catalogati. Inoltre, per quanto riguarda le misure pubblicate periodicamente dal CCI, la comunicazione non è puramente IEC 61850, in quanto l'utilizzatore (TSO), per tramite del DSO, utilizza differenti standard IEC. Nella Tabella 95 si prescrivono le performance attese sulla base della tipologia di informazione.

Tabella 93 – Modalità di comunicazione

Tipologia di informazione	Modalità di invio del messaggio	Performance attese (dove applicabile in accordo con CEI EN 61850-5)	Presenza
Caratteristiche dell'impianto	su richiesta	Type 3 - Low speed messages	Osservabilità Mandatorio
Stato operativo dell'impianto	su richiesta e su variazione	Type 3 - Low speed messages	Osservabilità Mandatorio
Misure dell'impianto	periodico 4 s	Type 3 - Low speed messages	Osservabilità Mandatorio
Valori dei parametri operative	su richiesta e su variazione	Type 3 - Low speed messages	Controllabilità Opzionale

Le latenze associate all'impostazione del Set-point di potenza ricadono nella Performance Class Type 3;

Seppure non sia prevista l'esposizione di un'interfaccia GOOSE da parte del CCI, tale dispositivo dovrà essere in grado di sottoscrivere messaggi GOOSE in merito alle funzioni di controllo (secondo lo "Schema generale del sistema CCI con relative interfacce funzionali" in Allegato O); eventuali sviluppi negli scambi informativi con servizi ad alta velocità ricadono nelle Performance Class di Type 1.

T.3.2.2 Definizione delle regole di accesso ai servizi IEC 61850 dell'unità CCI

Al fine di implementare regole di accesso ai servizi differenziate in base al ruolo dell'attore che si connette al server IEC 61850, è necessario individuare le relative modalità di autorizzazione in conformità a quanto previsto dalla normativa IEC 62351 (vedi Paragrafo T.3.3.4.3).

T.3.3 Soluzione tecnologica per l'implementazione dell'interfaccia secondo IEC 61850 associata al CCI

La presente sezione definisce la soluzione tecnologica da adottare in termini di Modello Dati, Servizi, mappatura su specifico protocollo e requisiti di cyber security, ai fini della realizzazione dell'unità CCI conforme ai requisiti definiti nella precedente sezione.

T.3.3.1 Modello dati IEC 61850 delle informazioni associate al CCI

Nella realizzazione del modello dati IEC 61850 corrispondente alle informazioni identificate nella precedente sezione, si è cercato di utilizzare il più possibile oggetti già definiti nello standard, in particolare con riferimento a CEI EN 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" o a volumi specifici per le DER (ad es. 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").

I parametri che identificano la versione di questo namespace sono:

- 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".

Si osservi che l'attributo "M/O/C" (mandatorietà) degli elementi che costituiscono una Common Data Class o un Logical Node è stato esteso aggiungendo gli attributi formalizzati nella tabella seguente:

Tabella 94 – Presenza dei dati nel modello

Attributo	Descrizione
M = Mandatorio	Dati obbligatori prescritti dallo standard
O = Opzionale	Dati opzionali previsti dallo standard
C = Condizionale	Dati disponibili secondo condizioni stabilite dallo standard
R = Richiesto	Dato standardizzato come O/C da IEC 61850 ma richiesto per abilitare le funzioni previste nell'Allegato O
E = Estensione	L'informazione è un'estensione in quanto non disponibile nello standard ed è richiesta per abilitare le funzioni previste nell'Allegato O
F = Vietato (Forbidden)	L'informazione non è applicabile per gli usi previsti dalla condizione di presenza (normalmente specificato in relazione agli usi statistici dell'informazione)

Il profilo, per semplicità di modello dei dati, è caratterizzato da un unico Logical Device:

Tabella 95 – Logical Device del CCI

Logical Device	Descrizione
LD_Plant	Contiene tutti i Logical Nodes relativi all'impianto (combinazione di generatori e sistemi di accumulo di energia)

Per differenziare le varie sezioni di impianto verrà utilizzato un prefisso (di seguito prefix) diverso per ogni sezione. Il prefisso sarà posto prima del nome di ogni nodo logico all'interno del Data Object LNName, per indicare la sezione di impianto al quale il nodo si riferisce. In particolare, si userà:

Tabella 96 – Prefisso LN per le specifiche sezioni di impianto

Prefix	Descrizione
Global	Modelli di dati relativi all'impianto nel suo insieme
St	Modelli di dati relativi al sistema di accumulo
GenPV	Modelli di dati relativi al generatore fotovoltaico
GenWi	Modelli di dati relativi al generatore eolico
GenTer	Modelli di dati relativi al generatore termoelettrico
GenIdr	Modelli di dati relativi al generatore idroelettrico

Di seguito, saranno modellate le informazioni tramite i "Logical Nodes (LN)", pertanto alcune tabelle saranno in lingua inglese poiché riportate direttamente dalle IEC 61850; ad esse seguirà un'ulteriore tabella di dettaglio (in italiano) per definire meglio le informazioni rilevanti (set prescritto di dati) dei singoli Data Object (DO), eventualmente specificando il principale Data Attribute (DA), utilizzate negli scambi informativi del CCI.

Si noti che i DO/DA specifici del LN e quelli ereditati dalla Common Logical Node Class saranno menzionati e dettagliati solo se esplicitamente utilizzati nello scambio informativo richiesto a soddisfare i requisiti espressi nei precedenti paragrafi. Resta inteso, per ragioni di conformità, che i modelli di dati ritenuti Mandatori dello standard dovranno comunque essere implementati nell'ambito della capability di modello del CCI.

I dati modellati tramite i LN/DO nei paragrafi seguenti, ove previsto dallo standard IEC 61850, saranno trasmessi includendo anche i relativi DA di "q" (qualità) e "t" (marca temporale).

Sono previste tre sezioni distinte, dedicate ai modelli di dati relativi alla:

- Osservabilità,
- Controllabilità (interamente Opzionale),
- Partecipazione al Mercato dei Servizi di Dispacciamento (interamente Facoltativa).

T.3.3.1.1 Modelli di dati relativi alla Osservabilità

I modelli di dati specificati nella sezione di Osservabilità, ove non diversamente specificato, sono da intendersi come Mandatori.

T.3.3.1.1.1 Logical node zero

Il nodo logico LLN0 deve essere presente come indicato in CEI EN 61850-7-4.

T.3.3.1.1.2 Informazioni sul device fisico

Il nodo logico LPHD (da CEI EN 61850-7-4) è utilizzato per identificare il CCI.

Per la lista completa dei Data Object si faccia riferimento alla CEI EN 61850-7-4.

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

Oltre a tutti i DO mandatori del LN, quelli sopra selezionati devono essere implementati nella capability di modello del CCI; essi devono essere utilizzati per la comunicazione del dispositivo ed hanno il seguente significato:

Nome DO	Nome DA	Significato	Esempio
PhyNam	vendor	Costruttore del CCI	123456
	swRev	Versione software del CCI	V02.00
	location	Identificativo del punto di connessione (POD)	IT000E123456789

T.3.3.1.1.3 Caratteristiche operative al punto di connessione

I nodi logici DPCC (4 istanze) e DGEN sono utilizzati per definire i dati operazionali che caratterizzano l'impianto complessivo al PdC.

Per la lista completa dei Data Object si faccia riferimento alla CEI EN IEC 61850-7-420.

Potenza attiva massima in immissione

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
…	…	…		…

Oltre a tutti i DO mandatori del LN, quelli sopra selezionati (set minimo di dati di targa al PdC) devono essere implementati nella capability di modello del CCI; essi devono essere utilizzati per la comunicazione del dispositivo ed hanno il seguente significato:

Nome DO	Nome DA	Significato	Esempio
WRtg	setMag	Punto di connessione - Potenza attiva massima in immissione	200 kW

Potenza attiva massima in assorbimento

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
…	…	…		…

Oltre a tutti i DO mandatori del LN, quelli sopra selezionati (set minimo di dati di targa al PdC) devono essere implementati nella capability di modello del CCI; essi devono essere utilizzati per la comunicazione del dispositivo ed hanno il seguente significato:

Nome DO	Nome DA	Significato	Esempio
WRtg	setMag	Punto di connessione - Potenza attiva massima in assorbimento	200 kW

Potenza reattiva induttiva massima

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
…	…	…		…

Oltre a tutti i DO mandatori del LN, quelli sopra selezionati (set minimo di dati di targa al PdC) devono essere implementati nella capability di modello del CCI; essi devono essere utilizzati per la comunicazione del dispositivo ed hanno il seguente significato:

Nome DO	Nome DA	Significato	Esempio
VArRtg	setMag	Punto di connessione - Potenza reattiva induttiva massima	50 kVAr

Potenza reattiva capacitiva massima

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
…	…	…		…

Oltre a tutti i DO mandatori del LN, quelli sopra selezionati (set minimo di dati di targa al PdC) devono essere implementati nella capability di modello del CCI; essi devono essere utilizzati per la comunicazione del dispositivo ed hanno il seguente significato:

Nome DO	Nome DA	Significato	Esempio
VArRtg	setMag	Punto di connessione - Potenza reattiva capacitiva massima	50 kVAr

Potenza apparente massima dell'impianto Smax

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

Oltre a tutti i DO mandatori del LN, quelli sopra selezionati (set minimo di dati di targa al PdC) devono essere implementati nella capability di modello del CCI; essi devono essere utilizzati per la comunicazione del dispositivo ed hanno il seguente significato:

Nome DO	Nome DA	Significato	Esempio
VARtg	setMag	Punto di connessione - Potenza apparente massima dell'impianto Smax	210 kVA

T.3.3.1.1.4 Regolazione dell'Impianto

Il nodo logico DECP è usato per rappresentare la disponibilità dell'impianto ad operare le funzioni di regolazione.

Per la lista completa dei Data Object si faccia riferimento alla CEI EN IEC 61850-7-420.

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

Oltre a tutti i DO mandatori del LN, quelli sopra selezionati devono essere implementati nella capability di modello del CCI; essi devono essere utilizzati per la comunicazione del dispositivo ed hanno il seguente significato:

Nome DO	**Nome DA**	**Significato**	**Esempio**
Beh	stVal	Disponibilità dell'impianto ad operare le funzioni di regolazione [1 = Disponibile, 5 = Non Disponibile]	Disponibile

T.3.3.1.1.5 Regolazione del macro-blocco di generazione

Il nodo logico DGEN è usato per rappresentare la disponibilità del macro-blocco di generazione ad operare le funzioni di regolazione.

Per la lista completa dei Data Object si faccia riferimento alla CEI EN 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
…	…	…		…

Oltre a tutti i DO mandatori del LN, quelli sopra selezionati devono essere implementati nella capability di modello del CCI; essi devono essere utilizzati per la comunicazione del dispositivo ed hanno il seguente significato:

Nome DO	**Nome DA**	**Significato**	**Esempio**
Beh	stVal	Disponibilità del macro-blocco di generazione ad operare le funzioni di regolazione [1 = Disponibile, 5 = Non Disponibile]	Disponibile

T.3.3.1.1.6 Regolazione del macro-blocco di accumulo

Il nodo logico DSTO è usato per rappresentare la disponibilità del macro-blocco di accumulo ad operare le funzioni di regolazione.

Per la lista completa dei Data Object si faccia riferimento alla 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
...	...	...		...

Oltre a tutti i DO mandatori del LN, quelli sopra selezionati devono essere implementati nella capability di modello del CCI; essi devono essere utilizzati per la comunicazione del dispositivo ed hanno il seguente significato:

Nome DO	Nome DA	Significato	Esempio
Beh	stVal	Disponibilità del macro-blocco di accumulo ad operare le funzioni di regolazione [1 = Disponibile, 5 = Non Disponibile]	Disponibile

T.3.3.1.1.7 Misure dell'impianto

Il nodo logico MMXU (multi-istanziato) è usato per rappresentare le misure dell'impianto sia al PdC che, ove presenti, delle singole tipologie di generazione e storage.

In Allegato O si prevedono misure per la stima dei flussi di potenza della rete MT inviate ogni 4 sec:

- P,Q,V al punto di connessione (opzionali le correnti di linea I);
- P per singola fonte di generazione e storage ove previsto;
- P per singolo gruppo di generazione.
- Per la lista completa dei Data Object si faccia riferimento alla CEI EN 61850-7-4.

Misure al punto di connessione a 4 sec

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
...	...	...		...

Oltre a tutti i DO mandatori del LN, quelli sopra selezionati (set minimo di misure richiesto al PdC) devono essere implementati nella capability di modello del CCI; essi devono essere utilizzati per la comunicazione del dispositivo ed hanno il seguente significato:

Nome DO	Nome DA	Significato	Esempio
TotW	Mag	Punto di connessione - potenza attiva totale istantanea (l'informazione veicolata al DSO può facoltativamente essere messa a disposizione dell'Aggregatore)	198 kW
TotVAr	Mag	Punto di connessione - potenza reattiva totale istantanea	-45 kvar
PPV	Mag	Punto di connessione - tensioni di linea (VL1L2, VL2L3, ...)	20000V, 20002V, 19993V
A	Mag	(Opz.) Punto di connessione - correnti di fase (IL1, IL2, IL3)	100A, 101A, 99A

Misure aggregate per singola fonte a 4 sec

MMXU class – type MMXU2 - prefix GenXX (tipo di generatore, come specificato in Tabella 95)				
Data object name	**CDC**	**Explanation**	**T**	**M/O/C**
...	...	...		...
TotW	MV	Total active power (total P)		R
...	...	...		...

Oltre a tutti i DO mandatori del LN, quelli sopra selezionati devono essere implementati nella capability di modello del CCI; essi devono essere utilizzati per la comunicazione del dispositivo ed hanno il seguente significato:

Nome DO	Nome DA	Significato	Esempio
TotW	Mag	Fotovoltaico/Eolico/Termoelettrico/Idroelettrico - potenza attiva istantanea	189 kW

Misure aggregate per Sistema di Accumulo a 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
...	...	...		...

Oltre a tutti i DO mandatori del LN, quelli sopra selezionati devono essere implementati nella capability di modello del CCI; essi devono essere utilizzati per la comunicazione del dispositivo ed hanno il seguente significato:

Nome DO	**Nome DA**	**Significato**	**Esempio**
TotW	Mag	Sistema di Accumulo - potenza attiva istantanea	189 kW

Misure per Singolo Gruppo di Generazione a 4 sec (multi-istanziabile con 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
...	...	...		...

Oltre a tutti i DO mandatori del LN, quelli sopra selezionati devono essere implementati nella capability di modello del CCI; essi devono essere utilizzati per la comunicazione del dispositivo ed hanno il seguente significato:

Nome DO	**Nome DA**	**Significato**	**Esempio**
TotW	Mag	Singolo Gruppo di Generazione (n) - Potenza attiva istantanea	189 kW

T.3.3.1.1.8 Stato operativo dell'impianto - posizione degli interruttori

Il nodo logico XCBR è usato per rappresentare la posizione dell'Interruttore (Aperto/Chiuso) del Dispositivo Generale per la separazione dell'impianto complessivo dalla rete.

Per la lista completa dei Data Object si faccia riferimento alla CEI EN 61850-7-4.

Posizione dell'Interruttore del Dispositivo Generale

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

Oltre a tutti i DO mandatori del LN, quelli sopra selezionati devono essere implementati nella capability di modello del CCI; essi devono essere utilizzati per la comunicazione del dispositivo ed hanno il seguente significato:

Nome DO	Nome DA	Significato	Esempio
Pos	stVal	Posizione dell'interruttore del Dispositivo Generale [intermediate-state | off | on | bad-state]	Closed

T.3.3.1.1.9 Stato operativo dell'impianto - singolo gruppo di generazione

Il nodo logico DGEN (multi-istanziato) è usato per rappresentare lo stato operativo di ogni singolo gruppo di generazione (Operativo/Non Operativo) ed è multi-istanziabile (con N= 1..99).

Per la lista completa dei Data Objects si faccia riferimento alla CEI EN 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
…	…	…		…

Oltre a tutti i DO mandatori del LN, quelli sopra selezionati devono essere implementati nella capability di modello del CCI; essi devono essere utilizzati per la comunicazione del dispositivo ed hanno il seguente significato:

Nome DO	Nome DA	Significato	Esempio
Health	stVal	Singolo Gruppo di Generazione (N) - Stato operativo Multi-istanziabile con N= 1..99 [1 = Operativo, 3 = Non Operativo]	Operativo
GnGrId	stVal	Numero Identificativo del singolo Gruppo di Generazione (N) [1..99]	17

T.3.3.1.2 Modelli di dati relativi alla Controllabilità (Opzionale)

La sezione di Controllabilità è da intendersi, nel suo complesso, Opzionale ed addizionale al modello della Osservabilità specificato in T.3.3.1.1. Se implementata, la presenza dei dati (M/O/C/R/E) segue le regole specificate in Tabella 94

L'operatività delle funzioni di regolazione del CCI è caratterizzata dagli stati specificati in Tabella 97.

Tabella 97 – Operatività delle funzioni di regolazione

DO	FctOpSt (Info di Stato all' attore abilitato remoto)	Mod (Configurazione da parte di attore abilitato remoto)	Beh (Info di Stato all' attore abilitato remoto)	Stato Sintetico	Note
Valore	Autonoma	Attiva	Operativa	Operativo = ACT	Funzione configurata per operare secondo logiche locali. Questa funzione è sempre Autonoma, indipendentemente dalla connessione con attore abilitato remoto
			Non Operativa	Attivo = ON	
		Inattiva	Non Operativa	A Riposo (Disattivo) = OFF	
	Asservita	Attiva	Operativa	Operativo = ACT	Funzione capace di operare secondo set-point remoto quando disponibile un canale di comunicazione. Quando il CCI è connesso almeno col DSO (alta priorità) la funzione è Asservita, in caso di perdita completa della comunicazione, per le funzioni che lo supportano diventa autonoma
			Non Operativa	Attivo = ON	
		Inattiva	Non Operativa	A Riposo (Disattivo) = OFF	
	Non disponibile	N.A.	Non Operativa	A Riposo (Disattivo) = OFF	

T.3.3.1.2.1 Funzione di Regolazione - limitazione della potenza attiva

Il nodo logico DWMX è usato per effettuare la configurazione/taratura e per rappresentare lo stato della funzione di regolazione del limite di P.

Per la lista completa dei Data Objects si faccia riferimento alla CE EN IEC 61850-7-420.

DWMX class – type DWMX1 - prefix WIim				
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
…	…	…		…
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
…	…	…		…

Oltre a tutti i DO mandatori del LN, quelli sopra selezionati devono essere implementati nella capability di modello del CCI; essi devono essere utilizzati per la comunicazione del dispositivo ed hanno il seguente significato:

Nome DO	Nome DA	Significato	Esempio
Beh	stVal	Stato operativo della funzione limite di potenza attiva [1 = Operativa, 5 = Non-Operativa]	Operativa
WMaxSptPct	ctlVal	Setpoint limite di potenza attiva in generazione (%, rispetto alla Potenza apparente massima dell'impianto Smax) - valore [0..100]	20
	origin	Setpoint limite di potenza attiva in generazione (%,rispetto alla Potenza apparente massima dell'impianto Smax) – identità dell'attore abilitato orCat = [automatic-station, remote-control]; orIdent = [DSO, AGGREGATORE]	automatic-station DSO
Mod	ctlVal	Attivazione/disattivazione modalità di funzionamento - limite di potenza attiva - solo su segnale dal DSO - valore [5 = Inattiva, 1 = Attiva]	Attiva
	origin	Attivazione/disattivazione modalità di funzionamento - limite di potenza attiva - solo su segnale dal DSO – identità dell'attore abilitato orCat = [automatic-station, remote-control]; orIdent = [DSO, AGGREGATORE]	automatic-station DSO
FctOpStAuto	stVal	Stato funzione limite di potenza attiva (interna per V prossima al 110%) [Non disponibile / Autonoma]	Autonoma
FctOpStEx	stVal	Stato funzione limite di potenza attiva (su segnale esterno dal DSO) [Non disponibile/Autonoma/Asservita (modalità prioritaria)]	Autonoma

T.3.3.1.2.2 Funzione di Regolazione - modulazione della potenza attiva in immissione/assorbimento al PdC

Il nodo logico DAGC è usato per effettuare la configurazione/taratura e per rappresentare lo stato della funzione di regolazione della modulazione di potenza attiva in immissione/assorbimento al PdC su comando esterno dal DSO.

Per la lista completa dei Data Objects si faccia riferimento alla CEI EN 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 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 operator. Processing of the quality status ('q') of the received data is the prerequisite for correct interpretation of the operating mode.		R / O

Nome DO	Nome DA	Significato	Esempio	
FctOpSt	ENS	CEI 0-16 specific		E / F
…	…	…		…

Oltre a tutti i DO mandatori del LN, quelli sopra selezionati devono essere implementati nella capability di modello del CCI; essi devono essere utilizzati per la comunicazione del dispositivo ed hanno il seguente significato:

Nome DO	Nome DA	Significato	Esempio
Beh	stVal	Stato operativo della funzione di modulazione della potenza attiva in immissione/assorbimento al PdC (su comando esterno dal DSO) [1 = Operativa, 5 = Non-Operativa]	Operativa
WSptPct	ctlVal	Setpoint modulazione della potenza attiva in immissione/assorbimento al PdC (percentuale, con segno, rispetto alla Potenza apparente massima dell'impianto Smax) su comando esterno dal DSO - valore [-100..+100]	20
	origin	Setpoint modulazione della potenza attiva in immissione/assorbimento al PdC (percentuale, con segno, rispetto alla Potenza apparente massima dell'impianto Smax) su comando esterno dal DSO – identità dell'attore abilitato [orCat = automatic-station, remote-control]; [orIdent = DSO, AGGREGATORE]	automatic-station DSO
Mod	ctlVal	Attivazione/disattivazione modalità di funzionamento - modulazione della potenza attiva in immissione/assorbimento al PdC su comando esterno dal DSO - valore [5 = Inattiva, 1 = Attiva]	Attiva
	origin	Attivazione/disattivazione modalità di funzionamento - modulazione della potenza attiva in immissione/assorbimento al PdC su comando esterno dal DSO - identità dell'attore abilitato [orCat = automatic-station, remote-control]; [orIdent = DSO, AGGREGATORE]	automatic-station DSO
FctOpSt	stVal	Stato funzione modulazione della potenza attiva in immissione/assorbimento al PdC (su comando esterno dal DSO) [Non disponibile/Asservita (modalità prioritaria)]	Asservita

T.3.3.1.2.3 Funzione di Regolazione – regolazione di tensione con erogazione di potenza reattiva Induttiva/Capacitiva

Il nodo logico DVAR è usato per effettuare la configurazione/taratura e per rappresentare lo stato della funzione di regolazione di tensione con erogazione di potenza reattiva induttiva/capacitiva su comando esterno dal DSO.

Per la lista completa dei Data Objects si faccia riferimento alla CEI EN 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 behaviour 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
…	…	…		…

Oltre a tutti i DO mandatori del LN, quelli sopra selezionati devono essere implementati nella capability di modello del CCI; essi devono essere utilizzati per la comunicazione del dispositivo ed hanno il seguente significato:

Nome DO	**Nome DA**	**Significato**	**Esempio**
Beh	stVal	Stato operativo della funzione di regolazione di tensione con erogazione di potenza reattiva induttiva/capacitiva su comando esterno dal DSO [1 = Operativa, 5 = Non-Operativa]	Operativa
VArTgtSptPct	ctlVal	Setpoint della funzione di regolazione di tensione con erogazione di potenza reattiva induttiva/capacitiva (percentuale, con segno, rispetto alla Potenza apparente massima dell'impianto Smax) su comando esterno dal DSO - valore [-100..+100]	20
	origin	Setpoint della funzione di regolazione di tensione con erogazione di potenza reattiva induttiva/capacitiva (percentuale, con segno, rispetto alla Potenza apparente massima dell'impianto Smax) su comando esterno dal DSO – identità dell'attore abilitato [orCat = automatic-station, remote-control]; [orIdent = DSO, AGGREGATORE]	automatic-station DSO
Mod	ctlVal	Attivazione/disattivazione modalità di funzionamento - regolazione di tensione con erogazione di potenza reattiva induttiva/capacitiva su comando esterno dal DSO - valore [5 = Inattiva, 1 = Attiva]	Attiva
	origin	Attivazione/disattivazione modalità di funzionamento - regolazione di tensione con erogazione di potenza reattiva induttiva/capacitiva su comando esterno dal DSO - identità dell'attore abilitato [orCat = automatic-station, remote-control]; [orIdent = DSO, AGGREGATORE]	automatic-station DSO
FctOpSt	stVal	Stato funzione set point di potenza reattiva scambiata Induttiva/Capacitiva (Funzionamento in regolazione di V con erogazione di Q) su comando esterno dal DSO [Non disponibile/Asservita (modalità prioritaria)]	Asservita

T.3.3.1.2.4 Funzione di Regolazione - set point del fattore di potenza

Il nodo logico DFPF è usato per effettuare la configurazione/taratura e per rappresentare lo stato della funzione di regolazione del set point di cosϕ.

Per la lista completa dei Data Objects si faccia riferimento alla CEI EN 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 behaviour 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
…	…	…		…

Oltre a tutti i DO mandatori del LN, quelli sopra selezionati devono essere implementati nella capability di modello del CCI; essi devono essere utilizzati per la comunicazione del dispositivo ed hanno il seguente significato:

Nome DO	**Nome DA**	**Significato**	**Esempio**
Beh	stVal	Stato operativo della funzione set point di cosϕ (Funzionamento in erogazione di Q con cosϕ costante) [1 = Operativa, 5 = Non-Operativa]	Operativa
PFGnTgtSpt	ctlVal	Setpoint di cosϕ in caso di generazione di potenza attiva - valore [-1.00..0.00]	-0.95
	origin	Setpoint di cosϕ in caso di generazione di potenza attiva – identità dell'attore abilitato [orCat = automatic-station, remote-control]; [orIdent = DSO, AGGREGATORE]	automatic-station DSO
PFLodTgtSpt	ctlVa	Setpoint di cosϕ in caso di assorbimento di potenza attiva - valore [0.00..1.00]	0.95
	origin	Setpoint di cosϕ in caso di assorbimento di potenza attiva – identità dell'attore abilitato [orCat = automatic-station, remote-control]; [orIdent = DSO, AGGREGATORE]	automatic-station DSO

Nome DO	Nome DA	Significato	Esempio
Mod	ctlVal	Attivazione/disattivazione modalità di funzionamento - set point di cosϕ (Funzionamento in erogazione di Q con cosϕ costante) - valore [5 = Inattiva, 1 = Attiva]	Attiva
	origin	Attivazione/disattivazione modalità di funzionamento - set point di cosϕ (Funzionamento in erogazione di Q con cosϕ costante) – identità dell'attore abilitato [orCat = automatic-station, remote-control]; [orIdent = DSO, AGGREGATORE]	automatic-station DSO
FctOpSt	stVal	Stato funzione set point di cosϕ (Funzionamento in erogazione di Q con cosϕ costante) [Non disponibile / Autonoma / Asservita (modalità prioritaria)]	Autonoma

T.3.3.1.2.5 Funzione di Regolazione - Q(V)

I nodi logici DVVR, DPMC (2 istanze) e DECP (2 istanze) sono usati, nel loro complesso, per effettuare la configurazione/taratura e per rappresentare lo stato della funzione di regolazione di Q(V).

Per la lista completa dei Data Objects si faccia riferimento alla CEI EN IEC 61850-7-420.

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
…	…	…		…

Oltre a tutti i DO mandatori del LN, quelli sopra selezionati devono essere implementati nella capability di modello del CCI; essi devono essere utilizzati per la comunicazione del dispositivo ed hanno il seguente significato:

Nome DO	Nome DA	Significato	Esempio
Beh	stVal	Stato operativo della funzione Q(V) (Funzionamento in erogazione automatica di Q secondo la curva Q=f(V) [1 = Operativa, 5 = Non-Operativa]	Operativa
Mod	ctlVal	Attivazione/disattivazione della funzione Q(V) (Funzionamento in erogazione automatica di Q secondo la curva Q=f(V)) - valore [5 = Inattiva, 1 = Attiva]	Attiva
	origin	Attivazione/disattivazione della funzione Q(V) (Funzionamento in erogazione automatica di Q secondo la curva Q=f(V)) – identità dell'attore abilitato [orCat = automatic-station, remote-control]; [orIdent = DSO, AGGREGATORE]	automatic-station DSO
FctOpSt	stVal	Stato funzione Q(V) (Funzionamento in erogazione automatica di Q secondo la curva Q=f(V)) [Non disponibile /Autonoma /Asservita (modalità prioritaria)]	Autonoma
K	setMag	Parametro K della funzione Q(V) [-1.00..1.00]	0.00 (per Fotovoltaici ed Accumulo)

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
…	…	…		…

Oltre a tutti i DO mandatori del LN, quelli sopra selezionati devono essere implementati nella capability di modello del CCI; essi devono essere utilizzati per la comunicazione del dispositivo ed hanno il seguente significato:

Nome DO	Nome DA	Significato	Esempio
WSpt1	ctlVal	Potenza di Lock-in della funzione Q(V) - valore [0.00..max] della $P_{Nominale}$ (P.U.)	0.20
	origin	Potenza di Lock-in della funzione Q(V) – identità dell'attore abilitato [orCat = automatic-station, remote-control]; [orIdent = DSO, AGGREGATORE]	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
…	…	…		…

Oltre a tutti i DO mandatori del LN, quelli sopra selezionati devono essere implementati nella capability di modello del CCI; essi devono essere utilizzati per la comunicazione del dispositivo ed hanno il seguente significato:

Nome DO	Nome DA	Significato	Esempio
WSpt1	ctlVal	Potenza di Lock-out della funzione Q(V) - valore [0.00..max] della $P_{Nominale}$ (P.U.)	0.05
	origin	Potenza di Lock-out della funzione Q(V) – identità dell'attore abilitato [orCat = automatic-station, remote-control]; [orIdent = DSO, AGGREGATORE]	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
…	…	…		…

Oltre a tutti i DO mandatori del LN, quelli sopra selezionati devono essere implementati nella capability di modello del CCI; essi devono essere utilizzati per la comunicazione del dispositivo ed hanno il seguente significato:

Nome DO	Nome DA	Significato	Esempio
VMax	setMag	Tensione superiore 1 della funzione Q(V) [0.00..max] della $V_{Nominale}$ (P.U.)	1.08
VMin	setMag	Tensione inferiore 1 della funzione Q(V) [0.00..max] della $V_{Nominale}$ (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
…	…	…		…

Oltre a tutti i DO mandatori del LN, quelli sopra selezionati devono essere implementati nella capability di modello del CCI; essi devono essere utilizzati per la comunicazione del dispositivo ed hanno il seguente significato:

Nome DO	Nome DA	Significato	Esempio
WMax	setMag	Tensione superiore 2 della funzione Q(V) [0.00..max] della $V_{Nominale}$ (P.U.)	1.10
WMin	setMag	Tensione inferiore 2 della funzione Q(V) [0.00..max] della $V_{Nominale}$ (P.U.)	0.90

T.3.3.1.2.6 Funzione di Regolazione - cosϕ = f(P)

Il nodo logico DPFW è stato appositamente creato per effettuare la configurazione/taratura e per rappresentare lo stato della funzione di regolazione di cosϕ = f(P) (Funzionamento con regolazione del cosϕ in funzione di 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

I seguenti DO devono essere implementati nella capability di modello del CCI; essi devono essere utilizzati per la comunicazione del dispositivo ed hanno il seguente significato

Nome DO	Nome DA	Significato	Esempio
Beh	stVal	Stato operativo della funzione cosϕ = f(P) (Funzionamento con regolazione del cosϕ in funzione di P) [1 = Operativa, 5 = Non-Operativa]	Operativa
Mod	ctlVal	Attivazione/disattivazione della funzione cosϕ = f(P) (Funzionamento con regolazione del cosϕ in funzione di P) - valore [5 = Inattiva, 1 = Attiva]	Attiva
	origin	Attivazione/disattivazione della funzione cosϕ = f(P) (Funzionamento con regolazione del cosϕ in funzione di P) – identità dell'attore abilitato [orCat = automatic-station, remote-control]; [orIdent = DSO, AGGREGATORE]	automatic-station DSO
FctOpSt	stVal	Stato funzione PF(P) (Funzionamento con regolazione del cosϕ in funzione di P) [Non disponibile /Autonoma / Asservita (modalità prioritaria)]	Asservita
WSetA	setMag	Valore P (punto A) [0.00..max] della $P_{Nominale}$ (P.U.)	0.20
PFSetA	setMag	Valore cosϕ (punto A) [-1.00..1.00]	1.00
WSetB	setMag	Valore P (punto B) [0.00..max] della $P_{Nominale}$ (P.U.)	0.50
PFSetB	setMag	Valore cosϕ (punto B) [-1.00..1.00]	1.00
WSetC	setMag	Valore P (punto C) [0.00..max] della $P_{Nominale}$ (P.U.)	1.00
PFSetC	setMag	Valore cosϕ (punto C) [-1.00..1.00]	0.95
VLkIn	setMag	Tensione di Lock-in della funzione cosϕ = f(P) [1.00..1.10] della $V_{Nominale}$ (P.U.)	1.05
VLkOut	setMag	Tensione di Lock-out della funzione cosϕ = f(P) [0.90..1.00] della $V_{Nominale}$ (P.U.)	0.98

T.3.3.1.3 Modelli di dati relativi alla Partecipazione all'MSD (Facoltativo)

La sezione dedicata all'Aggregatore è da intendersi, nel suo complesso, Facoltativa ed addizionale al modello della Osservabilità specificato in T.3.3.1.1. Se implementata, la presenza dei dati (M/O/C/R/E) segue le regole specificate in Figura 95

T.3.3.1.3.1 Misure dell'impianto

Il nodo logico MMXU è usato per rappresentare le misure dell'impianto al PdC. In Allegato O si prevedono la potenza attiva e reattiva riportate ogni 4 sec. Trattandosi della medesima informazione già modellata nel parafrafo dell'Osservabilità, per la sua descrizione si faccia riferimento al Paragrafo T.3.3.1.1.7 per le grandezze "TotW" e "TotVAr".

T.3.3.1.3.2 Funzione di Regolazione - set point di potenza attiva in immissione/ assorbimento

Il nodo logico DAGC è usato per effettuare la configurazione/taratura e per rappresentare lo stato della funzione di regolazione del set point di potenza attiva in immissione/assorbimento per le finalità previste dalla partecipazione all'MSD.

Per la lista completa dei Data Objects si faccia riferimento alla CEI EN IEC 61850-7-420.

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 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
…	…	…		…

Oltre a tutti i DO mandatori del LN, quelli sopra selezionati devono essere implementati nella capability di modello del CCI; essi devono essere utilizzati per la comunicazione del dispositivo ed hanno il seguente significato:

Nome DO	Nome DA	Significato	Esempio
Beh	stVal	Stato operativo della funzione set point di potenza attiva in immissione/assorbimento (per la partecipazione all'MSD) [1 = Operativa, 5 = Non-Operativa]	Operativa
WsptPct	ctlVal	Setpoint di potenza attiva in immissione/assorbimento (percentuale, con segno, rispetto alla Potenza apparente massima dell'impianto Smax) per la partecipazione all'MSD - valore [-100 .. +100]	20
	origin	Setpoint di potenza attiva in immissione/assorbimento (percentuale, con segno, rispetto alla Potenza apparente massima dell'impianto Smax) per la partecipazione all'MSD – identità dell'attore abilitato [orCat = automatic-station, remote-control]; [orIdent = DSO, AGGREGATORE]	automatic-station DSO

Nome DO	Nome DA	Significato	Esempio
Mod	ctlVal	Attivazione/disattivazione modalità di funzionamento - set point di potenza attiva in immissione/assorbimento per la partecipazione all'MSD - valore [5 = Inattiva, 1 = Attiva]	Attiva
	origin	Attivazione/disattivazione modalità di funzionamento - set point di potenza attiva in immissione/assorbimento per la partecipazione all'MSD – identità dell'attore abilitato [orCat = automatic-station, remote-control]; [orIdent = DSO, AGGREGATORE]	automatic-station DSO
FctOpSt	stVal	Stato funzione set point di potenza attiva in immissione/assorbimento per la partecipazione all'MSD [Non disponibile/ Asservita (modalità prioritaria)]	Asservita

T.3.3.1.3.3 Funzione di Regolazione - set point di potenza reattiva scambiata Induttiva/Capacitiva

Il nodo logico DVAR è usato per effettuare la configurazione/taratura e per rappresentare lo stato della funzione di regolazione del set point di potenza reattiva scambiata Induttiva/Capacitiva per le finalità previste dalla partecipazione all'MSD.

Per la lista completa dei Data Objects si faccia riferimento alla CEI EN IEC 61850-7-420.

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 behaviour 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
…	…	…		…

Oltre a tutti i DO mandatori del LN, quelli sopra selezionati devono essere implementati nella capability di modello del CCI; essi devono essere utilizzati per la comunicazione del dispositivo ed hanno il seguente significato:

Nome DO	Nome DA	Significato	Esempio
Beh	stVal	Stato operativo della funzione set point di potenza reattiva scambiata Induttiva/Capacitiva (per la partecipazione all'MSD) [1 = Operativa, 5 = Non-Operativa]	Operativa
VArTgtSptPct	ctlVal	Setpoint di potenza reattiva scambiata Induttiva/Capacitiva (percentuale, con segno, rispetto alla Potenza apparente massima dell'impianto Smax) per la partecipazione all'MSD - valore [-100 .. +100]	20
	origin	Setpoint di potenza reattiva scambiata Induttiva/Capacitiva (percentuale, con segno, rispetto alla Potenza apparente massima dell'impianto Smax) per la partecipazione all'MSD – identità dell'attore abilitato [orCat = automatic-station, remote-control]; [orIdent = DSO, AGGREGATORE]	automatic-station DSO
Mod	ctlVal	Attivazione/disattivazione modalità di funzionamento - set point di potenza reattiva scambiata Induttiva/Capacitiva per la partecipazione all'MSD [5 = Inattiva, 1 = Attiva]	Attiva
	origin	Attivazione/disattivazione modalità di funzionamento - set point di potenza reattiva scambiata Induttiva/Capacitiva per la partecipazione all'MSD – identità dell'attore abilitato [orCat = automatic-station, remote-control]; [orIdent = DSO, AGGREGATORE]	automatic-station ~~e~~ DSO
FctOpSt	stVal	Stato funzione set point di potenza reattiva scambiata Induttiva/Capacitiva (Funzionamento in regolazione di V con erogazione di Q) per la partecipazione all'MSD [Non disponibile / Asservita (modalità prioritaria)]	Asservita

T.3.3.1.4 Modello dei dati del CCI e privilegi di accesso ai fini della sicurezza

Il presente paragrafo disciplina i privilegi di accesso ai dati gestiti dal CCI per le finalità di monitoraggio nonché controllo/configurazione dell'IED riservate agli attori abilitati DSO e Aggregatore.

Il dispositivo dovrà consentire la fruizione dei privilegi di accesso solo previa identificazione ed autenticazione degli Attori secondo le logiche crittografiche descritte dal paragrafo T.3.3.4 e in accordo alle configurazioni descritte ai paragrafi T.3.3.4.9.4 e T.3.3.4.9.9.1.

In particolare, il dispositivo dovrà consentire la fruizione dei privilegi di accesso assegnati al DSO:

i) DSO_OPERATOR (vedi T.3.3.4.3.1)

ii) VIEWER

solo previa identificazione e autenticazione del DSO, escludendo l'accesso per ruoli presentati dal DSO diversi da quelli elencati.

Analogamente, per il ruolo di Aggregatore, il dispositivo dovrà consentire la fruizione dei privilegi di accesso assegnati all'Aggregatore:

i. AGGREGATOR_OPERATOR (vedi T.3.3.4.3.1, o ruolo equivalente, vedi T.3.3.4.4.2)

ii. VIEWER (o ruolo equivalente)

solo previa identificazione e autenticazione dell'Aggregatore, escludendo l'accesso per ruoli presentati dall'Aggregatore diversi da quelli elencati(238).

(238) Il CCI accetta sessioni di comunicazione client/server da più client contemporaneamente, ad esempio da diverse entità remote che hanno necessità di accesso con più ruoli contemporanei. Coerentemente il CCI deve offrire la possibilità di abilitare più istanze degli stessi report ai client connessi.

Questa classificazione supporta la definizione dei ruoli e privilegi secondo quanto prescritto in T.3.3.4.3.1.

I soggetti autorizzati all'accesso (ovvero identificati ed autenticati) non identificati come DSO o Aggregatore assumono i privilegi di accesso coerenti con il ruolo loro assegnato.

Tabella 98 – Dati riservati al DSO

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

Privilegi di Accesso	IED	LD	LN Type	LN Prefix	LN Class	LN Inst.	DO (.SDO)	CDC	DataSet / Report
RW	(1)	LD_Plant	DECP2	VArV	DECP	1	Vmin	ASG	(2)
RW	(1)	LD_Plant	DECP2	VArV	DECP	2	VMax	ASG	(2)
RW	(1)	LD_Plant	DECP2	VArV	DECP	2	Vmin	ASG	(2)
RO	(1)	LD_Plant	DPFW1	PFW	DPFW	1	Beh	ENS	(2)
RW	(1)	LD_Plant	DPFW1	PFW	DPFW	1	Mod	ENC	(2)
RO	(1)	LD_Plant	DPFW1	PFW	DPFW	1	FctOpSt	ENS	(2)
RW	(1)	LD_Plant	DPFW1	PFW	DPFW	1	WSetA	ASG	(2)
RW	(1)	LD_Plant	DPFW1	PFW	DPFW	1	PFSetA	ASG	(2)
RW	(1)	LD_Plant	DPFW1	PFW	DPFW	1	WSetB	ASG	(2)
RW	(1)	LD_Plant	DPFW1	PFW	DPFW	1	PFSetB	ASG	(2)
RW	(1)	LD_Plant	DPFW1	PFW	DPFW	1	WSetC	ASG	(2)
RW	(1)	LD_Plant	DPFW1	PFW	DPFW	1	PFSetC	ASG	(2)
RW	(1)	LD_Plant	DPFW1	PFW	DPFW	1	VLkIn	ASG	(2)
RW	(1)	LD_Plant	DPFW1	PFW	DPFW	1	VLkOut	ASG	(2)
RO	(1)	LD_Plant	MMXU1	PdC	MMXU	1	TotW	MV	(3) Misure PdC 4sec
RO	(1)	LD_Plant	MMXU1	PdC	MMXU	1	TotVAr	MV	(3) Misure PdC 4sec
RO	(1)	LD_Plant	MMXU1	PdC	MMXU	1	PPV.phsA/B/C	DEL	(3) Misure PdC 4sec
RO	(1)	LD_Plant	MMXU1	PdC	MMXU	1	A.phsA/B/C	WYE	(2)
RO	(1)	LD_Plant	MMXU2	GenPV	MMXU	1	TotW	MV	(3) Misure per fonte Gen. 4sec
RO	(1)	LD_Plant	MMXU2	GenWi	MMXU	1	TotW	MV	(3) Misure per fonte Gen. 4sec
RO	(1)	LD_Plant	MMXU2	GenTer	MMXU	1	TotW	MV	(3) Misure per fonte Gen. 4sec
RO	(1)	LD_Plant	MMXU2	GenIdr	MMXU	1	TotW	MV	(3) Misure per fonte Gen. 4sec
RO	(1)	LD_Plant	MMXU2	St	MMXU	1	TotW	MV	(3) Misure Accumulo 4sec
RO	(1)	LD_Plant	MMXU2	SGG	MMXU	1..N	TotW	MV	(3) Misure Singolo Gen. 4sec
RO	(1)	LD_Plant	XCBR1	IDG	XCBR	1	Pos	DPC	(3) Stati, Allarmi, Segnali
RO	(1)	LD_Plant	DGEN2	SSGG	DGEN	1..N	Health	ENS	(3) Stati, Allarmi, Segnali
RO	(1)	LD_Plant	DGEN2	SSGG	DGEN	1..N	GnGrId	INS	(3) Misure Singolo Gen. 4sec
RW	(1)	LD_Plant	DataSet_DSO (n)						(2)
RW	(1)	LD_Plant	ReportControl Block_ DSO (n)						(2)

NOTE:

(1) il nome dell'IED dipende dal progetto/impianto specifico.

(2) l'inclusione del dato in un DataSet, il nome del DataSet, il nome e i parametri del Report Control Block che si riferisce al DataSet dipendono dal progetto/impianto specifico.

(3) per i fini dell'Osservabilità, il nome del DataSet e il nome e i parametri del Report Control Block che si riferisce al DataSet dipendono dal progetto/impianto specifico.

RO = dato in sola Lettura.

RW = dato in Lettura/Scrittura.

Tabella 99 – Dati riservati all'Aggregatore

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

NOTE:

(1) il nome dell'IED dipende dal progetto/impianto specifico.

(2) l'inclusione del dato in un DataSet, il nome del DataSet, il nome e i parametri del Report Control Block che si riferisce al DataSet dipendono dal progetto/impianto specifico.

RO = dato in sola Lettura.

RW = dato in Lettura/Scrittura.

T.3.3.2 Servizi ACSI

A fronte del modello dati riportato nella precedente sezione, il server IEC 61850 dovrà implementare i seguenti servizi di comunicazione (CEI EN 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).

Tabella 100 – Classi e servizi ACSI

Classe ACSI	Servizi ACSI	Privilegi	DSO/Aggregatore
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

Classe ACSI	Servizi ACSI	Privilegi	DSO/Aggregatore
DataSet	GetDataSetValues	Dataset Permette al soggetto/ruolo di ottenere i valori e la struttura dei dataset senza permetterne la modifica	Applicable
	SetDataSetValues		Not Applicable
	CreateDataSet		Not Applicable
	DeleteDataSet		Not Applicable
	GetDataSetDirectory		Applicable
Buffered Report Control Block	Report	Reporting: Permette al soggetto/ruolo di utilizzare sia i buffered che unbuffered report senza permetterne la modifica	Applicable
	GetBRCBValues		Applicable
	SetBRCBValues		Not Applicable
UnBuffered Report Control Block	Report	Reporting: Permette al soggetto/ruolo di utilizzare sia i buffered che unbuffered report senza permetterne la modifica	Applicable
	GetURCBValues		Applicable
	SetURCBValues		Not Applicable

Per successivi sviluppi negli scambi informativi ad alta velocità con le protezioni (in prospettiva PG), secondo lo "Schema generale del sistema CCI con relative interfacce funzionali" in Allegato O, si prevede l'uso di servizi ACSI di classe GOOSE.

T.3.3.3 Mappatura su protocollo di comunicazione

Al fine di realizzare un CCI che risulti interoperabile rispetto ai sistemi a cui sarà interfacciato (DSO ed Attori Remoti Abilitati), è necessario specificare la mappatura dei concetti astratti riportati in T.3.1 e T.3.1.1 su uno specifico protocollo di comunicazione.

Al fine di individuare tale mappatura, si sono considerati i seguenti aspetti.

- La tipologia dello scambio informativo associato al CCI risulta compatibile con le tipologie "Type 2/Type 3[(239)]" previste nel Paragrafo 5.1 di CEI EN 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", che per tale tipologia di messaggi prevede una mappatura su protocollo MMS.
- La necessità di definire una correlazione tra ruoli (DSO, Attori Remoti Abilitati) e l'accesso a specifici servizi IEC 61850, suggerisce un "Application association model" di tipo "two-party application association" tipico del modello Client/Server.

Sulla base di tali considerazioni è stata selezionata la mappatura CEI EN 61850-8-1 basata su protocollo MMS (con le considerazioni di prospettiva per le comunicazioni GOOSE citate in T.3.2.1 e T.3.2.2).

Al fine di agevolare la realizzazione di dispositivi CCI interoperabili, sarà reso disponibile il relativo file di configurazione secondo il formalismo SCL previsto dallo standard IEC 61850.

T.3.3.4 Sicurezza informatica del CCI

Per quanto riguarda la sicurezza delle comunicazioni, le prescrizioni contenute in questo documento fanno riferimento all'architettura del dispositivo CCI specificata nell'Allegato O, la quale prevede due interfacce di rete per gli accessi remoti al dispositivo e una o più interfacce per gli accessi in locale. L'accesso remoto è previsto sia per funzioni di monitoraggio e controllo, sia per esigenze di gestione dell'impianto.

(239) Type 2 con performance calss P4; Type 3 con performance calls P5. Riferimento CEI EN 61850-5 paragrafi 11.2.2 e 11.2.3

In questa sezione la specifica della sicurezza delle funzioni di monitoraggio e controllo del CCI fa riferimento alla mappatura delle funzioni di comunicazione su protocollo MMS (Manufacturing Message Specification) indicata nel Paragrafo T.3.3 e specificata dalla CEI EN 61850-8-1.

Vengono inoltre specificati i meccanismi per la sicurezza delle comunicazioni GOOSE per le funzioni di subscriber del CCI.

La sicurezza dei profili di comunicazione IEC 61850 è stata normata dallo standard CEI EN IEC 62351-6 “Power systems management and associated information exchange - Data and communication security - Part 6: Security for IEC 61850”.

La specifica delle funzioni di sicurezza contenuta in questa sezione tiene conto delle evoluzioni previste dalle parti della IEC 62351 di interesse per il dispositivo CCI(240). Relativamente ai test di conformità alla IEC 62351 si rimanda all’Allegato O, Paragrafo O.15.5 “Conformità dell'apparecchiatura”. Nei paragrafi è strutturata come segue:

- nei Paragrafo T.3.3.4.1, T.3.3.4.3 e T.3.3.4.4 vengono presentati i meccanismi di base per la sicurezza degli scambi informativi basati sui protocolli IEC 61850;
- i Paragrafo T.3.3.4.5, T.3.3.4.6, T.3.3.4.7 e T.3.3.4.8 indicano le prescrizioni di sicurezza per i servizi di supporto;
- il Paragrafo T.3.3.4.9 presenta i processi relativi alla gestione dei certificati elettronici utilizzati sia dalle comunicazioni IEC 61850 sia dai servizi di supporto;
- il Paragrafo T.3.3.4.10 indica i requisiti di segregazione del traffico;
- il Paragrafo T.3.3.4.11 riguarda la sicurezza delle comunicazioni attraverso interfacce locali (non di rete).

T.3.3.4.1 Sicurezza delle comunicazioni IEC 61850/MMS

Lo standard CEI EN IEC 62351-6 approfondisce le specifiche di sicurezza dei protocolli di comunicazione mappati dallo standard. Per quanto riguarda le comunicazioni mappate sul protocollo MMS, CEI EN IEC 62351-6 rimanda allo standard CEI EN IEC 62351-4 “Power systems management and associated information exchange - Data and communications security - Part 4: Profiles including MMS and derivatives”.

Secondo quanto previsto da CEI EN IEC 62351-4, la sicurezza delle comunicazioni MMS si realizza definendo il profilo trasporto, nel seguito riferito anche come profilo-T, che indirizza i livelli 1-4 dello stack ISO/OSI, ed il profilo applicativo, che invece indirizza i livelli 5-7 del modello ISO/OSI.

Nel profilo applicativo devono essere garantite l’autenticazione delle parti in comunicazione e l’integrità delle comunicazioni. Deve inoltre essere implementato il supporto alla crittografia che garantisce la confidenzialità delle comunicazioni, ma questa funzionalità deve poter essere attivata o disattivata in funzione delle specifiche policy di sicurezza concordate tra le parti.

Gli algoritmi a chiave pubblica da utilizzare per il profilo applicativo sono:

- Crittografia RSA: object identifier { iso(1) member-body(2) us(840) ansi-x9-62(10045) keyType(2) 1}
- Crittografia a curve ellittiche:
- 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}

(240) Per ragioni di interoperabilità, le prescrizioni di sicurezza del CCI si applicano necessariamente ai dispositivi remoti che ospitano i corrispondenti client IEC 61850.

Devono essere supportate chiavi crittografiche RSA di lunghezza di 2048 bit, mentre, nel caso di chiavi crittografiche ECDSA, deve essere supportata la lunghezza di 256 bit; questi valori devono essere intesi come minimi: è fortemente raccomandato che siano supportate anche chiavi di lunghezza superiore a questi minimi (es. 3072 bit nel caso di chiavi RSA e/o 384 bit nel casi di chiavi ECDSA).

Deve essere utilizzato l'algoritmo di hash SHA256 sia per finalità di firma digitale sia per il calcolo di Integrity Check Value (ICV): object identifier { joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) hashalgs(2) 1 }

Per la firma digitale devono essere supportati i due seguenti algoritmi basati entrambi su SHA256:

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

Al fine di verificare l'integrità di un messaggio deve inoltre essere supportato il seguente algoritmo per il calcolo di Integrity Check Value:

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

Per quanto riguarda gli algoritmi di crittografia simmetrica devono essere supportati gli algoritmi:

- aes128-CBC: object identifier { joint-iso-itu-t(2) country(16) us(840)organization(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 }

Devono inoltre essere supportati i seguenti algoritmi che, oltre alla confidenzialità delle informazioni, possono garantire anche integrità e autenticazione:

- aes128-GCM: object identifier { joint-iso-itu-t(2) country(16) us(840)organization(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 particolare aes128-GCM e aes256-GCM devono potere essere utilizzati anche senza le funzionalità di confidenzialità delle comunicazioni e possono essere combinati in questo caso con aes128-CBC e aes256-CBC per fornire questa funzionalità.

Il certificato presentato dall'entità richiedente nella fase di creazione dell'associazione del profilo applicativo non deve superare 8192 ottetti.

Si devono prevedere meccanismi o procedure affinché l'orologio interno utilizzato per ricavare i riferimenti temporali rimanga sincronizzato con UTC; uno scostamento superiore a 10 minuti tra gli orologi delle due entità coinvolte nella comunicazione deve provocare il fallimento della comunicazione.

Nello scambio chiavi Diffie-Hellman (DH) deve essere supportato il gruppo DH "14" (2048-bit) quando sono usati gli algoritmi RSA; in caso di uso di algoritmi ECDH devono essere supportati sia il gruppo DH "23" (secp256r1) sia il gruppo DH "28" (BrainpoolP256r1).

Per il profilo applicativo ci si deve riferire a CEI EN IEC 62351-4 per quanto riguarda i requisiti del protocollo ACSE.

Per il profilo applicativo deve essere usata la sicurezza End-To-End (E2E) e ci si deve riferire a CEI EN IEC 62351-4 sulle prescrizioni circa la fase di creazione dell'associazione tra le due parti in comunicazione e la fase di trasferimento dati.

In fase di associazione le SecPDU devono contenere le PDU del protocollo MMS specificate, cui deve essere applicata la firma digitale per garantire l'integrità della comunicazione.

In fase di trasferimento dati si può optare per l'invio di PDU in chiaro, con verifica dell'integrità delle comunicazioni, o per l'invio di PDU cifrate per garantire la confidenzialità delle comunicazioni.

I fallimenti nella fase di associazione e nella fase di trasferimento dati devono essere gestiti tramite le apposite SecPDU sia nel caso l'origine sia riconducibile al protocollo MMS sia in nel caso l'origine sia riconducibile ad anomalie relative alla sicurezza. Vanno usati i codici diagnostici specificati dallo standard per indicare le cause di fallimento in fase di associazione o trasferimento dati.

Il profilo-T fornisce funzioni di autenticazione, integrità e confidenzialità a livello trasporto. Con riferimento alle implementazioni delle comunicazioni MMS che utilizzano il protocollo TCP per il livello trasporto, il profilo-T sicuro prevede l'impiego del TLS (Transport Layer Security) secondo quanto specificato dalla CEI EN 62351-3 "Power systems management and associated information exchange - Data and communications security - Part 3: Communication network and system security - Profiles including TCP/IP".

Il profilo TLS specificato dalla CEI EN 62351-3 stabilisce quanto segue:

- la porta TCP 3782 è definita come default per le comunicazioni del profilo-T con TLS;
- come versione TLS, deve essere supportata la versione v1.2(241) di TLS;
- come suite di cifratura è richiesto il supporto almeno delle tre seguenti cypher suite:
  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;
- oltre alle cypher suite indicate precedentemente è richiesto anche il supporto per la cypher suite TLS_RSA_WITH_NULL_SHA256. Non prevedendo cifratura del traffico, questa cypher suite può essere utilizzata, ad esempio per semplificare il monitoraggio del traffico, solo quando il dominio amministrativo ha stabilito che i dati scambiati non necessitano di confidenzialità e altre soluzioni sono in atto per proteggere adeguatamente la confidenzialità dei dati (es. VPN). Per prevenire l'utilizzo inconsapevole, questa cypher suite deve essere disattivata di default e si devono prevedere procedure per abilitarla intenzionalmente all'occorrenza;
- di default la rinegoziazione della sessione TLS dovrebbe avvenire in un tempo allineato al periodo di aggiornamento della CRL (Lista di Revoche di Certificati), ed in particolare almeno la metà di questo periodo; comunque per non sovraccaricare le comunicazioni di client e server l'intervallo di rinegoziazione non può essere inferiore a 10 minuti;
- al fine di rinnovare le chiavi di cifratura di sessione deve essere supportata la tecnica della resumption della sessione TLS. La resumption della sessione TLS evita anche di ripetere alcuni scambi informativi (es. trasmissione dei certificati digitali) che avvengono in caso di riconnessione e può quindi risultare efficace per ripristinare brevi interruzioni di connettività. La resumption della sessione TLS deve avvenire in un intervallo configurabile e comunque almeno ogni 2 ore; in ogni caso in un tempo inferiore a quello della rinegoziazione e allineato al periodo di aggiornamento della CRL;

(241) La futura Edizione 2 della CEI EN 62351-3 prevederà la migrazione alla versione TLS v 1.3, in conformità a quanto previsto dallo standard NIST SP 800-52 Rev. 2 "Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations", il quale richiede il supporto della versione TLS 1.3 entro gennaio 2024.

- si richiede il supporto di almeno cinque diversi *root certificate* relativi a diverse Autorità di Certificazione(242);
- la dimensione dei certificati a chiave pubblica utilizzati dovrebbe essere al massimo di 8192 ottetti per questioni di interoperabilità; l'implementazione deve gestire certificati almeno fino a questa dimensione;
- l'aggiornamento della CRL dovrebbe avvenire almeno ogni 24 ore. In caso di utilizzo del protocollo OCSP (Online Certificate Status Protocol), le risposte possono essere mantenute in cache per un massimo di 24 ore. Una sessione attiva non dovrà comunque essere terminata solo a causa del superamento di questi limiti.

Al fine di impedire sia l'accesso non autorizzato sia la modifica/intercettazione non autorizzata delle informazioni di controllo nelle diverse architetture di rete, si ritiene mandatorio che il CCI supporti sia il profilo applicativo E2E sia il profilo-T con specifiche di sicurezza TLS(243).

In questo paragrafo sono state riportate, sinteticamente, le indicazioni fornite dagli standard CEI EN 62351-3, CEI EN IEC 62351-4 e CEI EN IEC 62351-6 relativamente alla sicurezza delle comunicazioni IEC 61850/MMS cui si rimanda per i dettagli implementativi; nella seguente tabella vengono riassunti gli aspetti caratterizzanti del profilo degli standard di riferimento definito in questo documento.

Aspetto del profilo IEC 62351	Configurazione del profilo IEC 62351
Profilo applicativo	È richiesto il supporto delle specifiche di sicurezza E2E come indicato precedentemente in questo documento e nello standard di riferimento CEI EN IEC 62351-4(244).
Profilo trasporto	È richiesto il supporto delle specifiche di sicurezza TLS, come indicato precedentemente in questo documento e nello standard di riferimento CEI EN 62351-3.
Lunghezza delle chiavi pubblica/privata	È richiesto l'utilizzo, e quindi il supporto, per chiavi RSA di lunghezza minima di 2048 bit. Un limite minimo è indicato anche per chiavi crittografiche ECDSA selezionato in modo da garantire un livello di sicurezza almeno analogo a quello delle chiavi RSA(245).
Versioni del protocollo TLS	È richiesto l'utilizzo, e quindi il supporto, della versione v1.2 del protocollo TLS(246).
Cypher suite	Non è richiesto il supporto della cypher suite TLS_DH_RSA_WITH_AES_128_GCM_SHA256 anche se indicata dagli attuali standard di riferimento(247).
Root certificate	Si richiede il supporto di almeno cinque diversi *root certificate*(248).

(242) La futura Edizione 2 della CEI EN 62351-3 prevede questo limite inferiore; è stato recepito in questo documento con l'obiettivo di conformare preventivamente i dispositivi alle crescenti necessità di flessibilità operativa.

(243) La scelta del/i profili di sicurezza effettivamente configurati sul CCI dipende dalle politiche di sicurezza concordate tra le parti.

(244) Questa soluzione deriva da ragioni di stabilità nel tempo e completezza delle funzionalità di sicurezza offerte; si prevede che le future edizioni dello standard CEI EN IEC 62351-4 renderanno mandatoria l'opzione E2E mentre le attuali alternative potrebbero essere deprecate (vedi anche CEI EN IEC 62351-6:2020 – 5.2.1 e CEI EN IEC 62351-4:2018 – 7.1).

(245) Non si prevedono ragioni di retrocompatibilità che motiverebbero il supporto di chiavi crittografiche di dimensioni inferiori, ormai considerate non sufficientemente sicure.

(246) Non si prevedono ragioni di retrocompatibilità che motiverebbero il supporto di versioni precedenti di TLS, ormai considerate non sufficientemente sicure.

(247) Si prevede che le future edizioni degli standard di riferimento non indicheranno questa cypher suite.

(248) Il valore indicato deve essere considerato un valore minimo: si raccomanda di considerare valori anche superiori nell' ottica di una maggiore flessibilità e durabilità del dispositivo.

T.3.3.4.2 Sicurezza delle comunicazioni IEC 61850/GOOSE [Informativo]

La confidenzialità delle comunicazioni GOOSE non è resa obbligatoria da CEI EN IEC 62351-6 principalmente per soddisfare le esigenze di performance (in particolare latenza) di queste comunicazioni. Per garantire la massima flessibilità, lo standard consente la coesistenza di comunicazioni sicure e non sicure, in un'ottica di transizione verso livelli di sicurezza più elevati e di continuità operativa.

Anche quando la cifratura dei dati non è utilizzata, lo standard CEI EN IEC 62351-6 indica comunque soluzioni di sicurezza per garantire l'integrità e l'autenticazione delle comunicazioni; queste sono basate sull'estensione del formato delle Protocol Data Unit (PDU) scambiate, sull'utilizzo di funzioni di hash, message digest e crittografia a chiave pubblica.

Le PDU possono essere estese valorizzando opportunamente gli specifici campi Reserved1 e Reserved2 che andranno a contenere, rispettivamente, la lunghezza in ottetti dell'estensione contenente i parametri di sicurezza e una checksum calcolata sui contenuti della PDU estesa.

Per garantire l'autenticità dei contenuti della PDU viene utilizzato un Message Authentication Code (MAC) per il cui calcolo si utilizza il valore hash restituito dall'algoritmo HMAC-SHA256 o AES-GMAC sui contenuti della PDU estesa. In particolare, potranno essere considerati gli ottetti che vanno dall'Ethertype Identifier sino al termine della PDU. Il valore di hash può essere troncato a 128 o 256 bit.

Nella PDU estesa sono anche presenti i riferimenti temporali di validità della chiave corrente e della prossima chiave distribuita tramite il protocollo Group Key Management Protocol; conoscendo l'intervallo di validità di una chiave i riceventi possono premunirsi della successiva chiave che sarà resa disponibile per la distribuzione quando viene reso noto il momento della sua entrata in uso.

Alla ricezione di una PDU estesa contenente un MAC, il ricevente può verificare la correttezza del MAC prima di procedere ad ulteriore elaborazione dei contenuti della PDU.

I valori di Stnum e Sqnum delle PDU ricevute possono essere considerati al fine di identificare potenziali attacchi di tipo reply; anche nel caso l'arrivo di PDU con valori inferiori a quelli ricevuti possa essere motivato dall'utilizzo di comunicazioni multi-path, la PDU dovrebbe essere scartata come se fosse originata da un attacco di tipo reply.

T.3.3.4.3 Gestione dei ruoli nelle comunicazioni IEC 61850/MMS

Il server IEC 61850 del CCI viene predisposto per comunicare in modo differenziato con diversi attori opportunamente identificati, quali il DSO ed eventuali ulteriori operatori esterni abilitati al controllo da remoto, utilizzando i concetti di privilegi di accesso (Paragrafo T.3.3.1.4) e di ruolo. In particolare, per ogni ruolo abilitato, custom o standard, dev'essere configurato e verificato chi può assumere quel ruolo, definendo quali entità (DSO ed altri Attori) sono autorizzate a richiederlo. Nel caso vengano utilizzati i profili A e B, possono essere specificati, a tal fine, certificati individuali, o tutti quelli emessi da determinate CA. I dettagli relativi all'implementazione e gestione dei ruoli sono specificati dalla norma CEI EN IEC 62351-8 "Power systems management and associated information exchange - Data and communications security - Part 8: Role-based access control".

La CEI EN IEC 62351-8 definisce un insieme di sette ruoli mandatori che devono essere supportati e un insieme predefinito di privilegi ad essi associati.

Gli oggetti e le operazioni a cui si applicano i ruoli sono definiti dal modello dati utilizzato: per il CCI gli oggetti si mappano sui Data Object e le operazioni sui servizi IEC 61850 specificati nelle sezioni precedenti.

T.3.3.4.3.1 Definizione dei ruoli e privilegi

Il controllo degli accessi viene applicato sia per permettere che per proibire l'accesso ad un server ACSI attraverso un punto di accesso o, più puntualmente, ad ogni istanza della gerarchia logical-device, logical-node e data-object. L'assegnamento di un ruolo ad un determinato soggetto permetterà di ottenere risposte differenti ai servizi richiesti in base ai privilegi che sono stati assegnati a quel ruolo.

Nello specifico, considerando i servizi ACSI che devono essere implementati per la comunicazione con il CCI (Paragrafo T.3.2.2) sono necessari i seguenti privilegi derivati dallo standard:

- LISTOBJECTS: permette ad un soggetto/ruolo di effettuare la discovery di quali oggetti sono presenti all'interno del Logical Device attraverso il tipo e l'ID di questi oggetti. LISTOBJECTS includerà nella lista solo gli oggetti per i quali il soggeto/ruolo possiede il privilegio READVALUES;
- READVALUES: permette ad un soggetto/ruolo di ottenere alcuni o tutti i valori oltre al tipo e all'ID degli oggetti che afferiscono ad un Logical Device;
- CONTROL: permette ad un soggetto/ruolo di effettuare operazioni di controllo;
- CONFIG: permette al soggetto/ruolo di configurare localmente o da remoto tutti o alcuni oggetti che sono presenti nell'IED;
- DATASET: permette al soggetto/ruolo di avere accesso ai servizi dei dataset persistenti e non persistenti;
- REPORTING: permette al soggetto/ruolo di utilizzare sia il reporting bufferizzato e non bufferizzato relativo ai record control block di un nodo logico.

Nella Tabella 101 vengono indicati i privilegi per ciascun servizio ACSI con riferimento alle classi di servizi individuate come significative per l'implementazione del CCI.

Tabella 101 – Mapping dei privilegi sui servizi ACSI

Classe ACSI	Servizi ACSI	Privilegi
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

Lo standard CEI EN IEC 62351-8 prevede la possibilità di definire dei ruoli personalizzati per adattarsi al modello di sicurezza richiesto. Oltre ai ruoli mandatori definiti nello standard CEI EN IEC 62351-8, il CCI deve implementare i due ruoli personalizzati DSO_OPERATOR e AGGREGATOR_OPERATOR. In base alla loro definizione, il DSO avrà i privilegi di:

- "LISTOBJECTS",
- "READVALUES",
- "DATASET" con accesso in sola lettura,
- "REPORTING" con accesso in scrittura solo per report enable,
- "CONTROL" e "CONFIG" sui Data Object definiti nella Tabella 98 del Paragrafo T.3.3.1.4.

Analogamente l'Aggregatore avrà i seguenti privilegi (o equivalenti, vedi T.3.3.4.4.2):

- "LISTOBJECTS",
- "READVALUES",
- "DATASET" con accesso in sola lettura,
- "REPORTING" con accesso in scrittura solo per report enable,

"CONTROL" e "CONFIG" sui Data Object definiti nella Tabella 99 del Paragrafo T.3.3.1.4

La Tabella 102 riporta il mapping tra i ruoli identificati come rilevanti per l'operatività del CCI e i privilegi associati a ciascun ruolo.

Tabella 102 – Ruoli/Privilegi per il CCI

Value	Right Role	LISTOBJECTS	READVALUES	DATASET	REPORTING	FILERead	FILEWRITE	FILEMNGT	CONTROL	CONFIG	SETTING GROUP	SECURITY
-1	DSO_OPERATOR	X	X	C1	C2				C3	C3		
-2	AGGREGATOR_OPERATOR	X	X	C1	C2				C3	C3		

- C1= accesso in sola lettura al dataset
- C2= accesso in scrittura solo per report enable
- C3= accesso condizionato solamente a specifici Data Object descritti nelle tabelle del Paragrafo T.3.3.1.4

Lo scambio informativo necessario per l'assegnamento dei permessi ai ruoli del CCI deve essere descritto utilizzando XACML (eXtensible Access Control Markup Language) come definito dallo standard CEI EN IEC 62351-8. L'oggetto utilizzato per la definizione di un ruolo in formato XACML deve contenere i seguenti campi:

- RoleID: valore per l'identificazione del ruolo
- unique-ID:stringa random per garantire l'unicità all'interno del dominio del policy decision point (PDP)
- RoleName: contiene il nome del ruolo in forma leggibile
- roleDefinition: contiene un riferimento al documento che contiene la definizione del ruolo. Ad es. CEI EN IEC 62351-8
- revision: numero di revisione
- PermissionGroup: nome del gruppo contenente il set di permessi
- Permission: nome del permesso definito.

In particolare i nuovi ruoli sono definiti come segue:

- DSO_OPERATOR
  - Role-id: -1
  - Revision: 1.0
  - RoleDefinition: “CEI EN IEC 62351-8-CEI 0-16:2021”
- AGGREGATOR_OPERATOR
  - Role-id: -2
  - Revision: 1.0
  - RoleDefinition: “CEI EN IEC 62351-8-CEI016:2021”

T.3.3.4.3.2 Trasporto dei ruoli

Per il trasporto dei ruoli si utilizzano gli access tokens che possono avere diversi formati. Per il CCI si richiede il supporto al formato di access token specificato dal profilo A oppure dal profilo B nella CEI EN IEC 62351-8, inoltre si richiede opzionalmente il supporto ai profili C (webtoken basato su JSON) e D (token RADIUS).

Un access token deve contenere al minimo le informazioni contenute nella Tabella 103.

Tabella 103 – Campi mandatori dei access token [CEI EN 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

Inoltre in aggiunta ai campi precedenti, in riferimento ai profili A e B devono essere supportati anche i componenti in Tabella 104

Tabella 104 – Campi specifici per i profili A e B [CEI EN 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 Profilo A: estensione del certificato di identità a chiave pubblica ITU-T X.509

Il profilo A prevede che le informazioni relative al ruolo di ciascun attore autorizzato a comunicare con il CCI vengano fornite come estensioni del certificato di identità a chiave pubblica (X.509 ID certificate with extension). Il profilo A può essere utilizzato sia con i modelli PUSH che PULL. In particolare, è stata specificata l’estensione IECUserRoles extension, definita appositamente per i sistemi elettrici al fine di gestire correttamente il controllo degli accessi basato sui ruoli. La gestione dei certificati viene dettagliata nella CEI EN 62351-9, mentre la struttura degli access token per il profilo A viene dettagliata nella CEI EN IEC 62351-8.

L’access token viene identificato attraverso l’OID 1.0.62351.8.1.

Nel dettaglio un'estensione di certificato deve essere in accordo alla seguente definizione:

```
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
     }
```

Il valore OID è definito come segue:

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

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

Il valore per l'estensione è definito come segue:

```
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 Profilo B: certificato di attributo ITU-T X.509

Il profilo B prevede l'utilizzo di attribute certificate (AC) X.509 per il trasporto delle informazioni relative ai ruoli. L'utilizzo di questo profilo permette di avere una durata di validità del certificato più breve rispetto al certificato di identità a chiave pubblica X.509. Può essere utilizzato sia con il modello PUSH che PULL. La CEI EN IEC 62351-8 fornisce i dettagli sulla struttura e il formato dell'attribute certificate da utilizzare per questo profilo.

L'access token viene identificato attraverso l'OID 1.0.62351.8.1 e contiene diversi campi. I campi mandatori sono relativi al numero seriale di access token, il nome del soggetto proprietario del token, il ruolo assegnato, le informazioni riguardo l'emissione del token (soggetto emittente e relativo timestamp), validità del token e numero di revisione dell'assegnamento soggetto-a-ruolo. Inoltre, nell'access token è necessario indicare l'algoritmo di firma e la firma dell'istanza che l'ha emessa. L'estensione permette di assegnare più di un ruolo al medesimo soggetto.

L'object identifier per l'AttributeType è definito come il valore OID riportato nel profilo A. Il valore del campo AttributeValue è definito come l'estensione per il profilo A.

T.3.3.4.3.3 Mappatura con i sistemi di autorizzazione esistenti

La gestione dei ruoli prevede una relazione stretta con il sistema di autorizzazione implementato dall'organizzazione. Vengono infatti utilizzati ed estesi i meccanismi di autenticazione esistenti. In particolare, il profilo A è parte della PKI (Public Key Infrastructure) mentre il profilo B viene sviluppato per mezzo di una PMI (Privilege Management Infrastructure) interconnessa con la PKI come stabilito dallo standard ISO/IEC 9594-8. LA PMI fornisce il set completo di processi richiesti per la fornitura di un servizio di autorizzazione.

Nella tabella seguente viene rappresentato il mapping tra certificato di identità (ID certificate) e certificato di attributo (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 Algoritmi e chiavi per la gestione dei ruoli

In CEI EN IEC 62351-8 vengono inoltre indicati i requisiti minimi in termini di algoritmi e lunghezza delle chiavi utilizzate per la gestione dei ruoli. Viene raccomandato l'utilizzo di SHA-256 per le operazioni di hash. Per quanto riguarda le funzioni di firma si raccomanda RSA con chiave a 2048 bit. Inoltre, opzionalmente si possono utilizzare algoritmi basati su ECC con chiavi di 256 bit (con SHA-256). L'OID da utilizzare per ecdsa-with-SHA256 è: iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 2., allineato con quanto richiesto da CEI EN 62351-3.

T.3.3.4.3.5 Access token

Gli access token possono essere utilizzati a diversi livelli dello stack OSI. Generalmente ci si focalizza sul livello trasporto e applicazione, ma non sono escluse altre soluzioni. Per le comunicazioni MMS su TCP l'utilizzo degli access token può avvenire in due fasi:

- a livello trasporto, durante la creazione di una connessione sicura in accordo alla CEI EN 62351-3;
- a livello applicazione, durante il processo di autorizzazione che comprende l'assegnazione del token di accesso contenente il ruolo.

Le credenziali possono essere utilizzate con approccio orientato alla sessione o al singolo messaggio.

Un approccio basato su sessione assume che esista una comunicazione end-to-end tra due entità inizializzata facendo uso dell'autenticazione. Si prevede che tale autenticazione sia legata alle credenziali RBAC. Durante la fase di setup, è stabilita una chiave di sessione per proteggere crittograficamente la sessione di comunicazione e garantire l'autenticazione e l'autorizzazione. Una applicazione può riferirsi ai profili di sicurezza a livello applicativo descritti nell'CEI EN IEC 62351-4.

L'approccio basato su messaggi, invece, assume che le credenziali RBAC siano legate al contenuto del singolo messaggio. In diversi casi questo approccio è attuato per mezzo della firma digitale.

T.3.3.4.4 Sicurezza dei servizi di comunicazione con attori abilitati alla connessione remota diversi dal DSO

Secondo quanto previsto dall'Allegato O, il CCI dispone di un'interfaccia per l'accesso remoto da parte di tipologie di operatori diversi dal DSO, quali l'Utente e l'Aggregatore.

T.3.3.4.4.1 Utente

Al fine di abilitare le funzioni di monitoraggio, configurazione e manutenzione da parte dell'utenza autorizzata, il CCI ammette connessioni remote verso l'interfaccia per l'accesso remoto. Tali comunicazioni devono utilizzare protocolli standard dotati di servizi di sicurezza, atti a garantire confidenzialità, autenticità e integrità della sessione, quali ad esempio SSH o HTTPS. Si richiede l'utilizzo di credenziali crittografiche (e.g. certificati digitali) e si richiede di stabilire la mutua autenticazione delle parti in comunicazione.

Al fine di semplificare la gestione del dispositivo e permettere ai proprietari di impianto di definire una gerarchia di ruoli per la gestione in sicurezza del dispositivo, il CCI dovrà implementare un sistema di gestione dei permessi degli Utenti che permetta di operare una opportuna segregation of duty atta a limitare l'accesso a sottoinsiemi di funzioni e parametri del CCI, mediante l'attribuzione di ruoli specifici ai singoli Utenti (vedi sezione T.3.3.4.9.4).

T.3.3.4.4.2 Aggregatore

Per l'accesso remoto al CCI l'Aggregatore potrà utilizzare protocolli di comunicazione standard dotati di:

- un modello dati semantico documentato, in grado di garantire l'interoperabilità degli scambi informativi tra il CCI e i dispositivi client di Aggregatori diversi;
- funzioni di sicurezza end-to-end, in grado di garantire autenticazione, integrità e confidenzialità sull'intero percorso di comunicazione, dal nodo CCI al nodo dell'Aggregatore in qualunque tipo di architettura di rete utilizzata dall'organizzazione per l'implementazione delle comunicazioni su rete geografica;
- un sistema di gestione dei ruoli, che permetta di limitare l'accesso a sottoinsiemi di dati del CCI, mediante l'attribuzione di permessi definiti con la stessa granularità del sistema di controllo accessi specificato per il modello dati IEC 61850 del CCI (vedi sezione T.3.3.4.3).

T.3.3.4.5 Sincronizzazione temporale

Secondo quanto previsto dall' Allegato O (sezione O.13.1.5), la funzione di sincronizzazione temporale può essere svolta da un ricevitore GPS integrato nel CCI, oppure può essere fornita tramite un servizio di rete di comunicazione. Nel CCI tale funzione fornisce il riferimento per la marcatura temporale delle misure e dei segnali, per gli eventi del data logger e per la verifica della validità temporale dei certificati elettronici.

La marca temporale dovrà essere misurata con riferimento al tempo UTC (Coordinated Universal Time). Il valore della misura del tempo nell'unità di misura UTC coincide col valore espresso nell'unità tempo medio di Greenwich (Greenwich Mean Time o GMT), a meno di approssimazioni infinitesimali. L'incertezza del riferimento temporale non può essere superiore a +/- 100 ms.

Per soddisfare i requisiti di precisione richiesti alla funzione di sincronizzazione temporale del CCI, nel caso di sincronizzazione via rete di comunicazione si raccomanda l'utilizzo del protocollo NTP (Network Time Protocol).

NTP è un protocollo standard IETF client-server di livello applicativo, in ascolto sulla porta UDP 123. Il CCI è deputato a svolgere la funzione di client NTP attraverso una comunicazione unicast con server NTP che forniscono il riferimento temporale.

Per proteggere il CCI da attacchi cyber (ad esempio attacchi di spoofing dell'IP del server), il client CCI deve utilizzare la versione sicura NTS (Network Time Security) di NTP specificata dallo standard IETF RFC 8915 dotata di funzioni di autenticazione e integrità basate su TLS. Per l'implementazione del profilo TLS occorre fare riferimento al Paragrafo T.3.3.4.1.

Inoltre per proteggere il CCI da attacchi da parte di ticker falsi (cioè server che inviano riferimenti temporali scorretti), occorre utilizzare un'architettura ridondata di server NTP([249]).

T.3.3.4.6 Gestione dei log

Come specificato nell'Articolo O.14 "Data Logger" dell'Allegato O, il CCI deve essere dotato di funzioni di log degli eventi rilevanti per la verifica e il monitoraggio del suo stato di funzionamento e di sicurezza.

In questa sezione vengono fornite indicazioni circa la memorizzazione e la trasmissione dei log da parte del CCI. Inoltre, a titolo informativo, vengono dettagliati gli eventi rilevanti per la cybersecurity introdotti dalla IEC 62351-14 "Power systems management and associated information exchange - Data and communications security - Part 14: Cyber security event logging".

T.3.3.4.6.1 Memorizzazione e trasmissione dei log del CCI

La memorizzazione degli eventi nel CCI deve rispettare i requisiti specificati dallo standard IEEE 1686. Il CCI registrerà in un buffer circolare sequenziale (first in, first out) gli eventi di sicurezza nell'ordine in cui si verificano. Tale buffer circolare non potrà essere cancellato o modificato e dovrà memorizzare almeno 2048 eventi (IEEE 1686:2013) prima che il buffer circolare inizi a sovrascrivere l'evento più vecchio con l'evento più recente.

Per la trasmissione degli eventi di log dal CCI ad un server remoto (eventualmente integrato in un sistema per la collezione e il monitoraggio della sicurezza) si raccomanda l'utilizzo del protocollo Syslog in conformità agli standard IETF RFC 5424 e RFC 5425, i quali specificano il formato del protocollo e la sua cifratura con profilo TLS. Per l'implementazione del profilo TLS occorre fare riferimento al Paragrafo T.3.3.4.1

Nel caso in cui per la trasmissione dei messaggi in formato syslog RFC 5424 si volesse utilizzare il protocollo standard IETF SNMP (Simple Network Management Protocol)([250]), per effettuare la mappatura da Syslog a SNMP occorre utilizzare lo standard IETF RFC 5676.

Per le comunicazioni SNMP si raccomanda l'utilizzo della versione sicura SNMPv3 con profilo TSM (Transport Security Model, RFC 5591) basato su TLS (RFC 6353). Per l'implementazione del profilo TLS occorre fare riferimento al Paragrafo T.3.3.4.1.

T.3.3.4.6.2 Log sulla sicurezza del CCI [informativo]

Ogni evento viene caratterizzato da un identificativo mnemonico, un grado di severità e un testo descrittivo. Per il grado di severità di un evento di log vengono utilizzate quattro distinte categorie:

- alarm: attività di cybersecurity non autorizzata (vedi IEEE 1686 "IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities");
- error: condizione di errore;
- notice: attività di cybersecurity autorizzata, che si verifica, ad esempio, durante l'uso e la manutenzione di routine di un'entità (vedi IEEE 1686). Questo tipo di notifica è classificato come un evento di cybersecurity, ma non una violazione di sicurezza, o un attacco, o una deviazione dalle normali condizioni operative del CCI;
- warning: evento anormale, ovvero una deviazione dalle normali condizioni operative di un'entità, ma non necessariamente un attacco informatico. Ad esempio, se per l'handshake TLS viene utilizzata una versione TLS vulnerabile a problemi di cybersecurity, questo evento viene classificato come "warning". L'uso di una versione debole di TLS potrebbe essere imposto dalla politica di sicurezza locale dell'ambiente di destinazione.

(249) Un'architettura costituita da 4 server NTP protegge il client NTP da un singolo ticker falso. Detto n il numero di ticker falsi che si vuole tollerare, occorre ridondare l'architettura con un numero di server pari a 2n + 1.

(250) A tal proposito si segnala che lo standard CEI EN 62351-7 "Power systems management and associated information exchange – Data and communications security – Part 7: Network and System Management (NSM) data object models" specifica un insieme di oggetti rilevanti per la sicurezza del dispositvo e delle comunicazioni CCI mappati sul protocollo SNMP.

Nelle sezioni successive gli eventi di sicurezza vengono raggruppati in base alle funzioni di sicurezza del CCI descritte nelle sezioni precedenti, in particolare:

- eventi relativi alla sicurezza del sistema CCI;
- eventi relativi alla sicurezza del profilo TLS;
- eventi relativi alla sicurezza delle comunicazioni MMS;
- eventi relativi alla gestione dei certificati;
- eventi relativi alla gestione dei ruoli.

T.3.3.4.6.2.1 Log di sistema

Nel seguito vengono riportati gli eventi rilevanti per la sicurezza del sistema CCI.

Nome mnemonico	Severità	Testo
LOGIN_OK	notice	Log-in avvenuto con successo
LOGIN_OK_PW_EXPIRED	notice	Password scaduta, Log-in avvenuto con successo
LOGIN_FAIL_WRONG_CR	notice	Log-in fallito- Credenziali errate
LOGIN_FAIL_PW_EXPIRED	alarm	Log-in fallito- Password scaduta
LOGIN_FAIL_3_TIMES	alarm	Log-in fallito 3 volte
LOGIN_FAIL_SESSIONS_LIMIT	alarm	Log-in fallito per raggiunto limite di sessioni
LOCK_USER_WRONG_CR	alarm	Utente bloccato – credenziali errate
LOGOUT_USER	notice	Log-out utente
LOGOUT_TIMEOUT	notice	Log-out dovuta ad inattività dell'utente (timeout)by user inactivity (timeout)
VIEW_SEC_EV_LIST_OK	notice	Visualizzazione log di eventi di sicurezza avvenuta con successo
FILE_HASH_CHECK_FAIL	alarm	Controllo hash file fallito
FILE_DS_CHECK_FAIL	alarm	Controllo firma digitale fallito
WRITE_CERTS_FAIL	notice	Salvataggio e scrittura dei certificati nel componente fallita
SW_UPDATE_OK	notice	Software aggiornato con successo
SW_UPDATE_FAIL	alarm	Fallimento aggiornamento software
VIEW_SEC_EV_LIST_FAIL	notice	Visualizzazione dell'elenco degli eventi di sicurezza fallita
PW_RESET_FACTORY_DEF	alarm	Password resettata al valore di default
USER_ACCNT_CREATE_OK	notice	Account utente creato con successo
USER_ACCNT_ENABLE_OK	notice	Account utente abilitato con successo
USER_ACCNT_DISABLE_OK	notice	Account utente disabilitato con successo
USER_ACCNT_DEL_OK	notice	Account utente eliminato con successo
USER_ACCNT_CREATE_FAIL	notice	Creazione di un account utente fallita
USER_ACCNT_ENABLE_FAIL	notice	Abilitazione di un account utente fallita
USER_ACCNT_DISABLE_FAIL	notice	Disabilitazione di un account utente fallita

Nome mnemonico	Severità	Testo
USER_ACCNT_DEL_FAIL	notice	Eliminazione di un account utente fallita
USER_NEW_ROLE_OK	notice	Nuovo ruolo assegnato all'utente con successo
USER_PERMISSION_CHANGE_OK	notice	Permessi modificati con successo
USER_PERMISSION_ADDED_OK	notice	Permessi aggiunti con successo
USER_ROLE_REMOVED_OK	notice	Rimozione dell'assegnamento del ruolo all'utente avvenuta con successo
USER_PERMISSION_REMOVED_OK	notice	Permessi dell'utente rimossi con successo
NEW_ROLE_CREATE_OK	notice	Creazione nuovo ruolo avvenuta con successo
ROLE_DELETE_OK	notice	Ruolo eliminato con successo
USER_PW_CHANGE_OK	notice	Modifica password utente avvenuta con successo
USER_PW_CHANGE_FAIL	notice	Modifica password utente fallita
USER_NEW_ROLE_FAIL	notice	Fallimento nell'assegnamento nuovo ruolo utente
USER_PERMISSION_CHANGE_FAIL	notice	Fallimento nella modifica del permesso
USER_PERMISSION_ADDED_FAIL	notice	Fallimento aggiunta permesso
USER_PW_CHANGE_FAIL_SHORT	notice	Fallimento cambio password utente – troppo corta
USER_PW_CHANGE_FAIL_POLICY	notice	Modifica password utente fallita a causa delle policy
USER_SESSION_ROLE_CHANGE_OK	notice	Modifica ruolo sessione utente avvenuta con successo
USER_SESSION_ROLE_CHANGE_FAIL	notice	Fallimento cambiamento ruolo sessione utente
USER_ROLE_REMOVED_FAIL	notice	Fallimento rimozione assegnamento ruolo
USER_PERMISSION_REMOVED_FAIL	notice	Fallimento rimozione permesso utente
NEW_ROLE_CREATE_FAIL	notice	Fallimento creazione nuovo ruolo
ROLE_DELETED_FAIL	notice	Fallimento cancellazione ruolo
TCP_COMM_LOG_SUBS_FAIL	alarm	Comunicazione TCP con il sottoscrittore dei log di sicurezza fallita
LOG_DATA_HASH_FAIL	alarm	Controllo dell'hash dei dati di log fallito (dati di log alterati)
TCP_COMM_LOG_PUBL_FAIL	alarm	Comunicazione TCP con il publisher dei log di sicurezza fallita
TCP_COMM_LOG_SRV_FAIL	alarm	Comunicazioni TCP con il server dei log di sicurezza fallita (evento non inviato)
COMM_CS_NEGOTIATION_FAIL	alarm	Fallimento nella comunicazione – negoziazione della suite di cifratura fallita
COMM_KEY_NEGOTIATION_FAIL	alarm	Fallimento nella comunicazione – negoziazione della chiave fallita
COMM_PEER_AUTHENTICATION_FAIL	alarm	Fallimento nella comunicazione – autenticazione tra peer fallita

Nome mnemonico	Severità	Testo
COMM_PACKET_AUTHENTICATION_FAIL	alarm	Fallimento nella comunicazione – autenticazione del pacchetto fallita
TLS_CONN_OK	notice	TLS Connection successful
TLS_CERT_ACCEPTED_OK	notice	Connessione TLS/certificato accettato
TLS_CERT_CHECK_DIS_OK	notice	TLS certificate validation check disabled successfully
TLS_CONN_FAIL_CERT	alarm	Connessione TLS fallita – fallimento validazione del certificato
TLS_CONN_FAIL_IKE	alarm	Connessione TLS fallita – IKE fallito
TIME_SYNC_SRC_OK	notice	Sorgente per la sincronizzazione temporale OK
TIME_SYNC_SRC_FAIL	notice	Sorgente per la sincronizzazione temporale KO
AV_VIRUS_FOUND	alarm	Identificato codice malizioso o corrotto
NEW_CERT_GEN_OK	notice	Nuovo certificato generato correttamente
PKI_CSR_OK	alarm	CSR approvata e certificato emesso correttamente
PKI_CSR_FAIL	alarm	Richiesta firma del certificato fallita
PKI_CERT_EXP_NEAR	alarm	Certificato prossimo alla scadenza
X509_CERT_OK	alarm	Certificato validato con successo
X509_CERT_FAIL	alarm	Validazione del certificato fallita
X509_CERT_EXPIRED	alarm	Validazione del certificato fallita – certificato scaduto
X509_CERT_REVOKED	alarm	Validazione del certificato fallita – certificato revocato
X509_CERT_UNTRUSTED	alarm	Validazione del certificato fallita – controllo della firma del certificato fallita
CRL_TRANSFER_OK	notice	Trasferimento CRL nel componente avvenuto con successo
CRL_TRANSFER_FAIL	alarm	Fallimento nel trasferimento del CRL nel componente
CRL_NOT_AVAILABLE	alarm	Stato di revoca del certificato sconosciuto – CRL non disponibile
CRL_EXPIRED	alarm	CRL scaduta
OCSP_COMMUNICATION_FAIL	alarm	Fallimento nelle comunicazioni OCSP
OCSP_UNKNOWN_STATUS	alarm	OCPS: Stato di revoca del certificato sconosciuto
TRANSFER_CERTS_OK	notice	Certificato trasferito nel componente con successo
ADD_ENTITY_CERT_OK	alarm	Installazione del certificato nel componente avvenuta con successo
REMOVE_ENTITY_CERT_OK	alarm	Certificato rimosso dal componente con successo
ADD_TRUST_ANCHOR_CERT_OK	alarm	Trust anchor certificate installato con successo

Nome mnemonico	Severità	Testo
REMOVE_TRUST_ANCHOR_CERT_OK	alarm	Trust anchor certificate rimosso con successo
TRANSFER_CERTS_FAIL	notice	Fallimento nel trasferimento del certificato al componente
READ_CERTS_FAIL	notice	Lettura del certificato dal componente fallita
TRANSFER_PW_FILE_OK	notice	Trasferimento e salvataggio del file delle password avvenuto con successo
READ_PW_FILE_OK	notice	Lettura o esportazione del file delle password avvenuto con successo
TRANSFER_PW_FILE_FAIL	notice	Fallimento nel trasferimento del file delle password nel componente
READ_PW_FILE_FAIL	notice	Fallimento nella lettura del file delle password nel componente
UNKNOWN_SYSLOG_EV	notice	Evento Syslog non identificato

T.3.3.4.6.2.2 Log delle comunicazioni TLS

Di seguito si elencano gli eventi di log significativi relativi alla sicurezza del profilo TLS.

Nome mnemonico	Severità	Testo
TLS_WRONG_VERSION	alarm	Comunicazione non sicura
TLS_WEAK_VERSION	warning	Versione di TLS non sicura
TLS_VERSION_CHANGE	alarm	Individuato cambio di versione TLS
TLS_NO_RENEG	alarm	Intervallo di rinegoziazione scaduto
TLS_NO_ROOT_MATCH	alarm	Impossibile trovare il certificato della CA
TLS_CERT_SIZE_MISMATCH	alarm	Dimensione del certificato non supportata
TLS_NO_LOCAL_CERT	alarm	Certificato indisponibile
TLS_NO_CA_MATCH	alarm	Validazione del certificato: certificato della CA indisponibile
TLS_NO_IND_TRUST_MATCH	alarm	Validazione del certificato: certificato individuale indisponibile
TLS_NO_CRL	warning	CRL inaccessibile
TLS_NO_OCSP	warning	Risponditore OCSP inaccessibile
TLS_CRL_EXP	warning	Attenzione: CRL scaduta
TLS_OCSP_RES_EXP	warning	Risposta OCSP scaduta
TLS_SIG_ALG_MISMATCH	alarm	Validazione del certificato: la firma del certificato non può essere validata
TLS_CERT_VAL_ERR	alarm	Validazione del certificato: algoritmi non supportati
TLS_SHORT_KEY	alarm	Chiave di lunghezza insufficiente

T.3.3.4.6.2.3 Log delle comunicazioni MMS con profilo di sicurezza Applicativo

Di seguito si elencano gli eventi significativi relativi al profilo applicativo.

Nome mnemonico	Severità	Testo
SIGNATURE_ALGO_NOT_SUP_ASS_REQ	error	Una SecPDU di tipo HandshakeReq ha specificato algoritmi di firma digitale non supportati dal server
SIGNATURE_ALGO_MISMATCH_REQ	alarm	Una SecPDU di tipo HandshakeReq aveva un'incompatibilità negli algoritmi di cifratura per cui l'algoritmo protetto è differente da quello non protetto
INV_SIGNATURE_ASS_REQ	alarm	Una SecPDU di tipo HandshakeReq aveva una firma digitale non valida
PROTECTED_PROT_NOT_SUP_REQ	error	Una SecPDU di tipo HandshakeReq ha specificato un protocollo protetto non valido
PROTOCOL_ERR_ASS_REQ	error	Una SecPDU di tipo HandshakeReq aveva un errore di protocollo nell'informazione di controllo del protocollo di sicurezza E2E
ADDR_MISMATCH_ASS_REQ	alarm	Una SecPDU di tipo HandshakeReq aveva un'incompatibilità di indirizzo
UNEXP_VERSION_ASS_REQ	error	Una SecPDU di tipo HandshakeReq aveva specificato una versione inattesa
INV_TIME_ASS_REQ	error	Una SecPDU di tipo HandshakeReq aveva un valore temporale non valido
REPLAY_DETEC_ASS_REQ	alarm	Una SecPDU di tipo HandshakeReq era una ritrasmissione
UNSUP_DH_GROUP_ASS_REQ	error	Una SecPDU di tipo HandshakeReq ha specificato un gruppo DH non supportato
HMAC_ALGO_NOT_SUP_ASS_REQ	error	Una SecPDU di tipo HandshakeReq ha specificato un algoritmo HMAC non supportato
AEAD_NOT_SUP_ASS_REQ	error	Una SecPDU di tipo HandshakeReq ha selezionato la crittografia con autenticazione con informazioni associate, che non è supportata dal server
AEAD_WHEN_NO_ENCR_ASS_REQ	error	Una SecPDU di tipo HandshakeReq HandshakeReq ha selezionato la crittografia con autenticazione con informazioni associate quando la crittografia non è richiesta
AE_ALGO_NOT_SUP_ASS_REQ	error	Una SecPDU di tipo HandshakeReq HandshakeReq ha selezionato la crittografia con autenticazione con informazioni associate ma l'algoritmo(i) non è supportato
AE_IS_REQUIRED_ASS_REQ	error	Una SecPDU di tipo HandshakeReq HandshakeReq non ha selezionato la crittografia con autenticazione con informazioni associate ma è richiesto dal server
ENCR_NOT_REQ_ASS_REQ	error	Una SecPDU di tipo HandshakeReq non ha selezionato la crittografia con autenticazione con informazioni associate ma ha selezionato la crittografia, quando il server non vuole o non supporta la crittografia
ENCR_ALGO_NOT_SUP_ASS_REQ	error	Una SecPDU di tipo HandshakeReq ha specificato un algoritmo(i) a chiave simmetrica non supportati dal server

Nome mnemonico	Severità	Testo
ICV_ALGO_NOT_SUP_ASS_REQ	error	Una SecPDU di tipo `HandshakeReq` ha specificato un (degli) algoritmo(i) ICV non supportato(i) dal server
ENCR_NOT_REQUIRED_REQ	error	Una SecPDU di tipo HandshakeReq con il componente confidentiality di tipo Confidentiality richiede la crittografia quando il server non la accetta
ENCR_IS_REQUIRED_REQ	error	Una SecPDU di tipo HandshakeReq con il componente confidentiality di tipo Confidentiality non propone la crittografia quando il server la richiede
PROTOCOL_ERR_ASS_ACC	error	Una SecPDU di tipo HandshakeAcc ha prodotto un errore di protocollo nell'informazione di controllo del protocollo di sicurezza E2E
SIGNATURE_ALGO_MISMATCH_ACC	alarm	Una SecPDU di tipo HandshakeAcc aveva un'incompatibilità nell'algoritmo di firma digitale dove l'algoritmo protetto è differente da quello non protetto
SIGNATURE_ALGO_NOT_SUP_ASS_ACC	error	L'algoritmo(i) in una SecPDU di tipo HandshakeAcc SecPDU ricevuta non è supportato
INV_SIGNATURE_ASS_ACC	alarm	Firma digitale non valida in una SecPDU HandshakeAcc ricevuta
ADDR_MISMATCH_ASS_ACC	alarm	Una SecPDU di tipo HandshakeAcc aveva un'incompatibilità di indirizzo
UNEXP_VERSION_ASS_ACC	error	Una SecPDU di tipo HandshakeAcc aveva una versione specificata inattesa
INV_TIME_ASS_ACC	error	Una SecPDU di tipo HandshakeAcc aveva un valore temporale non valido
REPLAY_DETEC_ASS_ACC	alarm	Una SecPDU di tipo HandshakeAcc era una ritrasmissione
INV_DH_GROUP_ASS_ACC	error	Una SecPDU di tipo HandshakeAcc aveva un valore di gruppo DH non valido
INV_AE_ALGO_ASS_ACC	error	Una SecPDU di tipo HandshakeAcc ha specificato la crittografia autenticata con l'algoritmo dati specificato non tra quelli specificati nella corrispondente SecPDU HandshakeReq
SINGLE_AE_ALGO_REQ_ASS_ACC	error	Una SecPDU di tipo HandshakeAcc ha specificato algoritmi multipli di crittografia autenticata o non ne ha specificato alcuno, quando ne è richiesto uno solo
AEAD_NOT_USED_ASS_ACC	error	Una SecPDU di tipo HandshakeAcc ha selezionato l'alternativa aea della componente enc-mode, mentre la corrispondente SecPDU HandshakeReq SecPDU ha selezionato l'alternativa non-aea
INV_ENCR_ALGO_ASS_ACC	error	Una SecPDU di tipo HandshakeAcc ha specificato un algoritmo a chiave simmetrica non elencato nella corrispondente SecPDU di tipo HandshakeReq
SINGLE_ENCR_ALGO_ASS_ACC	error	Una SecPDU di tipo HandshakeAcc ha specificato una sequenza vuota oppure algoritmi a chiave simmetrica multipli
INV_ICV_ALGO_ASS_ACC	error	Una SecPDU di tipo HandshakeAcc ha specificato un algoritmo ICV non elencato nella corrispondente SecPDU di tipo HandshakeReq

Nome mnemonico	Severità	Testo
SINGLE_AE_ALGO_ASS_ACC	error	Una SecPDU di tipo HandshakeAcc ha specificato una sequenza vuota oppure algoritmi ICV multipli
ENCR_NOT_REQUIRED_ACC	error	Una SecPDU di tipo HandshakeAcc con il componente confidentiality di tipo Confidentiality richiede la crittografia quando la corrispondente SecPDU HandshakeReq non la propone
ENCR_IS_REQUIRED_ACC	error	Una SecPDU di tipo HandshakeAcc con il componente confidentiality di tipo Confidentiality non propone la crittografia quando la corrispondente SecPDU HandshakeReq la richiede
ALARM_SEC_HANDSHAKE_REJECT_RCV	alarm	A HandshakeSecReject SecPDU è stata ricevuta senza la componete diag, a indicazione che il server non ha accettato la HandshakeReq SecPDU e ha generato un allarme
SIGNATURE_ALGO_NOT_SUP_REQ_REJ	error	Una SecPDU di tipo HandshakeSecReject è stata ricevuta con il codice diagnostico invalid-signatureAlgorithm
PROTECTED_PROT_NOT_SUP_REJ	error	Una SecPDU di tipo HandshakeSecReject è stata ricevuta con il codice diagnostico protected-protocol-not-supported
PROTOCOL_ERR_ASS_REJ	error	Una SecPDU di tipo HandshakeSecReject è stata ricevuta con codice diagnostico protocol-error
UNEXP_VERSION_ASS_REQ_REJ	error	Una SecPDU di tipo HandshakeSecReject è stata ricevuta con codice diagnostico unexpected-version
INV_TIME_ASS_REJ	error	Una SecPDU di tipo HandshakeSecReject è stata ricevuta con codice diagnostico invalid-time-value
UNSUP_DH_GROUP_ASS_REJ	error	Una SecPDU di tipo HandshakeSecReject è stata ricevuta con codice diagnostico dhGroup-not-supported
HMAC_ALGO_NOT_SUP_ASS_REJ	error	Una SecPDU di tipo HandshakeSecReject è stata ricevuta con codice diagnostico hmac-algorithm-not-supported
AEAD_NOT_SUP_ASS_REJ	error	Una SecPDU di tipo HandshakeSecReject è stata ricevuta con codice diagnostico encr-mode-aea-not-supported
AEAD_WHEN_NO_ENCR_ASS_REJ	error	Una SecPDU di tipo HandshakeSecReject è stata ricevuta con codice diagnostico aea-select-but-encrypt-not-supp
AE_ALGO_NOT_SUP_ASS_REJ	error	Una SecPDU di tipo HandshakeSecReject è stata ricevuta con codice diagnostico aea-algorithms-not-supported
AE_IS_REQUIRED_ASS_REJ	error	Una SecPDU di tipo HandshakeSecReject è stata ricevuta con codice diagnostico aea-is-required
ENCR_NOT_REQ_ASS_REJ	error	Una SecPDU di tipo HandshakeSecReject è stata ricevuta con codice diagnostico encryption-not-required
ENCR_ALGO_NOT_SUP_ASS_REJ	error	Una SecPDU di tipo HandshakeSecReject è stata ricevuta con codice diagnostico encrypt-algorithms-not-supported.
ICV_ALGO_NOT_SUP_ASS_REJ	error	Una SecPDU di tipo HandshakeSecReject è stata ricevuta con codice diagnostico icv-algorithms-not-supported
ENCR_NOT_REQUIRED_REJ	error	Una SecPDU di tipo HandshakeSecReject è stata ricevuta con codice diagnostico encryption-not-required

Nome mnemonico	Severità	Testo
ENCR_IS_REQUIRED_REJ	error	Una SecPDU di tipo HandshakeSecReject è stata ricevuta con codice diagnostico encryption-is-required
ALARM_HANDSHAKE_SEC_ABORT	alarm	Una SecPDU di tipo HandshakeSecAbort è stata ricevuta senza la componente diag a indicazione che il client non ha accettati la SecPDU HandshakeAcc e ha emesso un allarme
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	Una SecPDU di tipo HandshakeSecAbort è stata ricevuta con codice diagnostico protocol-error
UNEXP_VERSION_ASS_ACC_ABT	error	Una SecPDU di tipo HandshakeSecAbort è stata ricevuta con codice diagnostico unexpected-version
INV_TIME_ASS_ABT	error	Una SecPDU di tipo HandshakeSecAbort è stata ricevuta con codice diagnostico invalid-time-value
INV_DH_GROUP_ASS_ABT	error	Una SecPDU di tipo HandshakeSecAbort è stata ricevuta con codice diagnostico illegal-dhGroup-selected
INV_AE_ALGO_ASS_ABT	error	Una SecPDU di tipo HandshakeSecAbort è stata ricevuta con codice diagnostico invalid-ae-algorithm
SINGLE_AE_ALGO_REQ_ASS_ABT	error	Una SecPDU di tipo HandshakeSecAbort è stata ricevuta con codice diagnostico single-ae-algorithm-required
AEAD_NOT_USED_ASS_ABT	error	Una SecPDU di tipo HandshakeSecAbort è stata ricevuta con codice diagnostico ae-not-used.
INV_ENCR_ALGO_ASS_ABT	error	Una SecPDU di tipo HandshakeSecAbort è stata ricevuta con codice diagnostico invalid-encryption-algorithm.
SINGLE_ENCR_ALGO_ASS_ABT	error	Una SecPDU di tipo HandshakeSecAbort è stata ricevuta con codice diagnostico single-encrypt-algo-required
INV_ICV_ALGO_ASS_ABT	error	Una SecPDU di tipo HandshakeSecAbort è stata ricevuta con codice diagnostico invalid-icv-algorithm
SINGLE_AE_ALGO_ASS_ABT	error	Una SecPDU di tipo HandshakeSecAbort è stata ricevuta con codice diagnostico single-icv-algo-required.
ENCR_NOT_REQUIRED_ABT	error	Una SecPDU di tipo HandshakeSecAbort è stata ricevuta con codice diagnostico encryption-not-required.
ENCR_IS_REQUIRED_ABT	error	Una SecPDU di tipo HandshakeSecAbort è stata ricevuta con codice diagnostico encryption-not-required
ALARM_DATATRF_SEC_ABORT	alarm	Una SecPDU di tipo DtSecAbort è stata ricevuta senza codice diagnostico
DATA_PROT_ERROR_ABT	error	Una SecPDU di tipo DtSecAbort è stata ricevuta con codice diagnostico protocol-error
ENCR_NOT_SEL_ABT	error	Una SecPDU di tipo DtSecAbort è stata ricevuta con codice diagnostico encryption-not-selected
ENCR_WAS_SEL_ABT	error	Una SecPDU di tipo DtSecAbort è stata ricevuta con codice diagnostico encryption-required
DATA_INV_TIME_ABT	error	Una SecPDU di tipo DtSecAbort è stata ricevuta con codice diagnostico invalid-time-value

Nome mnemonico	Severità	Testo
INV_SEQ_NR_ABT	error	Una SecPDU di tipo DtSecAbort è stata ricevuta con codice diagnostico invalid-sequence-number
UNEXP_RE_KEY_ABT	error	Una SecPDU di tipo DtSecAbort è stata ricevuta con codice diagnostico unexpected-rekey-req
UNEXP_CHG_KEYS_ABT	error	Una SecPDU di tipo DtSecAbort è stata ricevuta con codice diagnostico unexpected-changedKeys
CLEAR_DATA_PROT_ERROR_TRF	error	Una SecPDU di tipo ClearTransfer SecPDU aveva un errore di protocollo
ENCR_WAS_SEL_TRF	error	Una SecPDU di tipo ClearTansfer SecPDU è stata ricevuta quando la crittografia era stata richiesta in fase di associazione
CLEAR_INV_ICV_ALG_TRF	alarm	Una SecPDU di tipo ClearTransfer SecPDU ricevuta utilizzava un algoritmo ICV non concordato in fase di creazione dell'associazione
CLEAR_GMAC_NONCE_REQ	Error	Una SecPDU di tipo ClearTransfer SecPDU è stata ricevuta senza GMAC nonce quando nonce è richiesto
CLEAR_BAD_ICV	alarm	Una SecPDU di tipo ClearTransfer SecPDU ricevuta aveva un ICV che non verifica
CLEAR_DATA_INV_TIME_TRF	error	Una SecPDU di tipo ClearTransfer SecPDU ricevuta aveva una marcatura temporale non valida
CLEAR_DATA_REPLAY_DETECTED	alarm	Una SecPDU di tipo ClearTransfer SecPDU ricevuta sembra essere una ritrasmissione
CLEAR_INV_SEQ_NR_TRF	error	Una SecPDU di tipo ClearTransfer SecPDU ricevuta aveva una marcatura temporale non valida
CLEAR_UNEXP_RE_KEY_REQ	error	Una SecPDU di tipo ClearTransfer SecPDU ricevuta dal server aveva una richiesta inattesa di cambio chiave
CLEAR_UNEXP_CHG_KEYS_IND	error	Una SecPDU di tipo ClearTransfer SecPDU ricevuta dal client aveva un cambio chiave inatteso indicato
ENCR_DATA_PROT_ERROR_TRF	error	Una SecPDU di tipo ClearTransfer SecPDU ricevuta aveva un errore di protocollo.
ENCR_NOT_SEL_TRF	error	Una SecPDU di tipo EncrTansfer SecPDU è stata ricevuta quando la crittografia non era stata richiesta in fase di associazione
ENCR_INV_ICV_ALG_TRF	alarm	Una SecPDU di tipo EncrTansfer SecPDU è stata ricevuta con un algoritmo ICV non concordato in fase di associazione
ENCR_GMAC_NONCE_REQ	Error	Una SecPDU di tipo EncrTansfer SecPDU è stata ricevuta senza GMAC nonce quando nonce è richiesto
ENCR_BAD_ICV	alarm	Una SecPDU di tipo **EncrTansfer** SecPDU ricevuta aveva un ICV che non verifica
ENCR_DATA_INV_TIME_TRF	error	Una SecPDU di tipo **EncrTansfer** SecPDU ricevuta aveva una marcatura temporale non valida
ENCR_DATA_REPLAY_DETECTED	alarm	Una SecPDU di tipo **EncrTansfer** SecPDU ricevuta sembra essere una ritrasmissione
ENCR_INV_SEQ_NR_TRF	error	Una SecPDU di tipo **EncrTansfer** SecPDU ricevuta aveva una marcatura temporale non valida

Nome mnemonico	Severità	Testo
AES_IV_REQ	error	Una SecPDU di tipo EncrTansfer SecPDU ricevuta non include il vettore di inizializzazione AES
ENCR_UNEXP_RE_KEY_REQ	error	Una SecPDU di tipo EncrTansfer SecPDU ricevuta dal server aveva un cambio chiave inatteso indicato
ENCR_UNEXP_CHG_KEYS_IND	error	Una SecPDU di tipo EncrTansfer SecPDU ricevuta dal client aveva l'indicazione di un cambio chiave inatteso
TRUST_ANCHOR_NOT SUPPORTED	error	Una SecPDU di tipo EncrTansfer SecPDU include un percorso di certificazione che origina da un trust anchor non riconosciuto dal ricevente
BAD_PKC_CHAINING	error	Una SecPDU include un percorso di certificazione non concatenato correttamente
INVALID_SIGNATURE_ON_PKC	alarm	Una SecPDU di tipo EncrTansfer SecPDU include un percorso di certificazione dove una o più chiavi pubbliche non verifica
PKC_WITH_NOT_VALID_BEFORE_ERROR	error	Una SecPDU di tipo EncrTansfer SecPDU include un percorso di certificazione dove una o più certificati digitali ha un valore notBefore nel futuro
EXPIRRED_PKC	error	Una SecPDU di tipo EncrTansfer SecPDU include un percorso di certificazione dove una o più certificati digitali è scaduto
PKC_RPESENT_MORE_THAN_ONCE	error	Una SecPDU di tipo EncrTansfer SecPDU include un percorso di certificazione dove uno o più certificati è ripetuto
OSI_ENV_PROT_ERR	error	Errore di protocollo di ambiente operativo OSI
OSI_INV_INDR_REF	error	Riferimento indiretto non valido nell'ambiente operativo OSI
OSI_INV_PCI	error	Sicurezza PCI non valida

T.3.3.4.6.2.4 Log relativi certificati

IEC 62351-14 riporta come significativi i seguenti eventi di log relativi alla gestione dei certificati.

Nome mnemonico	Severità	Testo
CERT_PROFILE_MISMATCH	warning	Incompatibilità del profilo del certificato
CERT_ALG_MISMATCH	alarm	Incompatibilità di algoritmo, risultato: verifica fallita
CERT_FORM_MISMATCH	warning	Incompatibilità di formato, risultato: verifica fallita
CERT_PKCS12_MISMATCH	warning	Incompatibilità di formato obbligatorio (PKCS #12)
CERT_PKCS8_MISMATCH	warning	Incompatibilità di formato obbligatorio (PEM., PKCS#8)
CERT_OID_ERROR_AVL_EXT	warning	Errori di OID nell'uso di Estensioni della Certificate Authorization List (incompatibilità di avl62351Extention)
CERT_OID_ERROR_AVL_ENTRY	warning	Errori di OID nell'uso di Estensioni della Certificate Authorization List Entry (incompatibilità di avl62351EntryExt)

Nome mnemonico	Severità	Testo
CERT_OID_ERROR_AVL_PROTID	warning	Errori di OID nell'uso di Identificatori della della Certificate Authorization List Protocol
CERT_OID_ERROR_AVL_EXT	warning	Errori di OID nell'uso di Estensioni della Certificate Authorization List (incompatibilità di avl62351Extention)
NO_LOCAL_CERT	notice (results in inability to communicate securely)	Le parti della comunicazione devono avere almeno una coppia di chiavi pubblica/privata.
CERTREG_MISSING_CN	warning	Dati di registrazione insufficienti. Assenza di CN
CERTREG_MISSING_OTP	warning	Dati di registrazione insufficienti. OTP indisponibile
CERTREG_MISSING_PRE_CERT	warning	Dati di registrazione insufficienti. Credenziali preesistenti indisponibili
CERTREG_MISSING_DN	warning	Dati di registrazione insufficienti. Assenza di DN per la generazione di CSR
CERT_MISSING_RCERT	notice	Dati insufficienti. Assenza de certificati accettabili di root CA
CERT_NO_CA	warning	Mancanza di informazioni circa l'indirizzo della CA per l'arruolamento.
CERT_NO_REG_INFO	warning	Assenza delle informazioni di registrazione sulla entità da arruolare
CERT_POP_ERROR	error	Errore nella prova di possesso (Impossibile validare la CSR)
CERT_POI_ERROR	error	Errore nella prova di identità (Errore di OTP o del certificato del costruttore del device)
CERT_SCEP_PROT_ERROR	error	Errori relativi a SCEP
CERT_EST_PROT_ERROR	error	Errori relativi a EST
CERT_EST_TA-UPDATE_ERROR	error	Errori relativi a EST durante l'aggiornamento dei certificati CA (utilizzando l'aggiornamento della Root CA key).
CERT_TAMP_ERROR	error	Errori relativi a TAMP
CERT_VAL_EXPIRED	alarm	Certificato scaduto
CERT_VAL_SIG_ERROR	alarm	Fallimento nalle verifica della firma della CA
CERT_VAL_REVOKED	alarm	Certificato revocato
CERT_VAL_NO_AVL_MATCH	warning	Certificato non contenuto in CertAVL
AVL_VAL_SIG_ERROR	alarm	Errore nella verifica della firma di CertAVL
AVL_VAL_COMP_ERROR	warning	Fallimenti in componenti di CertAVL
AVL_VAL_EMPTY_LST	notice	Fornita una lista vuota

T.3.3.4.6.2.5 Log relativi ai ruoli

Per gli aspetti di sicurezza sono rilevanti i seguenti log relativi alla gestione dei ruoli.

Nome mnemonico	Severità	Testo
RBAC_USR_AUTH_AUTHZ_SUCCESS	Notice	L'autenticazione utente e associazione sul server è avvenuta con successo
RBAC_PERM_ASSIGN_SUCCESS	Notice	L'aggiornamento dell'assegnamento dei permessi è avvenuto con successo
RBAC_NO_REPO_CONN_PKI_REV	warning	Il repository delle revoche non risulta non disponibile
RBAC_NO_CRED	warning	Credenziali RBAC non fornite (es. Estensione del certificato mancante)
RBAC_INVALID_TOKEN	alarm	L'autenticazione del soggetto non è andata a buon fine
RBAC_TOKEN_VALIDITY_ERROR	alarm	La validità dell'access token non può essere verificata
RBAC_TOKEN_VERIFICATION_FAILED	alarm	L'autenticazione tramite l'access token non è andata a buon fine
RBAC_TOKEN_ROLEID_UNKNOWN	alarm	Il valore di RoleID risulta sconosciuto
RBAC_TOKEN_ROLEDEF_UNKNOWN	warning	La definizione del ruolo risulta sconosciuta
RBAC_TOKEN_AOR_UNKNOWN	warning	L'AoR non può essere risolto
RBAC_TOKEN_REV_MISMATCH	warning	Non compatibilità nel numero di revisione del token
RBAC_TOKEN_ALG_MISMATCH	alarm	Non compatibilità dell'algoritmo crittografico
RBAC_TOKEN_NO REVOCATION	warning	Le informazioni di revoca non risultano disponibili
RBAC_TOKEN_NO REVOCATION_EXP	warning	Informazioni di revoca scadute
RBAC_ATTRIB_INVALID	alarm	Il periodo di validità del token RBAC risulta fuori dalla validità delle credenziali
RBAC_ATTRIB_NO_MATCH_BASE_CRED	warning	Corrispondenza mancante delle credenziali per il token RBAC
RBAC_ATTRIB_NO_REV_INFO	warning	Le informazioni di revoca non risultano disponibili

T.3.3.4.7 Gestione e monitoraggio degli asset

Come indicato nel Paragrafo O.13.7.2 "Asset Inventory" dell'Allegato O il CCI deve essere predisposto per interfacciarsi ad un'infrastruttura di asset inventory.

A tale scopo il CCI deve poter essere configurato al fine di rendere disponibile un elenco aggiornato dei campi utili alla sua identificazione univoca.

Secondo quanto specificato nel Paragrafo T.3.3.1.1.2 il CCI è identificato dal nodo logico LPHD, ed in particolare dal Data Object PhyNam che include informazioni relative al costruttore, alla versione del software e all'identificativo del punto di connessione(1*).

T.3.3.4.8 Secure Boot e Aggiornamento firmware

Al fine di prevenire la contraffazione, garantire l'integrità del dispositivo e ridurre al minimo il rischio di eseguire codice non autorizzato al momento dell'avvio è necessario eseguire una sequenza di avvio affidabile (trusted secure boot), ovvero una sequenza di avvio (boot sequence) a fasi, in cui viene verificata la validità di ogni fase prima dell'installazione e successiva inizializzazione del firmware, che è generalmente archiviato nella memoria flash riprogrammabile del CCI. Come indicato nell' Allegato O, per ragioni di sicurezza l'aggiornamento del firmware del CCI è a carico dell'Utente e deve avvenire solo a valle di una procedura che prevede:

i. Il controllo delle credenziali e delle autorizzazioni dell'Utente che attiva la procedura di aggiornamento;

ii. La verifica della piena integrità ed autenticità del nuovo firmware tramite la verifica della firma digitale dello stesso, basata su certificato del costruttore dell'apparato;

iii. La disattivazione delle funzionalità del CCI in modo controllato;

iv. Registrazione dell'attività di aggiornamento firmware nel Data logger di sistema. Nessuna fase della procedura deve cancellare i dati presenti nel suddetto Data logger.

T.3.3.4.9 Gestione delle chiavi e dei certificati: l'infrastruttura a chiave pubblica (PKI)

Le funzioni crittografiche necessarie a mettere in sicurezza le operazioni del dispositivo CCI, richiedono che quest'ultimo sia dotato di almeno una coppia di chiavi asimmetriche correlate, note come chiave privata (Private Key) e chiave pubblica (Public Key) opportunamente memorizzate su di un supporto di memoria adeguato (vd. Allegato O.15.3 – Prove relative alla Cybersecurity Hardware).

Si considerano due scenari:

- il CCI genera le proprie coppie di chiavi crittografiche asimmetriche;
- il CCI conserva coppie di chiavi crittografiche asimmetriche generate esternamente da una fonte attendibile, distribuite e installate in modo sicuro in un luogo protetto.

Quest'ultimo approccio deve essere utilizzato se il dispositivo non è in grado di supportare una delle componenti critiche nella generazione delle chiavi, ovvero il generatore randomico di numeri casuali (RNG) (vd. Allegato B – CEI EN 62351-9).

Il CCI deve generare o ricevere nuove coppie di chiavi, al verificarsi di una delle seguenti condizioni:

- Nessuna coppia di chiavi è presente al momento dell'avvio;
- Modifica del controllo del dispositivo (modifica della proprietà, autorità di controllo e/o riconfigurazione del dispositivo);
- Comando di un'entità autorizzata (ad es. richiesta di rinnovo del certificato, richiesta certificato di servizio);
- La chiave privata del dispositivo è stata compromessa.

(*) Al fine di dotare l'infrastruttura di gestione degli asset di funzionalità di monitoraggio, lo standard CEI EN 62351-7 "Power systems management and associated information exchange - Data and communications security - Part 7: Network and System Management (NSM) data object models" fornisce ulteriori Data Objects sullo stato di funzionamento e di sicurezza di un dispositivo e. la mappatura di tali Data Object astratti sulla struttura dei MIB del protocollo SNMP. Il rapporto tecnico IEC 62351-90-3 "Power systems management and associated information exchange - Data and communications security - Part 90-3: Guidelines for network and system management" fornisce informazioni utili in merito all'utilizzo dei Data Objects di monitoraggio.

È necessaria una infrastruttura che garantisca la corretta gestione di tutte le chiavi crittografiche e dei metadati necessari a:

- Identificare ed autenticare il dispositivo;
- abilitare i profili di comunicazione sicura del CCI (es. sessioni TLS);
- abilitare i processi di aggiornamento sicuro del dispositivo (vedi T.3.3.4.8).

L'infrastruttura preposta a gestire il ciclo vita delle chiavi crittografiche e dei certificati digitali ad esse associati è la PKI, o infrastruttura a chiave pubblica. Si rimanda allo standard CEI EN 62351-9 per le puntuali indicazioni sulle caratteristiche e le componenti di tale infrastruttura.

T.3.3.4.9.1 Privilege Management Infrastructure - (PMI)

Ad integrazione dei servizi espletati dalla PKI e a supporto del profilo B (vedi. T.3.3.4.3.2.2) si dettaglia un'estensione dell'infrastruttura a chiave pubblica preposta alla gestione dei certificati di attributo. Tale estensione è chiamata PMI o Privilege Management Infrastructure. Si rimanda allo standard CEI EN 62351-9, allo standard CEI EN IEC 62351-8 e dalla ISO 9594-8/ITU-T Rec. X.509 per le puntuali indicazioni sulle caratteristiche e le componenti di tale estensione.

Di seguito sono specificate, in breve, le modalità di distribuzione dei Certificati di Attributo che devono essere supportate da parte del dispositivo e da parte dell'infrastruttura di privilege management al fine di abilitare un corretto accesso alle risorse del dispositivo da parte di un utente autorizzato:

- **Modello PUSH:** I Certificati di Attributo sono inviati dagli utenti ai dispositivi come parte del protocollo dell'applicazione che utilizza i certificati di attributo per l'autorizzazione.
- **Modello PULL:** I Certificati di Attributo degli utenti sono archiviati in un repository e recuperati dai dispositivi quando necessario.

In generale, il modello "PUSH" richiede modifiche nei protocolli dell'applicazione, ma è più efficiente, poiché non è necessaria un'ulteriore richiesta da parte del dispositivo per recuperare il certificato d'attributo dalla repository.

Al fine di garantire il massimo grado di interoperabilità si richiede il supporto di entrambe le modalità di recupero dei token autorizzativi. Inoltre, al fine di evitare potenziali attacchi di tipo replay ed in accordo con lo standard CEI EN 62351-9 si raccomanda di utilizzare Certificati di Attributo a breve durata (es. al di sotto delle 24h).

T.3.3.4.9.2 Procedure della PKI

La PKI è di supporto alla gestione dell'intero ciclo di vita delle chiavi, descrivendone le politiche di sicurezza nei vari momenti: dalla creazione all'attivazione, dall'immagazzinamento al trasporto e, infine, alla revoca.

Le principali procedure legate alla gestione delle chiavi e dei certificati ad esse associati sono descritte dallo standard CEI EN 62351-9 e possono essere riassunte come segue:

- **Registrazione del dispositivo**: configurazione delle informazioni identificative e delle credenziali finalizzate alla registrazione del dispositivo nei confronti della Registration Authority (RA) del dominio operativo.
- **Configurazione del dispositivo:** configurazione dei parametri necessari a permettere il corretto interfacciamento del dispositivo nei confronti della PKI del dominio operativo.
- **Arruolamento del CCI nell'infrastruttura PKI**: previo utilizzo delle credenziali specificate al momento della registrazione, arruolamento (enroll) del CCI nei confronti della PKI che emette il certificato atto ad abilitare le funzioni crittografiche del dispositivo.

- **Rinnovo del Certificato**: a cadenza temporale prestabilita o al verificarsi di determinate condizioni (es. richiesta da parte dell'utente amministrativo) le chiavi crittografiche vengono rinnovate e viene effettuata l'emissione di un nuovo certificato prima della scadenza del vecchio certificato. Ciò è indispensabile per garantire la continuità di funzionamento del CCI.
- **Revoca del certificato**: nel caso in cui l'identità digitale del CCI sia ritenuta compromessa viene effettuata la revoca del certificato.
- **Controllo dello stato di validità del certificato**: i dispositivi, a cadenza temporale prestabilita, devono controllare se i certificati proposti dalle altre entità comunicanti sono effettivamente in corso di validità implementando tali controlli mediante l'utilizzo di liste di revoca (CRL- Certificate Revocation List) o del protocollo real-time (OCSP– Online Certificate Status Protocol). Al fine di garantire il massimo grado di interoperabilità si richiede il supporto di entrambe le modalità di controllo.

A seconda dei protocolli utilizzati le procedure possono comprendere diversi passaggi atti ad assicurare crittograficamente l'effettiva identità del dispositivo. Tali passaggi si distinguono a seconda del tipo di protocollo utilizzato e sono specificati dallo standard CEI EN 62351-9.

T.3.3.4.9.3 Registrazione del dispositivo

Tutti i dispositivi devono essere registrati presso almeno un'autorità di registrazione (RA), che può essere co-situata con l'autorità di certificazione (CA) approvata dall'organizzazione. Questa RA deve essere in grado di verificare l'identità dei dispositivi relativa ad una richiesta di firma del certificato (CSR).

I dati necessari alla registrazione del dispositivo devono essere configurati dal costruttore e devono includere un subject, ovvero l'insieme dei parametri identificativi del certificato (vedi T.3.3.4.9.9), ed almeno uno dei seguenti elementi:

- Codice di attivazione unico una tantum (o OTP), che consente al dispositivo di autenticarsi nei confronti della RA, ad esempio, quando esegue una richiesta di firma (CSR).
- Certificato a chiave pubblica incorporato nel dispositivo dal costruttore firmato dalla PKI del costruttore (Trust Anchor del Costruttore).

I dati di registrazione devono essere installati e configurati individualmente nel CCI per garantire che la RA possa autenticare il dispositivo quando esegue una CSR.

I dati di registrazione corrispondenti devono essere importati presso la RA del dominio operativo e devono comprendere il subject identificativo e, a seconda dalla modalità di arruolamento prevista, il codice di attivazione unico una tantum (o OTP) configurato sul dispositivo, oppure il certificato a chiave pubblica della PKI emittente il Certificato di Arruolamento (Trust Anchor del Costruttore).

T.3.3.4.9.4 Configurazione del dispositivo

Oltre ai parametri di base del certificato definiti nella Norma ISO/IEC 9594-8: 201x|Rec. ITU-T 1122 X.509, i dati di configurazione del CCI devono includere quanto riportato nella tabella che segue:

Nome Parametro	Descrizione Parametro	Ruolo Abilitato alla configurazione/modifica del Parametro
Chiave Pubblica/Certificato emesso dalla CA del Dominio Amministrativo	Certificato/i emesso dalla CA del dominio amministrativo che il dispositivo attribuisce al Proprietario (o ad un suo delegato) atto a permettere l'autenticazione crittografica, l'identificazione, la fruizione dei permessi di accesso e dei ruoli così come descritto al paragrafo T.3.3.4.4.1 oltreché l'autenticazione dell'entità (PKI) con cui il dispositivo comunicherà durante le procedure di gestione delle chiavi (arruolamento, aggiornamento automatico dei Trust Anchor, controllo dello stato di validità, download delle liste di revoca, etc.)	Profili Utente con privilegi amministrativi (e.g.: Proprietario del dispositivo)
Chiave Pubblica/Certificato della CA del DSO	Certificato della CA che il dispositivo attribuisce esclusivamente al DSO atto a permettere l'autenticazione crittografica, l'identificazione e la fruizione dei permessi di accesso dedicati descritti al paragrafo T.3.3.1.4 e del ruolo dedicato descritto al paragrafo T.3.3.4.3.1	Profili Utente cui vengano riconosciuti privilegi amministrativi e/o operativi (i.e. Proprietario del dispositivo/Tecnico Autorizzato)
Indirizzo IP o un nome di Dominio (es. IEC 62351. LocalCA)	Indirizzo relativo all'endpoint della PKI del Dominio Amministrativo	Profili Utente cui vengano riconosciuti privilegi amministrativi e/o operativi (i.e. Proprietario del dispositivo/Tecnico Autorizzato)
Parametri di timeout della CSR stabiliti dalla CA	Frequenza di polling, numero di tentativi, ecc.	Profili Utenti cui vengano riconosciuti privilegi amministrativi e/o operativi (i.e. Proprietario del dispositivo/Tecnico Autorizzato)
Subject del certificato del dispositivo	L'insieme di campi che permettono di identificare univocamente il dispositivo e che verranno specificati dalla CSR (Certificate Signing Request) durante l'arruolamento	Profili Utente cui vengano riconosciuti privilegi amministrativi e/o operativi (i.e. Proprietario del dispositivo/Tecnico Autorizzato)
dnsName	Nome del DNS cui il dispositivo farà riferimento. Un dispositivo può ricevere più di un dnsName. Gli indirizzi IP possono essere utilizzati anche in ambienti senza servizi DNS	Profili Utente cui vengano riconosciuti privilegi amministrativi e/o operativi (i.e. Proprietario del dispositivo/Tecnico Autorizzato)
Chiave Pubblica/Certificato della CA del Costruttore di Apparato	Certificato della CA che il dispositivo attribuisce all'ente che emetterà gli aggiornamenti firmware del dispositivo atto a permettere l'autenticazione e la verifica di integrità così come descritto al paragrafo T.3.3.4.8.	Profili Utente cui vengano riconosciuti privilegi amministrativi e/o operativi (i.e. Proprietario del dispositivo/Tecnico Autorizzato) **N.B**. Benchè modificabile da parte dell'utenza amministrativa e/o tecnica autorizzata, tale parametro dovrà essere pre-configurato da parte del costruttore dell'apparto.

Il CCI garantisce l'autenticità e l'integrità dei dati di configurazione presenti in tabella, per mezzo di tecniche crittografiche dedicate.

T.3.3.4.9.5 Arruolamento (enrollment)

Terminata la procedura di configurazione il dispositivo deve essere in grado di portare a termine la procedura di arruolamento mediante le modalità previste dal protocollo di enrollment di riferimento che permetterà di presentare una richiesta di firma del certificato (Certificate Signing Request - CSR) alla PKI.

Solo i dispositivi registrati possono essere arruolati dalla RA/CA.

I dispositivi generano la CSR utilizzando il formato PKCS # 10 e inviano la CSR alla RA specificata durante la configurazione. La RA verifica la validità della richiesta verificando quanto segue:

- Prova del possesso della corrispondente chiave privata mediante verifica della firma CSR;
- Prova di identità (utilizzando il codice di attivazione (OTP) o un certificato già disponibile e la corrispondente chiave privata insieme ai dati di registrazione sulla RA).

Se la richiesta è valida, la RA deve inviare una richiesta alla rispettiva CA. La CA genera un certificato di chiave pubblica e lo invia alla RA, che lo invia all'entità richiedente.

Se la richiesta non è valida, la RA non invierà alcuna richiesta alla CA.

Questa procedura viene eseguita in maniera automatica mediante specifici protocolli che, previa verifica dell'identità del CCI presso la RA, consentono di richiedere l'emissione di un certificato validato dalla CA associato ad un client, con un proprio corrispondente identificativo e una propria corrispondente chiave pubblica.

La specifica CEI EN 62351-9 indica diversi protocolli che consentono di realizzare la suddetta procedura. Tra questi, due protocolli in particolare sono indicati per l'applicazione nel dominio dei sistemi elettrici, ovvero **SCEP** ed **EST:**

- **SCEP (*Simple Certificate Enrollment Protocol*)**, protocollo di enrollment specificato dalla IETF RFC 8894 che utilizza, come formato dei messaggi, la Cryptographic Message Syntax (CMS) ed i PKCS #10 veicolati attraverso un canale di comunicazione HTTP. Si raccomanda di non utilizzare versioni di SCEP considerate legacy (pre-2015).
- **EST (*Enrollment over Secure Transport)*** protocollo di enrollment specificato dalla IETF RFC 7030 che utilizza, come formato dei messaggi, la Cryptographic Message Syntax (CMS) veicolati attraverso su canale di comunicazione sicuro (TLS 1.2 o versioni future).

In accordo con quanto indicato dalla CEI EN 62351-9 (Annex A) e al fine di garantire il massimo grado di interoperabilità, le infrastrutture a chiave pubblica sono tenute a supportare entrambi i protocolli.

Per il dispositivo CCI si richiede il supporto di almeno uno tra i protocolli di arruolamento indicati (SCEP o EST).

T.3.3.4.9.6 Rinnovo del Certificato

I dispositivi devono generare o richiedere una nuova coppia di chiavi ed eseguire una CSR al verificarsi di una delle seguenti condizioni:

- dopo che le date di scadenza dei loro certificati a chiave pubblica raggiungono una certa percentuale della durata massima consentita, come specificato dalle politiche dei certificati dell'organizzazione;
- richiesta diretta di un utente amministrativo autorizzato.

I dispositivi devono rinnovare i loro certificati a chiave pubblica prima della scadenza e devono creare un log che attesti le azioni volte al rinnovo del certificato (come eventi riusciti o non riusciti).

I dispositivi devono consentire la configurazione della politica di rinnovo del certificato di chiave pubblica, ad esempio:

- Supporto o meno del rinnovo automatico attraverso i protocolli implementati;
- Periodo di tempo prima della scadenza per il rinnovo del certificato.

Occorre prestare particolare attenzione all'allineamento temporale tra il CCI e la RA perché questo permette la corretta sincronizzazione sulla scadenza del certificato utilizzando un protocollo dedicato (es. NTP). La sincronizzazione dell'ora deve essere implementata utilizzando NTS di IETF (vedi T.3.3.4.5).

T.3.3.4.9.7 Revoca del Certificato

In caso di sospetta compromissione del certificato (ad esempio manomissione del dispositivo, furto, etc.) o in caso di passaggio di proprietà o controllo ad altro sistema di telegestione è necessario revocare la possibilità di accesso autenticato del CCI alla precedente infrastruttura.

È necessario assicurare un'adeguata precisione della sincronizzazione temporale tra il CCI e il sistema che crea e distribuisce le CRL di modo che le informazioni temporali nelle CRL siano accurate e che le entità dispongano di informazioni accurate sui certificati revocati.

I certificati devono essere revocati in base ai seguenti motivi e utilizzando i reason codes definiti al Paragrafo 9.5.3.1 della Norma ISO/IEC 9594-8: 201x | Rec. ITU-T X.509:

- Si sospetta che la chiave privata sia compromessa;
- Si sospetta che la chiave privata CA associata al certificato della CA sia compromessa;
- L'affiliazione dell'entità è cambiata (cessione, consegna ad altro controllo, etc);
- Il certificato relativo alla chiave pubblica è stato sostituito;
- Cessazione del funzionamento del CCI;
- Il privilegio relativo al ruolo espresso dal certificato è stato ritirato;
- Si sospetta che la chiave privata della Attribute Authority (PMI) sia compromessa.

T.3.3.4.9.8 Controllo dello stato di validità del certificato

Il dispositivo dovrà essere configurato per supportare il controllo dello stato validità dei certificati mediante le seguenti modalità:

- richiesta delle Certificate Revocation Lists (CRL);
- protocollo Online Certificate Status Protocol (OCSP).

L'OCSP, definito dalla RFC 6960, è un'alternativa al recupero dello stato di validità dei certificati via CRL utile a prevenire il fenomeno di "bloating" delle CRL che potrebbe causare, nel tempo, l'esaurimento delle risorse di memoria del dispositivo.

Il protocollo prevede l'invio di una richiesta di verifica dello stato di revoca OCSP al server OCSP (o alla CA) responsabile del certificato dell'entità. Questa richiesta OCSP contiene:

- la versione del protocollo;
- la richiesta di servizio;
- l'identificatore del certificato dell'entità e le estensioni.

Per evitare attacchi replay, un "nonce" è obbligatorio per distinguere questa richiesta di stato da qualsiasi richiesta di stato precedente. Il risponditore OCSP quindi convalida il certificato e restituisce "buono", "revocato" o "sconosciuto", utilizzando la propria firma digitale per autenticare la risposta.

In genere, è richiesta una connettività persistente tra l'entità richiedente e il risponditore. Tuttavia, tale connettività continua può essere di difficile adozione per alcune configurazioni in campo. Inoltre, lo sforzo computazionale per l'elaborazione della risposta OCSP e il ritardo di comunicazione potrebbero non essere adeguati per alcuni scenari. Poiché i server OCSP non rilasciano aggiornamenti di stato spontanei a seguito di eventi di revoca dei certificati, ma il controllo è affidato ai dispositivi richiedenti, le risposte OCSP devono avere un tempo di validità breve.

Pertanto, a seconda della configurazione del sistema e delle capacità del dispositivo, una combinazione ibrida di CRL e OCSP può essere utilizzata laddove un'entità che normalmente ha la connettività agisce come un risponditore OCSP proxy. Questa entità proxy recupera un elenco CRL in un periodo di tempo specifico, ad esempio ogni ora o entro 24 ore. L'entità proxy (ad es. Controller di stazione) serve quindi come risponditore OCSP per altre entità che normalmente non hanno connessioni con OCSP. Questo approccio è dettagliato dallo standard CEI EN 62351-9 cui si rimanda per approfondimenti.

T.3.3.4.9.9 Certificati a Chiave Pubblica del CCI

Un certificato a chiave pubblica è un documento digitale che lega l'identità dell'entità ad una coppia di chiavi crittografiche (chiave privata/chiave pubblica). Questa associazione è verificata da una firma digitale della CA emittente. Oltre alla chiave pubblica e all'identità del proprietario del certificato a chiave pubblica, i certificati a chiave pubblica contengono informazioni verificate sul periodo di validità e l'identità dell'emittente.

Questo documento non impone né una durata minima né massima del certificato a chiave pubblica. È necessario scegliere una data di scadenza del certificato in base al tipo di certificato e alle politiche di sicurezza degli attori coinvolti.

Un certificato a chiave pubblica può includere estensioni che forniscono informazioni aggiuntive. Un'estensione è identificata da un identificatore di oggetto assegnato dall'organizzazione che definisce l'estensione. Un certificato a chiave pubblica può essere emesso per una CA e viene quindi chiamato certificato CA, o per un'entità finale e viene quindi chiamato certificato a chiave pubblica dell'entità finale.

I certificati a chiave pubblica e i certificati di attributo sono definiti da un set di base più le estensioni del set di base. Le estensioni sono identificate da un registro internazionale degli identificatori di oggetto (OID).

I certificati a chiave pubblica devono includere un'estensione relativa all'utilizzo della chiave privata, che specifica il periodo durante il quale la chiave privata corrispondente può essere utilizzata dal suo proprietario. Questo periodo è normalmente impostato per essere più breve del periodo di validità del certificato, assicurando che i certificati rimangano validi per un periodo minimo dopo l'uso da parte del loro proprietario. I dettagli sull'uso dell'estensione per l'utilizzo della chiave privata possono essere trovati nel Paragrafo 9.2.2.5 della ISO/IEC 9594-8 | Rec. A valle delle procedure di arruolamento il dispositivo CCI deve essere in possesso di almeno un certificato X.509 identificativo avente la funzione di:

- consentire l’autenticazione da parte delle altre entità coinvolte durante l’esecuzione della sua funzione;
- garantire l’integrità e l’autenticità delle comunicazioni del dispositivo;
- abilitare il dispositivo CCI a richiedere alla PKI ulteriori Certificati di Servizio (vedi T.3.3.4.9.9.3).

T.3.3.4.9.9.1 Trust Anchor

Quando un dispositivo attraversa una catena di approvvigionamento che comprende Costruttore, Acquirente, Installatore, ecc. è opportuno dotare il dispositivo dei certificati Trust Anchor delle CA la cui affidabilità è data per assunta e non deve essere derivata dal dispositivo previa verifica della Chain of Trust.

Si ritiene necessario dotare il CCI almeno dei seguenti elementi:

- Chiave Pubblica/Certificato della CA del DSO, che il DSO intende utilizzare come Trust Anchor;
- Chiave Pubblica/Certificato della CA del Dominio Amministrativo, che l'Utente intende utilizzare come Trust Anchor;
- Chiave Pubblica/Certificato della CA del Costruttore, che il Costruttore intende utilizzare come Trust Anchor.

Ai quali si vanno ad aggiungere i seguenti elementi opzionali:

- Chiave Pubblica/Certificato (Trust Anchor) della CA i cui certificati saranno utilizzati nel processo di firma digitale degli aggiornamenti del dispositivo, nel caso in cui il costruttore del CCI non sia direttamente responsabile degli aggiornamenti;
- Chiave Pubblica/Certificato (Trust Anchor) della CA dell'Aggregatore, nel caso l'Aggregatore sia presente;
- Chiave Pubblica/Certificato (Trust Anchor) della CA che emette il certificato utilizzato per accedere ai servizi PKI, nel caso di utilizzo di protocolli ove sia necessario stabilire una sessione SSL (e.g. EST - RFC7030).

Esempio di Certificato 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 Certificato di Pre-Arruolamento (Protocollo EST)

Il Certificato di Arruolamento è un certificato di tipo ITU-T X.509v3, utilizzato per stabilire una connessione TLS mutuamente autenticata tra CCI e PKI al fine di abilitare il processo di arruolamento mediante protocollo EST. Il Costruttore dovrà fornire il CCI del Certificato di Pre-Arruolamento firmato da una CA federata dalla PKI del dominio operativo.

T.3.3.4.9.9.3 Certificati di Servizio

I Certificati di Servizio sono dei certificati a chiave pubblica, contraddistinti da una coppia di chiavi pubblica/privata dedicata, di tipo ITU-T X.509v3 o altri formati previsti dall'infrastruttura (es. OpenSSH) firmati dalla CA del dominio operativo e finalizzati a:

- abilitare l'autenticazione delle comunicazioni del profilo Applicativo MMS così come descritto nel Paragrafo T.3.3.4.1 e specificato dalla CEI EN IEC 62351-4;
- abilitare l'autenticazione delle comunicazioni del profilo T (Transport Layer Security) descritto nel Paragrafo T.3.3.4.1 e specificato dalla CEI EN 62351-3;
- abilitare l'autenticazione delle comunicazioni del protocollo HTTPS così come dalla RFC 2818 (HTTP Over TLS);
- abilitare l'autenticazione delle comunicazioni del protocollo SNMPv3 profilo TSM;
- abilitare l'autenticazione delle comunicazioni del protocollo NTS;
- abilitare l'autenticazione delle comunicazioni SSH;
- abilitare le comunicazioni del protocollo syslog su trasporto sicuro TLS.

T.3.3.4.10 Segregazione del traffico del CCI

La segregazione degli accessi remoti al CCI, asserviti alle funzioni di monitoraggio, controllo, protezione e conduzione dell'impianto, è a carico di dispositivi router in grado di separare le reti interne dell'impianto dalle reti esterne e di segregare il traffico dei protocolli utilizzati dalle interfacce di rete. Il dispositivo router dovrà essere dotato di funzionalità di NAT, VLAN, firewalling e VPN con cifratura del canale. L'eventuale utilizzo di servizi di connettività su rete pubblica dovrà prevedere la configurazione di una VPN sicura ed escludere l'utilizzo del servizio di connettività per scopi diversi da quelli richiesti dalle comunicazioni per il controllo e la conduzione dell'impianto.

T.3.3.4.11 Sicurezza delle comunicazioni locali

Tutte le comunicazioni per la messa in servizio e la configurazione del CCI attraverso l'interfaccia locale devono essere protette da un sistema di autenticazione dell'Utente soggetto a specifiche policy di sicurezza.

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
Stampa in proprio
Autorizzazione del Tribunale di Milano N. 4093 del 24 Luglio 1956
Direttore Responsabile: Ing. G. Molina

Comitato Tecnico Elaboratore
CT 316-Connessioni alle reti elettriche Alta, Media e Bassa Tensione

Altre Norme di possibile interesse sull'argomento

Via Saccardo, 9
20134 Milano
Tel. 02.21006.1
Fax 02.21006.210
cei@ceinorme.it
www.ceinorme.it