COMITATO
ELETTROTECNICO
ITALIANO

Via Saccardo, 9
20134 Milano
Tel. 02/21006.1
fax 02/21006.210 Direzione
fax 02/21006.222 Vendite
mail cei@ceinorme.it

FAQ

Quesiti relativi alla Norma CEI 0-16
Quesiti e risposte relative all'Allegato O
Quesiti e risposte relative all'Allegato T

---------- o ----------

Quesiti e risposte relative all'Allegato O

Di seguito sono elencate le risposte dei comitati tecnici CEI CT 316 e CT 57, alle richieste di chiarimento presentate con maggiore frequenza, relative sia all'Allegato O che all'Allegato T della Norma CEI 0-16.

L'obiettivo è chiarire eventuali dubbi d'interpretazione dei requisiti normativi contenuti nei suddetti allegati e fornire esempi di possibili soluzioni, sia di implementazione del prodotto CCI, che di installazione del CCI sugli impianti. Gli esempi forniti non rappresentano soluzioni obbligatorie da rispettare, ma servono per meglio chiarire i requisiti richiesti e dimostrarne la fattibilità.

Gli argomenti riguardano:

O.2 - Campo di applicazione e O.11-Compatibilità e priorità fra funzioni di regolazione del CCI

O.5 - Modalità di funzionamento del CCI e O.9.1 Regolazione di Tensione

O.8.6 - Segnali relativi allo stato dell'impianto (PF1)

O.9.2.1 - Limitazione della Potenza attiva immessa per valori di tensione prossimi al 110% di Un

O.13.1.1.2 - Interfaccia per i servizi locali di Configurazione e Manutenzione del CCI

O.13.2.1 - Prescrizioni relative ai trasduttori ed ai convertitori di misura

O.13.5 Orologio interno e sincronizzazione e T.3.3.4.5 Sincronizzazione temporale

O.13.7 - Cybersecurity Hardware

O.15 - Prove e certificazione di conformità

O.15.4 - Certificazione IEC 62443

Segue l'elenco dei quesiti e delle relative risposte proposte, con segnalazione dei eventuali proposte di deroga normativa temporanea.

COMITATO
ELETTROTECNICO
ITALIANO

Via Saccardo, 9
20134 Milano
Tel. 02/21006.1
fax 02/21006.210 Direzione
fax 02/21006.222 Vendite
mail cei@ceinorme.it

O.2-Campo di applicazione e O.11-Compatibilità e priorità fra funzioni di regolazione del CCI

«Il CCI non è tenuto o proprio non può (gli è proibito) svolgere le funzioni di regolazione della P in seguito a eventi di sovra frequenza (LFSM-O 8.8.6.3.2) e di sotto frequenza (LFSM-U 8.8.6.3.3)? In ambito fotovoltaico sia all'estero che in Italia, per impianti in AT secondo A68, quelle funzioni vengono svolte dal plant controller a livello di impianto, perché i singoli convertitori non sono sempre in grado. In particolare, per la LFSM-U, che in ambito fotovoltaico richiede l'utilizzo di un margine di potenza attiva che non può che essere "gestito" dal PPC e non dal singolo generatore

Similmente, il modo di controllo FSM descritto in X.2 ma che non viene menzionato in O.2, può essere svolto dal CCI?»

Per gli impianti collegati in AT il CCI è fuori dal suo ambito di applicazione.

Per gli impianti collegati in MT, la norma CEI 0-16 al punto 8.8.6.3.2 "Limitazione della potenza attiva per transitori di sovra-frequenza originatisi sulla rete" prescrive che tutti i generatori devono disporre della funzione della riduzione della potenza in sovrafrequenza. Sempre la CEI 0-16 al punto O.2 prescrive che il CCI NON deve attuare alcuna azione di regolazione né per sovra né per sotto frequenza.

Tuttavia, come esplicitato al capitolo O.4 della 0-16, "Le funzioni del CCI possono essere anche integrate come funzionalità aggiuntiva in uno degli altri apparati costituenti l'impianto […]" ed anche "Altre unità funzionali utili alla gestione ottimale dell'impianto possono essere presenti e implementate nel CCI […]".

Quindi il costruttore, per gli impianti per i quali è ammessa la presenza di un plant controller per soddisfare i requisiti relativi ai transitori di frequenza, può aggiungere allo stesso plant controller le altre prestazioni funzionali del CCI.

O.5 Modalità di funzionamento del CCI e O.9.1 Regolazione di Tensione

«Nel caso non sia presente la connessione con il DSO, i modi di controllo della tensione Fixed CosPhi, CosPhi(P) e Q(V) vanno considerate funzioni autonome: in questo caso i parametri delle curve di regolazione da usare saranno indicati nel regolamento d'esercizio?»

Si, tutti i valori di default saranno definiti nel regolamento di esercizio

O.9.2.1 - Limitazione della Potenza attiva immessa per valori di tensione prossimi al 110% di Un

«A seguito di un'analisi del punto O.9.2.1 relativo al controllo della tensione quando maggiore del 110% della nominale tramite la gestione della potenza attiva non vi è riferimento, rispetto alle altre funzioni di controllo che sono spiegate nel dettaglio in maniera approfondita, si trova solamente un riferimento all'allegato J sempre della CEI 0-16, ma anche in questo punto non si hanno informazioni sulla struttura della funzione richieste rendono difficoltosa la implementazione stessa. Si richiede perciò un chiarimento sulle aspettative attese di questa funzione controllo.»

L'attivazione di questa funzione è lasciata al produttore, come pure le modalità (vedi CEI 016 8.8.6.3.1 e allegato J punto J.2: "qualora attivata essa può operare secondo una funzione scelta dal costruttore").

Il produttore può valutare, in relazione alle caratteristiche del proprio impianto, come realizzare questa funzione e, nel caso, può decidere di non attuare alcuna azione volta a mitigare il rischio di distacco per sovra-tensione.

COMITATO
ELETTROTECNICO
ITALIANO

Via Saccardo, 9
20134 Milano
Tel. 02/21006.1
fax 02/21006.210 Direzione
fax 02/21006.222 Vendite
mail cei@ceinorme.it

O.13.1.1.2 - Interfaccia per i servizi locali di Configurazione e Manutenzione del CCI

«L'esclusione della tecnologia IP riguarda solo la configurazione da locale o anche quella da remoto, che è contemplata da allegato T nella sezione T.3.3.4.6.1?

L'esclusione della tecnologia IP riguarda solo la prima configurazione, ed il ripristino in caso di disaster recovery? Oppure anche altre operazioni, come modifiche successive di parametri di configurazione e l'aggiornamento software/firmware da remoto (in modo sicuro come specificato da IEC 62443)?»

«Poiché la maggior parte dei dispositivi in commercio ha una porta d'ingegneria che utilizza comunicazione TCPIP per sua semplicità non esistono particolari standard di riferimento dove questa specifica viene richiesta. In aggiunta la velocità di comunicazione di porte seriali è in genere ridotta e quindi non sufficiente per accedere alla configurazione dei dispositivi. È quindi a seguito di quanto sopra riportato che si richiede cancellazione del punto O.13.1.1.2.»

O.13.1.1.2 Interfaccia per i servizi locali di Configurazione e Manutenzione del CCI

L'interfaccia è dedicata alle attività di prima configurazione o manutenzione di apparato in caso di recovery

Questa interfaccia può essere realizzata con tecnologia seriale o porta USB.

È esclusa la tecnologia di comunicazione IP per ragioni di sicurezza.

Su tale porta devono essere implementate tecnologie per il riconoscimento degli utenti che chiedono l'accesso all'apparato, al fine di assicurare una efficace protezione contro gli accessi non autorizzati.

L'esclusione della tecnologia IP riguarda la sola porta consolle per la configurazione da locale. La configurazione remota è possibile utilizzando i servizi logici di comunicazione con attori abilitati alla connessione remota (O.13.1.3) attraverso l'interfaccia di rete Eth_B, che prevede l'utilizzo di tecnologie IP. Si deve tener conto di quanto indicato nell'Allegato T riguardo alle prescrizioni di cybersecurity, per cui è obbligatorio che si adottino tutti i controlli compensativi previsti in Allegato T, quali, ad esempio, adozione di un canale sicuro (e.g. TLS con mutua autenticazione).

Tramite la suddetta interfaccia Eth_B possono anche essere effettuate le operazioni di prima configurazione o manutenzione di apparato in caso di recovery solo ed esclusivamente se anche tali operazioni possono essere effettuate adottando tutti i controlli compensativi previsti in Allegato T, quali, ad esempio, adozione di un canale sicuro (e.g. TLS con mutua autenticazione).

O.13.2.1 - Prescrizioni relative ai trasduttori ed ai convertitori di misura

«TA e TV con prestazione 15VA, essendo questa "migliorativa" rispetto ai 5 e 10 VA indicati, sono conformi alle indicazioni della norma?»

È possibile adottare TA e TV con prestazione superiore, purché siano rispettate tutte le altre prescrizioni.

«In caso non si utilizzino sistemi di misure con le prestazioni indicate (TA TV Classe 0.5 e Convertitore Classe 0.2) come si deve dimostrare che l'accuratezza delle misure rispetta i requisiti Terna espressi in A.6 (Errore massimo < 2.2%)? Tramite prove in laboratorio? Prove in campo su ogni impianto?»

Come riportato al O.13.2.1, con le prestazioni indicate si ottempera ai requisiti di accuratezza richiesti dall'Allegato A.6 al Codice di rete, Tabelle 5 e 6. Prestazioni differenti sono accettabili purché l'accuratezza delle misure da rendere disponibili all'interfaccia del CCI con il DSO siano congruenti con quanto prescritto dal citato allegato A.6

La verifica di accuratezza del convertitore deve essere effettuata nell'ambito delle prove di certificazione del CCI, secondo una metodologia ritenuta ammissibile dall'ente certificatore. La verifica di accuratezza del sistema

COMITATO
ELETTROTECNICO
ITALIANO

Via Saccardo, 9
20134 Milano
Tel. 02/21006.1
fax 02/21006.210 Direzione
fax 02/21006.222 Vendite
mail cei@ceinorme.it

complessivo deve essere effettuata secondo le indicazioni della norma CEI EN 61557-12, già richiamata in O.15.2

NB : In base alle definizioni riportate nella norma CEI EN 61557-12, si interpreta come “Convertitore” la parte operante funzionalità di acquisizione e di elaborazione della misura di un PMD privo di sensori esterni.

«Ci sono prescrizione sulla posizione di installazione dei TA e TV rispetto al DG? Possono essere installati sia a monte che a valle in base ai casi?»

Si veda quanto previsto nella norma CEI 0-16 – Allegato H in merito al posizionamento (ideale e consentito) dei trasduttori.

O.13.5 Orologio interno e sincronizzazione e T.3.3.4.5 Sincronizzazione temporale

«Per la sincronizzazione temporale è possibile usare la versione sicura NTS del protocollo NTP via rete internet (come indicato in T.3.3.4.5) o è necessario un GPS fisico locale in impianto (come indicato in O.13.5)?»

Si conferma la necessità di un GPS fisico in impianto, che può essere integrato nel CCI o esterno ad esso. Nel caso di GPS esterno al CCI, la trasmissione del segnale con l’informazione temporale avviene tramite la versione sicura NTS (Network Time Security) di NTP, specificata dallo standard IETF RFC 8915 e dotata di funzioni di autenticazione e integrità basate su TLS.

La valutazione dell’utilizzo di architetture ridondate di cui all’ultimo paragrafo del T 3.3.4.5 è rimandata al progettista in relazione alla valutazione delle vulnerabilità dell’impianto

O.13.7 - Cybersecurity Hardware

«Il CCI non deve esporre porte fisiche di test attive.

Il CCI deve inoltre essere protetto contro possibili manomissioni con soluzioni appropriate quali ad esempio:

- **Circuiti che invalidano la NVRAM quando viene aperto l'involucro**
- **Sensori che bruciano fusibili di sicurezza quando viene rilevata la luce**
- **Sensori che attivano un avviso quando viene modificata la posizione del dispositivo**
- **Copertura epossidica dei componenti del circuito core**
- **Avvisi generati quando componenti interni vengono rimossi dal dispositivo**

Domanda : E' sufficiente implementare solo una di queste funzionalità? Oppure è necessario prevederne più di una?»

Il requisito è che ci siano soluzioni appropriate atte a proteggere da possibili manomissioni, riportandone degli esempi per maggiore chiarezza. Non è un elenco esaustivo. Le misure riportate a titolo d’esempio incrementano la sicurezza del dispositivo riducendone il rischio di manomissione, ma non è necessario applicarle tutte. La scelta di quale o quali soluzioni applicare resta pertanto prerogativa del costruttore.

O.15 - Prove e certificazione di conformità

«Può un ente di certificazione accreditarsi per certificare la conformità del CCI agli allegati O e T della CEI 0-16 (come prodotto)? O la conformità può essere solo auto-dichiarata dal costruttore?»

COMITATO
ELETTROTECNICO
ITALIANO

Via Saccardo, 9
20134 Milano
Tel. 02/21006.1
fax 02/21006.210 Direzione
fax 02/21006.222 Vendite
mail cei@ceinorme.it

Un ente di certificazione in linea teorica può accreditarsi per certificare la conformità del CCI agli allegati O e T, sebbene la certificazione unica sia complessa per l'alto numero di accreditamenti da ottenere su tematiche molto diverse. La questione esula i compiti del comitato.

«Perché, a differenza dall'Allegato N dove viene indicato chiaramente che tutte le prove elencate devono essere svolte presso un laboratorio accreditato ISO 17025, in O.15 vengono elencate in modo eterogeneo diverse certificazioni da ottenere, e prove che possono essere svolte in modi differenti (alcune in laboratorio ISO 17025, altre alla presenza di ispettore ISO 17065)»

Nel capitolo O.15 viene prescritto che l'esecuzione delle prove di compatibilità ambientale (prove di isolamento, climatiche ed EMC) debba avvenire presso un laboratorio accreditato secondo CEI UNI EN ISO/IEC 17025.

Le prove funzionali, invece, sono ammesse in alternativa:

- presso il laboratorio di cui sopra, oppure
- presso i laboratori del costruttore, o laboratori esterni non accreditati.

In questo caso (lettera b), le prove devono avvenire sotto la sorveglianza e responsabilità di apposito organismo certificatore che abbia i requisiti della UNI CEI EN ISO/IEC 17065.

È quindi sempre possibile effettuare le prove di compatibilità ambientale e le prove funzionali presso un laboratorio accreditato. È altresì permesso che le prove funzionali, che possono richiedere dei sistemi esterni per la simulazione del campo e per la simulazione della comunicazione con gli operatori remoti, possano essere svolte presso i laboratori del costruttore.

«È possibile, magari per un periodo breve, auto-dichiarare la conformità se il CCI è conforme ad un certo requisito, ma non è ancora in possesso della relativa certificazione (per esempio certificazione IEC 62443-4-2 o prove IEC 62351-100-3)?»

Si veda in proposito il testo delle FAQ relativo alle certificazioni di cybersecurity.

O.15.4 - Certificazione IEC 62443

"Per la sicurezza del prodotto CCI è richiesta la certificazione ISASecure Embedded Device Security Assurance (EDSA) v3.0.0 di conformità alle norme IEC 62443-4-1 "Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements" e IEC 62443-4-2 "Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components".

La certificazione deve essere rilasciata in base allo schema ISASecure da un ente accreditato o sono equivalenti anche altri schemi di certificazione non IsaSecure?

Possono essere utilizzati anche altri schemi di certificazione equivalenti, ad esempio quello IEC-EE.

«Lo schema ISASecure EDSA è oramai obsoleto e sostituito dal CSA 1.0.0; (vedi https://isasecure.org/en-US/Certification/IEC-62443-CSA-Certification#tab1, in particolare al documento ISASecure-117): è confermato che la certificazione secondo schema CSA è conforme alle richieste della CEI 0-16 2022-03?»

Si conferma l'adeguatezza dello schema ISASecure CSA 1.0.0.

«La FAQ CEI del 23.11.21 "Quesiti relativi alla Norma CEI 0-16 "Controllore centrale d'impianto - CCI"" chiarisce che è richiesta una certificazione di conformità a IEC 62443-4-1 e IEC 62443-4-2, senza indicare lo schema di certificazione. In aggiunta, lo schema di certificazione indicato in norma EDSA è superato da CSA 1.0.0. Si chiede quindi conferma della validità della FAQ cui i costruttori hanno fatto riferimento, quindi inizialmente la certificazione di conformità a IEC 62443-4-1 ML2 e autocertificazione di IEC 62443-

COMITATO
ELETTROTECNICO
ITALIANO

Via Saccardo, 9
20134 Milano
Tel. 02/21006.1
fax 02/21006.210 Direzione
fax 02/21006.222 Vendite
mail cei@ceinorme.it

4-2 SL1, successivamente la certificazione ML3 e SL1 con capability SL2 nelle condizioni esplicitate nella Faq, indipendentemente dallo schema di certificazione.»

Si aggiorna la risposta alla FAQ n. 2 del 23/11/2021 come segue:

Il dispositivo CCI nel suo complesso richiede la certificazione di conformità alla norma IEC 62443- 4-1. Per la certificazione è ammessa l'applicazione di entrambi gli schemi di certificazione ISASecure (CSA) e IEC-EE.

Nel caso di applicazione dello schema IEC-EE:

- *è richiesta la certificazione di conformità alla norma IEC 62443-4-1 con livello minimo di maturità ML3.*
- *per un periodo transitorio limitato è ammessa la certificazione di conformità alla norma IEC 62443-4-1 con livello di maturità ML2*

Si ritiene che il periodo transitorio e limitato introdotto nella prima parte della risposta alla FAQ n. 3 del 23/11/2021 debba terminare il 31/12/2023 e che a valle di questa data si debba certificare il CCI alla norma IEC 62443-4-2 con livello SL1. Qualora vi fossero riscontri oggettivi in merito alla impossibilità di rispettare questa scadenza, il Comitato riesaminerà la tempistica prevista che oggi appare coerente con le informazioni a disposizione.

Per la certificazione è ammessa l'applicazione di entrambi gli schemi di certificazione ISASecure (CSA) e IEC-EE.

Si conferma la seconda parte della risposta alla FAQ n. 3 del 23/11/2021, precisando che per la certificazione è ammessa l'applicazione di entrambi gli schemi di certificazione ISASecure (CSA) e IEC-EE. Si conferma ancora ammissibile che tale procedura possa essere effettuata e garantita dal costruttore stesso.

Si consulti in merito la versione aggionata della FAQ.

Domanda:

« *Certificazione IEC 62351-100-3*

***Si evidenziano difficoltà nel trovare laboratori accreditati per le certificazioni IEC 62351-x. DNV-GL / KEMA dichiara di non essere pronta almeno fino a H2/2023 e che, a quanto ne sanno loro, non esistono al mondo laboratori accreditati. È pensabile prevedere una FAQ con deroga e autocertificazione analogamente a quanto già fatto per IEC 62443?* »**

Risposta:

Per un periodo transitorio che termina il 31/12/2023 è ammesso che la conformità alla norma IEC 62351-100-3 possa essere auto-certificata dal costruttore. Qualora vi fossero riscontri oggettivi a sostegno, il Comitato riesaminerà la tempistica prevista che oggi appare coerente con le informazioni a disposizione.

COMITATO
ELETTROTECNICO
ITALIANO

Via Saccardo, 9
20134 Milano
Tel. 02/21006.1
fax 02/21006.210 Direzione
fax 02/21006.222 Vendite
mail cei@ceinorme.it

---------- o ----------

Quesiti e risposte relative all'Allegato T - Elenco per punti

Gli argomenti riguardano:

T.3.2.1 Modalità di comunicazione

T.3.3.3 Mappatura su protocollo di comunicazione

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

T.3.3.4.3.2 Trasporto dei ruoli

T:3.3.4.10 Segregazione del traffico del CCI

Misure per l'osservabilità a 4 secondi

Sincronizzazione GPS

Dati riservati al DSO vs. dati riservati all'Aggregatore

T.3.3.4.1 Sicurezza delle comunicazioni IEC 61850/MMS

Segue l'elenco dei quesiti e delle relative risposte proposte, con segnalazione dei eventuali proposte di deroga normativa temporanea.

T.3.2.1 Modalità di comunicazione

«il CCI dovrà essere in grado di sottoscrivere messaggi GOOSE in merito alle funzioni di controllo": verso chi dovrà essere effettuata la sottoscrizione? Per quali DO?

Questo non è in contrasto con la sezione T.3.3.3 che indica la mappatura su MMS per tutti i modelli dati definiti?

Nel caso la subscription debba essere fatta con il DSO, la sicurezza del protocollo GOOSE non dovrebbe essere obbligatoria?»

Le interfacce di rete del CCI devono supportare servizi di comunicazione basati su protocolli della famiglia IEC 61850 (MMS, GOOSE); l'allegato T predispone l'utilizzo ed indica le performance dei GOOSE, ma non prevede il relativo caso d'uso. Poiché non sono ancora state chiarite le specifiche funzionalità, si parla ora solo di predisposizione. Si fa presente che, quando verranno implementate tali funzionalità, diverranno obbligatorie anche le sezioni relative alla sicurezza, opportunamente aggiornate.

T.3.3.3 Mappatura su protocollo di comunicazione

«Al fine di agevolare la realizzazione di dispositivi CCI interoperabili, sarà reso disponibile il relativo file di configurazione secondo il formalismo SCL"

Da chi sarà reso disponibili il file di configurazione CID? Dal costruttore del CCI o dal DSO come configurazione standard da rispettare?»

La questione formale su chi renderà disponibile il file CID sembra un tema da correlare all'Allegato U alla CEI 0-16 (Regolamento di Esercizio). Ad ogni buon conto, il CT57 ha approvato un esempio di file SCL, che è

COMITATO
ELETTROTECNICO
ITALIANO

Via Saccardo, 9
20134 Milano
Tel. 02/21006.1
fax 02/21006.210 Direzione
fax 02/21006.222 Vendite
mail cei@ceinorme.it

stato pubblicato dal CEI come Technical Report 57-126.

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

«Il protocollo GOOSE per motivi di sicurezza non necessita di crittografia, potrebbe però supportare funzionalità di autenticazione del messaggio: implementare l'autenticazione in GOOSE è facoltativo o obbligatorio? Se sì con che strumenti?»

Le funzioni di sicurezza per il protocollo GOOSE sono normate dalla IEC 62351-6. Poiché le comunicazioni GOOSE del CCI non sono ancora state specificate (vedi risposta alla domanda precedente), la sezione sulla sicurezza delle comunicazioni GOOSE è indicata come informativa.

Quando le comunicazioni GOOSE dovranno essere implementate, la sezione T.3.3.4.2 dovrà essere aggiornata per allineare le funzionalità di sicurezza all'ultima edizione della IEC 62351-6 e a quanto richiesto per la sicurezza delle VLAN Ethernet IEEE 802.1 Q.

T.3.3.4.3.2 Trasporto dei ruoli

«Sarà il DSO a indicare quale, tra i profili A, B, C e D usare per gli accessi token?»

Dei 4 profili indicati nella CEI EN 62351-8, il CCI l'Allegato T richiede i profili A e B (mandatori), mentre indica i profili C e D come facoltativi.

Avendo registrato l'assenza della intenzione di utilizzare da subito i profili C e D da parte dei DSO, si ritiene che si possa concedere una dilazione nell'obbligo di implementazione dei suddetti profili C e D da parte dei costruttori. I costruttori devono comunque dimensionare da subito i prodotti CCI in modo che abbiano la capacità di abilitare i profili C e D con un aggiornamento software/firmware.

T:3.3.4.10 Segregazione del traffico del CCI

«Nel caso in cui le funzionalità di segregazione del traffico siano svolte da un router/firewall esterno (non integrato nel CCI), i log del traffico devono essere riportati anche nel CCI o è sufficiente siano memorizzati all'interno del router/firewall?»

La Norma non prescrive che il CCI debba svolgere funzione di archiviazione dei log prodotti dagli altri apparati di networking esterni al CCI stesso eventualmente presenti. È responsabilità del gestore dell'impianto consultare i log registrati su tali apparati router/firewall.

NB: Si interpreta la domanda come riferita all'interfaccia ETH B, in quanto l'interfaccia ETH A è dedicata in via diretta ed esclusiva alla comunicazione fra l'impianto ed il DSO.

Misure per l'osservabilità a 4 secondi

«Ha senso richiedere di inviare i report a modulo di 4 secondi e avere anche la marca oraria del dato aggiornata allo stesso istante temporale?»

La risposta alla domanda è affermativa. L'obiettivo è far in modo che l'ultima misura disponibile, più prossima allo scadere del quarto secondo, venga presa in carico per essere spedita con il report. Dunque il time stamp del report dovrà avere cadenza temporale 00, 04, 08, .. mentre il time stamp della misura dovrà essere il più prossimo possibile al tempo di emissione del report. Dato che il TSO, per il calcolo della latenza temporale, utilizza come riferimento temporale il time stamp del dato di misura rispetto al tempo assoluto GPS è molto

COMITATO
ELETTROTECNICO
ITALIANO

Via Saccardo, 9
20134 Milano
Tel. 02/21006.1
fax 02/21006.210 Direzione
fax 02/21006.222 Vendite
mail cei@ceinorme.it

importante che non si consumi tempo in attesa di spedire il dato sul CCI. Si precisa che anche nel caso in cui la misura non vari nell'arco dei 4 secondi, dovrà essere aggiornato il time stamp del dato di misura. Il report dovrà essere inviato ogni 4 secondi, il tempo di invio del report indipendentemente dal momento di attivazione da parte del client deve essere sincronizzato allo scadere del primo quarto secondo (00, 04, 08, ..).

Sincronizzazione GPS

«A cosa deve essere riferita l'incertezza di +/-100ms sulla sincronizzazione oraria? Qualora la deriva temporale dovesse essere maggiore 1s al giorno è necessario alzare il bit di qualità del timestamp? Se sì, quale bit ha senso alzare (CLOCK NOT SYNC, CLOCK FAILURE, …)?»

L'incertezza è il valore di offset massimo ammesso. Qualora il CCI perdesse il segnale del GPS e non potesse sincronizzarsi, dovrà garantire tramite l'orologio interno una deriva temporale inferiore ad 1 secondo al giorno.

In fase di inizializzazione del dispositivo, entrambi i bit della TimeQuality, ClockFailure e ClockNotSynchronized devono essere valorizzati ad 1. Quando la fonte sincronizzante è connessa deve essere valorizzato a 0 il bit relativo al ClockFailure, successivamente quando l'offset risulta minore di 100ms deve essere valorizzato a 0 il bit relativo a ClockNotSynchronized.

Nella fase operativa del CCI, i bit ClockFailure e ClockNotSynchronized sono valorizzati a 1 quando il CCI rileva la condizione di impossibilità di sincronizzare il CCI con il riferimento temporale esterno (GPS) (es. per indisponibilità del segnale o per il deterioramento, anche temporaneo, delle caratteristiche di questo), in quanto non è più possibile determinare un offset avendo perso il riferimento temporale.

Il bit ClockNotSynchronized è valorizzato ad 1 anche quando il CCI rileva un valore di offset maggiore di 100ms; tale condizione permane fino a che il valore dell'offset risulta minore di 100ms, condizione in cui il bit ClockNotSynchronized deve essere valorizzato a 0.

Dati riservati al DSO vs. dati riservati all'Aggregatore

«È necessario gestire due CID diversi in funzione del ruolo con cui ci si collega (DSO vs. Aggregatore)? Il server IEC 61850 deve gestire CID diversi mantenendo inalterato solo il template?»

Il file CID è il medesimo, verrà gestito differentemente a seconda del ruolo.

T.3.3.4.1 Sicurezza delle comunicazioni IEC 61850/MMS

«[omissis] a pagina 49 risulta essere mandatorio avere sia E2E che Profilo T come applicativi di sicurezza per la comunicazione. Nonostante sia mandatorio avere entrambi gli applicativi è sufficiente che le parti (DSO e proprietario Impianto) concordino su uno dei due metodi.

[omissis] si propone un generale deroga che tenga conto dei tempi di rilascio dell'IEC 61850-90-19 e dei tempi necessari al fine che questo lo standard possa essere recepito»

La specifica prevede entrambi i profili per garantire l'interoperabilità e la sicurezza in caso le controparti determinino di necessitare delle differenti caratteristiche di sicurezza rese disponibili dai due profili (ad esempio la possibilità di garantire la sicurezza nel caso la comunicazione sia spezzata da eventuali gateway intermedi). I profili possono anche essere combinati per maggiore robustezza qualora ciò sia opportuno.

La sicurezza E2E deve essere implementata seguendo le specifiche di IEC 62351-4.

COMITATO
ELETTROTECNICO
ITALIANO

Via Saccardo, 9
20134 Milano
Tel. 02/21006.1
fax 02/21006.210 Direzione
fax 02/21006.222 Vendite
mail cei@ceinorme.it

Data la più recente introduzione della sicurezza E2E rispetto al profilo T (relativo la protocollo TLS) è stata segnalata dai costruttori la limitata disponibilità di strumenti di supporto allo sviluppo software (i.e. librerie software) o di procedure di test consolidate. Per questo motivo, avendo registrato l'assenza della intenzione di utilizzare da subito la sicurezza E2E da parte dei DSO, si ritiene che si possa concedere una dilazione nell'obbligo di implementazione della funzionalità di sicurezza E2E da parte dei costruttori. I costruttori devono comunque dimensionare da subito i prodotti CCI in modo che abbiano la capacità di abilitare questa funzionalità con un aggiornamento software/firmware entro il termine del periodo di dilazione.

NB

Si informa che la sottomissione a IEC della specifica tecnica IEC/TS 62351-100-4 "Conformance testing for 62351-4 with IEC 61850" è avvenuta il 9/12/2022. Secondo le tempistiche di pubblicazione di IEC si prevede che sia disponibile/pubblicata al più tardi a luglio 2023. Gli enti di certificazione necessiteranno di qualche mese per predisporre le relative procedure di prova, per cui si ritiene che il periodo di dilazione potrebbe trovare ragionevolmente termine al 31 dicembre 2023. Qualora vi fossero riscontri oggettivi in merito alla impossibilità di rispettare questa scadenza, il Comitato riesaminerà la tempistica prevista che oggi appare coerente con le informazioni a disposizione.

T.3.3.4.9 Gestione delle chiavi e dei certificati secondo IEC 62351-9: è possibile gestire un CCI, in conformità a questo requisito, ma privo di connessione internet?

Sì, è possibile implementare un'architettura di sistema che permetta al CCI di utilizzare una PKI (Public Key Infrastracture), per la gestione sicura delle chiavi e dei certificati, senza accesso ad internet; ma non è una scelta raccomandabile, perché porta ad un livello di sicurezza inferiore, ad un maggior sforzo di manutenzione manuale ed in generale ad una minore affidabilità, rispetto ad un'architettura con accesso a internet.

Di conseguenza si raccomanda di ricorrere a queste architetture solo per impianti isolati, dove non è tecnicamente possibile realizzare una connessione a internet.

La norma CEI 0-16 richiede, al paragrafo T.3.3.4.9, che il CCI utilizzi una PKI (Public Key Infrastracture) per la gestione sicura delle chiavi crittografiche e dei certificati digitali, come indicato, e motivato, nella parte 9 della IEC 62351 "Cyber security key management for power system equipment".

L'utilizzo di una PKI è necessario per garantire che la cifratura dei dati scambiati dal CCI, e l'autenticazione degli attori autorizzati a connettersi, siano sicure e affidabili. La sicurezza e l'affidabilità fornita da certificati "self-signed", senza l'uso di una PKI, non sono né comparabili né sufficienti.

La PKI svolge molte funzioni diverse durante il ciclo vita di una chiave e di un certificato, tra cui molto importanti sono il Rinnovo, per garantire il funzionamento del CCI alla scadenza naturale, la Revoca, in caso l'identità digitale sia compromessa, e la Verifica di Validità, per controllare che il certificato della controparte non sia stato revocato.

La durata della validità dei certificati dev'essere concordata tra il Produttore ed il DSO, ed eventualmente l'Aggregatore, in base alle analisi dei rischi che ogni parte conduce. Occorre comunque considerare che più corta è la scadenza di un certificato, più è alto il livello di sicurezza fornito, e che la CEI 0-16, in linea con la IEC 62351-9, richiede di aggiornare la lista dei certificati revocati ogni 24h al massimo.

In uno scenario in cui il CCI **non** è connesso tramite internet ad una PKI pubblica, o dove la PKI è privata e locale e non connessa a internet, queste operazioni devono essere fatte manualmente dal manutentore, Svolgere queste operazioni manualmente è complesso, ed è ancora più difficile farlo in modo sicuro, senza compromettere la sicurezza delle chiavi e dei certificati durante il processo. Infatti le PKI pubbliche sul mercato

COMITATO
ELETTROTECNICO
ITALIANO

Via Saccardo, 9
20134 Milano
Tel. 02/21006.1
fax 02/21006.210 Direzione
fax 02/21006.222 Vendite
mail cei@ceinorme.it

sono pensate per interazioni automatiche con altri sistemi, e difficilmente sono dotate di interfacce utente grafiche e di semplice utilizzo, per tutte le funzioni necessarie, come ad esempio ottenere la lista dei certificati revocati e caricarla sul CCI.

Considerato questo, è evidente che un CCI che può accedere ad una PKI pubblica tramite internet può svolgere queste operazioni automaticamente, e quindi più frequentemente, fornendo un livello di sicurezza più elevato, un minore sforzo di manutenzione "manuale" ed una maggiore affidabilità.

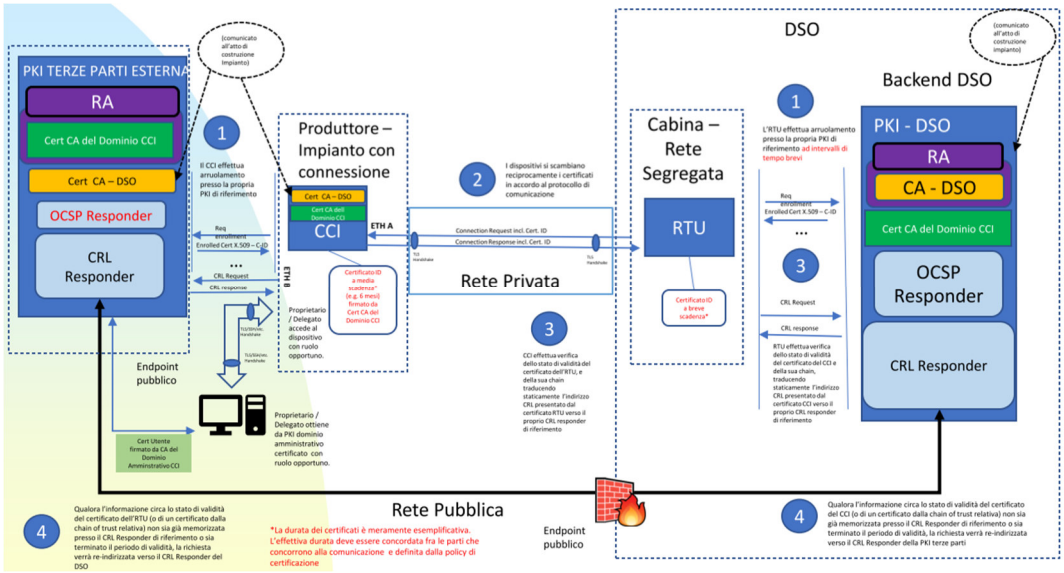
Di seguito sono presentate tre possibili architetture d'esempio, in tre diversi scenari:

1. CCI dotato di connessione ad una rete geografica e PKI terza parte connessa a internet
2. CCI privo di connessione geografica, PKI terza parte connessa a internet, aggiornamento totalmente manuale del CCI
3. CCI privo di connessione geografica, PKI locale non connessa a internet, PKI terza parte connessa a internet, aggiornamento manuale della PKI locale

Le tre architetture d'esempio mostrano come sia possibile implementare tutte le funzioni richieste da una gestione sicura delle chiavi e dei certificati utilizzando una PKI, nei tre diversi scenari, ma con diversi livelli di sicurezza, di sforzo di manutenzione manuale e di affidabilità.

Per le definizioni e le abbreviazioni si rimanda alla IEC 62351-9.

Caso 1: CCI dotato di connessione ad una rete geografica e PKI terza parte connessa a internet



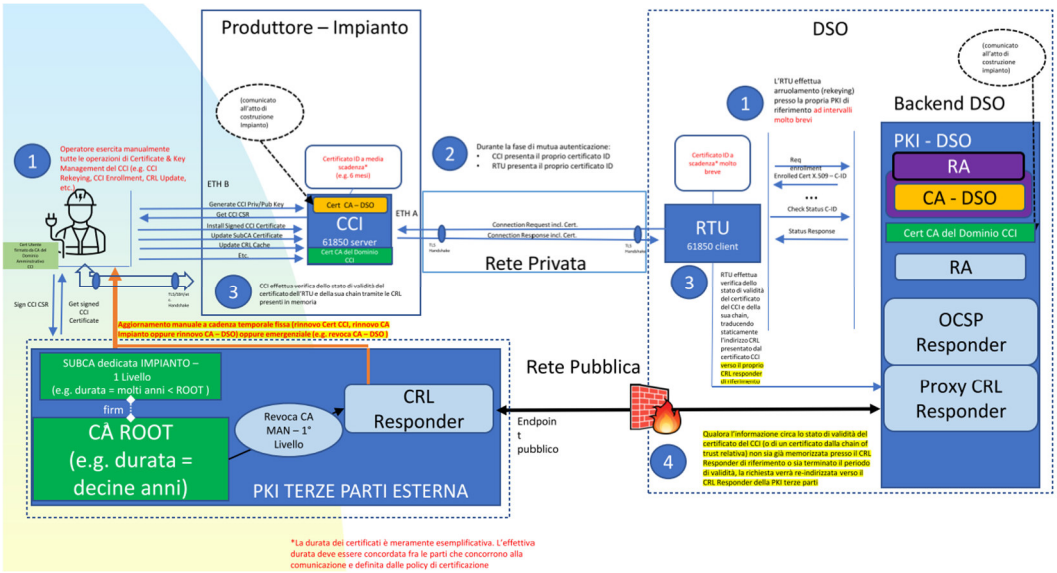
1: Mutua autenticazione CCI-RTU con entrambe le PKI pubbliche e connesse a internet

Questa soluzione offre un alto livello di sicurezza, e permette l'automatizzazione della gestione dell'intero ciclo vita delle chiavi e dei certificati. L'unica operazione manuale necessaria è lo scambio iniziale, tra Produttore e DSO, dei rispettivi certificati della *chain of trust*, cioè della catena delle CA che ha emesso il certificato "foglia" e che permette di considerarlo affidabile.

COMITATO
ELETTROTECNICO
ITALIANO

Via Saccardo, 9
20134 Milano
Tel. 02/21006.1
fax 02/21006.210 Direzione
fax 02/21006.222 Vendite
mail cei@ceinorme.it

Caso 2: CCI privo di connessione geografica, PKI terza parte connessa a internet, aggiornamento totalmente manuale del CCI



2: Mutua autenticazione CCI-RTU con CCI non connesso alla propria PKI esterna

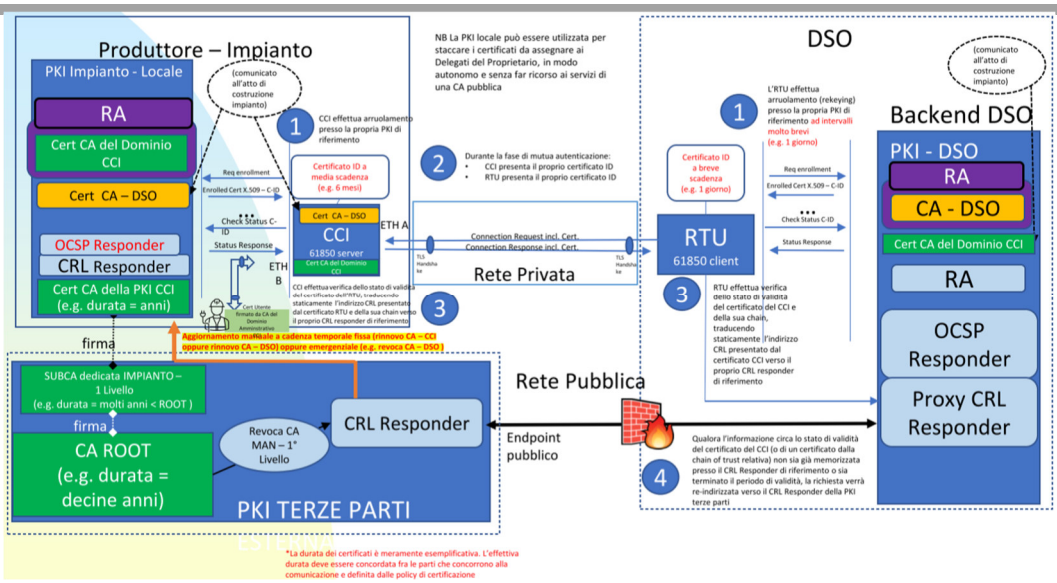
Questa soluzione richiede molte operazioni manuali, sia in fase di prima installazione che in fase di manutenzione del CCI, complesse da svolgere riuscendo a garantire la sicurezza dei certificati e delle chiavi.

In particolare si segnala la necessità di aggiornare manualmente il CCI sia a cadenza temporale fissa (e.g. 6 mesi), per il rinnovo dei certificati del CCI, della CA del CCI e della CA del DSO, sia in modo straordinario, ogni volta che un certificato viene revocato, non potendo soddisfare il requisito di aggiornamento della lista dei certificati revocati ogni 24 ore.

Caso 3: CCI privo di connessione geografica, PKI locale non connessa a internet, PKI terza parte connessa a internet, aggiornamento manuale della PKI locale

COMITATO
ELETTROTECNICO
ITALIANO

Via Saccardo, 9
20134 Milano
Tel. 02/21006.1
fax 02/21006.210 Direzione
fax 02/21006.222 Vendite
mail cei@ceinorme.it



3: *Mutua autenticazione CCI-RTU con CCI dotato di PKI locale e PKI esterna, non connesse tra loro*

Questa soluzione richiede di svolgere operazioni manuali meno frequentemente rispetto al caso 2, non essendo necessario aggiornare il CCI ogni volta che il suo certificato dev'essere rinnovato, a fronte però di un costo nettamente superiore, essendo basata su due distinte PKI, una locale ed una esterna, da mettere in piedi e manutenere.

Si segnala che in ogni caso è necessario aggiornare manualmente il CCI sia a cadenza temporale fissa (e.g.pochi anni), per il rinnovo dei certificati della CA del CCI e della CA del DSO, sia in modo straordinario, ogni volta che un certificato viene revocato, non potendo soddisfare il requisito di aggiornamento della lista dei certificati revocati ogni 24 ore.