

Controllore di Infrastruttura di Ricarica (CIR) per veicoli elettrici

Charging Infrastructure Controller (CIR) for electric vehicles



PAS

Sommario

La presente PAS fornisce la specifica di dettaglio dell'interfaccia logica di comunicazione tra un Controllore di Infrastruttura di Ricarica (CIR) per veicoli elettrici e un Operatore Remoto, ai fini dell'implementazione degli scambi informativi specificati dall'Allegato X della Norma CEI 0-21.

Rispetto all'edizione precedente, sono state apportate le modifiche tecniche necessarie per consentire l'utilizzo del protocollo MQTT per l'interfaccia di comunicazione CIR-RO.

DATI IDENTIFICATIVI

Norma CEI PAS 57-127

Classificazione CEI 57-127

RELAZIONI TRA DOCUMENTI

Riferimenti Nazionali PRJ-CEI 3614

Riferimenti Europei

Riferimenti Internazionali

Relazioni La presente Norma sostituisce totalmente la CEI PAS 57-127:2025 - Fascicolo 25976, che rimane applicabile fino al 31/01/2027.

Legenda: (EQV) Equivalente; (MOD) Modificata

INFORMAZIONI EDITORIALI

Pubblicazione PAS

Stato Edizione In Vigore

Entrata in vigore 01/08/2026

Fascicolo 26428

Comitato Tecnico CEI CT 57 | Scambio informativo associato alla gestione dei sistemi elettrici di potenza

Data di approvazione del Presidente del CEI 13/07/2026

Data di approvazione del CENELEC

Data di chiusura Inchiesta Pubblica CENELEC

ICS: 33.200

CEI richiama l'attenzione sulla possibilità che l'attuazione del presente documento possa comportare l'uso di uno o più brevetti o l'uso di diritti di proprietà intellettuale vantati da terzi.

CEI non assume alcuna posizione in merito alla fondatezza, validità o applicabilità di tali diritti rivendicati a riguardo. Alla data di pubblicazione del presente documento, CEI non aveva ricevuto notifica di uno o più brevetti e/o diritti di proprietà intellettuale vantati da terzi che potrebbero essere necessari per l'attuazione del presente documento.

Tuttavia, si avverte che tali informazioni potrebbero non essere aggiornate e si consiglia di consultare la lista dei brevetti disponibile su <https://www.ceinorme.it/>. CEI non potrà essere ritenuto responsabile per l'identificazione di alcuni o di tutti tali diritti brevettuali.



© CEI COMITATO ELETTROTECNICO ITALIANO - Milano 2026. Riproduzione vietata

Tutti i diritti sono riservati. Nessuna parte del presente Documento può essere riprodotta, messa in rete o diffusa con un mezzo qualsiasi senza il consenso scritto del CEI. Concessione per utente singolo. Le Norme CEI sono revisionate, quando necessario, con la pubblicazione sia di nuove edizioni sia di varianti. È importante pertanto che gli utenti delle stesse si accertino di essere in possesso dell'ultima edizione o variante.



PREFAZIONE

Questo documento CEI PAS 57-127:2026 costituisce un'estensione della Norma CEI PAS 57-127:2025 sviluppata dal Gruppo di Lavoro (GdL) PAS "Controllore di Infrastruttura di Ricarica (CIR) per veicoli elettrici", un gruppo congiunto a cui partecipano esperti dei seguenti Comitati Tecnici CEI:

- CT 57 (coordinatore) "Scambio informativo associato alla gestione dei sistemi elettrici di potenza";
- CT 13 "Misura e controllo dell'energia elettrica";
- CT 69 "Sistemi elettrici di trasferimento energia per veicoli stradali ed industriali (industrial trucks) alimentati elettricamente";
- CT 120 "Sistemi di accumulo di energia";
- CT 316 "Connessione alle reti elettriche di distribuzione Alta, Media e Bassa Tensione".

L'edizione CEI PAS 57-127:2025 rimane in vigore per un periodo di sei mesi dalla pubblicazione della presente edizione allo scadere del quale viene annullata e sostituita da questa edizione CEI PAS 57-127:2026.

L'edizione CEI PAS 57-127:2026 include le seguenti modifiche tecniche all'edizione precedente, necessarie al fine di consentire l'utilizzo del protocollo MQTT per l'interfaccia di comunicazione CIR-RO:

- estesa la lista degli acronimi (sezione 3.2);
- estesa la funzione di registrazione (sezione 5.2.1, sezione A.1) e di deregistrazione (sezione 5.2.6, sezione A.6);
- estesa la funzione di inizializzazione dell'interfaccia CIR-RO (sezione 5.2.2, sezione A.2.2, sezione B.2.2);
- introdotto il protocollo di comunicazione MQTT come alternativa al protocollo XMPP (sezione 6.2);
- introdotto il layer applicazione di MQTT (sezione 7.2);
- aggiornata la modellizzazione degli oggetti (sezione 7.3), il modello applicativo (sezione 7.4) e gli esempi di codifica JSON (sezioni C.4, C.5 e C.6);
- aggiornata la sezione TLS (sezione 8.1) e l'attivazione della comunicazione TLS (sezione 8.1.1);
- aggiornate le cipher suite (sezione 8.1.6);
- aggiunta l'autenticazione applicativa MQTT tramite CIR_ID nel certificato (sezione 8.3);
- aggiornate l'introduzione alle prove, i parametri di configurazione e i test di conformità (capitolo 9).

Questa CEI PAS 57-127:2026 ha validità di tre anni, al termine dei quali potrà essere estesa la sua validità per altri tre anni, senza possibilità di ulteriori proroghe, oppure trasformato in una *Technical Specification* (TS) o in una Norma in base ai riscontri di utilizzo.

Il testo di questa PAS include numerosi riferimenti a documenti di standard internazionali e/o di Norme italiane. Si precisa che, quando non diversamente specificato, il riferimento ad un documento di Norma o di standard è inteso all'ultima versione pubblicata.



INDICE

1	Scopo.....	6
2	Riferimenti Normativi	6
3	Attori e acronimi	9
3.1	Attori.....	9
3.2	Acronimi.....	10
4	Architettura di riferimento	11
4.1	Tecnologie dell'interfaccia di comunicazione CIR – RO.....	12
5	Casi d'uso	13
5.1	Business Use Case (BUC)	13
5.1.1	BUC-01: V1G	13
5.2	System Use Cases (SUC)	14
5.2.1	SUC-00: Registrazione CIR.....	14
5.2.2	SUC-01: Inizializzazione interfaccia CIR-RO	15
5.2.3	SUC-02: Invio misure e stati.....	16
5.2.4	SUC-03: Ricezione comandi.....	17
5.2.5	SUC-04: KeepAlive	18
5.2.6	SUC-05: Deregistrazione CIR.....	18
5.2.7	SUC-06: Perdita connessione	19
5.2.8	SUC-07: Aggiornamento configurazione	19
5.2.9	Macchina a stati	20
6	Modalità di comunicazione	22
6.1	Il protocollo XMPP	22
6.1.1	Schema architetturale	22
6.1.2	Indirizzamento	23
6.1.3	Comunicazioni XMPP	23
6.2	Il protocollo MQTT	27
6.2.1	Schema architetturale	27
6.2.2	Identificativo del client	28
6.2.3	Comunicazioni MQTT	28
7	Modello dati e scambi informativi.....	32
7.1	Livelli di presentazione e applicazione XMPP	32
7.2	Livelli di presentazione e applicazione MQTT	32
7.3	Modellizzazione e descrizione degli oggetti secondo IEC 61850.....	32
7.3.1	Modellizzazione degli oggetti secondo IEC 61850	32
7.3.2	Naming degli oggetti secondo IEC 61850	34
7.4	Modello applicativo	35
7.4.1	Application Data Unit - Misure Cicliche.....	35
7.4.2	Application Data Unit - Misure Spontanee	36
7.4.3	Application Data Unit – Stati e Allarmi.....	36
7.4.4	Application Data Unit – Comandi.....	38
7.4.5	Application Data Unit – Acknowledge comandi e misure.....	39
7.4.6	ErrorCode - Codice Invalidità delle misure	40
8	Cybersecurity	41
8.1	TLS	41
8.1.1	Attivazione della comunicazione TLS	41



8.1.2	Versioni del protocollo TLS	42
8.1.3	Autenticazione delle parti	42
8.1.4	Certificati digitali	42
8.1.5	Revoca dei certificati digitali.....	42
8.1.6	Cipher Suite	43
8.1.7	Chiavi Crittografiche.....	43
8.2	SASL per il protocollo XMPP	44
8.2.1	Certificati digitali	44
8.2.2	Regole di autenticazione	44
8.3	Autenticazione applicativa MQTT tramite CIR_ID nel certificato.....	45
8.4	PKI	45
8.4.1	Rinnovo dei certificati digitali.....	46
8.4.2	Lista di CA fidate.....	46
9	Prove di conformità e certificazioni	47
9.1	Formato test.....	47
9.2	Parametri di configurazione	48
9.3	Verifica Registrazione.....	49
9.3.1	Registrazione	49
9.3.2	Rinnovo del certificato.....	49
9.4	Verifica funzionamento in modalità asservita	49
9.4.1	Inizializzazione	49
9.4.2	Invio misure e stati	50
9.4.3	Ricezione comandi	51
9.4.4	KeepAlive	52
9.5	Verifica funzionamento in modalità autonoma	52
9.5.1	Ripresa connessione	52
9.5.2	Aggiornamento configurazione	53
	Bibliografia	54
	Allegato A – Casi d'Uso in formato standard IEC 62559-2.....	55
	Allegato B – Macchine a stati.....	86
	Allegato C – Esempi codifica JSON	93



CONTROLLORE DI INFRASTRUTTURA DI RICARICA (CIR) PER VEICOLI ELETTRICI

1 Scopo

Questo documento fornisce la specifica di dettaglio dell'interfaccia logica di comunicazione tra un Controllore di Infrastruttura di Ricarica per veicoli elettrici e un Operatore Remoto, ai fini dell'implementazione degli scambi informativi specificati dall'Allegato X della Norma CEI 0-21.

2 Riferimenti Normativi

<u>Pubblicazione</u>	<u>Titolo</u>	<u>Norme</u>
–	Allegato X - Controllore di Infrastruttura di ricarica per veicoli elettrici	CEI 0-21
–	Sistemi di misura dell'energia elettrica - Comunicazione con i dispositivi utente - Parte 2: Modello dati e livello applicativo	CEI TS 13-83
–	Sistemi di misura dell'energia elettrica - Comunicazione con i dispositivi utente - Parte 3-1: Profilo protocollare PLC nella banda 125 kHz - 140 kHz (banda C)	CEI TS 13-84
EN IEC 61850-7-2/A1	Reti e sistemi di comunicazione per l'automazione nell'ambito dei sistemi elettrici - Parte 7-2: Strutture di comunicazione di base - Livello di astrazione dell'interfaccia per i servizi di comunicazione (ACSI)	CEI 57-53
EN IEC 61850-7-4	Reti e sistemi di comunicazione per l'automazione nell'ambito dei sistemi elettrici - Parte 7-4: Strutture di comunicazione di base - Classi di nodi logici e classi di dati compatibili	CEI 57-55
EN IEC 61850-7-420	Reti e sistemi di comunicazione per l'automazione dei sistemi elettrici - Parte 7-420: Struttura di comunicazione di base - Nodi logici relativi alle risorse energetiche distribuite e all'automazione della distribuzione	CEI 57-76
EN IEC 61850-8-2	Reti e sistemi di comunicazione per l'automazione dei sistemi elettrici - Parte 8-2: Mappatura dei servizi di comunicazione specifici (SCSM) - Mappatura con XMPP (Extensible Messaging Presence Protocol)	CEI 57-112
EN IEC 62351-3	Gestione dei sistemi elettrici e scambio informativo associato - Sicurezza delle comunicazioni e dei dati - Parte 3: Profili che utilizzano TCP/IP	CEI 57-101
EN IEC 62351-9	Gestione dei sistemi di potenza e scambio informativo associato - Sicurezza dei dati e delle comunicazioni - Parte 9: Gestione delle chiavi di sicurezza informatica per le apparecchiature del sistema di potenza	CEI 57-108



<u>Pubblicazione</u>	<u>Titolo</u>	<u>Norme</u>
EN IEC 62559-2	Metodologia dei casi d'uso - Parte 2: Definizione del modello per i casi d'uso, l'elenco degli attori e l'elenco dei requisiti	CEI 8-16
EN 18031-1	Requisiti comuni di sicurezza per le apparecchiature radio - Parte 1: Apparecchiature radio connesse a Internet	CEI UNI 18031-1
IEC TR 61850-80-3	<i>Communication networks and systems for power utility automation - Part 80-3: Mapping to web protocols - Requirements and technical choices</i>	—
IEC TR 61850-90-8	<i>Communication networks and systems for power utility automation - Part 90-8: Object model for E-mobility</i>	—
IEC 62746-10-1	<i>Systems interface between customer energy management system and the power management system - Part 10-1: Open automated demand response</i>	—
IEC 63110-1	<i>Protocol for management of electric vehicles charging and discharging infrastructures – Part 1: Basic definitions, use cases and architectures</i>	—
IETF RFC 4422	<i>Simple Authentication and Security Layer (SASL)</i>	—
IETF RFC 5746	<i>Transport Layer Security (TLS) Renegotiation Indication Extension</i>	—
IETF RFC 6120	<i>Extensible Messaging and Presence Protocol (XMPP)</i>	—
IETF RFC 6121	<i>Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence</i>	—
IETF RFC 6122	<i>Extensible Messaging and Presence Protocol (XMPP): Address Format</i>	—
IETF RFC 6960 X.509	<i>Internet Public Key Infrastructure Online Certificate Status Protocol (OCSP)</i>	—
IETF RFC 7030	<i>Enrolment over Secure Transport</i>	—
IETF RFC 7590	<i>Use of Transport Layer Security (TLS) in the Extensible Messaging and Presence Protocol (XMPP)</i>	—
IETF RFC 8259	<i>The JavaScript Object Notation (JSON) Data Interchange Format</i>	—
ISO 15118-3:2015	<i>Road vehicles -- Vehicle to grid communication interface – Part 3: Physical and data link layer requirements</i>	—



<u>Pubblicazione</u>	<u>Titolo</u>	<u>Norme</u>
ISO 15118-20:2022	<i>Road vehicles - Vehicle to grid communication interface - Part 20: Network and application protocol requirements</i>	–
ISO/IEC 20922	<i>Information technology — Message Queuing Telemetry Transport (MQTT) v3.1.1</i>	–



3 Attori e acronimi

3.1 Attori

Tabella 3-1 – Attori

Attore	Definizione
CA	Certification Authority, soggetto che emette i certificati digitali e aggiorna le informazioni circa il loro stato di validità garantendo l'autenticità delle informazioni riportate mediante l'applicazione di firme digitali. Per la raccolta e la distribuzione delle informazioni si può servire del supporto di autorità separate e specializzate per questi compiti (es. RA e VA).
CIR	Controllore Infrastruttura di Ricarica, apparato destinato alla raccolta dati di potenza (scambiata con la rete e prelevata da CSI), allo scambio dati di potenza con RO, alla regolazione dinamica della potenza prelevata da rete per ricarica EV, alla fornitura di servizi di rete
CIR_USER	Utente CIR che si occupa dell'interazione (es. configurazione, aggiornamento, monitoraggio, ...) con il CIR tramite l'Interfaccia Uomo Macchina del CIR
CPO⁽¹⁾	Charging Point Operator, gestore dell'infrastruttura di ricarica (CSI)
CSI	Charging Station Infrastructure, Infrastruttura di Ricarica costituita da una o più stazioni di ricarica EV, collegate alla rete
EV	Electric Vehicle, veicolo elettrico
M1	Misuratore Intelligente al punto di consegna, tipicamente di seconda generazione (2G).
M2	Misuratore Intelligente, tipicamente di seconda generazione (2G), applicato ai generatori.
MSP	Mobility Service Provider, colui che vende il servizio di ricarica
RA	Registration Authority, soggetto designato da RO che conserva i dati di registrazione del CIR e verifica la sua identità. Raccoglie e verifica le informazioni che le parti interessate forniscono per l'inserimento all'interno di un certificato digitale. Se le verifiche hanno esito positivo la RA inoltra le informazioni alla CA per l'emissione del certificato digitale che verrà reso disponibile al richiedente. RA può essere co-situata presso l'autorità di certificazione (CA) di RO
RO	Remote Operator, soggetto esterno (Aggregatore/BSP per quanto riguarda la partecipazione ai mercati dei servizi di flessibilità; Distributore per l'eventuale controllo diretto in situazioni di emergenza o sulla base di specifici contratti di connessione flessibile) contrattualmente abilitato a comunicare da parte dell'Utente che ha installato il CIR
VA	Validation Authority, soggetto preposto alla verifica dello stato di validità dei certificati. Mette a disposizione le informazioni circa lo stato dei certificati digitali agli endpoint della comunicazione e, più in generale, a tutte quelle componenti di supporto, eventualmente presenti nell'architettura, che necessitano di queste informazioni (es. monitoraggio, ispezione). I servizi di OCSP responder e CRL distribution point, essenziali per il funzionamento del CIR, possono essere ricondotte a questa autorità. VA può essere co-situata presso l'autorità di certificazione (CA) di RO
XMPP_SERVER o MQTT_SERVER	Server dell'infrastruttura XMPP o MQTT presso cui il CIR è registrato

(1) Si ritiene utile evidenziare come un CPO: • in alcuni casi, possa non detenere la proprietà dell'infrastruttura di ricarica, ma occuparsi solo del funzionamento e della gestione di infrastrutture messe a disposizione da altri soggetti; • possa effettuare la vendita del servizio di ricarica al cliente finale sia in nome e per conto di un MSP (roaming), sia direttamente, cioè senza necessità di intermediazione da parte di un MSP.



3.2 Acronimi

Tabella 3-2 – Acronimi

Acronimo	Definizione
CEM	Customer Energy Manager
CN	Common Name
CRL	Certificate Revocation List
CSMS	Charging Station Management System
CSP	Charging Service Provider
CSR	Certificate Signing Request
EMMS	Elettro Mobility Management System
EST	Enrolment over Secure Transport
JSON	JavaScript Object Notation
MQTT	Message Queuing Telemetry Transport
MSF	Mercati dei Servizi di Flessibilità, ovvero dei servizi ancillari nazionali globali e locali, e dei servizi di ridispacciamento, ai sensi del Testo Integrato del Dispacciamento Elettrico (TIDE) dell'Autorità di Regolazione per Energia Reti e Ambiente (rif. Documento di Consultazione 685/2022/R/eel)
OCSP	Online Certificate Status Protocol
PAS	Public Available Specification
POD	Point of Delivery, punto di connessione alla rete elettrica
PKI	Public Key Infrastructure, infrastruttura di elaborazione e comunicazione che supporta l'erogazione del servizio di gestione dei certificati
TLS	Transport Layer Security
SAN	Subject Alternative Name
SASL	Simple Authentication and Security Layer
SoC	State of Charge, stato di carica di una batteria, pari al grado percentuale di riempimento rispetto alla capacità massima dell'accumulatore
V-to-G	Vehicle-to-Grid, l'interazione tra veicoli elettrici e sistema elettrico, che consente ai veicoli di erogare, tramite le infrastrutture di ricarica a cui sono connessi, servizi di riserva, bilanciamento, regolazione di frequenza e di tensione
V1G	Vehicle1Grid, caso particolare di V-to-G in cui il flusso di energia dalla rete elettrica al veicolo può essere variato di intensità, interrotto o anticipato/ritardato, ma non cambiare direzione (monodirezionale, dalla rete alla batteria del veicolo)
V2G	Vehicle2Grid, caso particolare di V-to-G in cui il flusso di energia può essere bidirezionale, cioè includere anche iniezioni di potenza dalla batteria del veicolo verso la rete
Wallbox	Dispositivo di ricarica adatto a piccole potenze
XEP	XMPP Extension Protocol
XMPP	Extensible Messaging and Presence Protocol

4 Architettura di riferimento

Esistono diverse opzioni per ricaricare i veicoli elettrici e ogni conducente è libero di scegliere come effettuare la ricarica:

- a) presso la propria abitazione o un posto auto ad uso esclusivo (ricarica in luogo privato ad uso individuale);
- b) presso infrastrutture di ricarica condivise tra un numero ristretto di utilizzatori, come quelle disponibili nei parcheggi interni del proprio luogo di lavoro o presso gli spazi condominiali, ove ciò sia consentito (ricarica in luoghi privati ad uso collettivo);
- c) presso le infrastrutture di ricarica in luoghi accessibili al pubblico, siano queste lungo le strade (“on-street charging” o “en-route charging”) oppure installate presso luoghi turistici o di interesse (es. strutture ricettive o commerciali, monumenti, stazioni, porti e aeroporti: “destination charging”).

Il presente documento riguarda esclusivamente le ricariche di tipo a) e b) effettuate in modalità V1G.

Le figure seguenti schematizzano le relazioni fra i principali attori.

Tipo a) Ricarica privata domestica

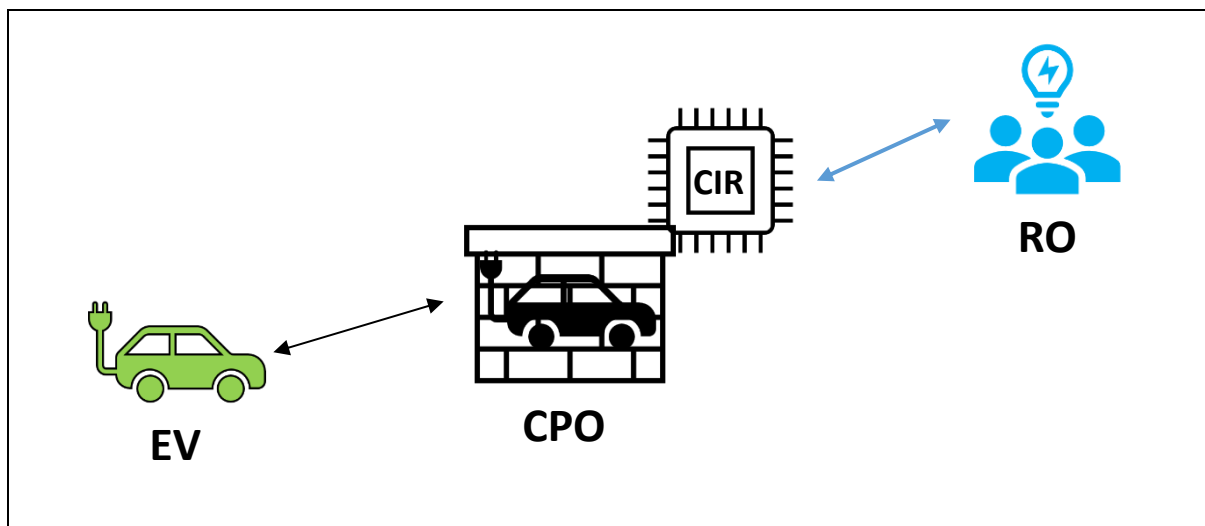


Figura 4-1 – Ricarica privata domestica

Nel caso della ricarica privata domestica, tipicamente il ruolo del CPO è assolto dal proprietario dell'abitazione. L'infrastruttura di ricarica è tipicamente costituita da una wallbox.

Tipo b) Ricarica privata non domestica

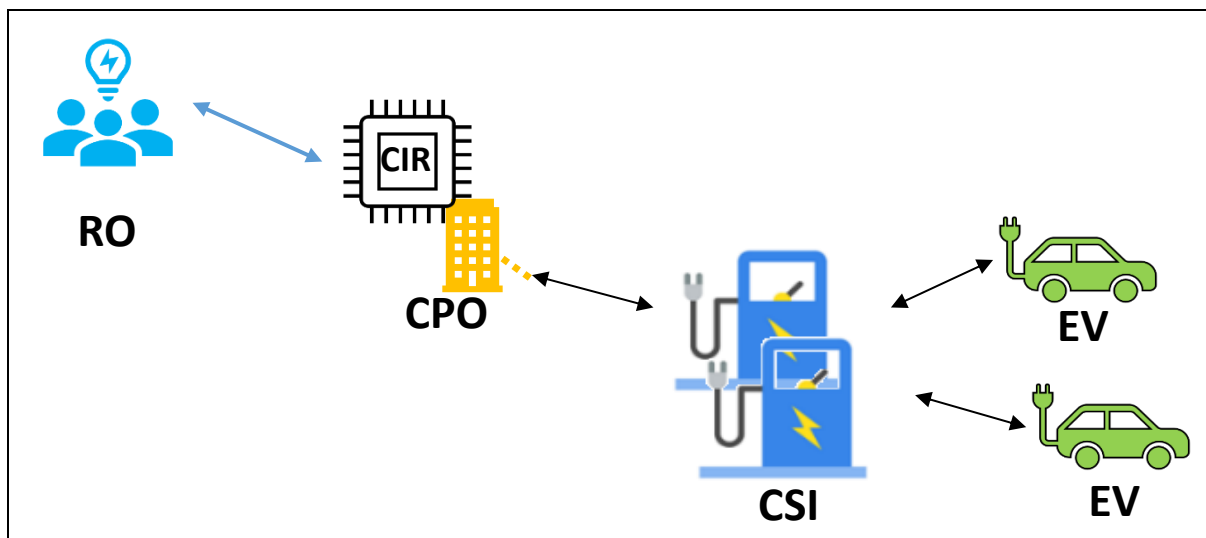


Figura 4-2 – Ricarica privata non domestica

Nel caso della ricarica privata non domestica, il ruolo del CPO è assolto dal soggetto che rende disponibile il servizio di ricarica privato (ad esempio: condominio, supermercato, hotel, azienda). Il CIR agisce da unica interfaccia di aggregazione con il RO per molteplici punti di ricarica.

4.1 Tecnologie dell'interfaccia di comunicazione CIR – RO

L'interfaccia di comunicazione CIR-RO è basata su protocollo di comunicazione XMPP o, in alternativa, MQTT basati sul livello di trasporto sicuro TLS.

Le rispettive architetture di rete sono presentate in Figura 4-3 e Figura 4-4.



Figura 4-3 – Interfaccia CIR-RO basata su protocollo XMPP

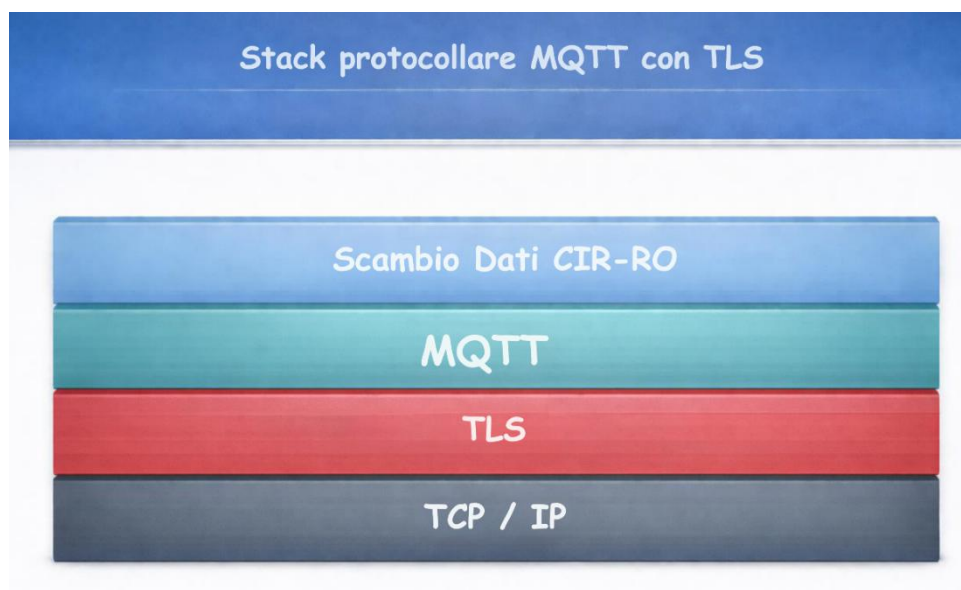


Figura 4-4 – Interfaccia CIR-RO basata su protocollo MQTT

5 Casi d'uso

5.1 Business Use Case (BUC)

5.1.1 BUC-01: V1G

Il Business Use Case 01 è relativo alla funzionalità di ricarica intelligente o smart charging del CIR (vedi Figura 5-1), la cui implementazione deve soddisfare i requisiti riportati in Tabella 5-1.

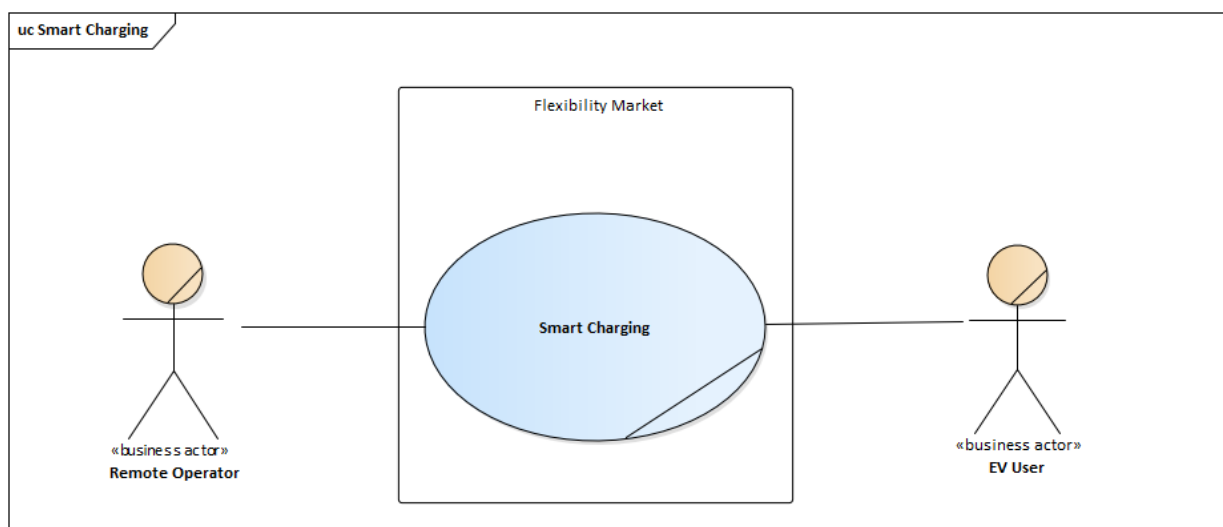


Figura 5-1 – Use Case Diagram

**Tabella 5-1 – Requisiti**

# Requisito	Descrizione
R1	Interoperabilità delle comunicazioni CIR-RO a fronte di molteplici tipologie di dispositivi che supportano la funzionalità di smart charging
R2	Cybersecurity delle comunicazioni CIR-RO a fronte di possibili minacce alla riservatezza, all'integrità e alla disponibilità dei dati
R3	Scalabilità dell'infrastruttura di aggregazione a fronte di un numero potenzialmente elevato di Infrastrutture di Ricarica
R4	Portabilità del servizio V1G da un Operatore ad un altro
R5	Volontarietà dell'utente di attivare o disattivare il servizio di smart charging
R6	Semplicità delle soluzioni che implementano gli scambi informativi a fronte di dispositivi di mercato caratterizzati da risorse hardware e software limitate

5.2 System Use Cases (SUC)

5.2.1 SUC-00: Registrazione CIR

L'obiettivo del System Use Case 00 relativo alla registrazione del dispositivo CIR è di attestare il dispositivo CIR presso un Operatore Remoto.

La procedura di registrazione garantisce il requisito di portabilità del servizio di flessibilità da un operatore ad un altro.

Al CIR viene fornito dal costruttore un certificato di pre-enrollment, Il CIR deve inoltre avere la capacità di generare chiavi crittografiche e CSR come specificato successivamente.

Nella stipula di un contratto di aggregazione con un RO, il CIR deve ricevere da quest'ultimo le seguenti informazioni che procede a inserire come propri parametri di configurazione:

- il nome di dominio (es. RO.tld) dell'endpoint EST o l'indirizzo IP e la relativa porta TCP;
- il certificato/i della CA dell'endpoint EST della PKI (Implicit TA);
- il nome di dominio del server (XMPP o MQTT) o l'indirizzo IP e la relativa porta TCP;
- l'identificativo CIR_ID, una stringa utilizzata dal RO per identificare univocamente il CIR, (ad esempio UUID - Universally Unique Identifier, IETF RFC 9562). Il formato del CIR_ID richiesto dal protocollo XMPP è il JabberID; per MQTT la stringa CIR_ID deve assumere una lunghezza massima compatibile con le dimensioni massime del Client_ID e del CN (Common Name);
- il JabberID del RO per XMPP e/o la stringa RO_ID per MQTT che identifica un client RO con cui il CIR scambierà i dati a conclusione del SUC-01.

A valle della configurazione di questi parametri di registrazione, il CIR utilizza il protocollo EST (Enrollment over Secure Transport, IETF RFC 7030) per eseguire la procedura di registrazione presso l'Autorità di Registrazione (RA) della PKI designata dal RO e ottenere il proprio certificato client valido per l'autenticazione al server (XMPP o MQTT):

- il CIR contatta l'endpoint /cacerts della PKI, validandolo con l'implicit TA installata sul dispositivo. Questo endpoint è pubblico, non ha bisogno di autenticazione da parte del client e chiamarlo significa scaricare tutta la serie di CA che si ritengono fidate (Explicit TA). Questa serie di CA verrà scaricata in formato pkcs7, in particolare verranno scaricati i certificati necessari all'identificazione del server (XMPP o MQTT) che il CIR dovrà installare in modo da poterli utilizzare per validare il certificato del server (XMPP o MQTT) al momento della connessione TLS (vedi paragrafo 8.4.2);
- il CIR genera e invia la richiesta CSR di firma del certificato all'endpoint /simpleenroll su canale protetto da TLS. Per la configurazione del profilo TLS da utilizzare si rimanda a quanto dettagliato nella Sezione 8.1. Il client CIR si autentica con il certificato fornito dal costruttore (certificato di preenrollment).



Nel caso in cui tale certificato non fosse disponibile, EST consente al CIR di autenticarsi utilizzando credenziali di tipo username/password la cui validità nel tempo o riutilizzabilità deve essere limitata lato RO per ragioni di sicurezza. IETF RFC 7030 raccomanda che la policy sugli attributi CSR venga reperita tramite l'endpoint EST/csrattrs. La richiesta di attributi CSR è facoltativa, ma le CA possono rifiutare le richieste di iscrizione che non sono codificate in base alla politica della CA della PKI complicando quindi l'emissione del certificato per il CIR. Si raccomanda quindi che il CIR implementi questo passaggio prima di generare e inviare la propria CSR. È comunque indispensabile che la CSR generata dal CIR contenga il CIR_ID in specifici campi: il JabberID nel campo SAN (Subject Alternative Name) per poter ottenere un certificato adatto alla connessione al server XMPP (come descritto nel Paragrafo 8.2.1) e/o l'identificativo univoco MQTT nel campo CN (Common Name) per connessioni al broker MQTT (come descritto nel Paragrafo 8.3).

La procedura di registrazione del CIR consiste nei seguenti passi:

- la RA elabora la richiesta CSR verificando l'identità del CIR utilizzando i dati di registrazione;
- se la richiesta CSR è valida, la RA invia una richiesta di creazione del certificato alla rispettiva CA. La CA genera e firma un certificato di chiave pubblica e lo invia alla RA, che lo invia al CIR;
- se la richiesta CSR non è valida, la RA non invierà alcuna richiesta alla CA;
- se il CIR riceve un certificato entro CSR time-out (vedi macchina a stati del SUC-00 nella sezione B.1), estrae e archivia il certificato ricevuto da RA ed esegue la procedura di inizializzazione specificata in SUC-01;
- se il CIR non riceve un certificato entro CSR time-out, invia una nuova richiesta CSR alla RA. La richiesta CSR può essere ripetuta un numero massimo di volte definito da CSR-max (vedi macchina a stati del SUC-00 nella sezione B.1).

Il certificato così ottenuto va utilizzato dal CIR in fase di autenticazione al server (XMPP o MQTT). All'interno del periodo di validità di questo certificato il protocollo EST con la procedura appena descritta va utilizzato dal CIR per la richiesta di rinnovo del certificato stesso, con la differenza che l'autenticazione del CIR non avverrà con il certificato fornito dal costruttore ma con il certificato di cui si chiede il rinnovo (vedi paragrafo 8.4.1).

In ogni momento il CIR risulta registrato presso una e una sola RA.

La registrazione del CIR presso RO rimane attiva fino alla richiesta di de-registrazione del CIR (SUC-05) a valle della cessazione del contratto con RO.

In questa fase è fondamentale che i certificati di pre-enrollment installati dal costruttore sul CIR vengano ritenuti validi dal server EST. In mancanza di un'autenticazione del CIR nei confronti del server EST non verrà rilasciato al CIR un certificato per la comunicazione con il server (XMPP o MQTT) e non sarà quindi possibile avviare le funzionalità di smart charging. Risulta pertanto necessario mantenere un registro di CA fidate firmatarie dei certificati costruttore accessibile a tutte le PKI incaricate di svolgere l'enrollment dei CIR, come descritto nel Paragrafo 8.4.2.

La specifica di dettaglio del SUC-00 si trova nella sezione A.1.

5.2.2 SUC-01: Inizializzazione interfaccia CIR-RO

Il System Use Case 01 definisce l'Inizializzazione dell'Interfaccia di Comunicazione CIR-RO.

Il CIR sta funzionando in modalità Autonoma: si creano le condizioni per il passaggio alla modalità Asservita (es. comando impartito tramite interfaccia utente, scadenza timer di riconnessione, completamento fase di registrazione).

Nel caso del protocollo XMPP il CIR attiva in sequenza:

- una connessione TCP con il server XMPP cui è registrato;



- uno stream XMPP sulla connessione TCP per la negoziazione della comunicazione sicura TLS;
- una comunicazione sicura tramite il protocollo TLS basata su mutua autenticazione e profilo TLS predefinito;
- uno stream XMPP sulla comunicazione TLS per la negoziazione dell'autenticazione SASL EXTERNAL;
- uno stream XMPP per il binding di risorsa, che rimane attivo per i successivi scambi informativi di livello applicativo ossia per la comunicazione di telecontrollo con il RO.

Nel caso del protocollo MQTT il CIR effettua in sequenza i seguenti passi:

- attiva una comunicazione sicura TLS basata su mutua autenticazione e profilo TLS predefinito con il server MQTT configurato;
- invia un pacchetto di controllo MQTT di tipo CONNECT indicando il proprio clientId;
- verifica il buon esito del passo precedente analizzando i contenuti del pacchetto di controllo di risposta CONNACK. La comunicazione rimane attiva per i successivi scambi informativi di livello applicativo ossia per la comunicazione di telecontrollo con il RO.

Il caso della Inizializzazione dell'Interfaccia di Comunicazione lato RO (SUC-01b) è del tutto analogo.

La specifica di dettaglio del SUC-01 si trova nella sezione A.2.

5.2.3 SUC-02: Invio misure e stati

L'obiettivo del System Use Case 02 è far pervenire periodicamente a RO i dati di misura di potenza istantanea e di stato di CSI, corretti e associati ai tempi di misura.

I dati di misura di potenza istantanea acquisiti da M1 (e da M2, se presente), e da CSI, unitamente allo stato di CSI, vengono trasmessi periodicamente a CIR, e da CIR vengono inoltrati a RO.

La procedura di invio misure e stati consiste nei seguenti passi.

- Il CIR riceve da M1 (Misuratore Intelligente 2G) i dati riportati nella Sezione X.7.1.2 dell'Allegato X alla CEI 0-21.
- Il CIR riceve da M2 (Misuratore Intelligente 2G) i dati riportati nella Sezione X.3 dell'Allegato X alla CEI 0-21.
- il CIR invia alla CSI una richiesta di ricezione dei dati riportati nella Sezione X.7.1.3.2 dell'Allegato X alla CEI 0-21.
- Il CIR riceve tali dati dal CSI.
- Il CIR invia a RO i dati aggregati di misura/stato ricevuti da M1, M2 e da CSI, ai dati sono associati il tempo di misura e un parametro di qualità del dato.

Le misure/stati inviati comprendono:

- potenza attiva istantanea prelevata da CSI (vedi Nota 1 e Nota 2);
- potenza attiva istantanea prelevata o immessa, rilevata dal misuratore intelligente 2G (M1);
- potenza attiva istantanea generata, se disponibile, rilevata dal misuratore intelligente 2G (M2);
- potenza disponibile;
- tempo residuo prima del distacco del limitatore;
- stato relativo alla infrastruttura di ricarica CSI (vedi Nota 3).

I dati di misura sono inviati ogni 20 secondi se CSI è nello stato Connesso.



In caso di ricezione corretta, RO invia una conferma di ricezione dati a CIR, che corrisponde ad un messaggio di Keep Alive.

Se la ricezione dati a RO non avviene correttamente, l'invio dei dati da CIR viene ripetuto dopo 2 secondi.

La ritrasmissione viene ripetuta fino a 5 volte.

Se dopo 5 ritrasmissioni la ricezione dati permane negativa, significa che il Keep Alive è fallito, che c'è un errore di comunicazione e che si ha una perdita di connessione.

NOTA 1 CSI ha il compito di convertire eventuali misure di corrente provenienti dalle EVSE in misure di potenza e di sommare tutti i dati in una sola misura di potenza aggregata da inviare a CIR.

NOTA 2 Le misure relative alle EVSE rilevate da CSI saranno conformi alle Norme applicabili (MID o altre).

NOTA 3 Lo stato di CSI è Connesso se almeno un EV è collegato ad una presa di EVSE, Non Connesso se non ci sono veicoli collegati, oppure Anomalia, se c'è un guasto.

La specifica di dettaglio del SUC-02 si trova nella sezione A3.

5.2.4 SUC-03: Ricezione comandi

Il System Use Case 03 descrive l'invio del Comando di Modulazione di Potenza (CMP) e/o di Sospensione della Ricarica dal RO al CIR.

L'obiettivo del System Use Case 02 è far pervenire al CIR il comando CMP (modulazione potenza di carica) e/o il comando di sospensione della carica in funzionamento Asservito, allo scopo di mantenere la potenza entro il limite massimo che può essere assorbito da rete.

Lo svolgimento del caso di uso prevede che il RO invii al CIR il CMP, Comando di Modulazione della Potenza, e/o il Comando di Sospensione. Il CMP è il valore della potenza massima da prelevare dalla Rete che l'Infrastruttura di Ricarica (CSI) governata dal CIR può utilizzare. Il CIR funziona in modalità Asservito.

Ai fini della partecipazione ai mercati MSF il RO coordina la distribuzione della potenza prelevata dalla rete dai vari CIR e da altre risorse di flessibilità, in base a informazioni e ordini provenienti da:

- altri RO;
- altri CIR;
- CEM, EMMS, CSMS, CSP;
- informazioni tariffarie;
- informazioni sullo stato della rete.

Dopo aver elaborato una distribuzione ottima di potenza sulle risorse di flessibilità disponibili, il RO invia al CIR un comando CMP con i dati indicati nella Sezione X.7.1.1.2 dell'Allegato X alla CEI 0-21 che possono comprendere:

- 1) modulazione della potenza massima dell'infrastruttura di ricarica CSI;
- 2) sospensione della ricarica della infrastruttura CSI.

Nel caso 1) il comando CMP include:

- potenza massima dell'infrastruttura di ricarica di X,xx kW per Y minuti, oppure
- potenza massima dell'infrastruttura di ricarica di X,xx kW fino alle hh:mm.

Nel caso 2) il comando CMP include:

- comando di sospensione della ricarica per "Y minuti", oppure
- comando di sospensione della ricarica "fino alle hh:mm".



Il CIR riscontra al RO la corretta ricezione del CMP, marcando il tempo della risposta.

Se il RO non riceve riscontro entro un time out YY si ha il fallimento dell'invio del CMP.

I comandi CMP consecutivi devono pervenire al CIR con cadenza temporale superiore al tempo Tatt, che corrisponde alla tempistica parametrizzabile per l'invio di comandi consecutivi al veicolo, per default pari a 30 secondi.

I comandi che pervenissero prima di tale tempo verranno scartati con segnalazione a RO attraverso il relativo messaggio di Acknowledge, secondo quanto descritto nel paragrafo 7.3.5.

Se l'utente decide di non aderire più al servizio, il CIR invia a RO un messaggio di passaggio allo stato di Non Abilitato al Servizio di Modulazione Potenza.

Se RO decide di interrompere la richiesta di Servizio Modulazione Potenza invia un messaggio al CIR di fine servizio (situazione diversa dalla sospensione della ricarica, che può essere una fase del servizio).

Per motivi di sicurezza andrà previsto che il CIR effettui una verifica sul JabberID del mittente e accetti esclusivamente comunicazioni originate dal RO con cui ha in attivo un contratto.

La specifica di dettaglio del SUC-03 si trova nella sezione A.4.

5.2.5 SUC-04: KeepAlive

Per non appesantire gli scambi informativi con traffico supplementare, ma far fronte alla necessità di identificare eventuali problemi di comunicazione, la funzionalità di KeepAlive viene implementata per mezzo di messaggi applicativi scambiati tra le parti. La procedura di KeepAlive viene gestita a livello di messaggi contenenti le misure inviate periodicamente (vedi SUC-02) a cui è associato un ACK a livello applicativo.

Nel caso si riscontrassero problemi alle comunicazioni il CIR esegue la procedura di perdita della connessione (vedi SUC-06).

La specifica di dettaglio del SUC-04 si trova nella sezione A.5.

5.2.6 SUC-05: Deregistrazione CIR

L'obiettivo del System Use Case 05 relativo alla deregistrazione definitiva del CIR presso RO è di interrompere l'aggregazione di un CIR dal RO con cui ha precedentemente stipulato il contratto di aggregazione al fine, per esempio, di permettere l'aggregazione con un nuovo RO.

Su iniziativa del RO, o su richiesta dell'utente CIR, viene eseguita la procedura di deregistrazione descritta nel seguito:

- RO chiede la revoca del certificato di connessione al server (XMPP o MQTT) del CIR alla CA che lo ha emesso; la revoca può impiegare un tempo variabile (es. giorni) sulla base del livello di servizio concordato tra RO e CA;
- il RO può decidere di cessare di accettare comunicazioni da parte del CIR anticipatamente alla diffusione dell'informazione relativa alla revoca del certificato del CIR (tramite CRL o OCSP), ad esempio filtrando il suo CIR_ID, in conformità con il contratto stipulato con l'utente CIR;
- la CA pubblica l'informazione di revoca tramite i meccanismi previsti da questa specifica (i.e. CRL e OCSP) che consentono agli attori di usufruirne per verificare l'abilitazione all'accesso all'infrastruttura;
- il CIR verifica periodicamente lo stato di revoca del proprio certificato mediante le soluzioni CRL o OCSP; la periodicità di questa verifica deve essere configurabile e allineata alla periodicità di emissione delle CRL (es. almeno giornaliera). Qualora il CIR determini che il proprio certificato è stato revocato per deregistrazione da parte del RO, passa in modalità autonoma terminando così eventuali connessioni attive verso i server dell'infrastruttura;



- sulla base di come è configurato, il CIR può eliminare le informazioni relative alla registrazione presso il RO dalla propria memoria. Questa funzionalità deve poter essere abilitata o disabilitata tramite un parametro configurabile nel dispositivo. Nel caso il CIR sia configurato per non eliminare attivamente le informazioni, queste verranno sovrascritte in occasione della successiva registrazione presso un RO.

Nel caso la richiesta di deregistrazione sia iniziativa dell'utente CIR, questi dovrà preventivamente contattare il RO con le modalità previste dal contratto, che non sono oggetto di questa specifica. Verrà quindi attivata la procedura sopra descritta. La specifica di dettaglio del SUC-05 si trova nella sezione A.6.

5.2.7 SUC-06: Perdita connessione

Il caso d'uso SUC-06 descrive le azioni che devono essere compiute in seguito alla perdita della connessione tra CIR e RO e passaggio alla modalità di funzionamento Autonoma del CIR.

La sessione fra CIR e RO è aperta e il CIR funziona in modalità "Asservita".

Sopravviene una interruzione del canale di comunicazione col RO, ad esempio segnalata dal SUC-04.

Sono possibili differenti casi:

- problemi nelle comunicazioni CIR – server (XMPP o MQTT);
- problemi nelle comunicazioni server (XMPP o MQTT) – RO;
- problemi in entrambe le comunicazioni;
- nel caso di più server (XMPP o MQTT): perdita di connessione tra uno o più server.

Il CIR passa in funzionamento "Autonomo".

Nella modalità di controllo autonoma, il CIR modula la potenza prelevata da CSI sulla base dei soli dati di potenza prelevata e immessa rilevati da M1 e sulla base di parametri impostati in precedenza dal gestore dell'impianto o dal progettista, tramite interfaccia locale o remota, ovvero operando la logica di *power management* descritta nell'Allegato X della Norma CEI 0-21.

Al fine di evitare l'intervento del sistema di protezione degli accumulatori dell'autoveicolo, l'invio di comandi consecutivi al veicolo avviene secondo un intervallo di tempo (Tatt) parametrizzabile tra 1 e 60 secondi con valore di default pari a 30 secondi. Il CIR tenta di ristabilire la connessione col RO ad intervalli prestabiliti.

Se il CIR ha perso la comunicazione con il server (XMPP o MQTT) il CIR rilancia la procedura di "Inizializzazione" descritta da SUC-01a (connessione tra CIR e server (XMPP o MQTT)).

Se RO rileva una perdita di connessione con il server XMPP rilancia la procedura di "Inizializzazione" descritta da SUC-01b (connessione tra RO e server XMPP o MQTT).

Se la procedura di inizializzazione va a buon fine, il CIR transita nella modalità "Asservita" altrimenti rimane nella modalità "Autonoma".

La specifica di dettaglio del SUC-06 si trova nella sezione A.7.

5.2.8 SUC-07: Aggiornamento configurazione

Il System Use Case 07 descrive l'aggiornamento della configurazione, e quindi dei parametri operativi, dell'Infrastruttura di Ricarica gestita dal CIR.

La sessione fra CIR e RO è aperta e il CIR funziona in modalità "Asservita".

L'Utente CIR vuole cambiare la configurazione di impianto.



A questo scopo l'Utente CIR, tramite l'Interfaccia Utente, invia al CIR il comando di passaggio alla modalità Autonoma (stop manuale).

Il CIR passa in modalità Autonoma.

L'utente CIR aggiorna la configurazione della CSI.

L'utente CIR aggiorna i parametri operativi della CSI nel CIR (oppure il CIR acquisisce automaticamente la nuova configurazione se abilitato a farlo).

Infine, l'Utente CIR, tramite l'Interfaccia Utente CIR, impartisce il comando di passaggio alla modalità Asservita.

La specifica di dettaglio del SUC-07 si trova nella sezione A.8.

5.2.9 Macchina a stati

L'Allegato B del presente documento riporta le macchine a stati rappresentative dei diversi casi d'uso dettagliati nell'Allegato A. Per facilitarne lettura e comprensione, tali macchine a stati sono state organizzate secondo logiche di raggruppamento funzionali.

Di seguito una breve descrizione per ciascuna delle macchine riportate in Figura 5-2.

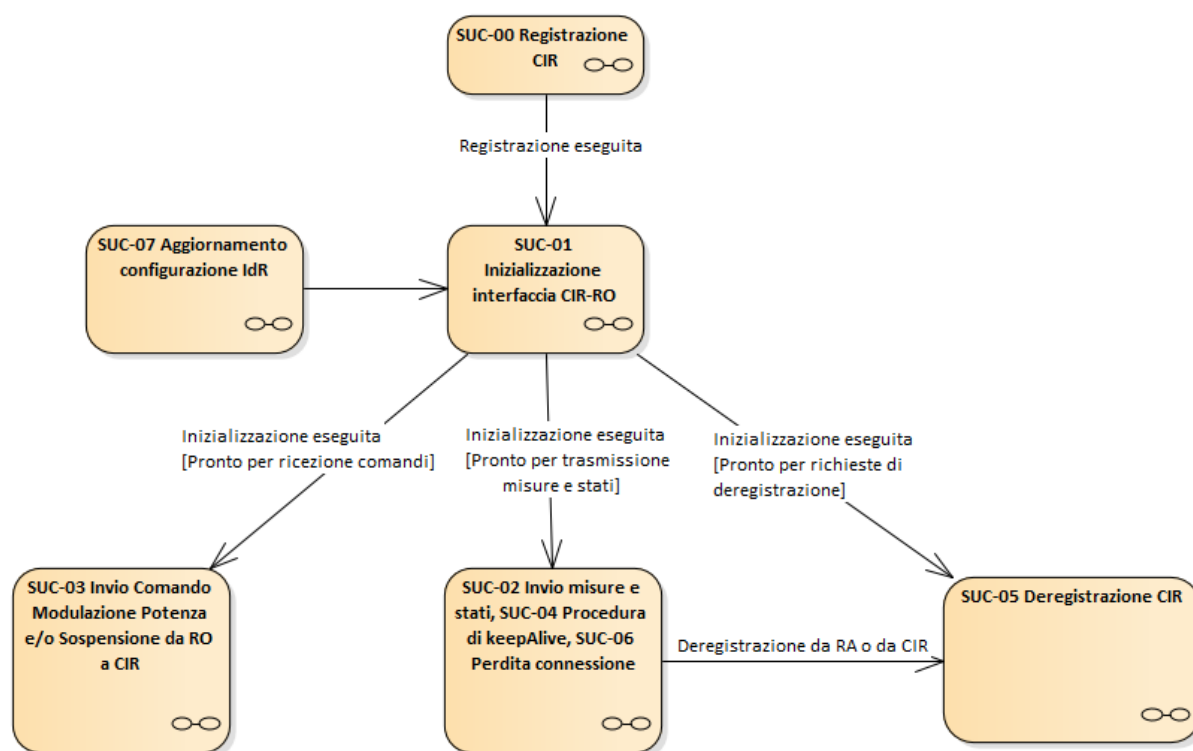


Figura 5-2 – Macchina a stati del CIR

SUC-00: Registrazione CIR

La macchina a stati rappresenta le operazioni necessarie alla registrazione del CIR partendo da una condizione preliminare di verifica sull'assenza del certificato e l'inserimento da parte dell'utente dei parametri di registrazione.

Il processo di registrazione termina con condizione di successo raggiungendo lo stato "Procedura di Inizializzazione [SUC-01]" descritto dalla relativa macchina a stati dedicata.



[SUC-01: Inizializzazione interfaccia CIR-RO](#)

La fase di inizializzazione viene raggiunta dopo che la registrazione è andata a buon fine. Il processo viene eseguito all'accensione e ripetuto periodicamente per verificare lo stato di validità del certificato.

In condizione di successo la macchina raggiunge il processo di invio periodico dei dati verso RO "SUC-02: Invio misure e stati".

[SUC-02: Invio misure e stati – SUC-04: Procedura di KeepAlive – SUC-06: Perdita connessione](#)

Per permettere una maggiore comprensione dei flussi nel meccanismo di invio di misure e dati, questa macchina a stati soddisfa diversi casi d'uso. All'interno del diagramma sono infatti descritti i flussi di invio misure e stati al RO, le logiche di verifica sullo stato di connessione con il server (XMPP o MQTT) (KeepAlive) e le relative contromisure (Modalità autonoma) in caso di perdita della connessione.

Nella tabella sottostante si riportano le condizioni che caratterizzano lo stato di funzionamento del CIR: le righe dalla 2 alla 7 descrivono le condizioni che determinano il passaggio dallo stato asservito allo stato autonomo.

Stop Manuale Attivo	Sottofrequenza	Connesso a RO	Funzionamento
No	No	Si	Asservito
No	No	No	Autonomo
Si	No	Si	Autonomo
No	Si	Si	Autonomo
Si	Si	No	Autonomo
No	Si	No	Autonomo
Si	No	No	Autonomo
Si	Si	Si	Autonomo

I comandi di modulazione che devono ancora essere eseguiti o che sono già in corso di esecuzione vengono revocati in condizione di stop manuale attivo e di sotto frequenza; vengono invece ancora considerati validi in caso di interruzione di comunicazione con RO.

Sono altresì presenti i rimandi ai SUC-00, SUC-01 e SUC-05 che sono trattati in dettaglio ciascuno da una macchina a stati dedicata.

[SUC-03: Invio del Comando di Modulazione di Potenza e/o di Sospensione dal RO al CIR](#)

Il diagramma viene interessato quando il controllore si trova nello stato "Pronto per la trasmissione" e ha pertanto completato la procedura di inizializzazione ed è connesso al server (XMPP o MQTT). Al ricevimento di comandi, il CIR abilita la modalità di funzionamento V1G dell'infrastruttura di ricarica asservendola al RO.

[SUC-05: Deregistrazione CIR](#)

Il diagramma descrive le due modalità di deregistrazione previste dal caso d'uso, ovvero quella avanzata dall'utente piuttosto che quella su iniziativa del RO. In entrambi i casi il CIR si disconnette dal RO e si pone in modalità autonoma di funzionamento.

[SUC-07: Aggiornamento configurazione della Infrastruttura di Ricarica gestita dal CIR](#)

Nell'eventualità di un aggiornamento di uno più parametri dell'infrastruttura di ricarica, il controllore viene interessato da un intervento manuale da parte dell'utente che interrompe la modalità asservita attraverso un comando (set) di stop manuale. La presa in carico dei nuovi parametri avviene al rilascio (reset) del comando di stop manuale e successiva esecuzione della procedura di inizializzazione.



6 Modalità di comunicazione

Nel seguito vengono presentate le caratteristiche di interesse dei protocolli XMPP e MQTT utilizzabili per l'implementazione delle comunicazioni CIR-RO specificate nell'Allegato X alla CEI 0-21.

6.1 Il protocollo XMPP

Il protocollo XMPP (Extensible Messaging and Presence Protocol) è nato come un insieme di tecnologie open per la messaggistica istantanea, le chat multi-parti, la segnalazione di presenza. È stato poi utilizzato in diversi settori in quanto rappresenta una soluzione efficace per lo scambio di informazioni in tempo reale. Precedentemente era conosciuto con il nome "Jabber" il cui progetto iniziò da parte di Jeremie Miller nel 1998 a cui seguì un primo rilascio pubblico nel 2000.

Il core della tecnologia comprende:

- un layer di streaming XML di base;
- crittografia del canale tramite Transport Layer Security (TLS);
- autenticazione avanzata tramite Simple Authentication and Security Layer (SASL);
- utilizzo di UTF-8 per il supporto completo di Unicode, inclusi gli indirizzi completamente internazionalizzati;
- informazioni integrate sulla disponibilità della rete ("presenza");
- sottoscrizione di presenza per autorizzazione bidirezionale;
- elenchi di contatti abilitati alla presenza ("roster").

L'insieme di protocolli di base che costituiscono l'XMPP è sviluppato dalla XMPP Standards Foundation (XSF) e sono stati adottati dall'IETF. In particolare, IETF RFC 6120 Extensible Messaging and Presence Protocol (XMPP) rappresenta la parte core del protocollo XMPP di streaming dell'XML, contiene gli aspetti di sicurezza e di internazionalizzazione, mentre IETF RFC 6121 Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence comprende le estensioni di base per la presenza quali le liste di contatti, la gestione delle sottoscrizioni e delle white/black list.

I protocolli XMPP non ancora adottati dall'IETF e ancora in parziale evoluzione sono definiti in XEP (XMPP Extension Protocol) dalla XSF.

6.1.1 Schema architetturale

XMPP è basato su un'architettura client/server in cui i diversi client comunicano tra loro attraverso uno o più server (nel caso i server non appartengano allo stesso dominio). Presenta similarità con altri protocolli applicativi quali ad esempio l'SMTP. In particolare, un client con un nome univoco comunica con gli altri client, anch'essi identificati con un nome univoco, per mezzo di uno o più server come mostrato in Figura 6-1. Ciascun nodo client implementa il modulo XMPP client del protocollo, mentre il server fornisce funzionalità di routing dei messaggi.

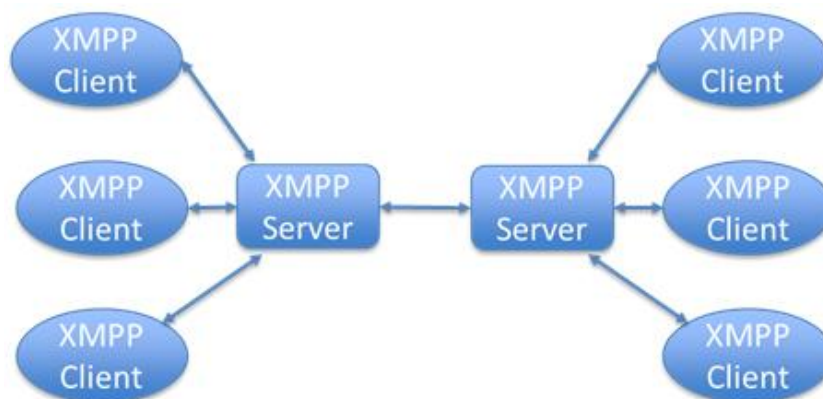


Figura 6-1 Architettura XMPP

6.1.2 Indirizzamento

L'indirizzamento all'interno dell'ecosistema XMPP avviene attraverso un Jabber Identifier (JID) il quale rappresenta l'identificativo del nodo, serve a collegarsi alla rete ed è simile a un indirizzo e-mail: nomeutente@esempio.com, ma può contenere tre parti invece di due. In particolare, nell'indirizzamento XMPP, la chiocciola @ è preceduta dal nodo (non obbligatorio) ed è seguita dal relativo server su cui è avvenuta la registrazione. Inoltre, opzionalmente, è possibile indicare una risorsa.

L'indirizzamento nella forma user@domain è detto bare JID, mentre se viene aggiunta la risorsa user@domain/resource è detto full JID.

6.1.3 Comunicazioni XMPP

Il protocollo XMPP è un protocollo relativamente semplice, si appoggia sullo stack TCP/IP e in particolare utilizza socket TCP per scambiare messaggi in formato XML. Comunica in maniera asincrona attraverso stream XML per mezzo di stanze XML (XML stanza). Uno stream XML permette di incapsulare uno scambio di informazioni in formato XML tra due diverse entità. Gli stream XML comunicano stanze XML, cioè unità discrete di informazione. Una stanza può essere utilizzata nel contesto XMPP per comunicare messaggi o stati di presenza.

La Figura 6-2 riporta un semplice esempio di comunicazioni XMPP in cui è possibile osservare l'apertura dello stream da parte di un client che funge da entità inizializzante lo stream (primo messaggio verde) che utilizza il campo "to" per identificare il dominio ricevente. Il client ricevente riceve il messaggio e risponde mediante un XML stream response (primo messaggio blu) utilizzando il campo "from". Successivamente è possibile effettuare diverse fasi di negoziazione, ad esempio per gli aspetti di sicurezza (autenticazione e cifratura). Terminata questa fase le due entità possono scambiarsi i messaggi. Le comunicazioni avverranno attraverso stanze. Esistono diversi tipi di stanza, come descritto nella sezione successiva. Terminata la comunicazione lo stream vien chiuso attraverso un messaggio da entrambe le parti (ultimi due messaggi in Figura 6-2).

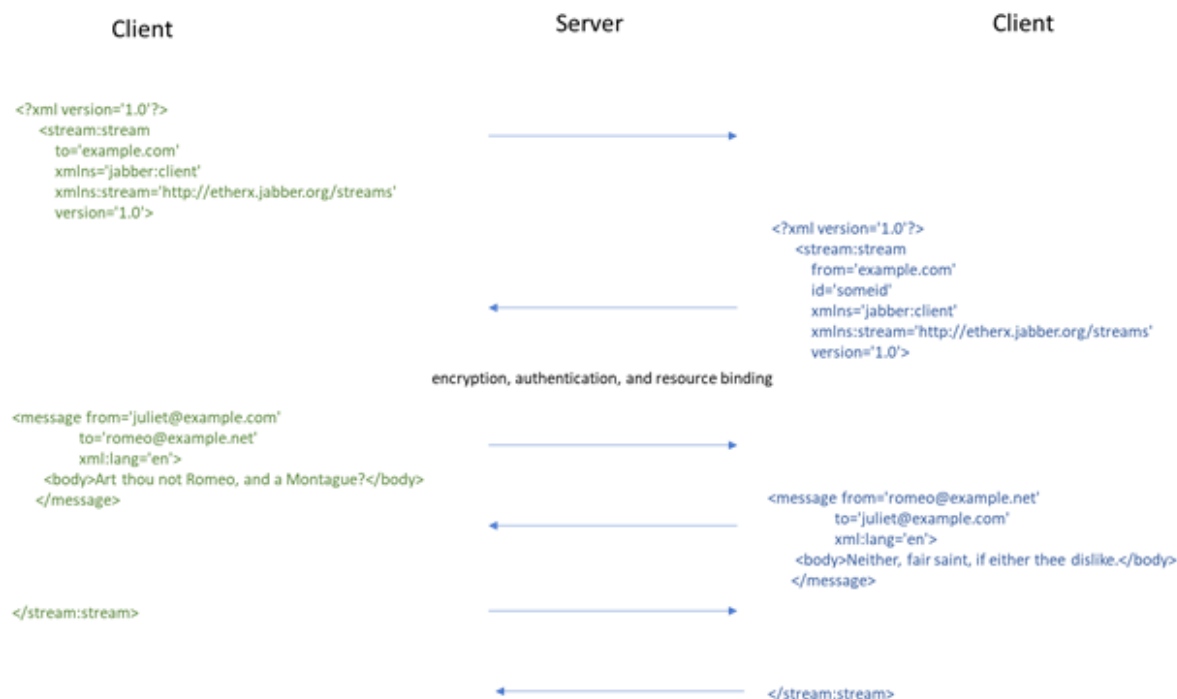


Figura 6-2 – Stream XMPP

6.1.3.1 Primitive di comunicazione

Come già anticipato l'unità base di informazione del protocollo XMPP è la stanza XML. Le stanze sono essenzialmente frammenti di XML che sono inviati su uno stream. Esistono tre tipi di stanza:

- message: utilizzata per messaggi generici;
- presence: per comunicare aggiornamenti di stato;
- iq (info/query): per comunicazioni richiesta-risposta.

Tutti i tipi di stanza condividono i seguenti attributi:

- id: utilizzato dal mittente per tracciare le risposte o eventuali errori relativi alla stanza;
- from: specifica l'indirizzo JID del mittente;
- to: specifica l'indirizzo JID del destinatario della stanza;
- type: specifica il contesto o il motivo della stanza message, presence o iq.

6.1.3.2 Pattern di comunicazione

I pattern di comunicazione descrivono le modalità con cui i messaggi possono essere trasportati nella rete e possono essere selezionati a seconda dei requisiti dell'applicazione in cui devono essere implementati.

Il protocollo XMPP prevede tre diversi pattern di comunicazione utilizzati per veicolare nel modo più appropriato i messaggi in base al contesto in cui questo sono scambiati.

Nel caso un client abbia necessità di ottenere informazioni da un altro client può utilizzare il paradigma **Request/Response**. È uno dei pattern tipici e più utilizzati in quanto permette a un client di richiedere informazioni ad un'altra entità. XMPP fornisce un metodo intrinseco per implementare il generico meccanismo richiesta/risposta attraverso l'utilizzo della stanza iq. Il destinatario del messaggio conosce chi ha originato la richiesta e il mittente è informato da chi ha ricevuto risposta.



Nel caso un client abbia necessità di inviare messaggi asincroni in tempo reale senza che vi sia stata una specifica richiesta, è possibile utilizzare i pattern **Asynchronous Messaging**. Questo può essere realizzato incapsulando il contenuto del messaggio in una stanza message. Il destinatario del messaggio è sempre informato di chi è il mittente.

Il pattern **Publish/Suscribe** permette di disassociare le comunicazioni rispetto allo stato dei client coinvolti. Viene utilizzato per la distribuzione di informazioni in maniera efficiente, riducendo il traffico di rete in quanto le informazioni destinate a più client vengono inviate solamente una volta al server che si occuperà di inviarle ai destinatari. Il client publisher pubblicherà sul server publish/subscribe le informazioni e i diversi client interessati (subscriber) riceveranno dal server le informazioni di loro pertinenza.

6.1.3.2.1 Asynchronous Messaging

In questa sezione viene approfondito il pattern Asynchronous Messaging selezionato per le comunicazioni tra CIR e RO. Questo tipo di pattern prevede un solo tipo di stanza: la stanza <message/> e consente di inviare il messaggio direttamente al client tramite uno o più server XMPP.

In particolare:

- se il destinatario è online, il server riceve il messaggio e lo inoltra al client di destinazione;
- se il destinatario è offline, il messaggio può essere memorizzato per una successiva consegna.

Il tipico formato di un messaggio asynchronous è il seguente:

```
<message from="utente1@server.com" to="utente2@server.com">
```

```
  <body>Questo è il contenuto del messaggio</body>
```

```
</message>
```

Ciascun CIR invia all'RO i messaggi contenenti le misure attraverso la stanza message come indicato in Figura 6-3. L'indirizzamento avviene attraverso la specifica del jabberid di destinazione, quello del RO, configurato nel CIR in fase di registrazione (vedi sezione 5.2.1). La conferma di ricezione della misura avverrà tramite apposito messaggio Acknowledge a livello di applicazione nel formato specificato in 7.4.5.

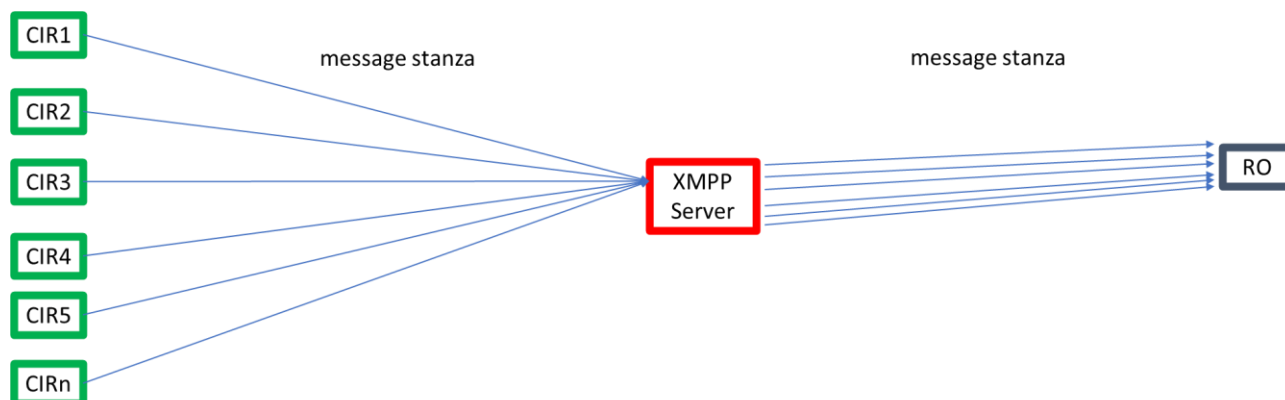


Figura 6-3 – Invio misure e stati



Nella Figura 6-4 viene rappresentato un dettaglio del formato del messaggio che il CIR invia per comunicare le misure. Il corpo del messaggio sarà strutturato secondo il formato JSON descritto nella Sezione 7.

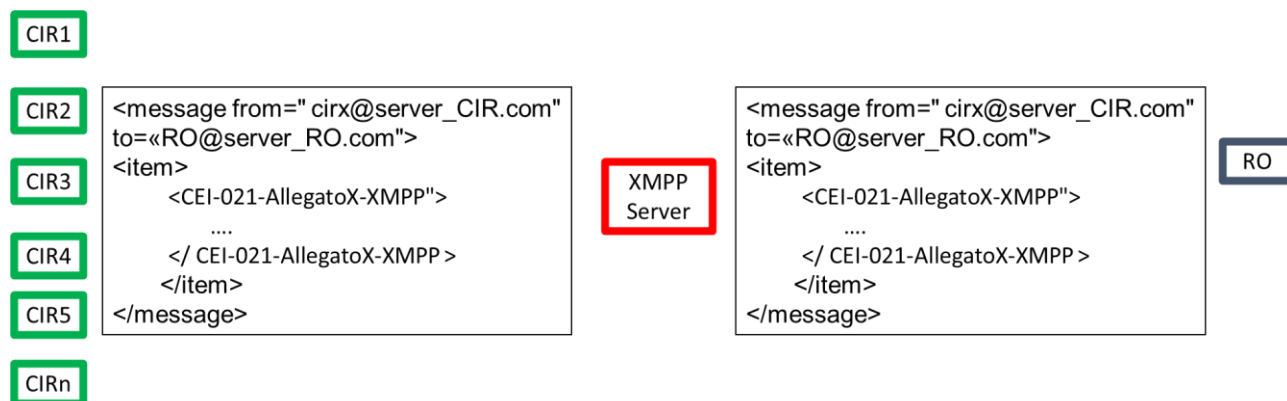


Figura 6-4 – Dettaglio messaggi Misure

Il RO invia i messaggi contenenti i comandi destinati a ciascun CIR coinvolto utilizzando la stanza message come mostrato in Figura 6-5.

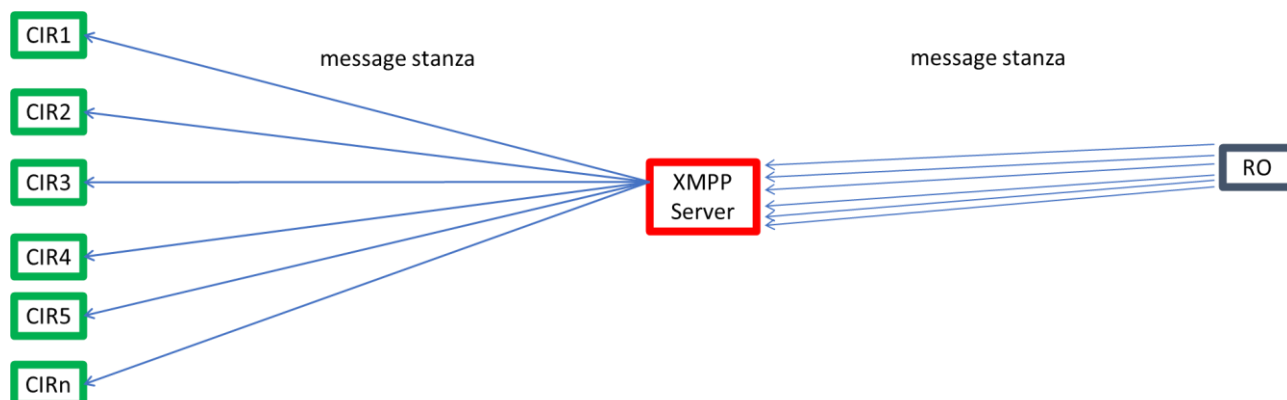


Figura 6-5 – Invio comandi

Il RO invia ai CIR un messaggio strutturato come in Figura 6-6. L'indirizzamento avviene attraverso la specifica del jabberid di destinazione, quello del CIR, conosciuto dal RO. La conferma di ricezione del comando avverrà tramite apposito messaggio Acknowledge a livello di applicazione nel formato specificato in 7.4.5.

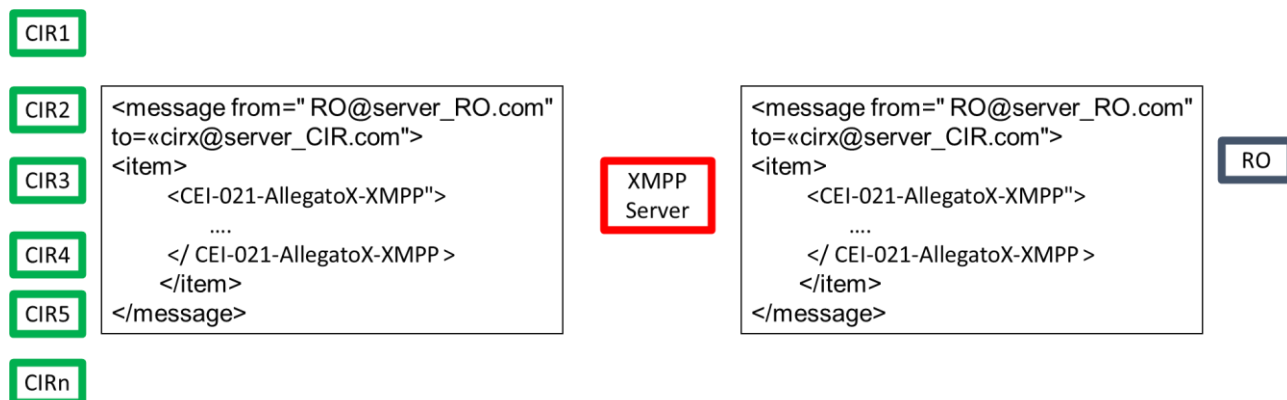


Figura 6-6 – Dettaglio messaggi Comandi

6.2 Il protocollo MQTT

MQTT (Message Queuing Telemetry Transport) è un protocollo di trasporto di messaggistica publish/subscribe per architettura client-server. Queste caratteristiche lo rendono ideale per l'uso in ambienti con risorse limitate.

Il protocollo è basato su TCP/IP, o su altri protocolli di rete bidirezionali. Le sue caratteristiche includono:

- l'uso del pattern di comunicazione publish/subscribe che supporta una distribuzione dei messaggi uno-a-molti e il disaccoppiamento delle applicazioni;
- un trasporto di messaggistica agnostico rispetto al contenuto del payload;
- il supporto di tre differenti livelli di Qualità di Servizio (QoS) per la trasmissione dei messaggi;
- l'utilizzo di topic come identificatori logici dei canali di comunicazione, espressi mediante stringhe di caratteri strutturate gerarchicamente secondo un modello ad albero e utilizzati dal broker per le operazioni di instradamento, filtraggio e distribuzione dei messaggi tra i client connessi.

La versione 3.1.1 del protocollo MQTT opera secondo le specifiche pubblicate da OASIS e standardizzate da ISO/IEC 20922.

I server (broker) basati su versioni MQTT superiori alla v3.1.1 devono garantire la retrocompatibilità con i client basati sulla versione v3.1.1. Il client MQTT del CIR deve essere sviluppato in modo da assicurare la compatibilità con la specifica MQTT versione 3.1.1 o superiori purché soddisfi tutte le funzioni definite in questo documento.

6.2.1 Schema architetturale

MQTT è basato su un'architettura client/server di tipo publish/subscribe in cui i diversi client (Publisher/Subscriber) comunicano tra loro attraverso un server (broker). Un client con un nome univoco (Client_ID) comunica con gli altri client, anch'essi identificati con un nome univoco, per mezzo di un server come mostrato in Figura 6-7. Ciascun nodo implementa il ruolo di client MQTT del protocollo, mentre il server fornisce funzionalità di routing dei messaggi.

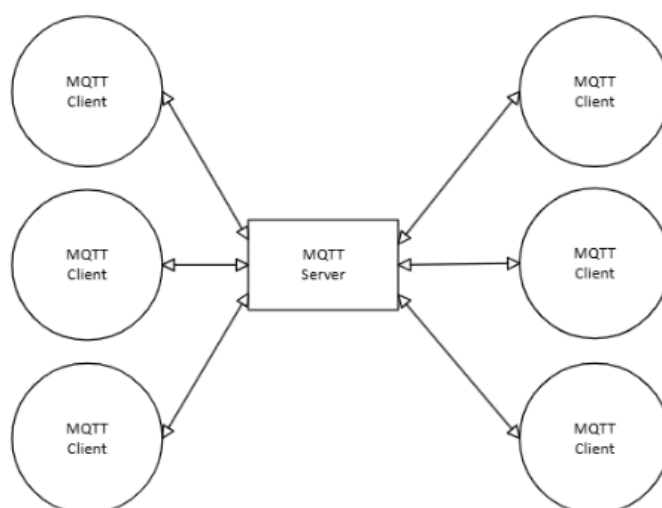


Figura 6-7 – Architettura MQTT

6.2.2 Identificativo del client

L'identificativo del client all'interno dell'ecosistema MQTT avviene attraverso un `Client_ID` il quale rappresenta il nodo ed è unico. Il `Client_ID` è caratterizzato da una stringa di caratteri alfanumerici. Il server MQTT (broker) utilizza il `Client_ID` per gestire le sessioni (es. nodo connesso/non connesso).

Il `Client_ID` utilizzato dal CIR e dal RO deve corrispondere, rispettivamente, al "`CIR_ID`" e al "`RO_ID`".

6.2.3 Comunicazioni MQTT

La comunicazione MQTT si basa sullo stack TCP/IP e prevede una serie di flussi di comunicazione e scambio messaggi di seguito descritti.

6.2.3.1 Flusso di apertura della connessione (CONNECT / CONNACK)

Ai fini dell'instaurazione di una sessione MQTT, il client avvia una connessione verso il broker tramite socket **TCP** su una porta impostata in fase di configurazione.

Una volta stabilito il canale TCP, il client trasmette il pacchetto **CONNECT**, contenente:

- identificativo del client (`Client_ID`)
- eventuali credenziali di autenticazione,

Il broker risponde mediante un pacchetto **CONNACK**, con il quale comunica l'esito dell'operazione di connessione, autorizzando o rifiutando l'accesso alla sessione. La sessione diviene attiva solo successivamente alla ricezione di tale conferma.

6.2.3.2 Flusso di pubblicazione dei messaggi (PUBLISH)

Nel corso della sessione attiva, il client può emettere un pacchetto **PUBLISH** indirizzato a un determinato *topic*. Il broker riceve tale pacchetto e provvede a:

1. validare il messaggio e il *topic* associato;
2. inoltrarlo a tutti i client registrati come subscriber del medesimo *topic*;
3. applicare il livello di *Quality of Service* (QoS) richiesto dal mittente in base ai requisiti di affidabilità del servizio. Il protocollo supporta tre livelli di QoS (0, 1 e 2), con meccanismi di conferma progressivamente più rigorosi.



6.2.3.3 Flusso di sottoscrizione (SUBSCRIBE / SUBACK)

Per poter ricevere informazioni su un determinato argomento, il client trasmette un pacchetto SUBSCRIBE, nel quale specifica uno o più *topic* di interesse.

Il broker risponde con un pacchetto SUBACK, con cui conferma la sottoscrizione e indica il livello di QoS concesso per ciascun *topic*. A partire da tale momento, il broker provvede all'inoltro verso tale client di tutti i messaggi PUBLISH compatibili con i *topic* sottoscritti.

6.2.3.4 Topic CIR

Per la comunicazione CIR-RO si utilizzano due distinti *topic*:

- *TopicCir* dedicato all'invio di misure/stati e risposte (Ack) del CIR verso RO;
- *TopicRo* dedicato all'invio di comandi e risposte (Ack) del RO verso il CIR.

Su *TopicCir* il CIR pubblica (publish):

- misure/stati;
- messaggi di conferma (Ack) relativi a comandi inviati precedentemente da RO sul *TopicRo*.

Sul *TopicRo* il CIR effettua una subscribe e resta in ascolto dei:

- comandi pubblicati dal RO;
- messaggi di conferma (Ack) inviati da RO relativi a misure/stati inviati in precedenza da CIR sul *TopicCir*.

I client CIR e RO ricoprono pertanto sia il ruolo di Publisher che di Subscriber.

- il client CIR è Publisher sul *TopicCir* e Subscriber sul *TopicRo*;
- il client RO è Publisher sul *TopicRo* e Subscriber sul *TopicCir*.

Il livello richiesto alla qualità di servizio QoS per la trasmissione dei messaggi CIR-RO è il livello 0.

I flag DUP e RETAIN dei messaggi PUBLISH devono assumere valore 0.

Di seguito si riporta una architettura del pattern publish/subscribe CIR-RO.

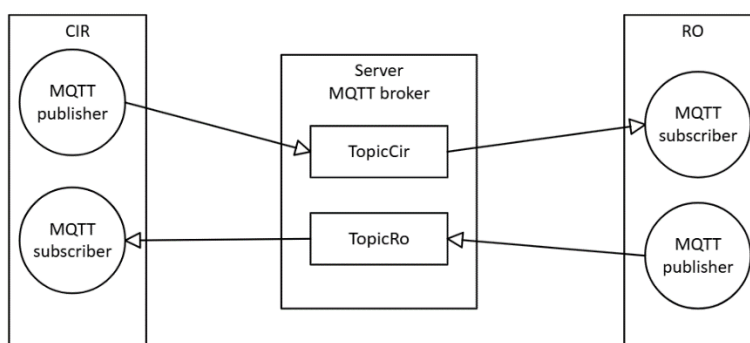


Figura 6-8 – Architettura Publish/Subscribe CIR-RO



L'identificativo del topic include sia chi invia sia chi riceve e deve rispettare la seguente sintassi:

- *TopicCir*: <RO_ID>/cir/<CIR_ID>
- *TopicRo*: <RO_ID>/ro/<CIR_ID>

dove “CIR_ID” e “RO_ID” sono identificativi univoci assegnati da parte di RO in fase di stipula di un contratto di aggregazione, come descritto nel SUC-00. Il parametro “CIR_ID” identifica in modo univoco il CIR. Il parametro “RO_ID” identifica in modo univoco un client RO² con cui il CIR scambierà i dati a conclusione del SUC-01.

Tutti i client con il ruolo di CIR invieranno messaggi al *TopicCir* (<RO_ID>/cir/<CIR_ID>) e riceveranno messaggi dal *TopicRo* (<RO_ID>/ro/<CIR_ID>) limitatamente al proprio identificativo “CIR_ID”.

Tutti i client con il ruolo di RO invieranno messaggi al *TopicRo* (<RO_ID>/ro/<CIR_ID>) e riceveranno messaggi dal *TopicCir* (<RO_ID>/cir/+) limitatamente al proprio identificativo “RO_ID”, dove il simbolo “+” viene utilizzato per indicare tutti le declinazioni di “CIR_ID”. La possibilità per il client RO di poter accedere contemporaneamente a tutti i dati pubblicati dai CIR attraverso la sottoscrizione al topic <RO_ID>/cir/+, evita al RO di dover creare tante subscribe quanti sono i CIR attestati sul broker.

Nel caso in cui sullo stesso broker dovessero attestarsi più RO sarà compito del broker stesso applicare le opportune regole di accesso alle risorse (CIR) sulla base del parametro <RO_ID>. Il broker avrà il compito di applicare le opportune policy per assicurare che ogni RO acceda soltanto ai messaggi scambiati con i CIR con i quali ha stipulato un contratto.

6.2.3.5 Applicazione alle comunicazioni CIR – RO

Con riferimento alla necessità da parte del CIR di comunicare al RO i dati di misura e di stato, il CIR rivestirà il ruolo di Publisher e l'RO di Subscriber come mostrato in Figura 6-9.

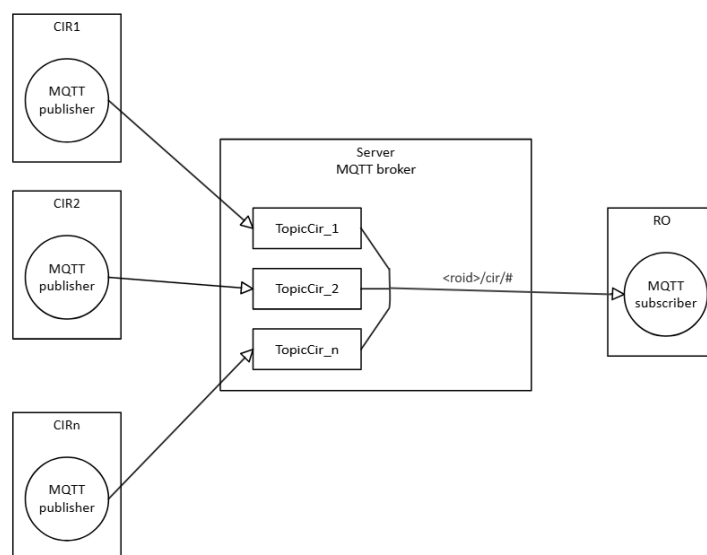


Figura 6-9 – Invio misure e stati

Un dettaglio del formato del messaggio contenente le misure cicliche pubblicato dal CIR e del relativo messaggio di Ack pubblicato dall'RO è presentato in Figura 6-10. Il corpo dei messaggi è codificato in formato JSON come descritto nella Sezione 7.

² Un'entità RO può avere più client RO per motivi architetturali o organizzativi.

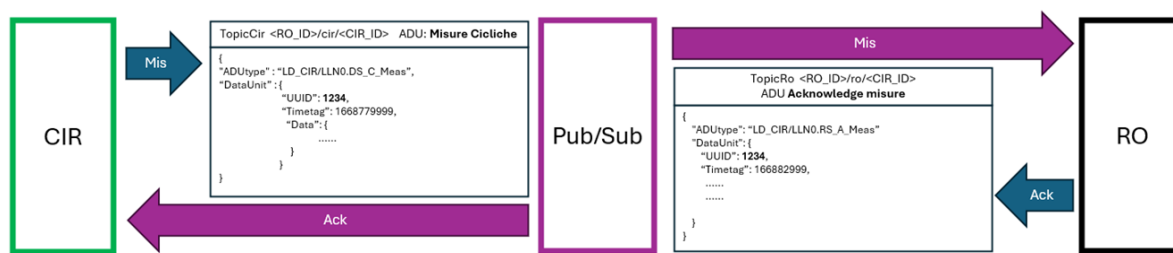


Figura 6-10 – Dettaglio messaggio Misure Cicliche

Per quanto riguarda i comandi i ruoli si invertono: RO ricopre il ruolo di publisher e il CIR di subscriber come mostrato in Figura 6-11.

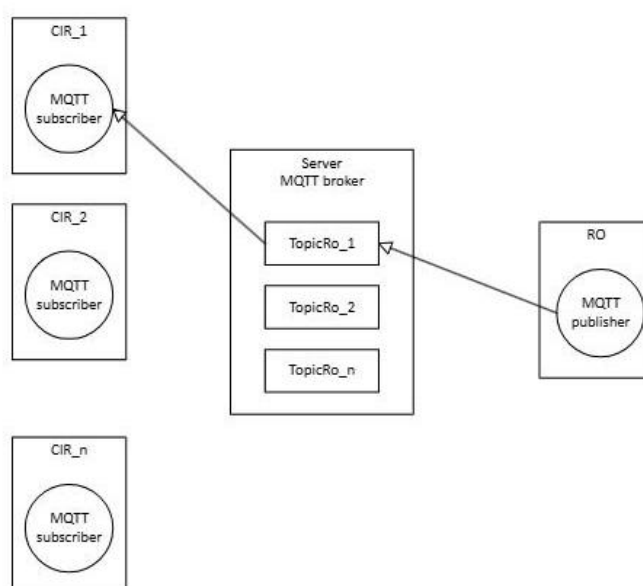


Figura 6-11 – Invio comandi

In Figura 6-12 sono riportate le strutture dei messaggi per la trasmissione e ricezione dei comandi. Il corpo dei messaggi è codificato in formato JSON come descritto nella Sezione 7.

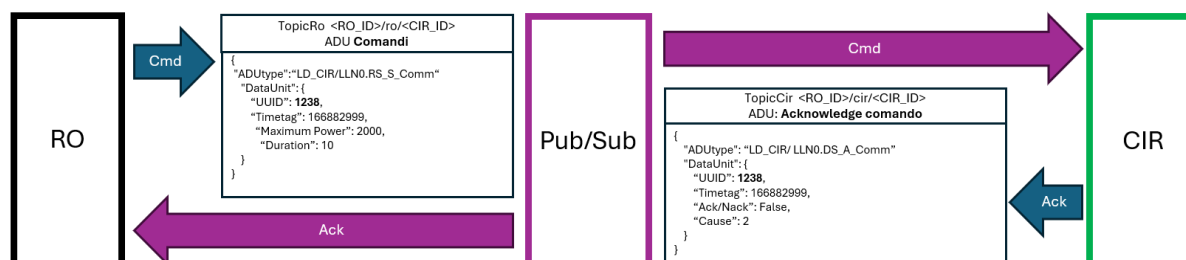


Figura 6-12 – Dettaglio messaggi Comandi



7 Modello dati e scambi informativi

7.1 Livelli di presentazione e applicazione XMPP

I messaggi applicativi per i dati inviati e ricevuti dal CIR attraverso XMPP nelle modalità definite nella Sezione 6.1, dovranno essere codificati a livello di presentazione, in linguaggio JSON in accordo con la IETF RFC 8259.

I dati del livello presentazione saranno quindi racchiusi in sezioni CDATA secondo standard XML, in modo da contenere *Application Data Unit* tra quelli definiti nella Sezione 7.4, uno per ogni sezione CDATA.

L'esempio seguente mostra la struttura dati XML corrispondente alla trasmissione di due *Application Data Unit* attraverso un unico messaggio.

```
<CEI-021-AllegatoX-XMPP">
  <CEI-021-AllegatoX-JSON>
    <![CDATA[
      ... Application Data Unit 1 ...
    ]]>
  </ CEI-021-AllegatoX-JSON >
  < CEI-021-AllegatoX-JSON >
    <![CDATA[
      ... Application Data Unit 2 ...
    ]]>
  </ CEI-021-AllegatoX-JSON>
</ CEI-021-AllegatoX-XMPP >
```

Per una descrizione dettagliata degli *Application Data Unit* e dei *Data Object*, si rimanda alla Sezione 7.4.

7.2 Livelli di presentazione e applicazione MQTT

Nel caso in cui il protocollo utilizzato sia l'MQTT, il contenuto applicativo dei messaggi inviati e ricevuti dal CIR sarà inserito nel payload dei pacchetti PUBLISH/SUBSCRIBE in formato JSON in accordo con la IETF RFC 8259.

L'associazione tra i topic MQTT e la tipologia di messaggio applicativo è specificata nel capitolo 6.2.5.

Il modello applicativo, gli *Application Data Unit* e i *Data Object* sono specificati nelle Sezioni 7.3 e 7.4.

7.3 Modellizzazione e descrizione degli oggetti secondo IEC 61850

7.3.1 Modellizzazione degli oggetti secondo IEC 61850

Il modello concettuale utilizzato per la descrizione delle informazioni gestite dal CIR è mutuato dalla Norma IEC 61850-7-2, di cui si applicano i seguenti oggetti informativi base:

- **Logical-Device (LD)** = Dispositivo logico, che raggruppa tutte le funzionalità coinvolte nello scambio informativo che si sta modellizzando, in questo caso il CIR;
- **Logical-Node (LN)** = Nodi logici, afferenti ad un Logical Device, raggruppanti dati di funzioni specifiche;
- **DATA Object (DO)** = Oggetti informativi caratterizzanti le funzioni, contenuti nei LN;
- **DATA Attribute (DA)** = Attributi informativi base costituenti i DATA Object;



- **DATA Set** = Raggruppamento di DO o DA trasmessi dal CIR attraverso gli *Application Data Unit*.

Per il raggruppamento dei dati dal Remote Operator al CIR è stato scelto di definire il seguente oggetto, non previsto dalla Norma IEC 61850:

- **RO DATA Set** = DO o DA trasmessi al CIR dal RO attraverso gli *Application Data Unit*.

Nella realizzazione del modello per il CIR, sono state applicati gli oggetti definiti dalla **IEC 61850-7-4** "Communication networks and systems for power utility automation - Part 7-4: Basic communication structure - Compatible logical node classes and data object classes", dalla **IEC 61850-7-420** "Part 7-420: Basic communication structure – Distributed energy resources and distribution automation logical nodes" e dalla **IEC 61850-90-8** "Communication networks and systems for power utility automation - Part 90-8: Object model for E-mobility", cui si rimanda per una trattazione più approfondita.

Nell'istanziamento dei LN sono stati utilizzati prefissi che richiassero il dispositivo o l'area di origine/destinazione delle informazioni contenute in essi: CSI per i dati riguardanti l'infrastruttura di ricarica, CIR per i dati riguardanti il dispositivo CIR in sé, M1 e M2 per i misuratori.

Il profilo IEC 61850 del modello dati CIR ottenuto è riportato nelle tabelle sottostanti.

Logical Device	Descrizione
LD_CIR	Contiene tutti i Logical Node relativi all'impianto monitorato/controllato dal CIR

Prefix	Logical Node	Descrizione LN	Data Object	Data Attribute
–	LLN0	Nodo Logico Zero	Loc	stVal
CSI	MMXU1	Misura	TotW	mag
M1	MMXU1	Misura	TotW	mag
M2	MMXU1	Misura	TotW	mag
M1	DWMX1	Definizione dei limiti di potenza di una DER	WMaxSpt	setMag
M1	DWMX1	Tempo residuo prima del distacco del limitatore	Ttli	operTimeout
CSI	DESE1	Monitoraggio e controllo di CSI	Beh	stVal
CSI	DAGC1	Modulazione di Potenza Attiva	Beh	stVal
CSI	DAGC1	Modulazione di Potenza Attiva	Flmod	stVal
–	LPHD	Informazioni su Device Fisico	PhyHealth	stVal
CIR	LTMS1	Informazioni sul sincronismo del Device Fisico	TmSynErr	stVal
CSI	DWMX1	Definizione dei limiti di potenza di una DER	WLimPctSpt	ctlVal
CSI	DWMX2	Definizione dei limiti di potenza di una DER	WLimPctSpt	ctlVal
CSI	DESE1	Monitoraggio e controllo di CSI	ClcStr	ctlVal
CSI	DESE2	Monitoraggio e controllo di CSI	ClcStr	ctlVal
CIR	GGIO1	Definizione di I/O fisici e logici generici	SPCSO1	ctlVal
CIR	QFVR1	Segnalazione di stato di sottofrequenza	UnHzStr	stVal



Dataset	Descrizione
DS_S_States	Dataset Stati e Allarmi - Invio Spontaneo
DS_C_Meas	Dataset Misure - Invio Ciclico
DS_S_Meas	Dataset Misure – Invio Spontaneo
DS_A_Comm	Dataset Acknowledge Comandi
RS_A_Meas	RO Dataset Acknowledge Misure
RS_S_Comm	RO Dataset Comandi

7.3.2 Naming degli oggetti secondo IEC 61850

A partire dal modello concettuale descritto nella Sezione 7.3.1, il *nome* di ciascun *Data Object* è stato definito seguendo le regole di costituzione dell'*ObjectReference* per i *DataAttribute*, ovvero *DataAttributeReference*, secondo Norma IEC 61850-7-2:

Nome *Data Object* = “LDName/LNName.DataObjectName.DataAttributeName”

Il *nome* degli *Application Data Unit* è stato definito applicando la definizione dei *DataSet Reference* e dell'attributo *DSRef* contenuto nella IEC 61850-7-2:

Nome *Application Data Unit* = “LDName/LNName.DataSetName”

La tabella dei nomi dei *Data Object* è la seguente:

Nome	Definizione
LD_CIR/CSIMMXU1.TotW.mag	Potenza attiva istantanea prelevata da CSI
LD_CIR/M1MMXU1.TotW.mag	Potenza attiva istantanea prelevata o immessa, rilevata da M1
LD_CIR/M2MMXU1.TotW.mag	Potenza attiva istantanea prelevata o immessa, rilevata da M2
LD_CIR/M1DWMX1.WMaxSpt.setMag	Potenza Disponibile
LD_CIR/M1DWMX1.Ttli.operTimeout	Tempo residuo prima del distacco del limitatore
LD_CIR/CSIDESE1.Beh.stVal	Stato dell'infrastruttura di ricarica CSI
LD_CIR/LLN0.Loc.stVal	CIR Asservito/Locale
LD_CIR/CSIDAGC1.Beh.stVal	Modulazione di Potenza On/Off
LD_CIR/CSIDAGC1.Flmod.stVal	Disponibilità di flessibilità della CSI
LD_CIR/LPHD.PhyHealth.stVal	Anomalia CIR
LD_CIR/CIRLTMS1.TmSynErr.stVal	Anomalia sincronizzazione CIR
LD_CIR/CSIDWMX1.WLimPctSpt.ctlVal	Comando Modulazione della potenza massima dell'infrastruttura di ricarica CSI, tipo 1
LD_CIR/CSIDWMX2.WLimPctSpt.ctlVal	Comando Modulazione della potenza massima dell'infrastruttura di ricarica CSI, tipo 2
LD_CIR/CSIDESE1.ClcStr.ctlVal	Comando di sospensione della ricarica, tipo 1
LD_CIR/CSIDESE2.ClcStr.ctlVal	Comando di sospensione della ricarica, tipo 2
LD_CIR/CIRGGIO1.SPCSO1.ctlVal	Comando di conferma ricezione pacchetto misure da RO
LD_CIR/CIRQFVR1.UnHzStr.stVal	Segnalazione di stato di sottofrequenza



La tabella dei nomi per le *Application Data Unit* (Dataset e RO Dataset) è la seguente:

Nome	Definizione
LD_CIR/LLN0.DS_S_States	Application Data Unit Stati e Allarmi
LD_CIR/LLN0.DS_C_Meas	Application Data Unit Misure Cicliche
LD_CIR/LLN0.DS_S_Meas	Application Data Unit Misure Spontanee
LD_CIR/LLN0.RS_A_Meas	Application Data Unit Acknowledge Misure Cicliche
LD_CIR/LLN0.RS_R_Comm	Application Data Unit Comandi
LD_CIR/LLN0.DS_A_Comm	Application Data Unit Acknowledge Comandi

7.4 Modello applicativo

L'organizzazione a livello applicativo è realizzata attraverso *Application Data Unit* che raggruppano, in base alle regole sintattiche JSON, le misure e gli stati che il CIR invia al centro remoto. Le *Application Data Unit* sono oggetti JSON (*ADUtype*) definiti a seconda dei dati che trasportano. Ognuna di esse contiene un oggetto (*DataUnit*) che raggruppa oggetti "figli" (*Data Object*) rappresentanti le misure o gli stati rilevati da campo. Nel seguito vengono definite le diverse tipologie di *Application Data Unit* delle comunicazioni CIR-RO.

7.4.1 Application Data Unit - Misure Cicliche

In accordo con le regole di costruzione definite nella Sezione 7.3.2, il nome dell'oggetto "ADUtype" è "LD_CIR/LLN0.DS_C_Meas" e raccoglie le misure inviate ciclicamente ogni 20 secondi all'operatore remoto. L'ADU Misure Cicliche deve essere sempre inviato nella sua interezza, includendo sempre tutti i Data Object di cui è formato con i relativi valori.

I valori da cui è costituito sono riportati nella tabella seguente.

Valori	Tipo JSON	Definizione
UUID	String	Universal Unique Identifier secondo ISO/IEC 9834-8
Timetag	Number	UTC in Secondi dal 1970-01-01 00:00:00 UTC come da formato Unix TimeStamp
Data	Object	Oggetto contenente l'insieme delle misure da trasmettere (Data Object)

L'oggetto "Data" a sua volta è costituito dall'insieme di oggetti (Data Object) definiti nelle tabelle seguenti.

- Potenza attiva istantanea prelevata da CSI: "LD_CIR/CSIMMXU1.TotW.mag"

Valori	Tipo JSON	Definizione
ValueN	Number	Valore in Watt
Invalidity	Number	Invalidità del dato trasmesso (Valido: 0, Invalido: 1, Discutibile: 2)
ErrorCode	Number	Codice di invalidità della misura ^(*)
Timetag	Number	UTC in Secondi dal 1970-01-01 00:00:00 UTC come da formato <i>Unix TimeStamp</i>
(*) Per una spiegazione dettagliata dell'ErrorCode per le misure, si faccia riferimento alla Sezione 7.4.6.		

- Potenza attiva istantanea prelevata o immessa, rilevata da M1: "LD_CIR/M1MMXU1.TotW.mag"

Valori	Tipo JSON	Definizione
ValueN	Number	Valore in Watt
Invalidity	Number	Invalidità del dato trasmesso (Valido: 0, Invalido: 1, Discutibile: 2)
ErrorCode	Number	Codice di invalidità della misura
Timetag	Number	UTC in Secondi dal 1970-01-01 00:00:00 UTC come da formato <i>Unix TimeStamp</i>



- Potenza attiva istantanea generata, rilevata da M2: “LD_CIR/M2MMXU1.TotW.mag”

Valori	Tipo JSON	Definizione
ValueN	Number	Valore in Watt
Invalidity	Number	Invalidità del dato trasmesso (Valido: 0, Invalido: 1, Discutibile: 2)
ErrorCode	Number	Codice di invalidità della misura
Timetag	Number	UTC in Secondi dal 1970-01-01 00:00:00 UTC come da formato <i>Unix TimeStamp</i>

- Potenza Disponibile: “LD_CIR/M1DWMX1.WMaxSpt.setMag”

Valori	Tipo JSON	Definizione
ValueN	Number	Valore in Watt
Invalidity	Number	Invalidità del dato trasmesso (Valido: 0, Invalido: 1, Discutibile: 2)
ErrorCode	Number	Codice di invalidità della misura
Timetag	Number	UTC in Secondi dal 1970-01-01 00:00:00 UTC come da formato <i>Unix TimeStamp</i>

7.4.2 Application Data Unit - Misure Spontanee

Il nome dell'oggetto “ADUtype” è “LD_CIR/LLN0.DS_S_Meas” in accordo con le regole di costruzione definiti nel Sezione 7.2 e raccoglie le misure inviate tramite procedura di invio spontaneo all'operatore remoto. I valori da cui è costituito sono i seguenti:

Valori	Tipo JSON	Definizione
UUID	String	<i>Universal Unique Identifier</i> secondo ISO/IEC 9834-8
Timetag	Number	UTC in Secondi dal 1970-01-01 00:00:00 UTC come da formato <i>Unix TimeStamp</i>
Data	Object	Oggetto contenente l'insieme delle misure da trasmettere (Data Object)

- Tempo residuo prima del distacco del limitatore: “LD_CIR/M1DWMX1.Ttli.operTimeout”

Valori	Tipo JSON	Definizione
ValueN	Number	Tempo in secondi
Invalidity	Number	Invalidità del dato trasmesso (Valido: 0, Invalido: 1, Discutibile: 2)
ErrorCode	Number	Codice di invalidità della misura
Timetag	Number	UTC in Secondi dal 1970-01-01 00:00:00 UTC come da formato <u>Unix TimeStamp</u>

7.4.3 Application Data Unit – Stati e Allarmi

Il nome dell'oggetto “ADUtype” è “LD_CIR/LLN0.DS_S_States” in accordo con le regole di costruzione definiti nel Sezione 7.2 e raccoglie gli stati e gli allarmi che il CIR invia, tramite procedura spontanea, all'operatore remoto. Il CIR invierà all'operatore remoto solo le informazioni dell'ADU che hanno subito una variazione di stato rispetto all'invio precedente. I valori di cui è costituito sono i seguenti:

Valori	Tipo JSON	Definizione
UUID	String	<i>Universal Unique Identifier</i> secondo ISO/IEC 9834-8
Timetag	Number	UTC in Secondi dal 1970-01-01 00:00:00 UTC come da formato <i>Unix TimeStamp</i>
Data	Object	Oggetto contenente l'insieme degli stati da trasmettere (Data Object)



I valori di cui è costituito sono i seguenti:

- Stato relativo alla infrastruttura CSI: “LD_CIR/CSIDESE1.Beh.stVal”

Valori	Tipo JSON	Definizione
ValueN	Number	Codice numerico indicante lo stato dell'infrastruttura
Invalidity	Boolean	Invalidità del dato trasmesso (Valido: 0, Invalido: 1)
Timetag	Number	UTC in Secondi dal 1970-01-01 00:00:00 UTC come da formato Unix TimeStamp

I numeri che compaiono nel campo “ValueN” indicanti lo stato dell'infrastruttura hanno il seguente significato, valido sia per infrastrutture a singolo punto di ricarica, sia per infrastrutture con numerosi punti di ricarica:

“ValueN”	Descrizione
0	Almeno 1 EV connesso, possibilità di mandare comandi
1	Nessun EV connesso, impossibilità di mandare comandi
2	Generico allarme dall'infrastruttura, impossibilità di mandare comandi

- CIR Asservito/Locale: “LD_CIR/LLN0.Loc.stVal”

Valori	Tipo JSON	Definizione
ValueB	Boolean	True: Asservito, False: Locale
Invalidity	Boolean	Invalidità del dato trasmesso (Valido: 0, Invalido: 1)
Timetag	Number	UTC in Secondi dal 1970-01-01 00:00:00 UTC come da formato <i>Unix TimeStamp</i>

- Modulazione di Potenza On/Off: “LD_CIR/CSIDAGC1.Beh.stVal”

Valori	Tipo JSON	Definizione
ValueB	Boolean	True: Mod. Potenza On, False: Mod. Potenza Off
Invalidity	Boolean	Invalidità del dato trasmesso (Valido: 0, Invalido: 1)
Timetag	Number	UTC in Secondi dal 1970-01-01 00:00:00 UTC come da formato <i>Unix TimeStamp</i>

- Disponibilità di flessibilità CIR: “LD_CIR/CSIDAGC1.Flmod.stVal”³

Valori	Tipo JSON	Definizione
ValueB	Boolean	True: Disponibile, False: Non disponibile
Invalidity	Boolean	Invalidità del dato trasmesso (Valido: 0, Invalido: 1)
Timetag	Number	UTC in Secondi dal 1970-01-01 00:00:00 UTC come da formato <i>Unix TimeStamp</i>

- Anomalia CIR: “LD_CIR/LPHD.PhyHealth.stVal”

Valori	Tipo JSON	Definizione
ValueB	Boolean	True: CIR in Anomalia, False: CIR funzionante
Invalidity	Boolean	Invalidità del dato trasmesso (Valido: 0, Invalido: 1)
Timetag	Number	UTC in Secondi dal 1970-01-01 00:00:00 UTC come da formato <i>Unix TimeStamp</i>

³ La Disponibilità di flessibilità CIR è determinata dalla volontà da parte dell'utente di partecipare o meno alla flessibilità attraverso il comando di stop manuale disponibile nell'interfaccia utente del CIR



- Anomalia Sincronizzazione CIR: “LD_CIR/CIRLTMS1.TmSynErr.stVal”

Valori	Tipo JSON	Definizione
ValueB	Boolean	True: Anomalia sincronismo, False: Sincronismo funzionante
Invalidity	Boolean	Invalidità del dato trasmesso (Valido: 0, Invalido: 1)
Timetag	Number	UTC in Secondi dal 1970-01-01 00:00:00 UTC come da formato <i>Unix TimeStamp</i>

- Stato di funzionamento CIR in sottofrequenza: “LD_CIR/CIRQFVR1.UnHzStr.stVal”

Valori	Tipo JSON	Definizione
ValueB	Boolean	True: Stato sottofrequenza on, False: Stato sottofrequenza off
Invalidity	Boolean	Invalidità del dato trasmesso (Valido: 0, Invalido: 1)
Timetag	Number	UTC in Secondi dal 1970-01-01 00:00:00 UTC come da formato <i>Unix TimeStamp</i>

7.4.4 Application Data Unit – Comandi

Le ADU che modellizzano i comandi si definiscono come oggetti contenenti un solo *Data Object* rappresentante il comando, tra quelli previsti, che l'operatore remoto manda al CIR.

Il nome dell'oggetto “ADUtype” è “LD_CIR/LLN0.RS_S_Comm”.

Per i comandi l'oggetto JSON ADU coincide con il Data Object ivi rappresentato.

I Data Object relativi ai comandi sono:

- Comando Modulazione della potenza massima dell'infrastruttura di ricarica CSI, tipo 1: “LD_CIR/CSIDWMX1.WLimPctSpt.ctlVal”

Valori	Tipo JSON	Definizione
UUID	String	<i>Universal Unique Identifier</i> secondo ISO/IEC 9834-8
Timetag	Number	UTC in Secondi dal 1970-01-01 00:00:00 UTC come da formato <i>Unix TimeStamp</i>
Maximum Power	Number	Valore in W della potenza massima della CSI
Duration	Number	Durata della modulazione in minuti

- Comando Modulazione della potenza massima dell'infrastruttura di ricarica CSI, tipo 2: “LD_CIR/CSIDWMX2.WLimPctSpt.ctlVal”

Valori	Tipo JSON	Definizione
UUID	String	<i>Universal Unique Identifier</i> secondo ISO/IEC 9834-8
Timetag	Number	UTC in Secondi dal 1970-01-01 00:00:00 UTC come da formato <i>Unix TimeStamp</i>
Maximum Power	Number	Valore in W della potenza massima della CSI
Tmax	Number	TimeTag target di fine modulazione potenza massima, Unix TimeStamp



- Comando di sospensione della ricarica, tipo 1: “LD_CIR/CSIDSESE1.ClcStr.ctlVal”

Valori	Tipo JSON	Definizione
UUID	String	<i>Universal Unique Identifier</i> secondo ISO/IEC 9834-8
Timetag	Number	UTC in Secondi dal 1970-01-01 00:00:00 UTC come da formato <i>Unix TimeStamp</i>
Duration	Number	Durata della sospensione in minuti

- Comando di sospensione della ricarica, tipo 2: “LD_CIR/CSIDSESE2.ClcStr.ctlVal”

Valori	Tipo JSON	Definizione
UUID	String	<i>Universal Unique Identifier</i> secondo ISO/IEC 9834-8
Timetag	Number	UTC in Secondi dal 1970-01-01 00:00:00 UTC come da formato <i>Unix TimeStamp</i>
Tmax	Number	TimeTag target di fine interruzione, Unix TimeStamp

7.4.5 Application Data Unit – Acknowledge comandi e misure

Le procedure di acknowledge sono rappresentate dalle seguenti due tipologie:

- 1) l'invio da parte del CIR di messaggi di corretta o errata ricezione dei comandi mandati dal RO;
- 2) l'invio da parte del RO del messaggio di corretta o errata ricezione dell'*Application Data Unit* “Misure cicliche”.

- Messaggio Acknowledge Comandi ricevuti da RO

Il nome dell'oggetto “ADUtype” è “LD_CIR/LLN0.DS_A_Comm”.

Le Application Data Unit di Acknowledge con cui il CIR conferma o rifiuta i comandi ricevuti da RO sono oggetti JSON con la stessa struttura del comando ricevuto e con gli stessi valori ivi contenuti, a cui vengono aggiunti ulteriori informazioni relative all'esito del processo di ricezione del comando stesso.

È importante sottolineare che il TimeTag contenuto nel messaggio di acknowledge deve essere aggiornato al tempo di conferma ricezione del comando stesso, mentre l'UUID rimane quello originale contenuto nel comando ricevuto.

In particolare, per un generico comando X, si implementi la seguente struttura:

Valori	Tipo JSON	Definizione
Oggetto Comando X	Object	Oggetto del comando ricevuto con Timetag aggiornato al T dell'ack
Ack/Nack	Boolean	True: comando accettato, False: comando rifiutato
Cause	Number	Codice numerico che identifica le cause di rifiuto

La seguente Tabella mostra la semantica del campo Cause in relazione alle tipologie di rifiuto.

“Cause”	Descrizione
0	Comando ricevuto e accettato, valore associato all'Ack
1	Tempo trascorso dall'ultimo comando minore di Tatt
2	CIR non in grado di eseguire il comando per problemi di comunicazione con l'infrastruttura di ricarica
3	Comando Sintatticamente Invalido



- Messaggio Acknowledge pacchetto misure: “LD_CIR/CIRGGIO1.SPCSO1.ctlVal”

Il nome dell'oggetto “ADUtype” è “LD_CIR/LLN0.RS_A_Meas”.

Questo messaggio, contenente nel Valore “Description” la stringa “Acknowledge misure inviate da CIR”, è inviato dal RO a conferma della corretta ricezione del pacchetto misure da parte del CIR. I valori di cui è costituito sono i seguenti:

Valori	Tipo JSON	Definizione
UUID	String	<i>Universal Unique Identifier</i> del pacchetto misure di cui si conferma la ricezione
Timetag	Number	UTC in Secondi dal 1970-01-01 00:00:00 UTC come da formato <i>Unix TimeStamp</i>
Description	String	“Acknowledge misure inviate da CIR”
ValueB	Boolean	True: misure ricevute False: Misure ricevute ma non corrette

7.4.6 ErrorCode - Codice Invalidità delle misure

Il Campo *ErrorCode* deve essere valorizzato sulla base della *Quality type definition* descritto nella Norma IEC 61850-7-3, i cui valori vengono riportati nella tabella seguente per comodità:

Valori	ErrorCode	Definizione
overflow	1	Valore misura oltre il valore rappresentabile dal dispositivo di misura
outOfRange	2	Valore misura oltre al predefinito range di valori ammissibili
badReference	3	Valore misura non accurato a causa di un valore di riferimento fuori calibrazione all'atto della misura
oscillatory	4	Il valore di misura oscillante (solo per input binari)
failure	5	Misura invalida per un'anomalia nel sistema di misurazione
OldData	6	Il valore di misura non è aggiornato da un tempo maggiore del tempo di refresh minimo tollerabile predefinito
inconsistent	7	Valore misura non accurato a causa di un'anomalia rilevata da una funzione di valutazione specifica
inaccurate	8	Il valore di misure potrebbe essere non accurato poiché non è rispondete ai criteri di precisione richiesti alla sorgente di misura

La tabella di associazione tra i valori dell'*ErrorCode* e il campo *Invalidity* delle misure, ispirato alla Norma IEC 61850-7-3 è mostrato nella tabella seguente:

ErrorCode	Invalidity=1= Dato Invalido	Invalidity=2=Discutibile
overflow	X	
outOfRange	X	
badReference	X	
oscillatory	X	
failure	X	
OldData		X
inconsistent		X
inaccurate		X

Esempi di messaggi JSON contenenti gli Application Data Unit e Data Object descritti sono mostrati in Allegato C.



8 Cybersecurity

8.1 TLS

Il protocollo TLS rappresenta una soluzione consolidata e ampiamente diffusa per la protezione delle telecomunicazioni da intercettazioni, alterazioni e contraffazioni del contenuto dei messaggi da parte di soggetti terzi non autorizzati. Le finalità principali sono quelle di fornire riservatezza e integrità delle comunicazioni. Per il raggiungimento di questi obiettivi TLS specifica l'utilizzo combinato di crittografia a chiave pubblica e a chiave privata, per ottenere un adeguato livello di protezione ed efficienza delle comunicazioni.

Oggigiorno le versioni di TLS che possono essere considerate adeguatamente sicure per un ampio spettro di scenari di telecontrollo in ambito elettrico sono la versione 1.2 (TLS 1.2) e la più recente versione 1.3 (TLS 1.3). TLS 1.3 introduce migliorie prestazionali, e un rafforzamento della sicurezza rispetto a TLS 1.2 vietando gli algoritmi che nel tempo si sono dimostrati non sicuri. TLS 1.2 rimane comunque un protocollo sicuro a patto di selezionare opportunamente le opzioni disponibili (algoritmi crittografici, chiavi crittografiche, etc.) e beneficia di un'ampia gamma di strumenti di supporto alla integrazione in dispositivi come il CIR.

La serie di standard IEC 62351 definisce profili di sicurezza adeguati alle telecomunicazioni di telecontrollo in ambito elettrico; le specifiche indicate possono essere generalmente adottate anche per i protocolli applicativi XMPP o MQTT su cui si basano gli scambi informativi del CIR. Pertanto, si ritiene che ci si possa riferire alla serie di standard IEC 62351 e in particolare alla parte IEC 62351-3 per la specifica di dettaglio del profilo che deve essere implementato sugli endpoint della comunicazione TLS.

I protocolli XMPP e MQTT d'altro canto supportano nativamente la comunicazione TLS come specificato in IETF RFC 6120 in IETF RFC 7590 per quanto riguarda XMPP e dalle specifiche OASIS per MQTT in cui la gestione di TLS viene rimandata a IETF RFC 5246; esistono di fatto differenze tra quanto specificato in IEC 62351 e nelle specifiche dei protocolli XMPP e MQTT; in genere si tratta di differenze che possono essere conciliate in quanto si tratta di dettagliare o circoscrivere alcuni parametri di sicurezza. In altri casi le differenze non sono conciliabili; in questo caso, soprattutto quando si tratta di differenze che non pregiudicano significativamente la sicurezza delle comunicazioni, si privilegeranno, per quanto possibile, le indicazioni native di XMPP o MQTT principalmente per ragioni di compatibilità con le specifiche dei protocolli e quindi delle implementazioni disponibili e, di conseguenza, di interoperabilità dei dispositivi.

Nel caso di XMPP e MQTT gli endpoint della comunicazione TLS non sono il CIR e l'RO in quanto mittente e il destinatario dei dati di telecontrollo, bensì il CIR in quanto client della comunicazione TCP e il server a cui il CIR si connette e che svolge il ruolo di server XMPP o broker MQTT in base al protocollo CIR utilizzato. La controparte server costituisce un elemento essenziale per l'inoltro dei dati da CIR a RO e viceversa.

Il profilo TLS che il CIR deve implementare prevede i parametri indicati nei seguenti sottoparagrafi.

8.1.1 Attivazione della comunicazione TLS

Nel caso del protocollo XMPP, il meccanismo di avvio della comunicazione TLS è il meccanismo STARTTLS sulla connessione TCP attivata. I parametri TLS definiti in IEC 62351, intesi per protocolli applicativi che prevedono il meccanismo di attivazione noto come "implicit TLS", in genere possono essere applicati anche a comunicazioni attivate con il metodo STARTTLS.

Per quanto riguarda invece il protocollo MQTT, è previsto l'avvio di TLS tramite il meccanismo "implicit TLS": le comunicazioni sono cifrate apriori prima di qualsiasi comunicazione del protocollo applicativo MQTT. Una porta TCP predefinita è dedicata alle comunicazioni MQTT cifrate (MQTTs) senza quindi necessità di negoziazione esplicita. La porta dedicata alle comunicazioni MQTTs suggerita dalle specifiche OASIS è la 8883. Il CIR deve prevedere un parametro di configurazione che permetta di specificare la porta TCP utilizzata per la connessione alla controparte server.

Qualunque sia il protocollo utilizzato il CIR deve permettere la configurazione dell'indirizzo IP della controparte server e della relativa porta TCP da utilizzare (vedi anche 5.2.1).



8.1.2 Versioni del protocollo TLS

Deve essere supportata la versione 1.2 del protocollo TLS; in conseguenza della IETF RFC 7525, indicata in IETF RFC 7590 e della IETF RFC 8996 “Deprecating TLS 1.0 and TLS 1.1” che a sua volta la aggiorna, le versioni precedenti del protocollo devono essere disabilitate in quanto non si ravvisano esigenze per il loro supporto (es. esigenze di retrocompatibilità o interoperabilità). È raccomandato il supporto della versione 1.3 ma questo documento non specifica parametri specifici per queste versioni di protocollo. La versione 1.3 di TLS deve essere disabilitata di default e deve poter essere abilitata agendo su uno specifico parametro di configurazione. Nel caso le parti concordino di utilizzare queste nuove versioni di protocollo TLS, i parametri TLS devono garantire un livello di sicurezza analogo a quanto indicato in questo documento e devono essere uniformati ai vigenti standard di settore (es. standard EN IEC 62351-3).

8.1.3 Autenticazione delle parti

L'autenticazione di entrambe le parti a livello trasporto (i.e. a livello TCP) deve avvenire esclusivamente mediante scambio di certificati digitali; se una delle parti non è in grado di presentare un certificato digitale valido la comunicazione deve essere terminata.

8.1.4 Certificati digitali

Le parti devono supportare certificati digitali almeno fino alla dimensione di 8192 ottetti; se una delle parti presenta un certificato di dimensione non superiore a questo limite, la controparte non può terminare la comunicazione in conseguenza dell'impossibilità di gestirlo per superamento dei limiti relativi alla dimensione del certificato.

Per la validazione di un certificato il dispositivo CIR deve essere in grado di gestire almeno 5 trust anchor relativi a CA (Certification Authority) e deve quindi disporre di adeguato spazio di memorizzazione interno.

La validazione del certificato, comprendente la verifica dell'eventuale revoca della validità, deve avvenire ad ogni avvio di una sessione TLS, mediante i meccanismi interni della soluzione TLS (es. libreria software TLS), e comunque periodicamente, in caso di connessioni di lunga durata; il limite massimo dell'intervallo di tempo che intercorre tra due verifiche successive deve essere configurabile e comunque inferiore alle 24 ore. Il dispositivo CIR può riattivare questo controllo riavviando una comunicazione (i.e. terminandola e stabilendola nuovamente) entro il suddetto limite massimo. Questa possibilità deve essere supportata e deve poter essere disabilitata mediante parametri di configurazione.

In alternativa alla precedente modalità può essere implementato il meccanismo della rinegoziazione TLS a intervalli regolari, che implica una riverifica dello stato di validità dei certificati digitali; dato che la rinegoziazione è un meccanismo opzionale per le specifiche TLS deve essere verificato che la controparte della comunicazione (i.e. server XMPP o MQTT) la supporti. Nel caso di utilizzo della rinegoziazione TLS, deve essere implementata anche la “TLS Renegotiation Extension” (IETF RFC 5746) che protegge le comunicazioni rispetto a debolezze nelle specifiche iniziali.

Una ulteriore possibilità consiste nell'implementare la verifica dello stato di validità dei certificati a livello applicativo; in questo caso le applicazioni devono tenere traccia del certificato inviato dalla controparte ed effettuare le verifiche periodiche rispettando i limiti temporali massimi indicati precedentemente.

8.1.5 Revoca dei certificati digitali

Deve essere supportato il meccanismo di diffusione dello stato di revoca dei certificati basato su Certificate Revocation List (CRL). Ogni CRL deve essere aggiornata periodicamente, sulla base di un intervallo impostabile tramite un apposito parametro di configurazione, che non deve comunque essere superiore alle 24 ore.



Deve inoltre essere supportato il protocollo OCSP (Online Certificate Status Protocol) specificato da IETF RFC 6960 per la verifica dello stato di validità dei certificati digitali che richiede minori risorse di memorizzazione locale rispetto a quello delle CRL, risultando di particolare beneficio nel caso di PKI ed in particolare VA (Validation Authority) che presentano CRL di dimensioni consistenti. Le risposte OCSP possono essere considerate valide per l'intervallo temporale definito nella risposta e comunque non oltre le 24h in analogia a quanto avviene per l'aggiornamento di una CRL. Un apposito parametro di configurazione deve poter permettere di ridurre questo limite massimo sulla base di specifiche relative all'infrastruttura o alla singola installazione.

Sebbene CRL e OCSP debbano essere entrambe supportate dal CIR, essendo due soluzioni entrambe finalizzate alla verifica dello stato di validità dei certificati digitali, si prevede che un'installazione possa disabilitare, tramite specifico parametro di configurazione, una delle due soluzioni sulla base, ad esempio, di circostanze architetturelle dell'infrastruttura e dei dispositivi quali la capacità di memorizzazione locale, la connettività ad Internet, la frequenza degli intervalli di verifica impostati, o altro.

8.1.6 Cipher Suite

Per ragioni di interoperabilità devono essere supportate almeno le seguenti cipher suite:

- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256.

In aggiunta alle precedenti, si raccomanda il supporto per le seguenti cipher suite:

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256.

Possono essere supportate altre cipher suite che abbiano caratteristiche di sicurezza uguali o superiori a quelle elencate. Non possono essere adottate cipher suite che:

- prevedano un algoritmo di hashing inferiore a SHA256 (es. SHA1 e MD5 non sono consentiti);
- non prevedano la cifratura del traffico (es. TLS_RSA_WITH_NULL_SHA256);
- prevedano algoritmi di cifratura inferiori a AES_128 (es. TLS_*_DES_).

La cipher suite TLS_RSA_WITH_AES_128_CBC_SHA deve essere disabilitata in quanto viola le regole sopra citate, nonostante sarebbe altrimenti richiesta dalla IETF RFC 6120.

8.1.7 Chiavi Crittografiche

Devono essere supportate chiavi crittografiche ECDSA della dimensione minima di 256bit e possibilmente anche di dimensioni superiori.

Nel caso siano supportate anche cipher suite che utilizzano chiavi RSA, devono essere supportate chiavi RSA della dimensione minima di 2048bit e possibilmente anche di dimensioni superiori (almeno fino a 3072bit e superiori).



8.2 SASL per il protocollo XMPP

SASL (Simple Authentication and Security Layer) è un'architettura di autenticazione che si pone a livello intermedio tra un protocollo di telecomunicazione e un insieme di meccanismi di autenticazione. Disaccoppiando il protocollo e i meccanismi di autenticazione permette l'aggiornamento indipendente delle due componenti e semplifica l'introduzione di nuovi meccanismi e funzionalità; SAL è definito nella IETF RFC 4422. Diversi protocolli di telecomunicazione fanno riferimento a SASL per la realizzazione delle funzionalità di autenticazione, cui è finalizzato; in particolare il protocollo XMPP fa riferimento a SASL all'interno di IETF RFC 6120 cui si rimanda per le specifiche generali relative all'implementazione.

Nel seguito di questa sezione e sottosezioni si indicano gli scostamenti e le limitazioni che sono richiesti per l'implementazione del protocollo XMPP nel CIR, rispetto alle possibilità offerte dalle specifiche XMPP relativamente a SASL.

Il CIR deve implementare il meccanismo di autenticazione EXTERNAL, basato sui certificati digitali scambiati nel corso della negoziazione TLS. Qualsiasi altro meccanismo di autenticazione SASL deve essere disabilitato di default e si devono prevedere parametri di configurazione su cui agire esplicitamente per attivare eventuali altri meccanismi che siano implementati nel CIR.

Si richiede che i server della infrastruttura siano analogamente configurati in modo da proporre alla controparte client (il CIR) esclusivamente il meccanismo SASL EXTERNAL o, se ciò non fosse possibile, almeno prioritariamente.

8.2.1 Certificati digitali

Il supporto al meccanismo di autenticazione SASL EXTERNAL prevede che i certificati digitali scambiati dalle parti nel corso della negoziazione TLS contengano informazioni necessarie al funzionamento del meccanismo; in particolare si richiede che il certificato digitale installato sul CIR e inviato al server XMPP contenga i Jabber ID (JID) utilizzato per l'autenticazione nei confronti del server XMPP mediante il meccanismo SASL EXTERNAL; si può fare riferimento alla specifica XEP 0178 "Best Practices for Use of SASL EXTERNAL with Certificates" ed in particolare alla sezione "Client-to-Server Recommendation" per i dettagli relativi agli scambi informativi che caratterizzano questa funzionalità.

Si prevede quindi che i certificati digitali caricati sul CIR contengano uno o più JID, incapsulati nell'*object identifier* id-on-xmppAddr (xmppAddr).

8.2.2 Regole di autenticazione

Se il certificato digitale inviato dal CIR durante la negoziazione TLS contiene un singolo JID in xmppAddr allora il CIR non deve includere una *authorization identity*. Un tentativo di utilizzare una *authorization identity* diversa da quella specificata in xmppAddr deve determinare di default un fallimento dell'autenticazione SASL; la possibilità di utilizzare una *authorization identity* diversa dal JID incluso nel certificato può essere supportata (es. per finalità di test) ma deve essere disabilitata di default e deve potere essere abilitata all'occorrenza agendo esplicitamente su parametri di configurazione specifici.

Se il certificato digitale inviato dal CIR durante la negoziazione TLS contiene molteplici JID in xmppAddr allora il CIR deve includere una *authorization identity* che definisca quale tra queste JID intende utilizzare per l'autenticazione. Un tentativo di utilizzare una *authorization identity* diversa da quella specificata deve determinare di default un fallimento dell'autenticazione SASL; la possibilità di utilizzare una *authorization identity* diversa dai JID inclusi nel certificato può essere supportata (es. per finalità di test) ma deve essere disabilitata di default e deve potere essere abilitata all'occorrenza agendo esplicitamente su parametri di configurazione specifici.

Non si prevede che il CIR sia dotato di certificati digitali privi di JID da utilizzare per la negoziazione TLS verso server XMPP; tale possibilità può comunque essere supportata, in conformità con XEP 0178, ma deve essere disabilitata di default e si devono prevedere parametri di configurazione che devono essere modificati esplicitamente perché sia abilitata.



8.3 Autenticazione applicativa MQTT tramite CIR_ID nel certificato

Quando MQTT viene utilizzato con mutua autenticazione a livello trasporto (mTLS), le sezioni 5.4.1 e 5.4.3 di ISO/IEC 20922 per MQTT v3.1.1 e le sezioni 5.4.1 e 5.4.3 di OASIS per MQTT v5.0 prevedono che i certificati TLS scambiati tra client e server possano essere utilizzati per la reciproca autenticazione. In particolare, l'autenticazione TLS del client CIR presso il server MQTT deve essere utilizzata in sostituzione dell'autenticazione con Username e Password (opzione prevista in 5.4.11.3 di ISO/IEC 20922 per MQTT v 3.1.1 e in 5.4.12.3 di OASIS per MQTT v5.0).

Il CIR deve quindi stabilire unicamente connessioni che richiedano l'autenticazione tramite certificato a livello applicativo e non devono essere utilizzati altri metodi di autenticazione. Il certificato del CIR per la connessione al server MQTT deve contenere il CIR_ID nel campo "Common Name" del certificato. Si richiede che i server della infrastruttura siano analogamente configurati in modo da proporre alla controparte client (il CIR) esclusivamente tale meccanismo di autenticazione.

Il CIR in fase di inizializzazione della connessione al broker deve inoltre comunicare il CIR_ID come proprio identificativo Client ID.

8.4 PKI

Una infrastruttura a chiave pubblica (PKI – Public Key Infrastructure) è un insieme di servizi relativi alla gestione di certificati digitali, in genere offerti grazie al supporto di software che possono essere sia *open-source* sia proprietari, e che possono essere gestiti in autonomia degli utilizzatori finali dei certificati digitali o offerti da aziende terze specializzate.

L'acronimo PKI non identifica un'architettura precisa o un insieme preciso di servizi, ma è un'espressione generica che comprende tutti i possibili servizi relativi alla gestione dei certificati digitali, non necessariamente tutti essenziali in ogni scenario. L'utilizzatore finale dei certificati digitali è chiamato a identificare i servizi opportuni per il proprio caso di utilizzo e l'architettura più adeguata che possa mettere a disposizione questi servizi. Ognuno dei servizi di una PKI può essere ricondotto ad alcune specifiche autorità che assolvono a tre macro-funzioni amministrative; un'autorità non è definita nel dettaglio, ma si può immaginare costituita da individui, procedure, software e hardware di supporto, o solo da alcuni di questi elementi.

Tipicamente vengono identificate tre autorità: RA, CA e VA le cui rispettive funzioni sono descritte nelle Tabella degli Attori della Sezione 3.1.

La scomposizione netta delle funzioni delle autorità non si verifica costantemente nella realtà: accade spesso che le funzionalità di due, o anche più autorità, siano concentrate all'interno dei medesimi dispositivi, software o funzioni organizzative e non siano facilmente isolabili.

Una distinzione rilevante nell'ambito delle PKI riguarda la natura pubblica o privata della fiducia (trust) circa il contenuto dei certificati digitali, le cui caratteristiche sono descritte nella tabella sottostante.

Trust	Caratteristiche
Pubblico	La fiducia circa l'affidabilità di una PKI pubblica in molti casi viene assunta in origine, grazie al fatto che i certificati digitali root della relativa CA godono di un'ampia e spesso automatica distribuzione e accessibilità. L'accesso ai servizi di una PKI pubblica può avvenire sottoscrivendo opportuni contratti, che ne danno accesso, in genere tramite portali o applicazioni web/internet.
Privato	La fiducia può essere ottenuta solo a seguito della distribuzione dei certificati digitali root della PKI privata alle parti che ne devono fare uso, mediante procedure e strumenti che devono essere definiti per lo specifico scenario. La gestione di una PKI privata si può considerare generalmente più onerosa rispetto a quella di una PKI pubblica, ma abilita ad un livello superiore di flessibilità (es. contenuti dei certificati digitali e creazione di gerarchie di CA/SubCA), che può controbilanciare il maggiore onere iniziale.



Nel caso del telecontrollo del CIR le parti coinvolte nella comunicazione sono due: CIR e RO; possono quindi ragionevolmente essere coinvolte al più due distinte PKI (CIR-PKI e RO-PKI) che possono essere di natura pubblica, privata o mista (i.e. una pubblica e l'altra privata).

Gli scenari che si ritengono più verosimili sono riportati nella tabella sottostante.

Trust	Caratteristiche
Singola PKI privata	I certificati digitali di CIR e dispositivo di telecontrollo lato RO sono entrambi emessi da una singola PKI; il certificato del CIR deve essere caricato sul CIR. In genere si può ipotizzare che la PKI privata sia di proprietà/gestita dal RO in quanto soggetto deputato al telecontrollo e di capacità/dimensioni organizzative non limitate ⁴ .
Singola PKI pubblica	Analoga al precedente, da cui è distinta dalla natura pubblica della PKI; si può prevedere un minore onere gestionale della PKI (da parte del RO prevedibilmente), ma, al contempo la necessità di verificare che la PKI pubblica supporti tutte le funzionalità necessarie per il telecontrollo del CIR (es. informazioni presenti nel certificato, disponibilità di OCSP responder, disponibilità di CRL distribution point).
Doppia PKI	Non si entra nei dettagli di questo scenario per via della articolata natura delle combinazioni di PKI (pubbliche, private, miste). Si noti tuttavia che ciascuna parte deve essere configurata con i trust anchor della controparte, e che entrambe le PKI devono supportare le funzionalità previste per il CIR.

8.4.1 Rinnovo dei certificati digitali

La PKI deve supportare il protocollo EST mettendo a disposizione server EST cui i CIR devono fare riferimento per l'arruolamento (enrollment) del dispositivo presso RO, come descritto in SUC-00, e per il rinnovo automatico dei certificati prima della scadenza del periodo di validità.

Per questo motivo i CIR devono prevedere un parametro di configurazione che definisce il margine temporale di anticipo in cui avviene il rinnovo del certificato rispetto alla scadenza e devono implementare il client EST per supportare questa funzionalità.

Il CIR deve pertanto generare la CSR da inviare al server EST includendo la nuova chiave pubblica che deve essere utilizzata per le future comunicazioni.

Il rinnovo dei certificati digitali mediante EST è una procedura completamente automatica che non richiede interventi manuali, a patto che avvenga prima della scadenza del periodo di validità del certificato da sostituire.

L'anticipo temporale che deve essere impostato nel dispositivo rispetto alla scadenza del certificato digitale da sostituire deve tenere in considerazione l'intervallo di verifica dello stato di validità dei certificati digitali, oltre che della eventualità di dovere ripetere la procedura in caso di fallimento temporaneo.

Ulteriori dettagli a questo riguardo sono riportati in EN IEC 62351-9.

8.4.2 Lista di CA fidate

Al fine di consentire un adeguato e omogeneo livello di sicurezza dell'infrastruttura di telecontrollo in cui operano CIR e RO, garantire la continuità dei servizi che ne derivano e per agevolare alcune operazioni di configurazione, risulterà verosimilmente utile predisporre una lista (i.e. un registro) di CA considerate affidabili. La lista contiene sostanzialmente i certificati delle CA e sub-CA ritenute affidabili.

I costruttori dei dispositivi, così come i RO e i gestori dei server intermedi di comunicazione, potranno fare riferimento a questa lista per limitare la comunicazione dei loro dispositivi e/o sistemi esclusivamente a controparti a cui sia stato rilasciato un certificato digitale firmato da una CA presente in questa lista.

⁴ La specifica del caso d'uso SUC-00 relativo alla registrazione del CIR fa riferimento a questo scenario.



Esempi di utilizzo di questa lista sono i seguenti.

- Un costruttore può precaricare, nei propri dispositivi CIR, questa lista di certificati (o un sottoinsieme di essa) per consentire la comunicazione con le RA e i server intermedi.
- Una PKI può utilizzare questa lista per verificare l'autenticità dei certificati di *preenrollment* utilizzati dai CIR.
- Una PKI può comunicare questa lista di certificati (o un sottoinsieme di essa) *all'endpoint* /cacerts del servizio EST così da aggiornare ed integrare la lista precaricata sul dispositivo e consentirgli la comunicazione con la porzione di infrastruttura opportuna.
- Il server (XMPP o MQTT) può utilizzare questa lista di certificati (o un sottoinsieme di essa) per verificare l'autenticità dei certificati del CIR (o del RO) al momento della loro autenticazione.

Verosimilmente la possibilità di introdurre o mantenere una CA in questa lista sarà condizionata alla possibilità di eseguire verifiche periodiche dell'affidabilità della CA e del rispetto di livelli di sicurezza adeguati da parte di soggetti preposti, sia per le infrastrutture sia per le procedure messe in atto dalla PKI.

9 Prove di conformità e certificazioni

Le prove da eseguire sul CIR, al fine di verificarne la conformità a quanto specificato in questa PAS sono:

- a) prove funzionali corrispondenti alla comunicazione CIR-RO secondo ciascun caso d'uso specificato in Appendice A;
- b) prove relative alla cybersecurity della comunicazione CIR-RO corrispondenti alle specifiche riportate alla Sezione 8.

I parametri di configurazione e l'elenco dei test relativi alle prove a) e b) sono dettagliati nelle sezioni 9.2, 9.3, 9.4 e 9.5.

La rispondenza ai requisiti elencati nei punti precedenti deve essere inclusa nella "Dichiarazione di conformità" emessa a cura e responsabilità del Costruttore utilizzando il template fornito nell' Allegato X.1 alla CEI 0-21 e deve essere resa disponibile a RO dal proprietario del CIR all'atto della stipula del contratto.

Le prove funzionali e di cybersecurity possono in alternativa avvenire:

- a) presso un laboratorio accreditato secondo CEI UNI EN ISO/IEC 17025, oppure
- b) presso laboratori esterni non accreditati, oppure
- c) presso i laboratori del costruttore.

Nei casi b) e c) le prove devono avvenire sotto la sorveglianza e responsabilità di apposito organismo certificatore che abbia i requisiti della UNI CEI EN ISO/IEC 17065.

La documentazione attestante il superamento delle prove (rapporti di prova) deve essere conservata dal costruttore e mantenuta aggiornata ad ogni aggiornamento del firmware. La medesima documentazione deve comunque essere resa disponibile a RO a cura del Costruttore.

9.1 Formato test

La specifica di un test di conformità utilizza un formato tabellare a tre colonne contenenti un identificativo, una descrizione e riferimenti documentali.

Identificativo	Descrizione	Riferimenti
Numero Sezione.Numero sottosezione.Numero test	Comportamento da testare (normale/atteso o anormale/inatteso)	Es. SUC-n, sezione CEI PAS 57-127, sezione IEC 62351-x



9.2 Parametri di configurazione

I test di conformità devono verificare che tutti i parametri di configurazione del CIR siano rispettati. I parametri di configurazione del CIR sono indicati nella descrizione dei casi d'uso e nel capitolo 8. Per comodità nella tabella seguente vengono raccolti i parametri riferiti nei test di conformità.

Parametro	Valori
Versioni TLS	v1.2, v1.3 (opzionale)
Cipher Suite TLS 1.2	– TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 – TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 – TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256. – TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (opzionale) – TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (opzionale) – TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (opzionale)
Dimensione minima delle chiavi crittografiche	RSA: 2048 bit, ECDSA: 256 bit
Intervallo temporale massimo tra verifiche successive dello stato di validità dei certificati	24 h
Metodi di verifica della validità dei certificati	CRL, OCSP
Numero minimo di trust anchor supportati	5
Dimensione dei certificati supportata	Almeno fino a 8192 byte
Protocollo PKI	EST
Tatt	1-60 sec, default: 30 sec

I test che riferiscono i parametri di configurazione vanno eseguiti per un campione rappresentativo dei valori di ciascun parametro.



9.3 Verifica Registrazione

9.3.1 Registrazione

Identificativo	Descrizione	Riferimenti
9.3.1.1	Verifica che il CIR contatti l'endpoint /cacerts della PKI e salvi l'Explicit TA	CEI PAS 57-127, SUC-00
9.3.1.2	Verifica che il CIR generi una CSR contenente il CIR_ID nel campo opportuno del certificato (JabberID nel campo SANXmppAddr per XMPP, una stringa univoca nel campo CN per XMPP)	CEI PAS 57-127, SUC-00 8.2.1
9.3.1.3	Verifica che il CIR invii la richiesta CSR all'endpoint /simpleenroll della PKI autenticandosi con il proprio certificato di preenrollment e salvi il certificato che gli viene restituito	CEI PAS 57-127, SUC-00

9.3.2 Rinnovo del certificato

Identificativo	Descrizione	Riferimenti
9.3.2.1	In prossimità della scadenza verifica che il CIR invii la richiesta CSR per il rinnovo del certificato all'endpoint /simpleenroll della PKI autenticandosi con il proprio certificato in scadenza e salvi il certificato che gli viene restituito	CEI PAS 57-127, SUC-00

9.4 Verifica funzionamento in modalità asservita

9.4.1 Inizializzazione

Identificativo	Descrizione	Riferimenti
9.4.1.1	Il CIR stabilisce una connessione verso il server (XMPP o MQTT) utilizzando l'indirizzo IP e la porta TCP configurati. In particolare, il CIR è in grado di utilizzare la porta TCP di default indicata dalle specifiche XMPP o MQTT	CONNESSIONE TCP CEI PAS 57-127, 8.1.1
9.4.1.2 (nel caso XMPP)	Il CIR supporta il metodo denominato STARTTLS per la transizione alla comunicazione sicura TLS	XMPP CEI PAS 57-127, 8.1.1
9.4.1.3	Il CIR supporta la versione v1.2 di TLS (TLS v1.2)	VERSIONE TLS CEI PAS 57-127, 8.1.2
9.4.1.3.a	La versione v1.3 di TLS, se supportata dal CIR, può essere abilitata/disabilitata mediante un parametro di configurazione	VERSIONE TLS CEI PAS 57-127, 8.1.2
9.4.1.4	Il CIR verifica la validità del certificato TLS ricevuto dalla controparte (i.e. validità temporale, autorità di certificazione emittente, firma digitale valida, identità riportata nel certificato)	CERTIFICATI TLS CEI PAS 57-127, 8.1.4
9.4.1.5	Il CIR gestisce certificati digitali di diverse dimensioni inclusa la dimensione massima prevista	CERTIFICATI TLS CEI PAS 57-127, 8.1.4
9.4.1.6	Il CIR permette di configurare almeno il numero minimo previsto di trust anchor	PKI CEI PAS 57-127, 8.1.4
9.4.1.7	Il CIR supporta il meccanismo di distribuzione delle informazioni di validità dei certificati digitali basato su CRL secondo le modalità specificate	PKI CEI PAS 57-127, 8.1.5
9.4.1.8	Il CIR supporta il meccanismo di distribuzione delle informazioni di validità dei certificati digitali basato su OCSP secondo le modalità specificate	PKI CEI PAS 57-127, 8.1.5
9.4.1.9	Il CIR supporta tutte le cipher suite mandatorie	TLS CEI PAS 57-127, 8.1.6



Identificativo	Descrizione	Riferimenti
9.4.1.10	Il CIR supporta chiavi ECDSA della lunghezza specificata	CERTIFICATI TLS CEI PAS 57-127, 8.1.7
9.4.1.11a (nel caso XMPP)	Il CIR supporta il meccanismo di autenticazione di livello applicativo SASL EXTERNAL con certificati digitali contenenti le informazioni specificate	XMPP CEI PAS 57-127, 8.2
9.4.1.11b (nel caso MQTT)	Il CIR supporta la mutua autenticazione e presenta al broker MQTT un certificato con il CIR_ID nel campo CN	MQTT CEI PAS 57-127, 8.3
9.4.1.12	Il CIR termina la connessione con il server (XMPP o MQTT) quando quest'ultimo è configurato per proporre esclusivamente un parametro di connessione di livello inferiore al minimo consentito, o espressamente vietato (in particolare per quanto riguarda versioni di TLS, cipher suite, dimensione e tipologia di chiavi e certificati digitali, meccanismi di distribuzione delle informazioni di validità dei certificati digitali, meccanismi di autenticazione XMPP diversi da SASL External). La terminazione della connessione avviene prima della possibilità di invio di misure o di ricezione di comandi	XMPP o MQTT CEI PAS 57-127, 8.2

9.4.2 Invio misure e stati

Identificativo	Descrizione	Riferimenti
Nota	Il CIR è connesso ad una controparte di comunicazione XMPP o MQTT che simula il servizio di connessione al Remote Operator (Simulatore di connessione a RO). Al server XMPP o MQTT è connesso anche un client RO che simula il RO.	
9.4.2.1	Verifica che il CIR invii ogni 20 secondi l'ADU "Misure cicliche"	CEI PAS 57-127, 7.3.1
9.4.2.2	Verifica che l'ADU "Misure Cicliche" sia inviato nella sua interezza, includendo sempre tutti i Data Object di cui è formato	CEI PAS 57-127, 7.3.1
9.4.2.3	Verifica che i Data Object dell'ADU "Misure cicliche" contengano i (valori di) Data attribute "ValueN" "Invalidity" "ErrorCode" "Timetag"	CEI PAS 57-127, 7.3.1
9.4.2.4	Verifica che i valori contenuti nei Data Object corrispondano ai valori e alla validità delle misure in campo	CEI PAS 57-127, 7.3.1
9.4.2.5	Verifica che i nomi dell'ADU e dei Data Object siano conformi a quanto specificato	CEI PAS 57-127, 7.2
9.4.2.6	Verifica che il CIR invii, tramite procedura di invio spontaneo, la ADU "Misure Spontanee"	CEI PAS 57-127, 7.3.2
9.4.2.7	Verifica che l'ADU "Misure Spontanee" contenga solo i Data Object dell'ADU che hanno subito una variazione di stato rispetto all'invio precedente (per variazione di stato di un data object si intende la variazione di almeno uno tra i Data Attribute che costituiscono il Data Object)	CEI PAS 57-127, 7.3.2
9.4.2.8	Verifica che i Data Object dell'ADU "Misure Spontanee" contengano i Data Attribute "ValueN" "Invalidity" "ErrorCode" "Timetag"	CEI PAS 57-127, 7.3.2
9.4.2.9	Verifica che i valori contenuti nei Data Object corrispondano a valori delle misure in campo e alla loro validità	CEI PAS 57-127, 7.3.2
9.4.2.10	Verifica che i nomi dell'ADU e dei Data Object siano conformi a quanto specificato	CEI PAS 57-127, 7.2
9.4.2.11	Verifica che il CIR invii, tramite procedura di invio spontaneo, la ADU "Stati e Allarmi"	CEI PAS 57-127, 7.3.3



Identificativo	Descrizione	Riferimenti
9.4.2.12	Verifica che L'ADU "Stati e Allarmi" contenga solo i Data Object dell'ADU che hanno subito una variazione di stato rispetto all'invio precedente (per variazione di stato di un Data Object si intende la variazione di almeno uno tra i Data Attribute che costituiscono il Dataobject)	CEI PAS 57-127, 7.3.3
9.4.2.13	Verifica che i Data Object dell'ADU "Stati e Allarmi" contengano sempre tutti i Data Attribute previsti dalla Norma	CEI PAS 57-127, 7.3.3
9.4.2.14	Verifica che i valori contenuti nei Data Object corrispondano ai valori degli stati e degli allarmi presenti in campo	CEI PAS 57-127, 7.3.3
9.4.2.15	Verifica che i nomi dell'ADU e dei Data Object siano conformi a quanto specificato	CEI PAS 57-127, 7.2
9.4.2.16a	Verifica che per le misure, gli allarmi e gli stati il cui timetag è settato dal CIR stesso (e non da device esterni), il timetag corrisponda al tempo di sincronismo del CIR	CEI PAS 57-127, 7.3
9.4.2.16b	Verifica che il time tag di misure provenienti dalla Chain2 venga mantenuto inalterato dal CIR	CEI PAS 57-127, 7.3
9.4.2.17	Verifica che il CIR gestisca ed invii tutti i valori del Codice Invalidità delle misure	CEI PAS 57-127, 7.3.6
9.4.2.18	Verifica che in caso di mancanza sincronizzazione del CIR, venga inviato il Data Object "Anomalia Sincronizzazione CIR" con ValueB = true	CEI PAS 57-127, 7.3.3
9.4.2.19	Verifica che il CIR sia sincronizzato da una sorgente di sincronismo esterna	
9.4.2.20	Verifica del passaggio alla modalità autonoma al verificarsi delle condizioni di sottofrequenza e stop manuale attivo (opt-out utente)	CEI PAS 57-127, pag. 21 tabella stati di funzionamento

9.4.3 Ricezione comandi

Identificativo	Descrizione	Riferimenti
Nota	Il CIR è connesso ad una controparte di comunicazione (XMPP o MQTT) che simula il servizio di connessione al Remote Operator (Simulatore di connessione a RO). Al server XMPP o MQTT è connesso anche un client RO che simula il RO.	
9.4.3.1	Verifica della corretta ricezione da parte del CIR dei quattro comandi: 1) Comando Modulazione della potenza massima dell'infrastruttura di ricarica CSI, tipo 1; 2) Comando Modulazione della potenza massima dell'infrastruttura di ricarica CSI, tipo 2; 3) Comando di sospensione della ricarica, tipo 1; 4) Comando di sospensione della ricarica, tipo 2	CEI PAS 57-127, 7.3.4
9.4.3.2a	Verifica della corretta lettura da parte di CIR dei valori contenuti in ciascuna delle 4 ADU "Comandi" inviate dal simulatore di RO	CEI PAS 57-127, 7.3.4
9.4.3.2b	Verifica della corretta elaborazione da parte del CIR di ciascuna delle 4 ADU "Comandi" inviate dal simulatore di RO e della corretta trasmissione sull'interfaccia CIR-CSI degli output corrispondenti	CEI PAS 57-127, 7.3.4



Identificativo	Descrizione	Riferimenti
9.4.3.3	Verifica, per ognuno dei 4 tipi di comando, che il CIR confermi o rifiuti il comando ricevuto dal simulatore di RO, attraverso le Application Data Unit di Acknowledge	CEI PAS 57-127, 7.3.5
9.4.3.4	Verifica che il TimeTag contenuto nel messaggio di acknowledge sia aggiornato al tempo di conferma ricezione del comando stesso inserito dal CIR, mentre che l'UUID sia quello originale contenuto nel comando ricevuto	CEI PAS 57-127, 7.3.5
9.4.3.5	Verifica che il CIR gestisca ed invii tutte le cause di rifiuto dei comandi (0,1,2,3)	CEI PAS 57-127, 7.3.5
9.4.3.6	Verifica che i comandi ricevuti a distanza di tempo inferiore a Tatt, noto e impostato dal costruttore, vengano rifiutati	CEI PAS 57-127,
9.4.3.7	Verifica della priorità del Power Management rispetto ai comandi di modulazione: durante il mantenimento di un comando, aumentare i carichi concorrenti alla CSI verificando che venga rispettato il limite di potenza disponibile al POD	Allegato X

9.4.4 KeepAlive

Identificativo	Descrizione	Riferimenti
9.4.4.1	Verifica corretta ricezione da parte del CIR dell'ADU "Messaggio Acknowledge pacchetto misure" inviata dal Simulatore di RO a fronte dell'ADU "Misure cicliche" inviata dal CIR (test di keep-alive della comunicazione RO-CIR)"	CEI PAS 57-127, 7.3.5
9.4.4.2a	Verifica che in caso di mancata ricezione del messaggio di keep-alive, il CIR ritrasmetta fino a 5 volte, con periodicità di 2 secondi l'ADU "Misure Cicliche"	CEI PAS 57-127, SUC-02
9.4.4.2b	Verifica che in caso di mancata risposta da parte del Simulatore di RO dopo 5 ritrasmissioni dell'ADU "Misure Cicliche", il CIR passi in modalità di funzionamento Autonoma	CEI PAS 57-127, SUC-02
9.4.4.3	Verifica della corretta ricezione da parte del CIR e della corretta lettura di entrambi i valori possibili (true e false) di "ValueB" nel "Messaggio Acknowledge pacchetto misure"	CEI PAS 57-127, 7.3.5

9.5 Verifica funzionamento in modalità autonoma

9.5.1 Ripresa connessione

Identificativo	Descrizione	Riferimenti
9.5.1.1	Partendo dalla modalità Autonoma in conseguenza al fallimento del keep-alive (test 9.4.4.2b), verifica che il CIR effettui il tentativo di riconnessione attraverso la procedura di inizializzazione	CEI PAS 57-127, 5.2.7
9.5.1.2a	Verifica l'avvenuta riconnessione attraverso la ripresa dell'invio dei messaggi "Misure Cicliche" da parte del CIR	CEI PAS 57-127, 5.2.7
9.5.1.2b	Verifica del ritorno in modalità asservita attraverso l'invio di un comando dal Simulatore di RO e la corretta esecuzione del comando da parte del CIR	CEI PAS 57-127, 5.2.7
9.5.1.3	Verifica che nel caso in cui la riconnessione non vada a buon fine il CIR rimanga in modalità Autonoma attraverso l'invio di un comando da parte del Simulatore di RO e la verifica che il CIR non invii un messaggio di Acknowledge	CEI PAS 57-127, 5.2.7



9.5.2 Aggiornamento configurazione

Identificativo	Descrizione	Riferimenti
9.5.2.1	Aggiornamento configurazione manuale: comando di stop manuale attivato dall'utente (opt-out utente) Verifica del passaggio manuale alla modalità autonoma da parte dell'operatore, assicurandosi che il CIR interrompa l'invio dei dati e l'esecuzione di comandi	CEI PAS 57-127, 7.3.3 Nota 2 pag. 33, B.3 macchina a stati
9.5.2.2	Aggiornamento configurazione manuale: comando di stop manuale disattivato dall'utente (opt-in utente) Partendo da una condizione di modalità Autonoma, impostare tramite interfaccia utente la modalità Asservita. Verificare in successione: - Il ripristino della connessione con il RO - Il ripristino dell'invio di Misure Cicliche - Il ripristino della capacità di ricezione ed esecuzione comandi	CEI PAS 57-127, 7.3.3 Nota 2 pag. 33
9.5.2.3	Aggiornamento configurazione manuale: Aggiornamento configurazione CSI Eseguire la presente verifica solo nel caso in cui il CIR preveda la possibilità di aggiornare la configurazione della CSI. Partendo da modalità Asservita, iniziare la procedura di cambio configurazione secondo le interfacce predisposte dal costruttore. Prima di procedere, verificare l'attivazione della modalità Autonoma attraverso l'interruzione dell'invio delle Misure Cicliche. Procedere al cambio di configurazione e salvare le nuove impostazioni. Attendere e verificare la corretta ripresa dell'invio delle Misure Cicliche e della ricezione dei comandi	CEI PAS 57-127, SUC-07



Bibliografia

- [1] Elaadnl “Public Key Infrastructure for ISO 15118”, 2022 <https://elaad.nl/wp-content/uploads/downloads/PKI-for-ISO-15118-2022-pdf.pdf>
- [2] OCA OCPP Open Charge Point Protocol, v. 2.0.1
- [3] VDE report “Handling of certificates for electric vehicles, charging infrastructure and backend systems within the framework of ISO 15118” (English translation of VDE-AR-E 2802-100-1:2019-12)
- [4] XSF XEP 0060 Publish-Subscribe
- [5] XSF XEP 0163 Personal Eventing Protocol
- [6] XSF XEP 0178 Best Practices for Use of SASL EXTERNAL with Certificates
- [7] XSF XEP 0394 Message Markup Abstract
- [8] OASIS MQTT Version 5.0, Committee Specification 02, 15 May 2018



Allegato A

Casi d'Uso in formato standard IEC 62559-2

A.1 SUC-00: Registrazione CIR

Viene nel seguito descritto il System Use Case 00 relativo alla registrazione del dispositivo CIR.

Descrizione del Caso di Uso

Ambito e Obiettivi

Ambito e Obiettivi	
Ambito	Abilitare il servizio di flessibilità del CIR
Obiettivi	Attestare il dispositivo CIR presso un Operatore Remoto

Narrativa del Caso di Uso

Narrativa del Caso di Uso
Descrizione breve Attestare il dispositivo CIR presso un Operatore Remoto.
Descrizione completa La procedura di registrazione garantisce il requisito di portabilità del servizio di flessibilità da un operatore ad un altro. Al CIR viene fornito dal costruttore un certificato di pre-enrollment, Il CIR deve inoltre avere la capacità di generare chiavi crittografiche e CSR come specificato successivamente. Nella stipula di un contratto di aggregazione con un RO, il CIR deve ricevere da quest'ultimo le seguenti informazioni che procede a inserire come propri parametri di configurazione : - il nome di dominio (es. RO.tld) dell'endpoint EST o indirizzo IP e relativa porta TCP; - il certificato/i della CA dell'endpoint EST della PKI (Implicit TA); - il nome di dominio del server (XMPP o MQTT) o indirizzo IP e relativa porta TCP; - l'identificativo CIR_ID, una stringa utilizzata dal RO per identificare univocamente il CIR, (ad esempio UUID - Universally Unique Identifier, IETF RFC 9562). Il formato del CIR_ID richiesto dal protocollo XMPP è il JabberID; - il JabberID del RO con cui il CIR scambierà i dati per XMPP e/o l'identificativo dei topic per MQTT su cui il CIR dovrà attestarsi per pubblicare i propri dati e sottoscrivere i comandi del RO a conclusione del SUC-01. A valle della configurazione di questi parametri di registrazione, il CIR utilizza il protocollo EST (Enrollment over Secure Transport, IETF RFC 7030) per eseguire la procedura di registrazione presso l'Autorità di Registrazione (RA) della PKI designata dal RO e ottenere il proprio certificato client valido per l'autenticazione al server (XMPP o MQTT): - il CIR contatta l'endpoint /cacerts della PKI, validandolo con l'implicit TA installata sul dispositivo. Questo endpoint è pubblico, non ha bisogno di autenticazione da parte del client e chiamarlo significa scaricare tutta la serie di CA che si ritengono fidate (Explicit TA). Questa serie di CA verrà scaricata in formato pkcs7, in particolare verranno scaricati i certificati necessari all'identificazione del server (XMPP o MQTT) che il CIR dovrà installarli in modo da poterle utilizzare per validare il certificato del server (XMPP o MQTT) al momento della connessione TLS. - Il CIR genera e invia la richiesta CSR di firma del certificato all'endpoint /simpleenroll su canale protetto da TLS. Per la configurazione del profilo TLS da utilizzare si rimanda a quanto dettagliato nella Sezione 8.1. Il client CIR si autentica con il certificato fornito dal costruttore (certificato di pre-enrollment). Nel caso in cui tale certificato non fosse disponibile, EST consente al CIR di autenticarsi utilizzando credenziali di tipo username/password la cui validità nel tempo o riutilizzabilità deve essere limitata lato RO per ragioni di sicurezza. IETF RFC 7030 raccomanda che la policy sugli attributi CSR venga reperita tramite l'endpoint EST /csrattrs. La richiesta di attributi CSR è facoltativa, ma le CA possono rifiutare le richieste di iscrizione che non sono codificate in base alla politica della CA della PKI complicando quindi l'emissione del certificato per il CIR, si raccomanda quindi che il CIR implementi questo passaggio prima di generare e inviare la propria CSR. È comunque indispensabile che la CSR generata dal CIR contenga il CIR_ID in specifici campi: il JabberID nel campo SAN (Subject Alternative Name) per poter ottenere un certificato adatto alla connessione al server XMPP e/o l'identificativo univoco MQTT nel campo CN (Common Name) per connessioni al broker MQTT.



La procedura di registrazione del CIR consiste nei seguenti passi:

- La RA elabora la richiesta CSR verificando l'identità del CIR utilizzando i dati di registrazione;
- se la richiesta CSR è valida, la RA invia una richiesta di creazione del certificato alla rispettiva CA. La CA genera e firma un certificato di chiave pubblica e lo invia alla RA, che lo invia al CIR;
- se la richiesta CSR non è valida, la RA non invierà alcuna richiesta alla CA.
- se il CIR riceve un certificato entro CSR time-out (vedi macchina a stati del SUC-00 nella sezione B.1), estrae e archivia il certificato ricevuto da RA ed esegue la procedura di inizializzazione specificata in SUC-01;
- se il CIR non riceve un certificato entro un certo tempo (CSR time-out), invia una nuova richiesta CSR alla RA. La richiesta CSR può essere ripetuta un numero massimo di volte definito da CSR-max (vedi macchina a stati del SUC-00 nella sezione B.1).

Il certificato così ottenuto va utilizzato dal CIR in fase di autenticazione al server (XMPP o MQTT). All'interno del periodo di validità di questo certificato il protocollo EST con la procedura appena descritta va utilizzato dal CIR per la richiesta di rinnovo del certificato stesso, con la differenza che l'autenticazione del CIR non avverrà con il certificato fornito dal costruttore ma con il certificato di cui si chiede il rinnovo.

8.1 In ogni momento il CIR risulta registrato presso una e una sola RA.

La registrazione del CIR presso RO rimane attiva fino alla richiesta di de-registrazione del CIR (SUC-05) a valle della cessazione del contratto con RO.

In questa fase è fondamentale che i certificati di pre-enrollment installati dal costruttore sul CIR vengano ritenuti validi dal server EST. In mancanza di un'autenticazione del CIR nei confronti del server EST non verrà rilasciato al CIR un certificato per la comunicazione con il server (XMPP o MQTT) e non sarà quindi possibile avviare le funzionalità di smart charging. Risulta pertanto necessario mantenere un registro di CA fidate firmatarie dei certificati costruttore accessibile a tutte le PKI incaricate di svolgere l'enrollment dei CIR.

Per i dettagli relativi alla procedura di registrazione fare riferimento allo standard IEC 62351-9.

Per i dettagli relativi all'implementazione della CSR fare riferimenti allo standard IETF RFC 7030.

La procedura sopra descritta si riferisce alla predisposizione del CIR per una prima connessione a RO. Il protocollo EST deve essere usato anche per il rinnovo del certificato digitale entro il termine del suo periodo di validità. La procedura è del tutto analoga a quella illustrata nel diagramma di sequenza SUC-00 ma è semplificata rispetto a quanto indicato precedentemente perché può essere completamente automatizzata sulla base del certificato digitale in uso e dei parametri precedentemente configurati. Il CIR deve comunque prevedere i parametri di configurazione e gli strumenti software che supportano il funzionamento di questa procedura (es. attivazione periodica, verifica della scadenza del certificato, margine di anticipo rispetto alla scadenza).

Attori

RO, CIR, RA, CA (vedi Sezione 3.1).

Condizioni del Caso di Uso

Prerequisiti	
– Esiste un contratto di flessibilità con RO siglato da CIR; – I dati di configurazione del CIR sono presenti nel dispositivo; – CIR genera una coppia di chiavi privata/pubblica.	

Analisi passo-passo dello scenario⁵

Passo No	Nome del processo/attività	Descrizione del processo/attività	Mittente (attore)	Destinatario (attore)	Informazione scambiata (IDs)
1.0	Installazione Explicit TA	Il CIR scarica l'elenco di CA fidate	CIR	CIR	Info0
1.1	Creazione CSR	Il CIR crea la struttura dati CSR	CIR	CIR	Info1 Info2
1.2	Invio Richiesta Certificato	Il CIR invia la richiesta di creazione e firma del certificato	CIR	RA	Info3

⁵ I passi in rosso identificano passi da cui dipendono indirettamente le comunicazioni CIR-RO.



Passo No	Nome del processo/attività	Descrizione del processo/attività	Mittente (attore)	Destinatario (attore)	Informazione scambiata (IDs)
1.3	Estrazione dati	RA estrae da CSR i dati necessari alla sua verifica	RA	RA	Info3
1.4	Verifica CSR	RA esegue le verifiche di validità della CSR	RA	RA	Info1
1.5	Creazione CSR	RA crea la struttura dati CSR	RA	RA	Info1 Info2
1.6	Invio Richiesta Certificato	RA invia la richiesta di creazione e firma del certificato	RA	CA	Info4
1.7	Creazione e Firma Certificato	CA crea e firma il certificato	CA	CA	Info4
1.8	Invio Certificato	CA invia il certificato firmato a RA	CA	RA	Info5
1.9	Invio Certificato	RA invia il certificato firmato a CIR	RA	CIR	Info5
1.10	Archiviazione Certificato e avvio inizializzazione	CIR archivia il certificato e avvia l'inizializzazione dell'interfaccia CIR-RO	CIR	CIR	Info5

Informazioni scambiate

Identificativo	Nome della informazione	Descrizione della informazione scambiata
Info0	Explicit TA	Elenco CA fidate
Info1	ID	Dati identificativi del CIR
Info2	PK	Chiave Pubblica del CIR
Info3	CSR	Richiesta di creazione e firma del certificato
Info4	CSR1	Richiesta di creazione e firma del certificato
Info5	Certificato Firmato	Certificato in formato standard ITU-T X.509

Requisiti

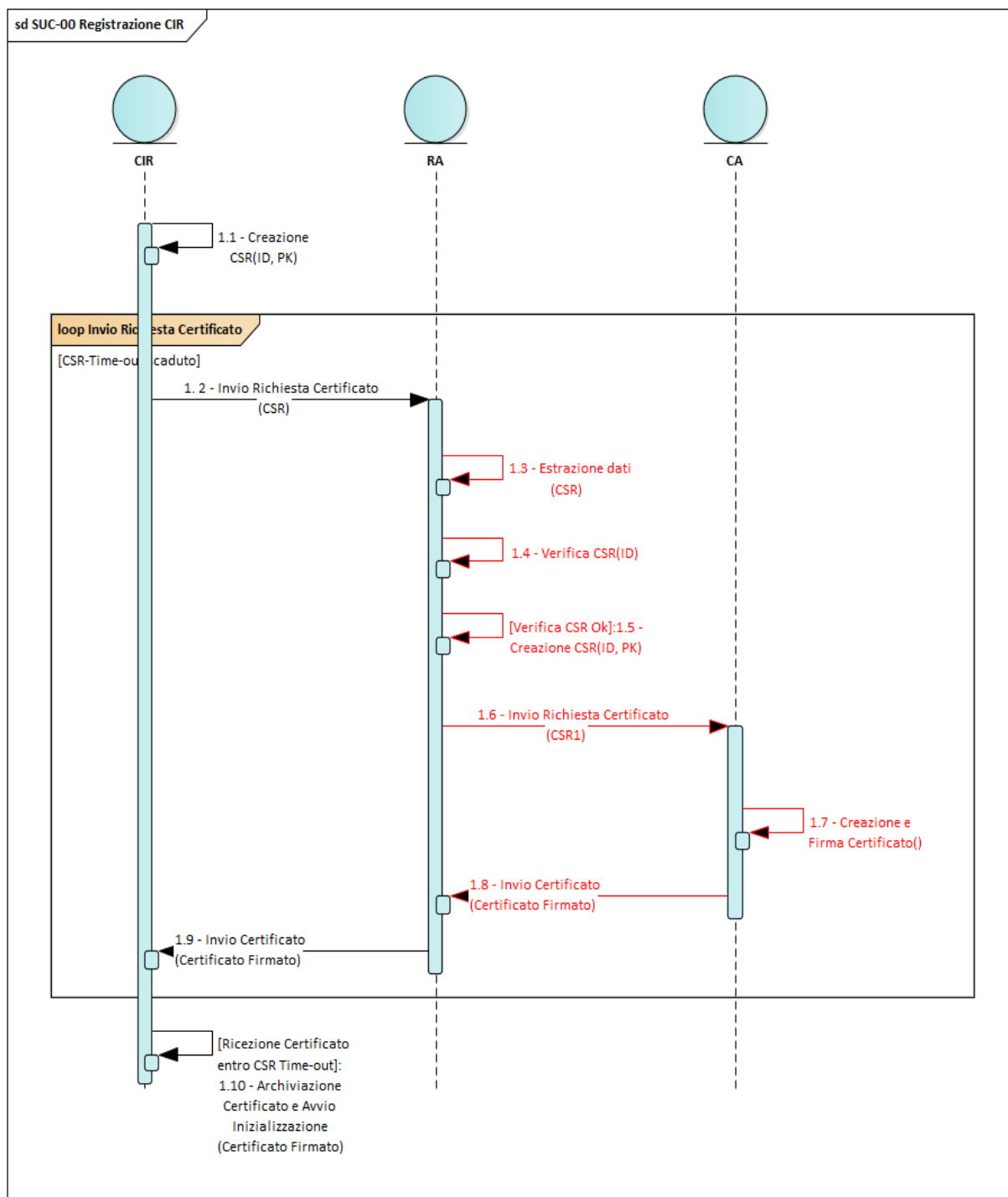
Identificativo	Nome	Descrizione del Requisito
Req1		Il CIR dispone di tutti i dati necessari alla creazione della CSR (Info1, Info2)
Req 2		Il CIR dispone di un certificato di preenrollment

Condizioni di uscita

Identificativo	Nome	Descrizione della Condizione di Uscita
EndC1		Il CIR riceve un certificato entro un CSR time-out
EndC2		La richiesta CSR fallisce per un numero di volte pari a CSR-max



Diagramma Sequenze





A.2 SUC-01: Inizializzazione interfaccia CIR-RO

Il System Use Case 01 definisce l'Inizializzazione dell'Interfaccia di Comunicazione CIR-RO. Per evidenziare la completa analogia della fase di inizializzazione lato CIR e lato RO si riportano i diagrammi di sequenza di due casi (SUC-01a per il CIR, SUC-01b per il RO), sebbene in forma concisa per SUC-01b.

Nel seguito viene fornita la descrizione di dettaglio del caso d'uso, differenziata in base al protocollo di comunicazione utilizzato.

A.2.1 Descrizione del Caso di Uso per il protocollo XMPP

Ambito e Obiettivi

Ambito e Obiettivi	
Ambito	Inizializzazione interfaccia CIR-RO
Obiettivi	Inizializzare interfaccia CIR-RO

Narrativa del Caso di Uso

Narrativa del Caso di Uso	
Descrizione breve	
Inizializzare l'interfaccia CIR-RO.	
Descrizione completa	
Il CIR sta funzionando in modalità Autonoma: si creano le condizioni per il passaggio alla modalità Asservita (es. comando impartito tramite interfaccia utente, scadenza timer di riconnessione, completamento fase di registrazione). Il CIR attiva in sequenza (SUC-01a): – una connessione TCP con il server XMPP cui è registrato; – uno stream XMPP sulla connessione TCP per la negoziazione della comunicazione sicura TLS; – una comunicazione sicura tramite il protocollo TLS basata su mutua autenticazione e profilo TLS predefinito; – uno stream XMPP sulla comunicazione TLS per la negoziazione dell'autenticazione SASL EXTERNAL; – uno stream XMPP per il binding di risorsa, che rimane attivo per i successivi scambi informativi di livello applicativo ossia per la comunicazione di telecontrollo con il RO. NOTA Il caso della inizializzazione dell'interfaccia di comunicazione lato RO (SUC-01b) è del tutto analogo e viene pertanto riportato in forma sintetica.	

Attori

RO, CIR, XMPP_SERVER_X, XMPP_SERVER_Y (vedi Sezione 3.1).

Requisiti

Req1		Il CIR è stato installato correttamente ivi comprese le connessioni alle soluzioni di comunicazione dati con la CSI e con il RO.
Req2		Le soluzioni di comunicazione sono state configurate correttamente, sia per quanto riguarda le connessioni locali riferite al punto precedente, sia per quanto riguarda le connessioni a lunga distanza (es. il percorso verso il RO).
Req3		Il CIR è stato abilitato preventivamente alla comunicazione con il RO previa procedura di registrazione.
Req4		Il CIR è stato configurato correttamente con gli endpoint di comunicazione e con il materiale necessario per il funzionamento delle soluzioni di cybersecurity (es. certificati digitali).



Analisi passo-passo dello scenario

Passo No	Nome del processo/attività	Descrizione del processo/attività	Mittente (attore)	Destinatario (attore)	Informazione scambiata (IDs)
1.1	Attivazione connessione TCP	Il CIR inizia la comunicazione TCP con il server XMPP cui fa riferimento, che la	CIR	XMPP_SERVER_X	
1.2	Attivazione stream XMPP	Il CIR inizia la comunicazione XMPP con il server XMPP, che la	CIR	XMPP_SERVER_X	
1.3	Proposta comunicazione TLS	Il server XMPP propone l'utilizzo di TLS	XMPP_SERVER_X	CIR	
1.4	Accettazione comunicazione TLS	Il CIR accetta l'utilizzo di TLS	CIR	XMPP_SERVER_X	
1.5	Conferma avvio comunicazione TLS: STARTTLS	Il CIR conferma l'utilizzo di TLS per tutte le comunicazioni successive	CIR	XMPP_SERVER_X	
1.6	Conferma avvio comunicazione TLS: PROCEED	Il server XMPP conferma l'utilizzo di TLS per tutte le comunicazioni successive	XMPP_SERVER_X	CIR	
1.7	Handshake TLS; comunicazioni client	Il CIR avvia la comunicazione TLS e svolge il ruolo del client	CIR	XMPP_SERVER_X	Certificato digitale CIR
1.8	Handshake TLS; comunicazioni server	Il server XMPP svolge il ruolo del server nella comunicazione TLS	XMPP_SERVER_X	CIR	Certificato digitale server XMPP
1.9	Attivazione stream XMPP	Il CIR attiva un nuovo stream XMPP con il server XMPP, che lo accetta	CIR	XMPP_SERVER_X	
2.0	Attivazione autenticazione SASL EXTERNAL	Il server XMPP propone l'utilizzo del meccanismo di autenticazione SASL EXTERNAL e il CIR lo accetta	XMPP_SERVER_X	CIR	



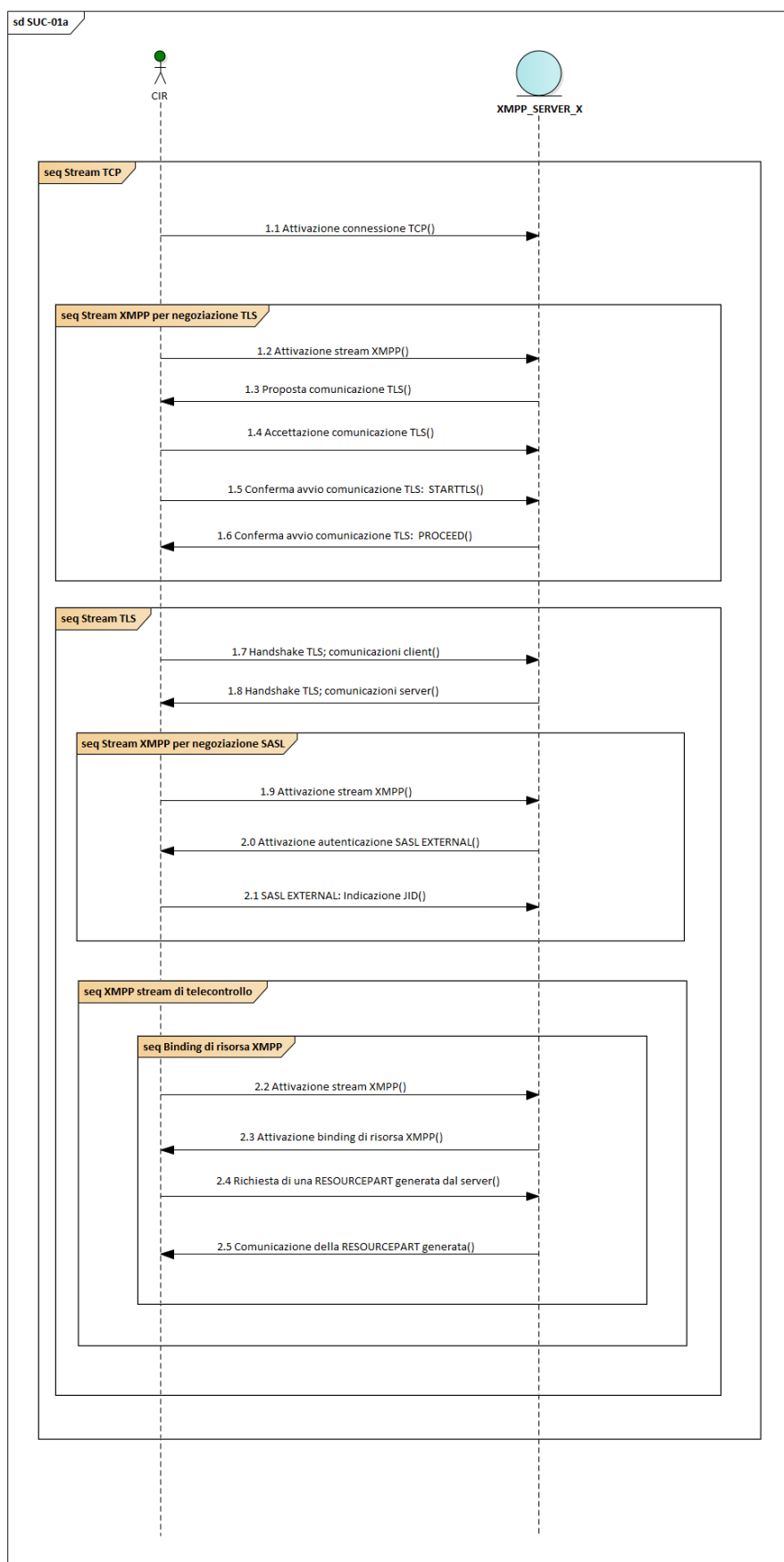
Passo No	Nome del processo/attività	Descrizione del processo/attività	Mittente (attore)	Destinatario (attore)	Informazioni scambiate (IDs)
2.1	SASL EXTERNAL: Indicazione JID	Il CIR indica il JabberID (JID) che intende utilizzare per l'autenticazione, e il server XMPP conferma il successo dell'operazione	CIR	XMPP_SERVER_X	JID
2.2	Attivazione stream XMPP	Il CIR attiva un nuovo stream XMPP con il server XMPP, che lo accetta	CIR	XMPP_SERVER_X	
2.3	Attivazione binding di risorsa XMPP	Il server XMPP avvia la negoziazione con il CIR della RESOURCEPART	XMPP_SERVER_X	CIR	
2.4	Richiesta di una RESOURCEPART generata dal server	Il CIR lascia al server XMPP il compito di generare una RESOURCEPART per il CIR	CIR	XMPP_SERVER_X	
2.5	Comunicazione della RESOURCEPART generata	Il server XMPP ha il compito di generare una RESOURCEPART per il CIR	XMPP_SERVER_X	CIR	RESOURCE PART

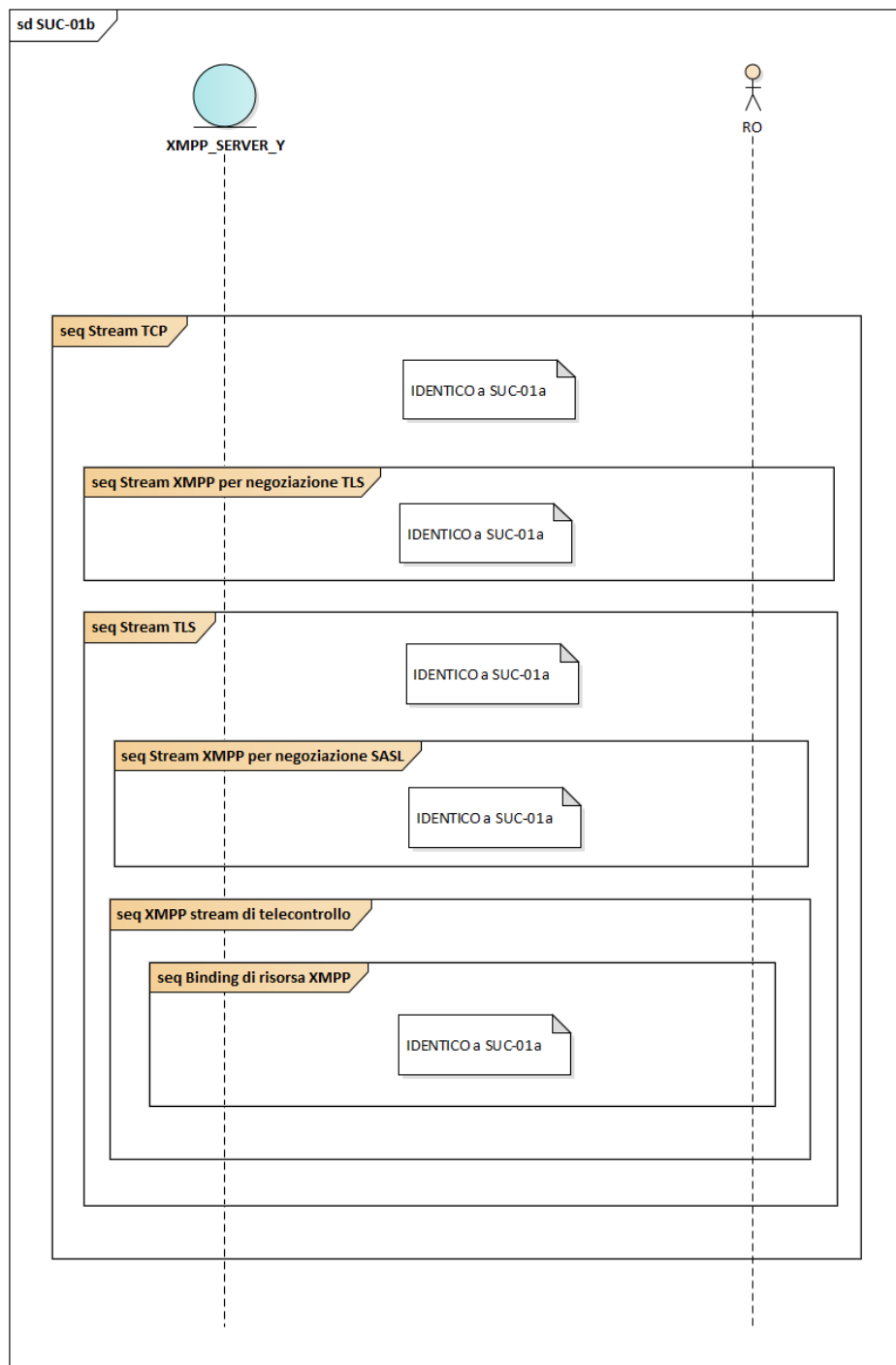
Informazioni scambiate

Identificativo	Nome della informazione	Descrizione della informazione scambiata
Info1	Certificato digitale del server XMPP (XMPP_server_X)	
Info2	Certificato digitale del CIR	
Info3	Jabber ID	Login (JID) da utilizzare per l'autenticazione nella architettura XMPP. Deve essere una JID contenuta nel certificato digitale perché viene usato il metodo di autenticazione SASL EXTERNAL.
Info 4	XMPP resource part	



Diagramma di sequenza SUC-01a



**Diagramma di sequenza SUC-01b**



A.2.2 Descrizione del Caso di Uso per il protocollo MQTT

Ambito e Obiettivi

Ambito e Obiettivi	
Ambito	Inizializzazione interfaccia CIR-RO
Obiettivi	Inizializzare interfaccia CIR-RO

Narrativa del Caso di Uso

Narrativa del Caso di Uso
Descrizione breve
Inizializzare l'interfaccia CIR-RO.
Descrizione completa
Il CIR sta funzionando in modalità Autonoma: si creano le condizioni per il passaggio alla modalità Asservita (es. comando impartito tramite interfaccia utente, scadenza timer di riconnessione, completamento fase di registrazione). Il CIR realizza la seguente sequenza di passi (SUC-01a-mqtt), ognuno dei quali deve essere completato con successo per l'avanzamento al successivo: – attiva una comunicazione TLS basata su mutua autenticazione e profilo TLS predefinito con il server MQTT configurato; – invia un pacchetto di controllo MQTT di tipo CONNECT indicando il proprio clientId; – verifica il buon esito del passo precedente analizzando i contenuti del pacchetto di controllo di risposta CONNACK. La comunicazione rimane attiva per i successivi scambi informativi di livello applicativo ossia per la comunicazione di telecontrollo con il RO. NOTA La comunicazione TLS implica una connessione TCP su cui la prima si basa. Nel caso di "implicit TLS", adottato da MQTT, le due vengono attivate in modo coordinato e unitario. Pertanto, si preferisce non indicarle separatamente in questa sezione, ma solo negli schemi successivi. NOTA 2 Il caso della inizializzazione dell'interfaccia di comunicazione lato RO (SUC-01b (MQTT)) è del tutto analogo e viene pertanto riportato in forma sintetica.

Attori

RO, CIR, MQTT_SERVER_X, MQTT_SERVER_Y (vedi Sezione 3.1).

Requisiti

Req1		Il CIR è stato installato correttamente ivi comprese le connessioni alle soluzioni di comunicazione dati con la CSI e con il RO.
Req2		Le soluzioni di comunicazione sono state configurate correttamente, sia per quanto riguarda le connessioni locali riferite al punto precedente, sia per quanto riguarda le connessioni a lunga distanza (es. il percorso verso il RO).
Req3		Il CIR è stato abilitato preventivamente alla comunicazione con il RO previa procedura di registrazione.
Req4		Il CIR è stato configurato correttamente, indicando gli endpoint di comunicazione e il materiale necessario per il funzionamento delle soluzioni di cybersecurity (es. certificati digitali).

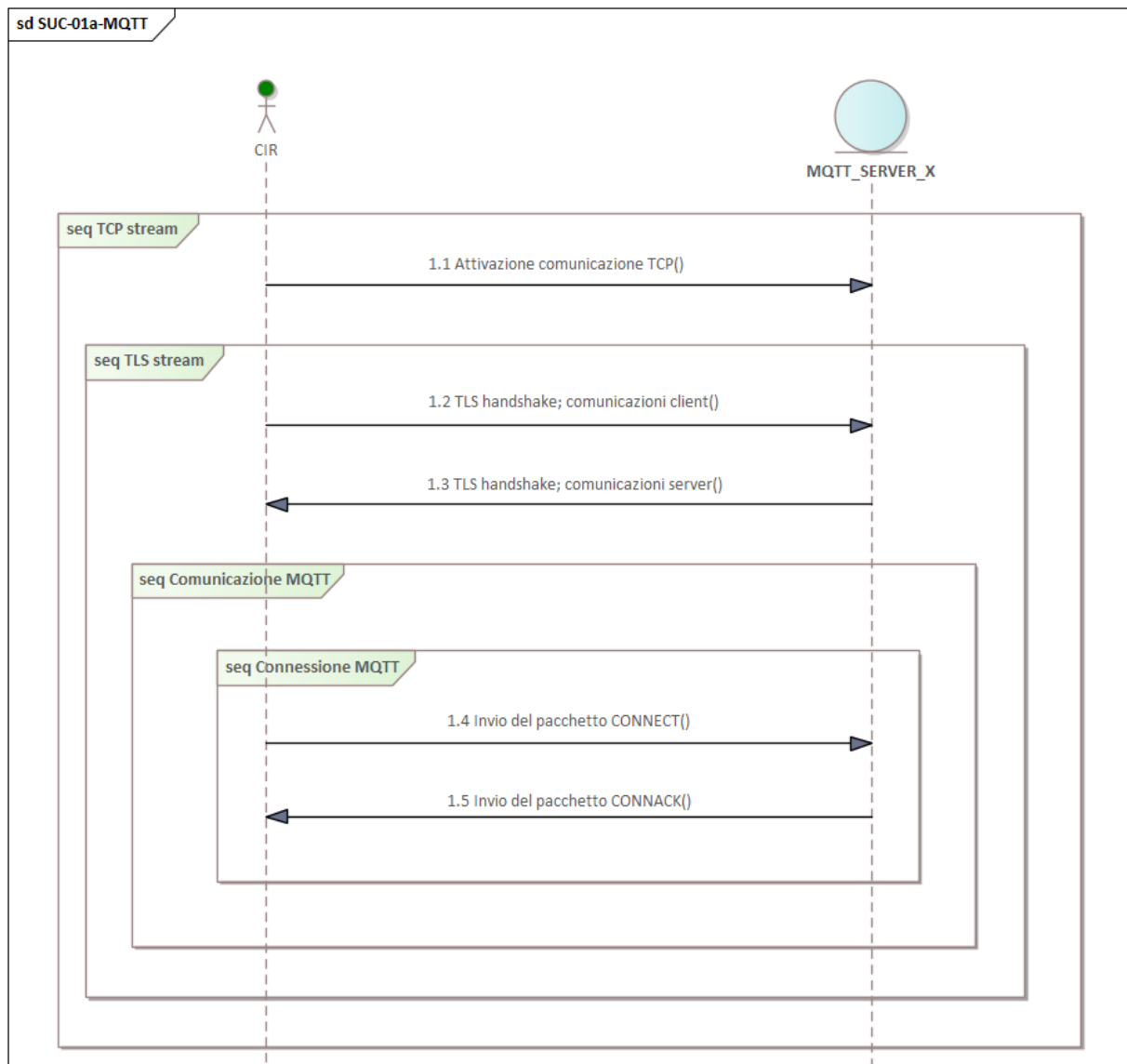


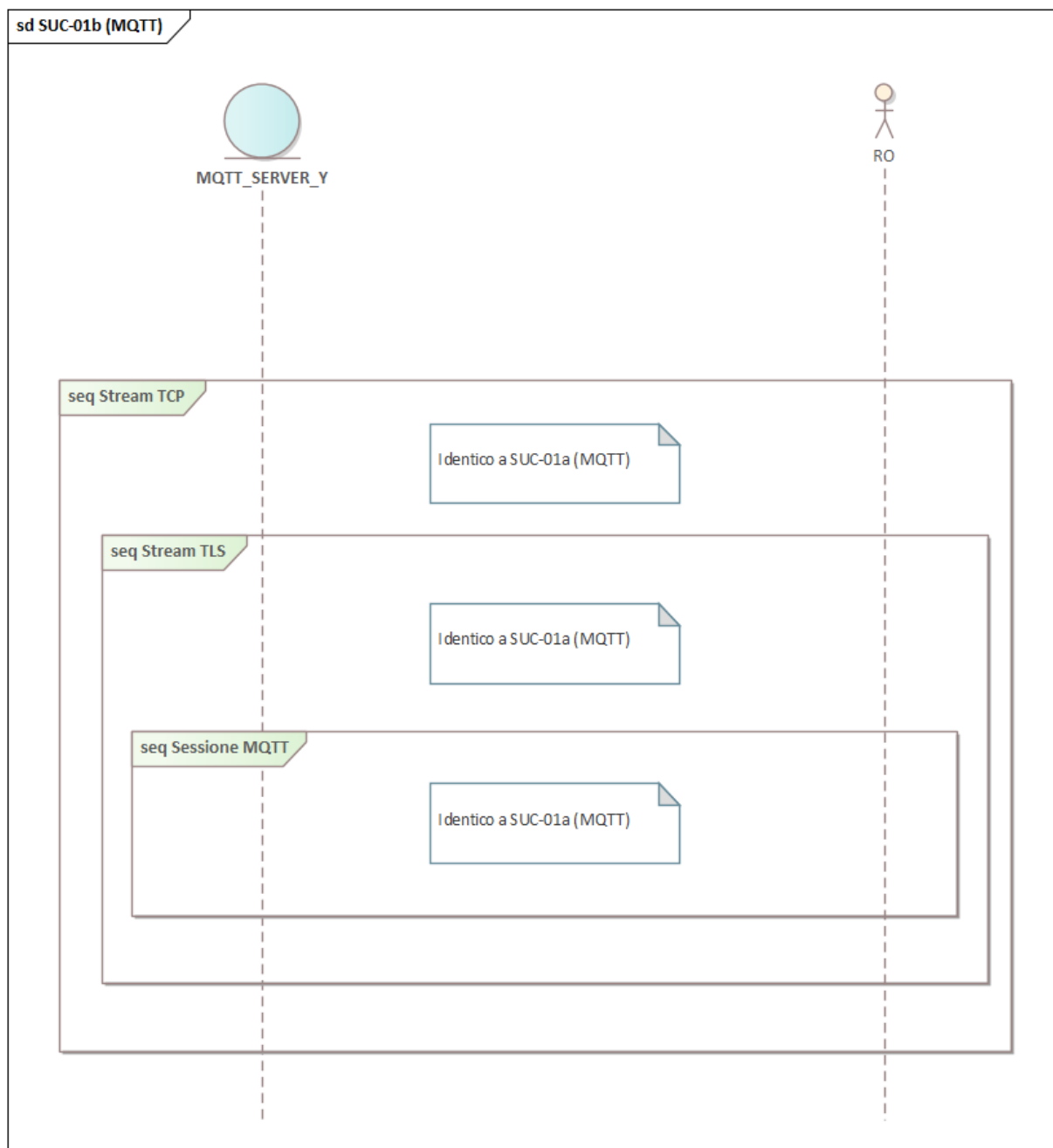
Analisi passo-passo dello scenario

Passo No	Nome del processo/attività	Descrizione del processo/attività	Mittente (attore)	Destinatario (attore)	Informazioni scambiate (IDs)
1.1	Attivazione comunicazione TLS su TCP	Il CIR inizia la comunicazione TCP per TLS con il server MQTT cui fa riferimento, che la accetta. Il CIR agisce come client TCP	CIR	MQTT_SERVER_X	
1.2	Handshake TLS; comunicazioni client	Il CIR svolge il ruolo del client nella comunicazione TLS	CIR	MQTT_SERVER_X	Certificato digitale CIR
1.3	Handshake TLS; comunicazioni server	Il server MQTT svolge il ruolo del server nella comunicazione TLS	MQTT_SERVER_X	CIR	Certificato digitale server MQTT
1.4	Invio del pacchetto MQTT CONNECT	Il CIR specifica i parametri di connessione da utilizzare tra cui il clientId	CIR	MQTT_SERVER_X	clientId
1.5	Invio del pacchetto MQTT di risposta CONNACK	Il server MQTT conferma il risultato della richiesta precedente (punto 1.4)	MQTT_SERVER_X	CIR	clientId

Informazioni scambiate

Identificativo	Nome della informazione	Descrizione della informazione scambiata
Info1	Certificato digitale del server MQTT (MQTT_server_X)	
Info2	Certificato digitale del CIR	
Info3	clientId.	Identificativo CIR_ID definito e comunicato dal RO in fase di Registrazione

**Diagramma di sequenza SUC-01a (MQTT)**

**Diagramma di sequenza SUC-01b (MQTT)**



A.3 SUC-02: Invio misure e stati

Viene nel seguito descritto il System Use Case 02 che riguarda l'invio al RO dei dati specifici del CIR.

Ambito e Obiettivi

Ambito e Obiettivi	
Ambito	I dati di misura di potenza istantanea acquisiti da M1 (e da M2, se presente), e da CSI, unitamente allo stato di CSI, vengono trasmessi periodicamente a CIR, e da CIR vengono inoltrati a RO
Obiettivi	Far pervenire periodicamente a RO i dati di misura di potenza istantanea e di stato di CSI, corretti e associati ai tempi di misura

Attori

CIR, RO, M1, M2, CSI (vedi Sezione 3.1).

Narrativa del Caso di Uso
Descrizione breve
Comunicare al RO i dati di misura di potenza e di stato indicati in X.7.1.1.1
Descrizione completa
Il CIR riceve da M1 i dati riportati nella Sezione X.7.1.2. Il CIR riceve da M2 i dati riportati nella Sezione X.7.3. Il CIR invia alla CSI una richiesta di ricezione dei dati riportati nella Sezione X.7.1.3.2. Il CIR riceve tali dati dal CSI. Il CIR invia a RO i dati aggregati di misura/stato ricevuti da M1, M2 e da CSI, ai dati sono associati il tempo di misura e un parametro di qualità del dato. Le misure/stati inviati comprendono: – Potenza attiva istantanea prelevata da CSI (nota1 e nota2) – Potenza attiva istantanea prelevata o immessa, rilevata dal misuratore intelligente 2G (M1) – Potenza attiva istantanea generata, se disponibile, rilevata dal misuratore intelligente 2G (M2) – Potenza disponibile – Tempo residuo prima del distacco del limitatore – Stato relativo alla infrastruttura di ricarica CSI (nota3). I dati di misura sono inviati ogni 20 secondi se CSI è nello stato Connesso. In caso di ricezione corretta, RO invia una conferma di ricezione dati a CIR, che corrisponde ad un messaggio di Keep Alive. Se la ricezione dati a RO non avviene correttamente, l'invio dei dati da CIR viene ripetuto dopo 2 secondi. La ritrasmissione viene ripetuta fino a 5 volte. Se dopo 5 ritrasmissioni la ricezione dati permane negativa, significa che il Keep Alive è fallito, che c'è un errore di comunicazione e che si ha una perdita di connessione. Se viene selezionato il comando di stop manuale il CIR notifica al RO sia lo stato di "CIR Asservito/Locale" a False che lo stato di "Disponibilità di flessibilità CIR" a False e successivamente passa alla modalità autonoma. NOTA 1 CSI ha il compito di convertire eventuali misure di corrente provenienti dalle EVSE in misure di potenza e di sommare tutti i dati in una sola misura di potenza aggregata da inviare a CIR. NOTA 2 Le misure relative alle EVSE rilevate da CSI saranno conformi alle Norme applicabili (MID o altre). NOTA 3 Lo stato di CSI è Connesso se almeno un EV è collegato ad una presa di EVSE, Non Connesso se non ci sono veicoli collegati, oppure Anomalia, se c'è un guasto.



Condizioni del Caso di Uso

Prerequisiti
– Esiste un canale di comunicazione sicuro tra CIR e RO, essendo attivato uno Stream con il Server XMPP del RO – Dopo l'apertura della sessione col RO, il CIR è nello stato di funzionamento "Asservito". – Esiste un canale di comunicazione sicuro tra CIR e M1 – Esiste un canale di comunicazione sicuro tra CIR e M2 – Esiste un canale di comunicazione attivo tra CIR e CSI

Analisi passo-passo dello scenario

Passo No	Nome del processo/attività	Descrizione del processo/attività	Mittente (attore)	Destinatario (attore)	Informazione scambiata (IDs)
1.1	Misure da M1	Il CIR riceve da M1 i dati di misura	M1	CIR	Info1 - misure secondo X.7.1.2
1.1bis	Misure da M2 (se presente)	Il CIR riceve da M2 i dati di misura	M2	CIR	Info1bis - misure secondo X.7.3
1.2	Richiesta dati a CSI	Il CIR invia a CSI una richiesta dati di misura.	CIR	CSI	Info2 – richiesta dati misura secondo X.7.1.3.2
1.3	Misure da CSI	Il CIR riceve da CSI i dati di misura	CSI	CIR	Info3 – misure secondo X.7.1.3.2
1.4	Misure a RO	Il CIR invia ad RO i dati di misura/stato ricevuti da M1 e da CSI,	CIR	RO	Info 4 – misure ricevute da M1 e CSI
1.5	Ritrasmissione	Se RO non riceve correttamente i dati, CIR ritrasmette dopo 2 secondi e ripete la trasmissione fino a 5 volte.	CIR	RO	Info 4 – misure ricevute da M1 e CSI
1.6	Conferma	RO invia a CIR una conferma di corretta ricezione, che corrisponde ad un messaggio Keep Alive	RO	CIR	Info5 – Ack ricezione dati



Informazioni scambiate

Identificativo	Nome della informazione	Descrizione della informazione scambiata
Info1	misure da M1 secondo X.7.1.2	Potenza attiva istantanea prelevata Potenza attiva istantanea immessa Tempo residuo prima del distacco del limitatore Potenza disponibile Tempo relativo alla misura effettuata
Info1 bis	Misure da M2 secondo X.7.3	Potenza attiva istantanea generata
Info2	richiesta dati di misura e stati a CSI	richiesta dei dati riportati in X.7.1.3.2.
Info3	Misure/stati da CSI secondo X.7.1.3.2	Potenza attiva istantanea prelevata da CSI Stato relativo alla infrastruttura CSI Tempo relativo alla misura effettuata
Info4	Misure/stati ricevute da M1, M2 e CSI e inviate a RO da CIR	Potenza attiva istantanea prelevata da CSI Potenza attiva istantanea prelevata o immessa, rilevata dal misuratore intelligente 2G (M1) Potenza attiva istantanea generata, se disponibile, rilevata dal misuratore intelligente 2G (M2) Potenza disponibile Stato relativo alla infrastruttura CSI Tempo relativo alle misure inviate Tempo residuo prima del distacco del limitatore
Info5	Ack corretta ricezione dei dati	Conferma inviata da RO, corrisponde ad un messaggio di Keep Alive

Requisiti

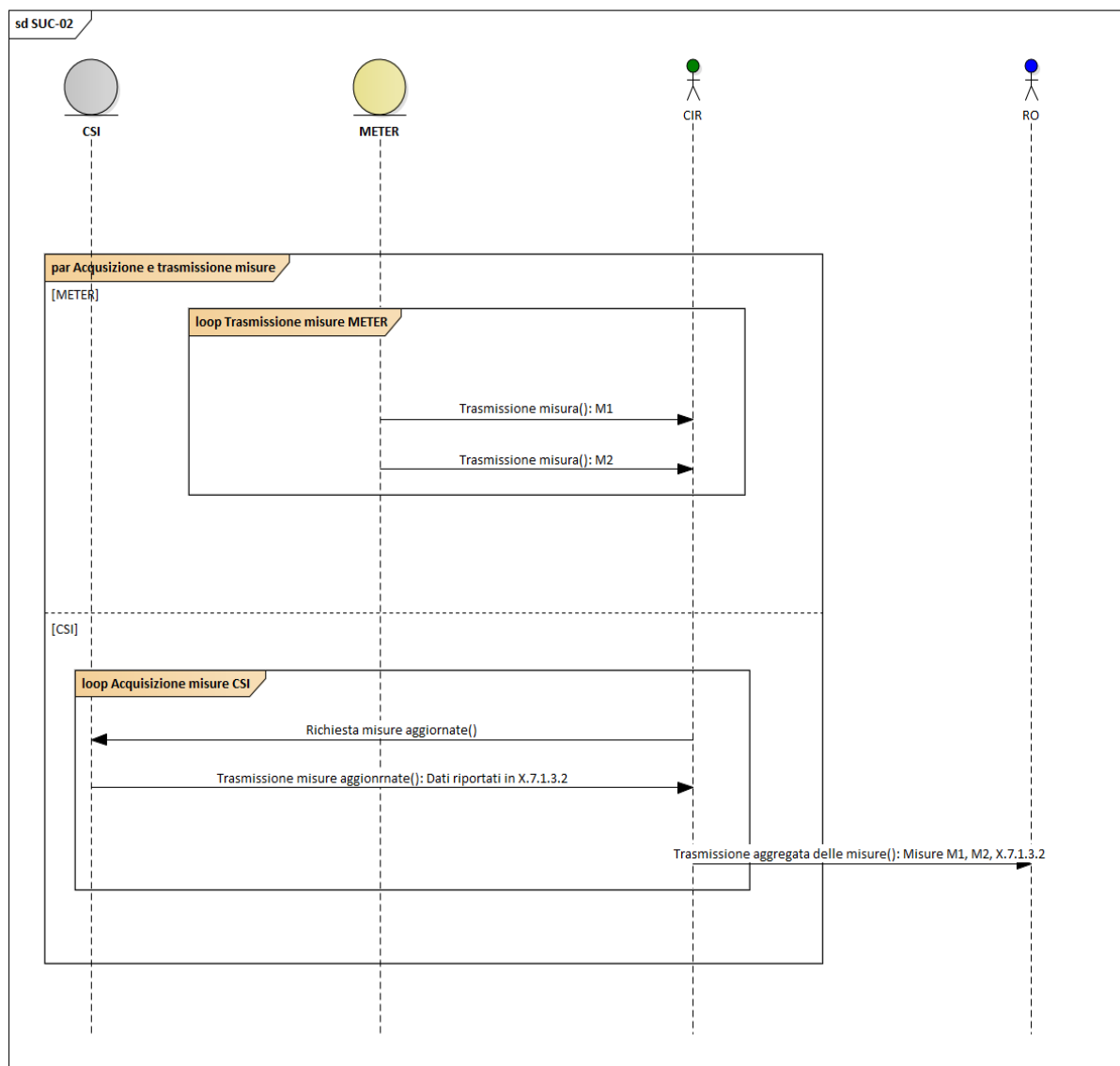
Identificativo	Nome	Descrizione del Requisito
Req1		CSI è in grado di raccogliere dalle EVSE i dati di misura/stati richiesti

Condizioni di uscita

Identificativo	Nome	Descrizione della Condizione di Uscita
EndC1		La comunicazione con RO si interrompe
EndC2		La comunicazione con M1 si interrompe
EndC3		La comunicazione con M2 si interrompe
EndC4		La comunicazione con CSI si interrompe



Diagramma Sequenze





A.4 SUC-03: Ricezione Comandi

Viene nel seguito descritto il System Use Case 03 che descrive l'invio del Comando di Modulazione di Potenza (CMP) e/o di Sospensione della Ricarica dal RO al CIR.

Ambito e Obiettivi

Ambito e Obiettivi	
Ambito	Modulazione della potenza di carica e sospensione della ricarica nel funzionamento Asservito del CIR, allo scopo di mantenere la potenza entro il limite massimo che può essere assorbito da rete
Obiettivi	Far pervenire al CIR il comando CMP (modulazione potenza di carica) e/o il comando di sospensione della carica in funzionamento Asservito

Attori

CIR, RO, M1, M2 e CSI (vedi Sezione 3.1).

Descrizione del Caso di Uso

Narrativa del Caso di Uso
Descrizione breve Il RO invia al CIR il CMP, Comando di Modulazione della Potenza, e/o il Comando di Sospensione. Il CMP è il valore della potenza massima da prelevare dalla Rete che l'Infrastruttura di Ricarica (CSI) governata dal CIR può utilizzare. Il CIR funziona in modalità Asservito
Descrizione complete Ai fini della partecipazione ai mercati MSF il RO coordina la distribuzione della potenza prelevata dalla rete dai vari CIR e da altre risorse di flessibilità, in base a informazioni e ordini provenienti da: • Altri RO; • Altri CIR; • CEM, EMMS, CSMS, CSP; • Informazioni tariffarie; • Informazioni sullo stato della rete. Dopo aver elaborato una distribuzione ottima di potenza sulle risorse di flessibilità disponibili, il RO invia al CIR un comando CMP con i dati indicati in X.7.1.1.2 che possono comprendere: 1) Modulazione della potenza massima dell'infrastruttura di ricarica CSI; 2) Sospensione della ricarica della infrastruttura CSI. Nel caso 1 il comando CMP include: • Potenza massima dell'infrastruttura di ricarica di X,xx kW per Y minuti, oppure • Potenza massima dell'infrastruttura di ricarica di X,xx kW fino alle hh:mm. Nel caso 2 il comando CMP include: • Comando di sospensione della ricarica per "Y minuti", oppure • Comando di sospensione della ricarica "fino alle hh:mm". Il CIR riscontra al RO la corretta ricezione del CMP, marcando il tempo della risposta. Se il RO non riceve riscontro entro un time out YY si ha il fallimento dell'invio del CMP. I comandi CMP consecutivi devono pervenire al CIR con cadenza temporale superiore al tempo Tatt, che corrisponde alla tempistica parametrizzabile per l'invio di comandi consecutivi al veicolo, per default pari a 30 secondi. I comandi che pervenissero prima di tale tempo verranno scartati con segnalazione a RO attraverso il relativo messaggio di Acknowledge, secondo quanto descritto nel paragrafo 7.3.5. Se l'utente decide di non aderire più al servizio, il CIR invia a RO un messaggio di passaggio allo stato di Non Abilitato al Servizio di Modulazione Potenza. Se RO decide di interrompere la richiesta di Servizio Modulazione Potenza invia messaggio al CIR di fine servizio (situazione diversa dalla sospensione della ricarica, che può essere una fase del servizio). Per motivi di sicurezza andrà previsto che il CIR effettui una verifica sul JabberID del mittente e accetti esclusivamente comunicazioni originate dal RO con cui ha in attivo un contratto.



Condizioni del Caso di Uso

Prerequisiti
– Esiste un canale di comunicazione sicuro tra CIR e RO, essendo attivato uno Stream con il Server XMPP del RO – Esiste un canale di comunicazione attivo tra CIR e CSI – Il CIR è nello stato di funzionamento “Asservito”. – RO ha elaborato la distribuzione ottima di potenza tra le risorse aggregate disponibili

Analisi passo-passo dello scenario

Passo No	Nome del processo/attività	Descrizione del processo/attività	Mittente (attore)	Destinatario (attore)	Informazione scambiata (IDs)
1.1	Comando CMP al CIR	RO invia al CIR il comando CMP di modulazione potenza o di sospensione ricarica	RO	CIR	Info1 – comando CMP secondo X.7.1.1.2
1.2	Conferma ricezione CMP da CIR	Il CIR invia a RO un riscontro di ricezione del comando CMP, con segnalazione se deve essere scartato perché arrivato prima del tempo minimo di attesa	CIR	RO	Info2 – riscontro ricezione CMP
1.3	Invio comandi a CSI	Il CIR invia comandi a CSI dopo elaborazione CMP	CIR	CSI	
1.4	Fine servizio e invio CMP	RO invia al CIR segnale di fine servizio modulazione potenza. A causa di fallimento della comunicazione comando CMP al CIR, oppure per decisione di RO.	RO	CIR	Info3 – fine servizio modulazione potenza



Informazioni scambiate

Identificativo	Nome della informazione	Descrizione della informazione scambiata
Info1	comando CMP secondo X.7.1.1.2	1) Modulazione della potenza massima dell'infrastruttura di ricarica CSI; 2) Sospensione della ricarica della infrastruttura CSI Nel caso 1 il comando CMP include: Potenza massima dell'infrastruttura di ricarica di X,xx kW per Y minuti, oppure Potenza massima dell'infrastruttura di ricarica di X,xx kW fino alle hh:mm Nel caso 2 il comando CMP include: Comando di sospensione della ricarica per "Y minuti", oppure Comando di sospensione della ricarica "fino alle hh:mm"
Info2	Ricezione di CMP	Riscontro di ricezione del comando CMP, con marcatura del tempo. In caso di comando CMP da scartare, perché ricevuto prima del tempo limite, viene segnalato a RO
Info3	Fine modulazione potenza	RO comunica la fine del Servizio di Modulazione Potenza e dello invio di comandi CMP al CIR

Requisiti

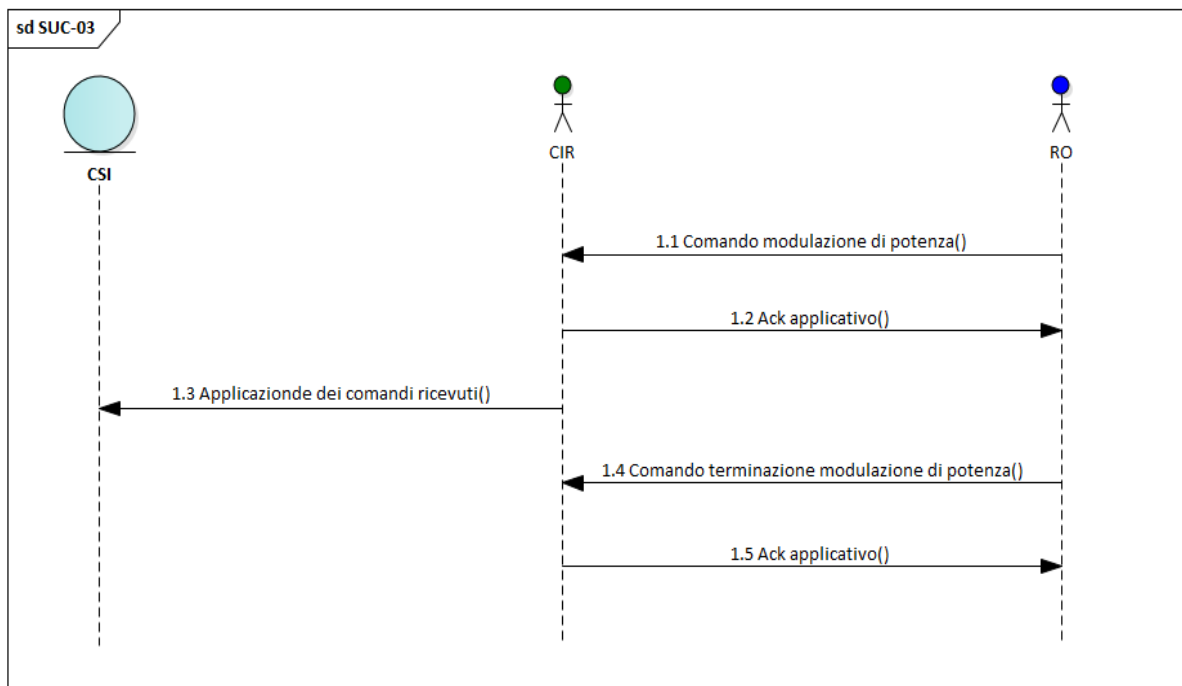
Identificativo	Nome	Descrizione del Requisito
Req1		RO è in grado di elaborare la distribuzione ottima di potenza sulle risorse aggregate e continua ad inviare comandi CMP al CIR
Req2		Il canale di comunicazione tra RO e CIR funziona correttamente
Req3		Il canale di comunicazione tra CIR e CSI funziona correttamente
Req4		IL CIR permane nello stato Asservito

Condizioni di uscita

Identificativo	Nome	Descrizione della Condizione di Uscita
EndC1		La comunicazione tra CIR e RO si interrompe
EndC2		La comunicazione tra CIR e CSI si interrompe
EndC3		RO cessa invio di comandi CMP per fine servizio (invio segnalazione di fine del Servizio di Modulazione Potenza) o per altri motivi
EndC4		Il CIR passa dallo stato Asservito allo stato Autonomo



Diagramma Sequenze





A.5 SUC-04: KeepAlive

Viene nel seguito descritto il System Use Case 04 che descrive la procedura di KeepAlive.

SUC-04.1 Descrizione del Caso di Uso

Narrativa del Caso di Uso
Descrizione breve
La procedura di KeepAlive viene gestita a livello di messaggi applicativi
Descrizione complete
Per non appesantire gli scambi informativi con traffico supplementare, ma far fronte alla necessità di identificare eventuali problemi di comunicazione, la funzionalità di KeepAlive viene implementata per mezzo dei messaggi applicativi scambiati tra le parti. La procedura di KeepAlive viene gestita a livello di messaggi contenenti le misure inviate periodicamente (vedi SUC-02) a cui è associato un ACK a livello applicativo. Nel caso si riscontrassero problemi alle comunicazioni il CIR esegue la procedura di perdita della connessione (vedi SUC-06).

Ambito e Obiettivi

Ambito e Obiettivi	
Ambito	Procedura di KeepAlive per verificare in modo continuo la connessione tra RO e CIR
Obiettivi	Monitorare lo stato della connessione tra RO e CIR e intervenire in caso di interruzione

Attori

RO, CIR, XMPP/MQTT_SERVER (vedi Sezione 3.1).

Condizioni del Caso di Uso

Prerequisiti
Prerequisiti:
- Esiste un canale di comunicazione sicuro tra CIR e RO, essendo attivato uno Stream con il Server XMPP o una sessione con il broker MQTT del RO - Dopo l'apertura della sessione col RO, il CIR è nello stato di funzionamento "Asservito".

Analisi passo-passo dello scenario

Passo No	Nome del processo/attività	Descrizione del processo/attività	Mittente (attore)	Destinatario (attore)	Informazione scambiata (IDs)
1.1	Messaggio applicativo	Il CIR invia un messaggio applicativo all'RO	CIR	RO	Msg
1.2	Risposta	RO invia conferma ricezione del messaggio tramite un ACK applicativo	RO	CIR	Msg_ack

Informazioni scambiate

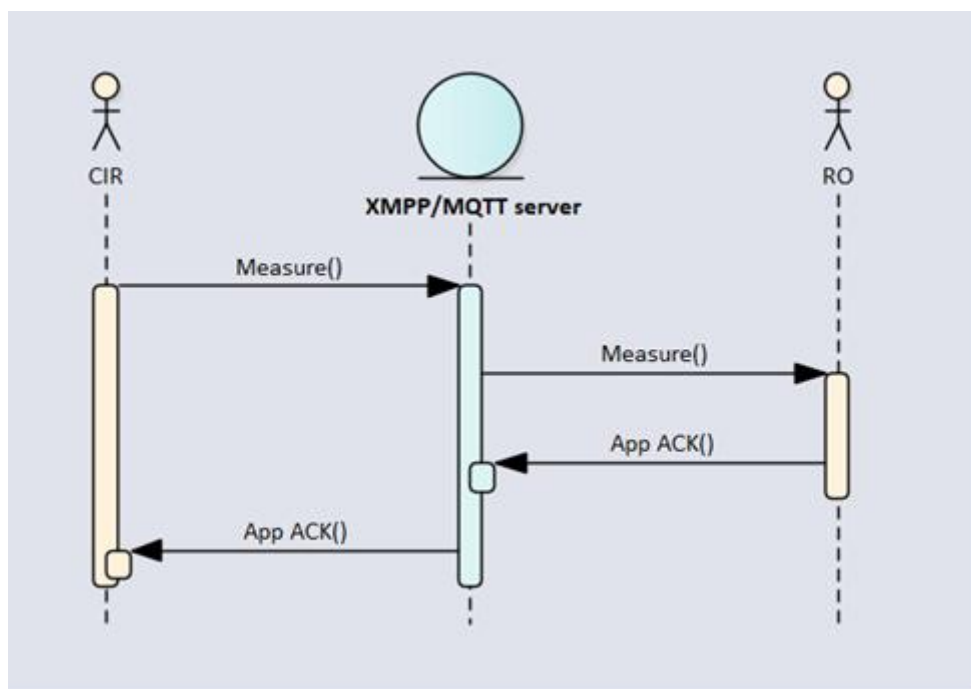
Identificativo	Nome della informazione	Descrizione della informazione scambiata
Msg	Messaggio applicativo	Messaggio contenente misure
Msg_ack	Messaggio ricezione messaggio	Messaggio contenente un ack di ricezione a livello applicativo



Condizioni di uscita

Identificativo	Nome	Descrizione della Condizione di Uscita
EndC1		Il CIR riceve il messaggio di conferma e rimane nella modalità asservita
EndC2		Il CIR non riceve il messaggio di conferma dall'RO e esegue procedura perdita connessione (SUC-06)

Diagramma Sequenze





A.6 SUC-05: Deregistrazione CIR

Viene nel seguito descritto il System Use Case 05 relativo alla procedura di Deregistrazione definitiva del CIR presso RO.

SUC-05.1 Descrizione del Caso di Uso

Ambito e Obiettivi

Ambito e Obiettivi	
Ambito	Deregistrazione definitiva del CIR presso RO
Obiettivi	Interrompere l'operatività del servizio di flessibilità fornito dal CIR a RO

Narrativa del Caso di Uso	
Descrizione breve	
Il RO provvede alla de-registrazione del CIR, che comporta la revoca del certificato presso la CA che lo ha emesso e la disabilitazione delle comunicazioni tra CIR ed RO.	
Descrizione completa	
Su iniziativa del RO, o su richiesta dell'utente CIR, viene eseguita la procedura di de-registrazione descritta nel seguito: • RO chiede la revoca del certificato di connessione al server (XMPP o MQTT) del CIR alla CA che lo ha emesso; la revoca può impiegare un tempo variabile (es. giorni) sulla base del livello di servizio concordato tra RO e CA. • Il RO può decidere di cessare di accettare comunicazioni da parte del CIR anticipatamente alla diffusione dell'informazione relativa alla revoca del certificato del CIR (tramite CRL o OCSP) ad esempio filtrando il suo CIR_ID, in conformità con il contratto stipulato con l'utente CIR; • La CA pubblica l'informazione di revoca tramite i meccanismi previsti da questa specifica (i.e. CRL e OCSP) che consentono agli attori di usufruirne per verificare l'abilitazione all'accesso all'infrastruttura; • Il CIR verifica periodicamente lo stato di revoca del proprio certificato mediante le soluzioni CRL o OCSP; la periodicità di questa verifica deve essere configurabile e allineata alla periodicità di emissione delle CRL (es. almeno giornaliera). Qualora il CIR determini che il proprio certificato è stato revocato per deregistrazione da parte del RO, passa in modalità autonoma terminando così eventuali connessioni attive verso i server dell'infrastruttura; • Sulla base di come è configurato, il CIR può eliminare le informazioni relative alla registrazione presso il RO dalla propria memoria. Questa funzionalità deve poter essere abilitata o disabilitata tramite un parametro configurabile nel dispositivo. Nel caso il CIR sia configurato per non eliminare attivamente le informazioni, queste verranno sovrascritte in occasione della successiva registrazione presso un RO. Nel caso la richiesta di deregistrazione sia iniziativa dell'utente CIR, questi dovrà preventivamente contattare il RO con le modalità previste dal contratto, che non sono oggetto di questa specifica. Verrà quindi attivata la procedura sopra descritta.	



Attori

RO, CIR, CA (vedi Sezione 3.1).

Condizioni del Caso di Uso

Prerequisiti
– Contratto CIR-RO scaduto o revocato da una delle parti

Analisi passo-passo dello scenario

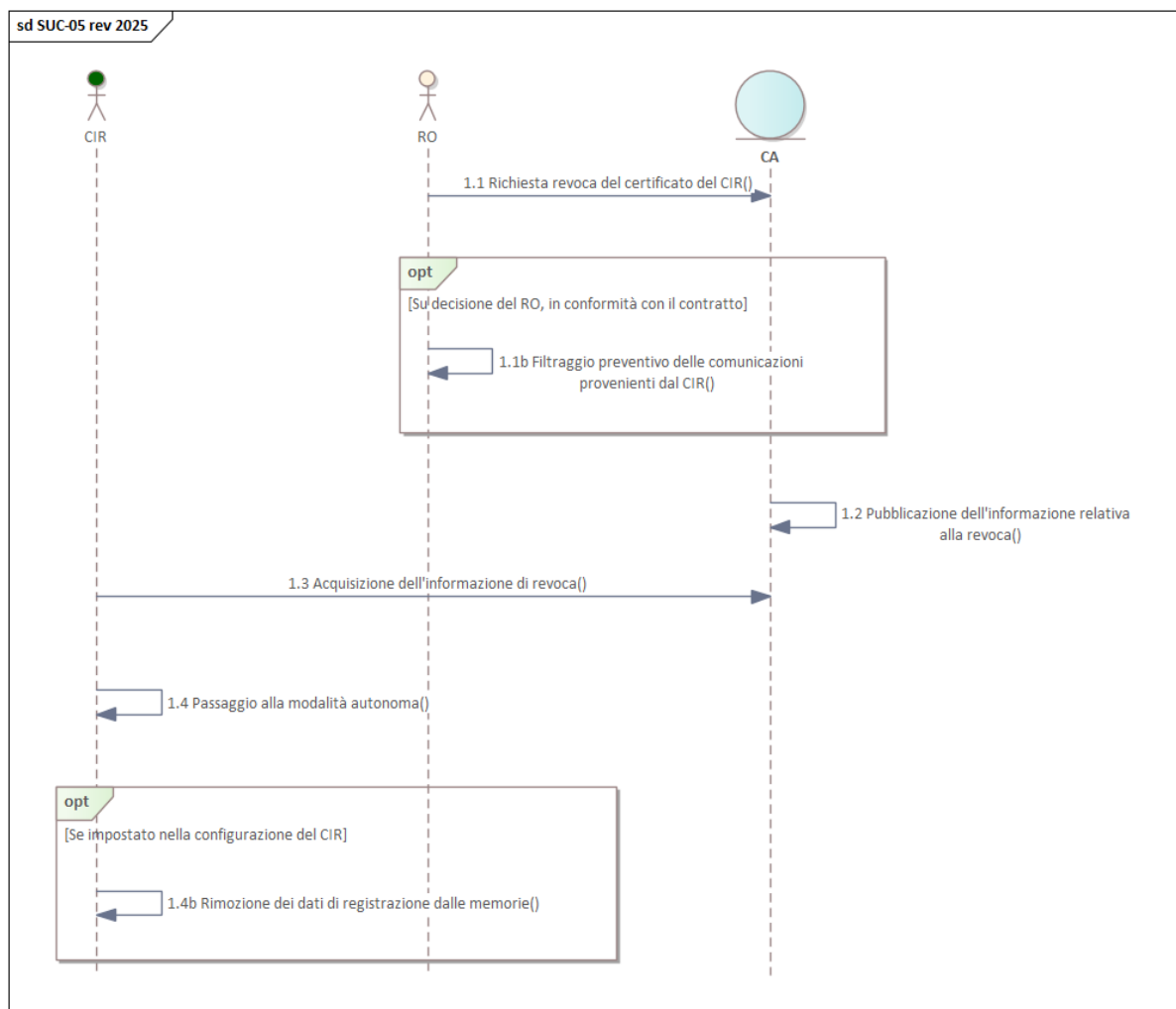
Passo No	Nome del processo/attività	Descrizione del processo/attività	Mittente (attore)	Destinatario (attore)	Informazioni e scambiata (IDs)
1.1	Richiesta revoca del certificato del CIR	Il RO chiede la revoca del certificato attraverso il quale il CIR si connette ai server XMPP/MQTT	RO	CA	Info1
1.1b	Filtraggio preventivo delle comunicazioni provenienti dal CIR	Il RO, se lo ritiene opportuno e se conforme con il contratto stipulato con l'utente CIR, cessa di accettare dati provenienti dal CIR anticipatamente alla diffusione della revoca del certificato da parte della CA.	RO	RO	Info2
1.2	Pubblicazione dell'informazione relativa alla revoca	La CA pubblica, con i meccanismi previsti (i.e. CRL, OCSP), l'informazione di revoca del certificato del CIR.	CA	CA	
1.3	Acquisizione dell'informazione di revoca	Il CIR, se non preventivamente disabilitato, verifica periodicamente lo stato del proprio certificato.	(Client XMPP/MQTT) CIR	CA	Info1
1.4	Passaggio alla modalità autonoma	Nel caso il proprio certificato sia stato revocato per deregistrazione il CIR passa alla modalità autonoma.	(Client XMPP/MQTT) CIR	(Client XMPP/MQTT) CIR	
1.4b	Rimozione dei dati di registrazione dalle memorie	Nel caso il proprio certificato sia stato revocato e se configurato opportunamente il CIR può rimuovere i dati di registrazione dalle memorie interne.	(Client XMPP/MQTT) CIR	(Client XMPP/MQTT) CIR	



Informazioni scambiate

Identificativo	Nome della informazione	Descrizione della informazione scambiata
Info1	Identificativo CIR a livello CA	Informazione per identificare univocamente presso la CA il CIR che deve essere deregistrato (es. numero seriale del certificato digitale)
Info2	Identificativo CIR a livello protocollo XMPP/MQTT	Informazione per identificare univocamente a livello del protocollo applicativo (es. JabberID o stringa CIR_ID)

Diagramma Sequenze





A.7 SUC-06: Perdita della connessione CIR-RO e passaggio a funzionamento Autonomo

Viene nel seguito descritto il System Use Case 06 che descrive il caso di perdita della connessione tra CIR e RO e il passaggio alla modalità di funzionamento Autonomo.

Descrizione del Caso di Uso

Narrativa del Caso di Uso	
Descrizione breve	
Perdita della connessione tra CIR e RO e passaggio alla modalità di funzionamento Autonomo del CIR.	
Descrizione completa	
La connessione fra CIR e RO è aperta e il CIR funziona in modalità "Asservita". Sopravviene una interruzione del canale di comunicazione col RO, ad esempio segnalata dal SUC-04. Sono possibili differenti casi: • Problemi nelle comunicazioni CIR – server (XMPP o MQTT) • Problemi nelle comunicazioni server (XMPP o MQTT) – RO • Problemi in entrambe le comunicazioni Il CIR passa in funzionamento "Autonomo". Nella modalità di controllo autonomo e in assenza di un comando di modulazione in corso, il CIR modula la potenza prelevata da CSI sulla base dei soli dati di potenza prelevata e immessa rilevati da M1 e sulla base di parametri impostati in precedenza dal gestore dell'impianto o dal progettista, tramite interfaccia locale o remota, ovvero operando la logica di <i>power management</i> descritta nell'Allegato X della Norma CEI 0-21. Nel caso in cui la perdita di connessione avvenga durante un comando di modulazione in corso, il comando viene portato a termine dal CIR (il limite di potenza richiesto dal comando viene mantenuto fino alla scadenza del comando). Al fine di evitare l'intervento del sistema di protezione degli accumulatori dell'autoveicolo, l'invio di comandi consecutivi al veicolo avviene secondo un intervallo di tempo (Tatt) parametrizzabile tra 1 e 60 secondi con valore di default pari a 30 secondi. Il CIR tenta di ristabilire la connessione col RO ad intervalli prestabiliti: Se il CIR ha perso la comunicazione con il server (XMPP o MQTT) il CIR rilancia la procedura di "Inizializzazione" descritta da SUC-01a (connessione tra CIR e server XMPP o MQTT). Se RO rileva una perdita di connessione con il server (XMPP o MQTT) rilancia la procedura di "Inizializzazione" descritta da SUC-01b (connessione tra RO e server XMPP o MQTT). Se la procedura di inizializzazione va a buon fine, il CIR transita nella modalità "Asservita" altrimenti rimane nella modalità "Autonoma".	

Ambito e Obiettivi

Ambito e Obiettivi	
Ambito	Perdita della connessione tra RO e CIR, passaggio al funzionamento Autonomo e tentativi di ripristino della connessione
Obiettivi	In caso di interruzione della connessione tra CIR e RO operare il passaggio al funzionamento Autonomo e tentare di ripristinare la connessione fino alla sua riattivazione



Attori

CIR (vedi Sezione 3.1).

Condizioni del Caso di Uso

Prerequisiti
– Esiste un canale di comunicazione sicuro tra CIR e RO, essendo attivato uno Stream con il Server XMPP o una sessione con il broker MQTT del RO – Dopo l'apertura della sessione col RO, il CIR è nello stato di funzionamento "Asservito".

Analisi passo-passo dello scenario

Passo No	Nome del processo/attività	Descrizione del processo/attività	Mittente (attore)	Destinatario (attore)	Informazione scambiata (Ids)
1.1	Modalità autonoma	Non c'è comunicazione tra CIR e RO e il CIR passa in modalità autonoma	CIR	CIR	
1.2	Modalità asservita	Viene ripristinata la comunicazione tra CIR e RO	CIR	CIR	

Informazioni scambiate

Identificativo	Nome della informazione	Descrizione della informazione scambiata
Pot_prel	Potenza prelevata	Messaggio a CSI per modulare potenza prelevata
Pot_prel_imm	Potenza prelevata e immessa	Messaggio da M1 contenente potenza prelevata e immessa
Sett	Parametri di funzionamento	Parametri impostati in precedenza dal gestore dell'impianto o dal progettista, tramite interfaccia locale o remota

Condizioni di uscita

Identificativo	Nome	Descrizione della Condizione di Uscita
EndC1		Il CIR riesce a riconnettersi passando alla modalità asservita
EndC2		Il CIR non riesce a riconnettersi e rimane in modalità autonoma



A.8 SUC-07: Aggiornamento configurazione

Il System Use Case 07 descrive l'aggiornamento della configurazione, e quindi dei parametri operativi, dell'Infrastruttura di Ricarica gestita dal CIR.

Descrizione del Caso di Uso

Narrativa del Caso di Uso	
Descrizione breve	
Aggiornamento della configurazione e della Infrastruttura di Ricarica (CSI) gestita dal CIR.	
Descrizione completa	
La sessione fra CIR e RO è aperta e il CIR funziona in modalità "Asservita". L'Utente CIR vuole cambiare la configurazione di impianto. A questo scopo l'Utente CIR, tramite l'Interfaccia Utente, invia al CIR il comando di passaggio alla modalità Autonoma. Il CIR passa in modalità Autonoma (stop manuale). L'utente CIR aggiorna la configurazione della CSI. L'utente CIR aggiorna i parametri operativi della CSI nel CIR (oppure il CIR acquisisce automaticamente la nuova configurazione se abilitato a farlo). Infine l'Utente CIR, tramite l'Interfaccia Utente CIR, impartisce il comando di passaggio alla modalità Asservita.	

Ambito e Obiettivi

Ambito e Obiettivi	
Ambito	Aggiornamento dei parametri di configurazione della CSI, per intervenute modifiche nella composizione della Infrastruttura di Ricarica.
Obiettivi	Riprogrammare il CIR per inserire la nuova configurazione della CSI dopo le modifiche.

Attori

CIR, CIR_USER, CSI, XMPP_SERVER o MQTT_SERVER

Requisiti

Identificativo	Nome	Descrizione del Requisito
Req1		Il CIR si trova in modalità Asservita.



Analisi passo-passo dello scenario

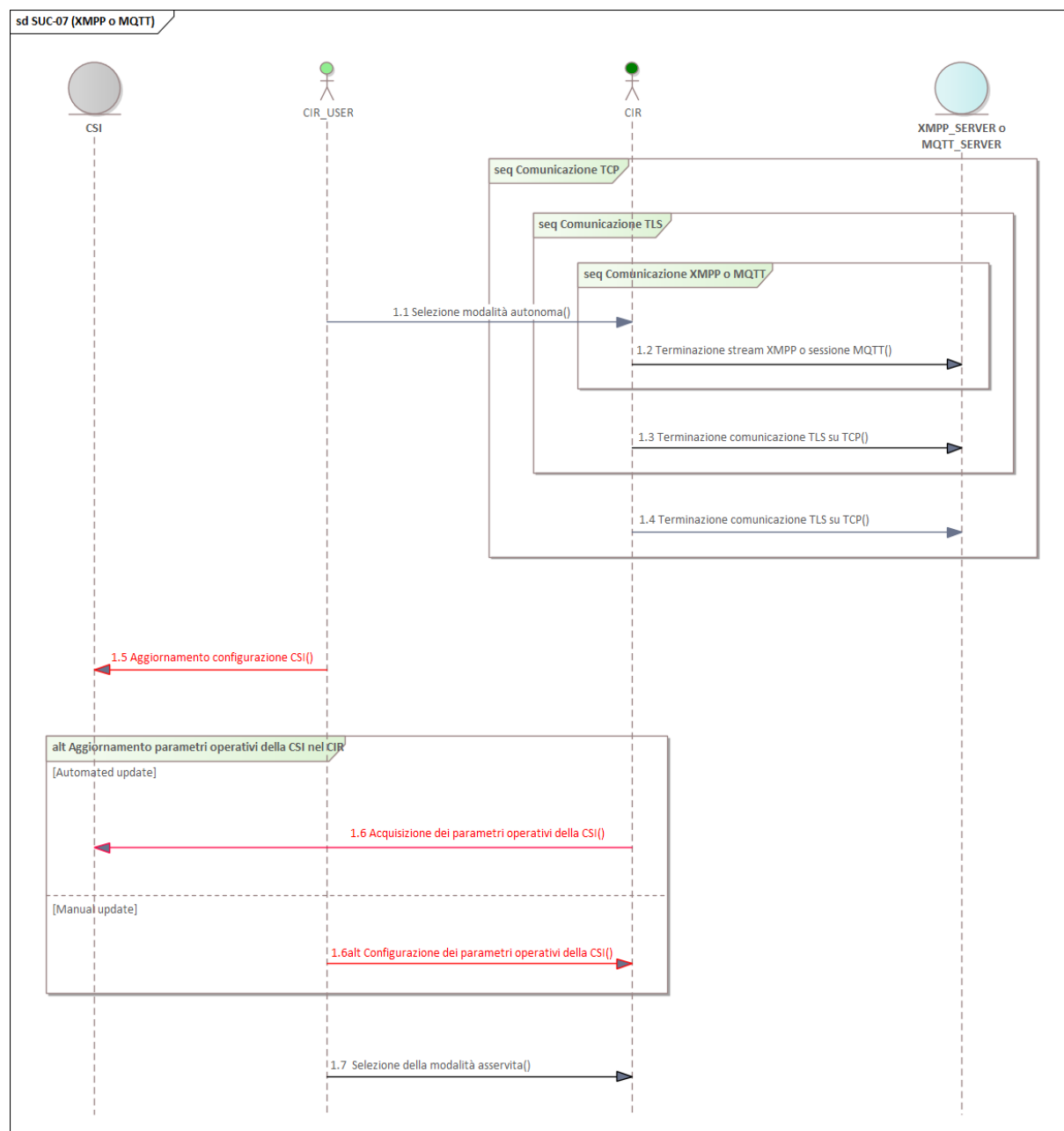
Passo No	Nome del processo/attività	Descrizione del processo/attività	Mittente (attore)	Destinatario (attore)	Informazioni scambiate (Ids)
1.1	Selezione modalità autonoma	L'utente CIR seleziona la modalità autonoma tramite l'interfaccia utente.	CIR_USER	CIR	
1.2	Terminazione stream XMPP o sessione MQTT	Il CIR termina lo stream XMPP o la sessione MQTT con il server XMPP/MQTT di riferimento, che prende atto della terminazione.	CIR	XMPP_SERVER_X o MQTT_SERVER_X	
1.3	Terminazione comunicazione TLS	Il CIR termina la comunicazione TLS con il server XMPP di riferimento, che prende atto della terminazione.	CIR	XMPP_SERVER_X o MQTT_SERVER_X	
1.4	Terminazione comunicazione TCP	Il CIR termina la comunicazione TCP con il server XMPP/MQTT di riferimento, che prende atto della terminazione.	CIR	XMPP_SERVER_X o MQTT_SERVER_X	
1.5	Aggiornamento configurazione CSI	L'utente CIR aggiorna la configurazione della Infrastruttura di ricarica.	CIR_USER	CSI	
1.6	Acquisizione dei parametri operativi della CSI	Il CIR acquisisce in modo automatico i parametri operativi aggiornati della CSI	CIR	CSI	Parametri operativi aggiornati
1.6 alt	Configurazione dei parametri operativi della CSI	In alternativa al punto precedente, l'utente CIR configura i parametri operativi aggiornati tramite l'interfaccia utente.	CIR_USER	CIR	Parametri operativi aggiornati
1.7	Selezione modalità asservita	L'utente CIR seleziona la modalità asservita tramite l'interfaccia utente.	CIR_USER	CIR	



Informazioni scambiate

Identificativo	Nome della informazione	Descrizione della informazione scambiata
Info 1	Parametri operativi della CSI	Sono i parametri operativi della infrastruttura CSI che permettono al CIR di interagire con essa.

Diagramma di sequenza

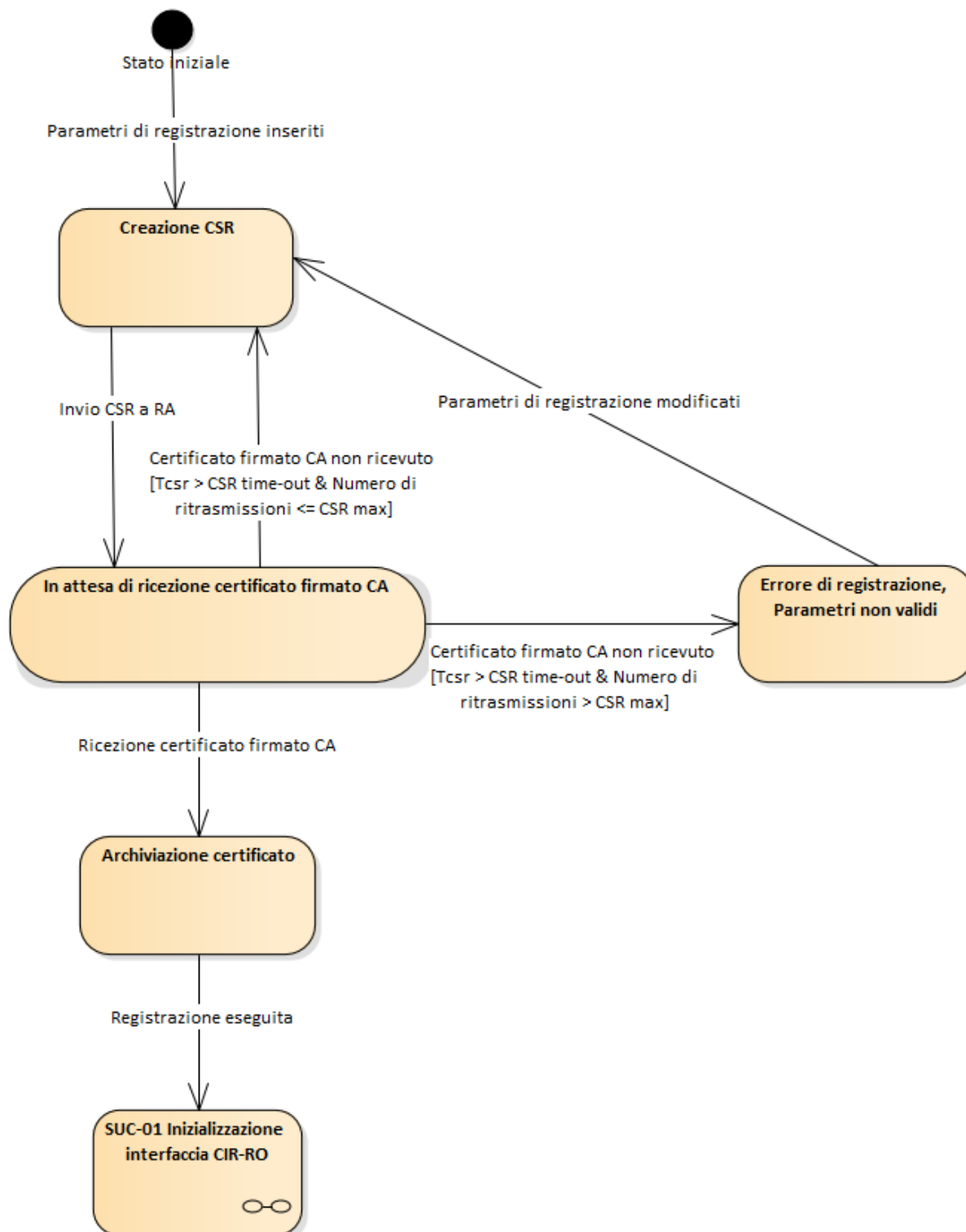




Allegato B

Macchine a stati

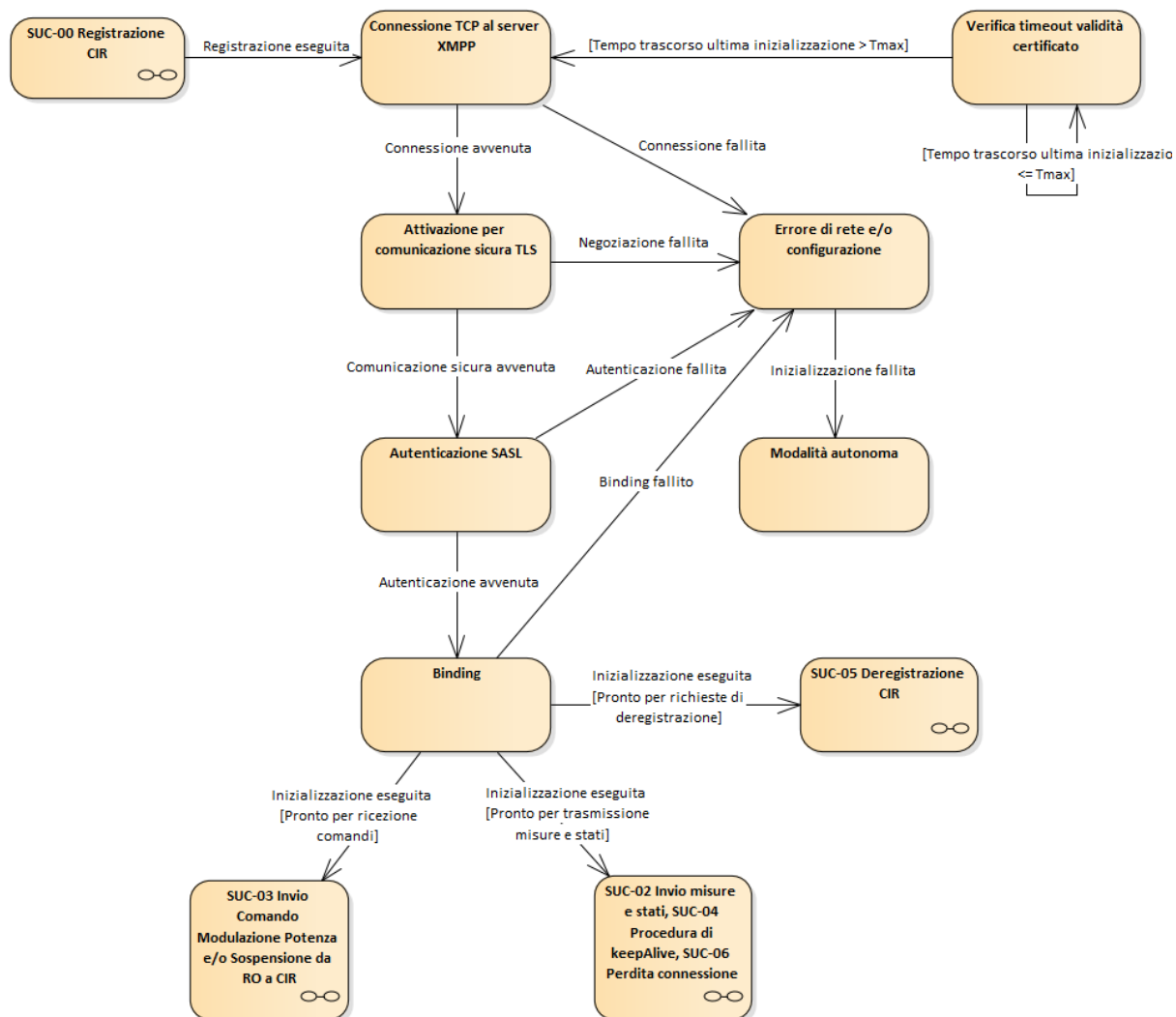
B.1 SUC-00: Registrazione CIR





B.2 SUC-01: Inizializzazione interfaccia CIR-RO

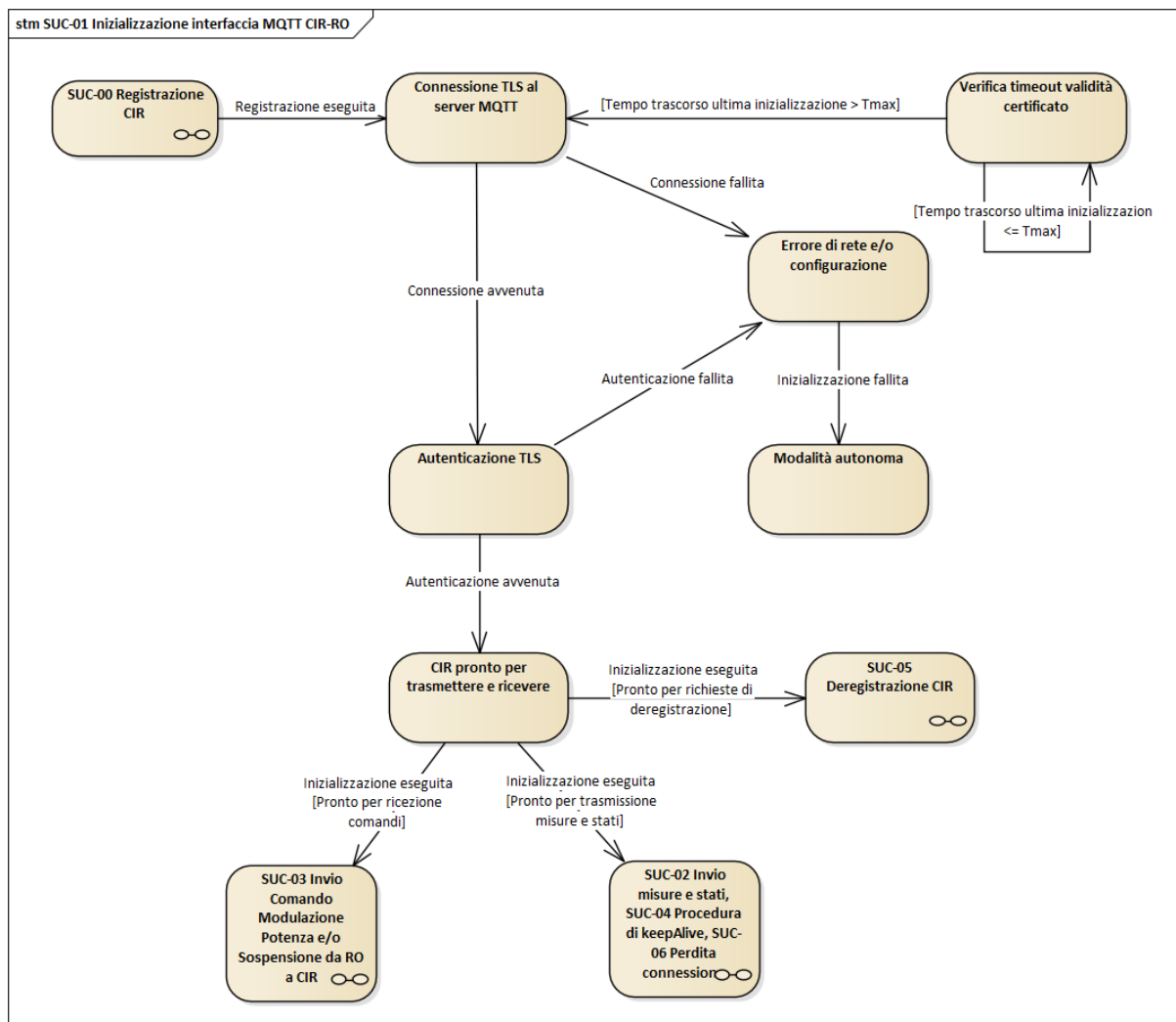
B.2.1 Inizializzazione XMPP



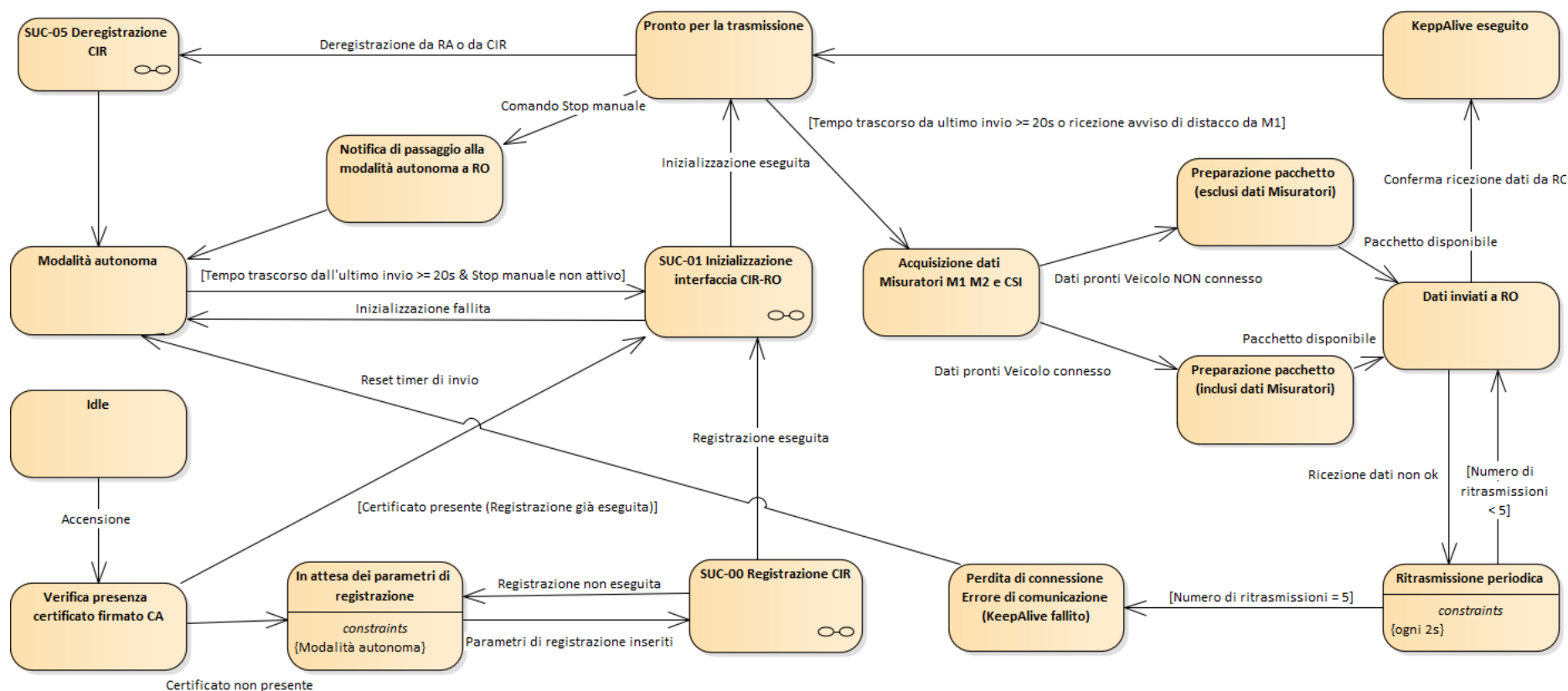
NOTA Lo stato "Verifica timeout validità certificato" ha lo scopo di verificare periodicamente se il certificato sia ancora valido oppure se scaduto o revocato.



B.2.2 Inizializzazione MQTT

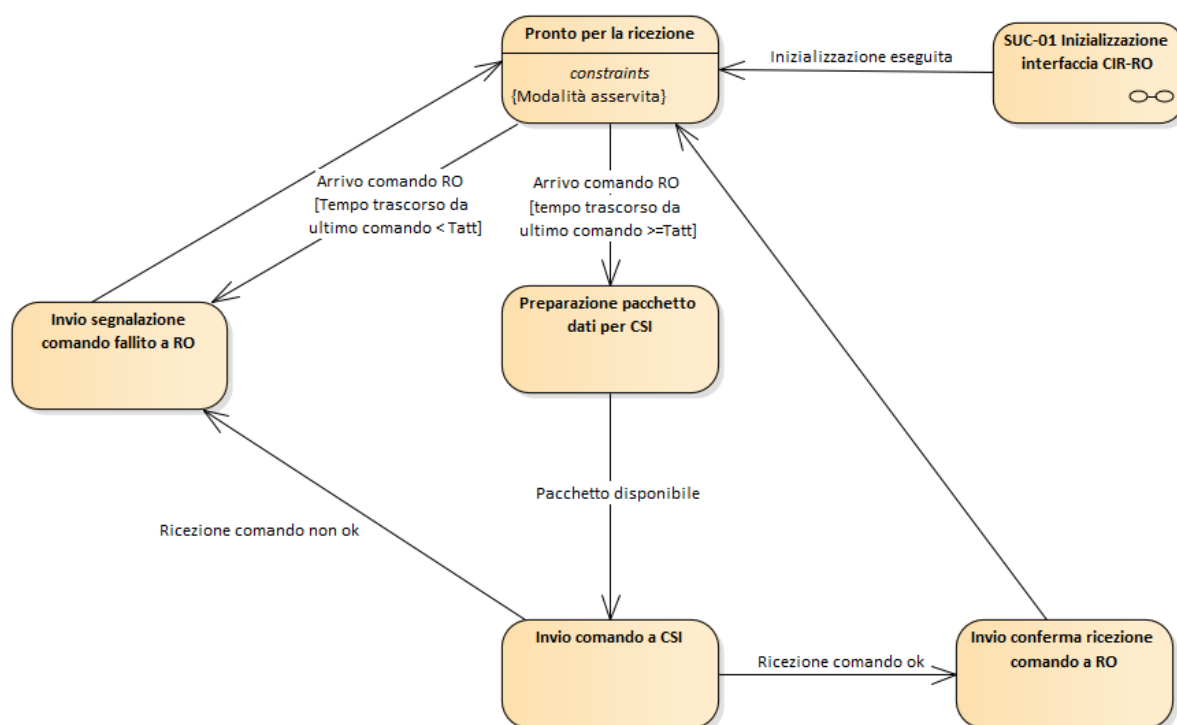


B.3 SUC-02: Invio misure e stati – SUC-04: Procedura di KeepAlive – SUC-06: Perdita connessione



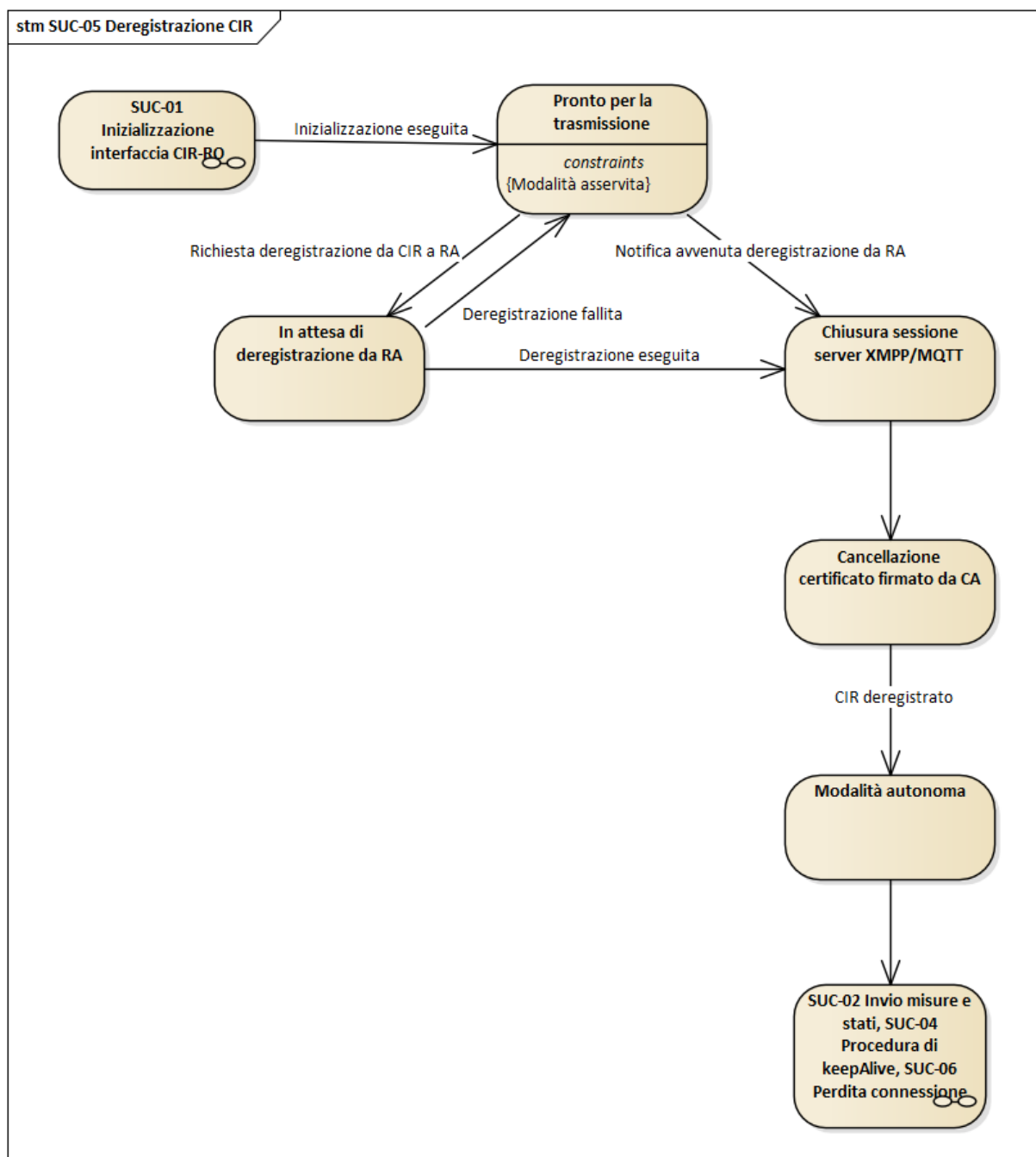


B.4 SUC-03: Invio del Comando di Modulazione di Potenza e/o di Sospensione dal RO al CIR



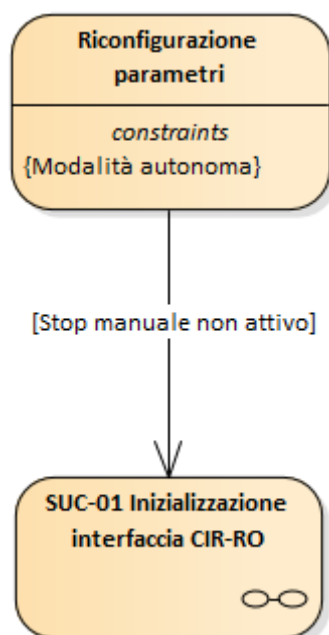


B.5 SUC-05: Deregistrazione CIR





B.6 SUC-07: Aggiornamento configurazione della Infrastruttura di Ricarica gestita dal CIR





Allegato C

Esempi codifica JSON

C.1 ADU Misure Cicliche

```
{
  "ADUtype" : "LD_CIR/LLN0.DS_C_Meas",
  "DataUnit" : {
    "UUID": 1234,
    "Timetag": 1668779999,
    "Data": {
      "LD_CIR/CSIMMXU1.TotW.mag": {
        "ValueN": 234,
        "Invalidity": 0,
        "ErrorCode": 0,
        "Timetag": 1668779108
      },
      "LD_CIR/M1MMXU1.TotW.mag": {
        "ValueN": 134,
        "Invalidity": 1,
        "ErrorCode": 1,
        "Timetag": 1668779108
      },
      "LD_CIR/M2MMXU1.TotW.mag": {
        "ValueN": 254,
        "Invalidity": 1,
        "ErrorCode": 2,
        "Timetag": 1668779108
      },
      "LD_CIR/M1DWMX1.WMaxSpt.setMag": {
        "ValueN": 254,
        "Invalidity": 1,
        "ErrorCode": 3,
        "Timetag": 1668779108
      }
    }
  }
}
```

C.2 ADU Misure Spontanee

```
{
  "ADUtype" : "LD_CIR/LLN0.DS_S_Meas",
  "DataUnit" : {
```



```

    "UUID": 1234,
    "Timetag": 1668779108,
    "Data": {
      "LD_CIR/M1DWMX1.Ttli.operTimeout": {
        "ValueN": 1000,
        "Invalidity": 0,
        "ErrorCode": 0,
        "Timetag": 1668779108
      }
    }
  }
}

```

C.3 ADU Segnali e Allarmi

```

{
  "ADUtype" : "LD_CIR/LLN0.DS_S_States":
  "Dataunit" : {
    "UUID": 1234,
    "Timetag": 1668779108,
    "Data": {
      "LD_CIR/CSIDESE1.Beh.stVal": {
        "ValueN": 4,
        "Invalidity": false,
        "Timetag": 1668779108
      },
      "LD_CIR/LLN0.Loc.stVal": {
        "ValueB": true,
        "Invalidity": false,
        "Timetag": 1668779108
      },
      "LD_CIR/CSIDAGC1.Beh.stVal": {
        "ValueB": true,
        "Invalidity": false,
        "Timetag": 1668779108
      },
      "LD_CIR/CSIDAGC1.Flmod.stVal": {
        "ValueB": true,
        "Invalidity": false,
        "Timetag": 1668779108
      },
      "LD_CIR/CIRLPHD.PhyHealth.stVal": {
        "ValueB": false,
        "Invalidity": false,
        "Timetag": 1668779108
      },
    }
  }
}

```



```

        "LD_CIR/CIRLTMS1.TmSynErr.stVal": {
            "ValueB": false,
            "Invalidity": false,
            "Timetag": 1668779108
        }
        " LD_CIR/CIRQFVR1.UnHzStr.stVal ":{
            "ValueB": false,
            "Invalidity": false,
            "Timetag": 1668779108
        }
    }
}

```

C.4 Comandi (4 tipologie)

```

{
    "ADUtype" : "LD_CIR/LLN0.RS_S_Comm",
    "Dataunit" : {
        "UUID" : 1234,
        "Timetag": 1668779108,
        "Data": {
            "LD_CIR/CSIDWMX1.WLimPctSpt.ctlVal": {
                "Maximum Power": 2000,
                "Duration": 10
            }
        }
    }
}

{
    "ADUtype" : "LD_CIR/LLN0.RS_S_Comm",
    "Dataunit" : {
        "UUID" : 1234,
        "Timetag": 1668779108,
        "Data" : {
            "LD_CIR/CSIDWMX2.WLimPctSpt.ctlVal": {
                "Maximum Power": 2000,
                "Tmax": 1668779108
            }
        }
    }
}

```



```
{
  "ADUtype": "LD_CIR/LLN0.RS_S_Comm",
  "Dataunit": {
    "UUID" : 1234,
    "Timetag": 1668779108,
    "Data" : {
      "LD_CIR/CSIDESE1.ClcStr.ctlVal": {
        "Duration": 100
      }
    }
  }
}
```

```
{
  "ADUtype" : "LD_CIR/LLN0.RS_S_Comm",
  "Dataunit" : {
    "UUID" : 1234,
    "Timetag": 1668779108,
    "Data" : {
      "LD_CIR/CSIDESE2.ClcStr.ctlVal": {
        "Tmax": 1668999999
      }
    }
  }
}
```

C.5 ADU Acknowledge misure

```
{
  "ADUtype": "LD_CIR/LLN0.RS_A_Meas",
  "DataUnit": {
    "UUID": 1234,
    "Timetag": 1668779108,
    "Data": {
      "LD_CIR/CIRGGIO1.SPCSO1.ctlVal": {
        "ValueB": true
      }
    }
  }
}
```



C.6 ADU Acknowledge comandi (esempio di acknowledge del comando specifico “LD_CIR/CSIDESE1.ClcStr.ctlVal”)

```
{  
  "ADUtype" : "LD_CIR/LLN0.DS_A_Comm",  
  "DataUnit" : {  
    "UUID" : 1234,  
    "Timetag": 1668779108,  
    "Data" : {  
      "LD_CIR/CSIDESE1.ClcStr.ctlVal": {  
  
        "Duration": 100,  
        "Ack/Nack": False,  
        "Cause": 2  
      }  
    }  
  }  
}
```

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

Editore CEI, Comitato Elettrotecnico Italiano, Milano

Comitato Tecnico Elaboratore

CEI CT 57 | Scambio informativo associato alla gestione dei sistemi elettrici di potenza



Via Saccardo, 9
20134 Milano

Tel. 02.21006.1

www.ceinorme.it

info@ceinorme.it



COMITATO ELETTROTECNICO ITALIANO