Federico Bellio
Enel Produzione S.p.A.
Via Torino 14
30172 Venezia-Mestre (VE)
tel . +390418215592
mail: federico.bellio@enel.com

Gian Luigi Pugni
Enel S.p.A.
Viale Italia, 26
20099 Sesto San Giovanni (MI)
tel: +390223207827
mail: gianluigi.pugni@enel.com

Marco Biancardi
ABB S.p.A.
Via Albareto, 35
16153 Genova (GE)
tel: +390106073369
mail: marco.biancardi@it.abb.com

Mauro Casalini
ABB S.p.A.
Via Albareto, 35
16153 Genova (GE)
tel: +390106073692
mail: mauro.casalini@it.abb.com

IEC 62351: implementazione nei sistemi di controllo per la Generazione Italia di Enel

Abstract

La norma IEC 62351 "Power systems management and associated information exchange – Data and communications security" è stata sviluppata in ambito IEC dal TC-57 ad iniziare dai primi anni 2000, le prime parti sono state pubblicate nel 2007 nella forma di Technical Specification (TS). La norma esce ora in forma matura come International Standard (IS) e si indica come IEC 62351. La norma vuole rispondere all'esigenza di sicurezza che deriva dall'aver adottato per il controllo dei sistemi dedicati alla Generazione, Trasporto e Distribuzione dell'Energia Elettrica, infrastrutture sempre più evolute e complesse da un punto di vista informatico. Il problema della sicurezza è affrontato a tutto tondo nel modo classico per un ambito informatico: rendere lo scambio dati tra sistemi adeguato in termini di confidenzialità, integrità, disponibilità e non ripudio. Gli autori presentano questo terzo lavoro sui temi IEC 62351 al Forum telecontrollo, dopo quelli illustrativi della norma del 2011 e del 2013, dedicato alla implementazione della norma in un sistema realmente in campo.

Verranno illustrati i criteri di progetto per la messa in sicurezza del sistema di Telecontrollo per la Teleconduzione degli impianti idroelettrici di Generazione Italia di Enel basato sulla versione sicura del protocollo IEC 60870-5-104. Verrà descritta l'architettura del sistema di telecontrollo in cui è stata inserita una nuova infrastruttura (“Certification Authority”) necessaria ad implementare le funzioni di sicurezza basate su certificati digitali che vanno a garantire l'identità

di apparati che costituiscono il sistema e l'identità di chi vi opera (operatori, manutentori, amministratori di sistema, ecc.).

Si descriverà l'implementazione delle parti 3, 5, 8 e 9 della norma IEC 62351 e della nuova parte 60870-5-7 necessarie a realizzare le connessioni cifrate e mutuamente autenticate fra centro di controllo (SCADA) e terminali di impianto (RTU). Si descriverà anche una prima implementazione della parte 7 "Network and System Management", di cui quest'anno è stata redatta la versione CD del nuovo pacchetto della norma in forma IS.

IEC 62351: implementation within the Enel Generazione Italia control system

Abstract

The IEC 62351 standard "Power systems management and associated information exchange – Data and communications security" was developed in the IEC application from TC-57 starting from the early 2000s. The first segments were published in 2007 as Technical Specifications. The standard has now matured and is now published as International Standard (IS), known as IEC 62351. The standard has been created to answer the security needs related to control systems for electricity generation, transport and distribution, which are quickly evolving, becoming more complex by the day under an IT point of view. Security issues are faced in a classic way for IT environments: making data exchange between different systems adequate in terms of confidentiality, integrity, availability and non-repudiation. The authors present this third project on the IEC 62351 topics at the Forum Telecontrollo, following the previous ones in 2011 and 2013 regarding the standard implementation on a real system.

The paper will explain cyber security criteria applied to remote control system of Enel Generazione Italia hydro power plants, based on the secure version of the IEC 60870-5-104 protocol. The remote control system architecture has been enriched with a new infrastructure ("Certification Authority") which is essential for the implementation of security functions based on digital certificates which will grant the identity of both the equipment and the operators, technicians, system administrators, etc).

Parts 3, 5, 8 e 9 of the IEC 62351 standard will be explained as well as parts 60870-5-7, which are essential for the creation of coded connections mutually authenticated between the control center (SCADA) and the plant's terminals (RU). The first implementation of part 7 "Network and System Management" will also be explained and the CD version of such has just been released in the standard under IS form.

Indice

1 Premessa 5

2 Introduzione - IEC 62351 la struttura della norma 6

3 Il Sistema di Telecontrollo basato su IEC 60870-5-104 con IEC 62351 7

3.1 L'infrastruttura di chiave pubblica PKI (Public Key Infrastructure) 8

3.2 Esempio d'uso delle chiavi crittografiche in ambienti con PKI 9

3.3 Nuovi processi sono richiesti per gestire chiavi e certificati 11

3.4 Inserimento dello stack IEC 62351 nel driver del protocollo IEC 60870-5-104 15

3.5 Il monitoraggio del traffico in presenza di canali cifrati 17

4 Conclusioni 18

1 Premessa

Nelle edizioni 2011 e 2013 del nostro Forum abbiamo presentato due lavori di illustrazione della norma TS 62351 "Power systems management and associated information exchange – Data and communications security"[1,2] (Figura 1).

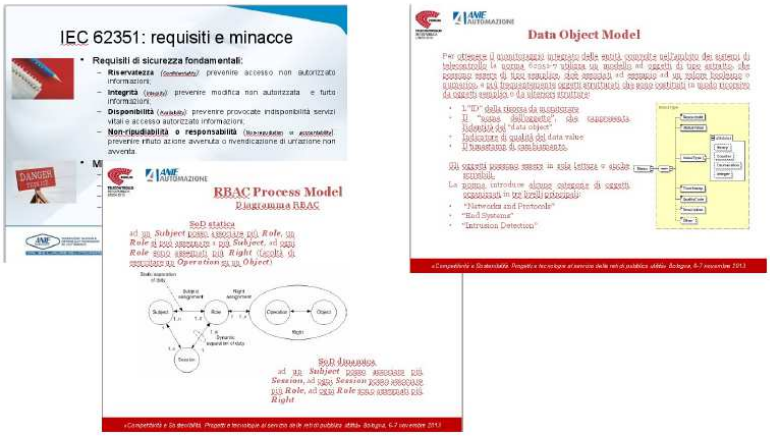

Figura 1 - Le due precedenti edizioni del Forum Telecontrollo

In questo lavoro vogliamo presentare una realizzazione pratica della norma per un sistema di telecontrollo basato sul ben noto protocollo di telecontrollo IEC 60870-5-104.

Per la normativa di messa in sicurezza IEC 62351[3] in questo ultimo biennio sono iniziate le pubblicazioni in formato International Standard (IS) come evoluzione naturale del formato precedente Technical Specification (TS) a conferma della raggiunta maturità della norma. L'insieme di norme per la messa in sicurezza dello scambio dati nei sistemi di automazione e telecontrollo applicabili ai sistemi delle reti del settore elettrico si indica semplicemente con IEC 62351 ad indicare l'insieme di norme International Standard 62351.

Illustreremo alcuni aspetti che sono nuovi per chi si occupa di telecontrollo, ma sono familiari a chi si occupa di sicurezza informatica. Alcuni concetti sono espressi in modo semplificato per far comprendere le nuove parti necessarie ad un sistema di telecontrollo che vuole essere conforme a IEC 62351. Pertanto ci scusiamo con gli esperti di sicurezza informatica che si dovessero imbattere in questa memoria per la poca rigorosità di alcuni concetti esposti.

Questa memoria vuole essere anche un primo elenco di cose necessarie per la realizzazione di un sistema basato sul protocollo IEC 60870-5-104 conforme a IEC 62351. Quindi è rivolta in modo particolare a qui responsabili di sistemi di telecontrollo che si apprestano a valutare o hanno già iniziato a valutare nuove misure di sicurezza da inserire nei loro sistemi di telecontrollo.

2 Introduzione - IEC 62351 la struttura della norma

La struttura della norma IEC 62351 aggiornata al 2015 è riportata in Figura 2. L'oggetto della nostra implementazione è contornata da un tratteggio azzurro. La correlazione fra le varie parti va letta come segue: La messa in sicurezza del protocollo IEC 60870-5-104 richiede di implementare 62351-5 che a sua volta richiede di implementare 62351-3, l'implementazione di parte 3 e 5 implica l'adozione delle parte d'interesse in 62351-8, 62351-7 e 62351-9.

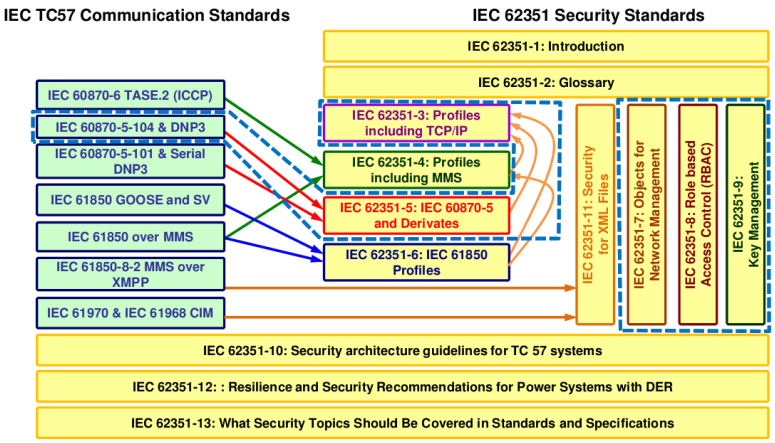

Figura 2- La struttura della norma IEC 62351

Prima di illustrare più in dettaglio cosa significhi implementare le varie parti di IEC 62351 vediamo anche nell'architettura della normativa curata dal TC 57 (IEC Technical Committee 57 – Power System management and associated information Exchange) come s'inquadra la nostra implementazione (vedi Figura 3).

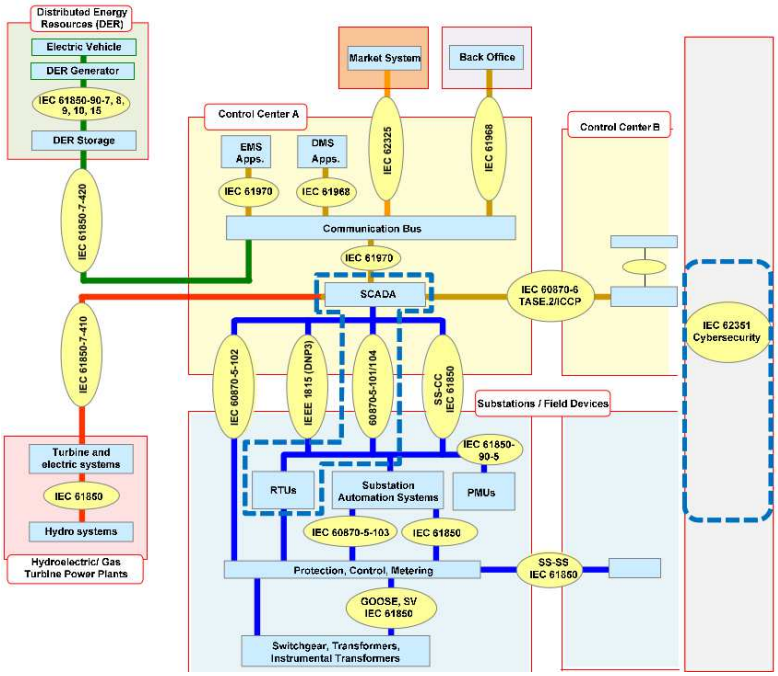

Figura 3- Architettura delle norme curate da IEC TC 57

Anche in questa figura l'ambito dell'implementazione oggetto della memoria è incorniciato con tratteggio azzurro. Il nostro ambito è quello che riguarda il dialogo tra sistemi SCADA (Supervisory, Control and Data Acquisition) nei Centri di Controllo e le RTU (Remote Terminal Unit) in impianto (indicato come *substation* nella norma). IEC 62351 è trasversale a tutti i vari protocolli curati dal TC 57, cioè descrive le modalità e le tecniche di messa in sicurezza di ogni protocollo curato dal TC57. Illustreremo modalità e tecniche applicabili al protocollo IEC 60870-5-104 dedicato allo scambio dati fra Centro di controllo ed impianto su una rete IP (Internet Protocol) su trasporto TCP (Transport Control Protocol).

3 Il Sistema di Telecontrollo basato su IEC 60870-5-104 con IEC 62351

Nella Figura 4 è illustrata l'architettura del sistema di telecontrollo come l'avevamo descritta nella memoria del 2013[2]: sistema di telecontrollo degli impianti (SCADA-RTU) affiancato da un NSM (Network and System Management). Già questo è l'applicazione di quanto raccomandato in IEC 62351-7.

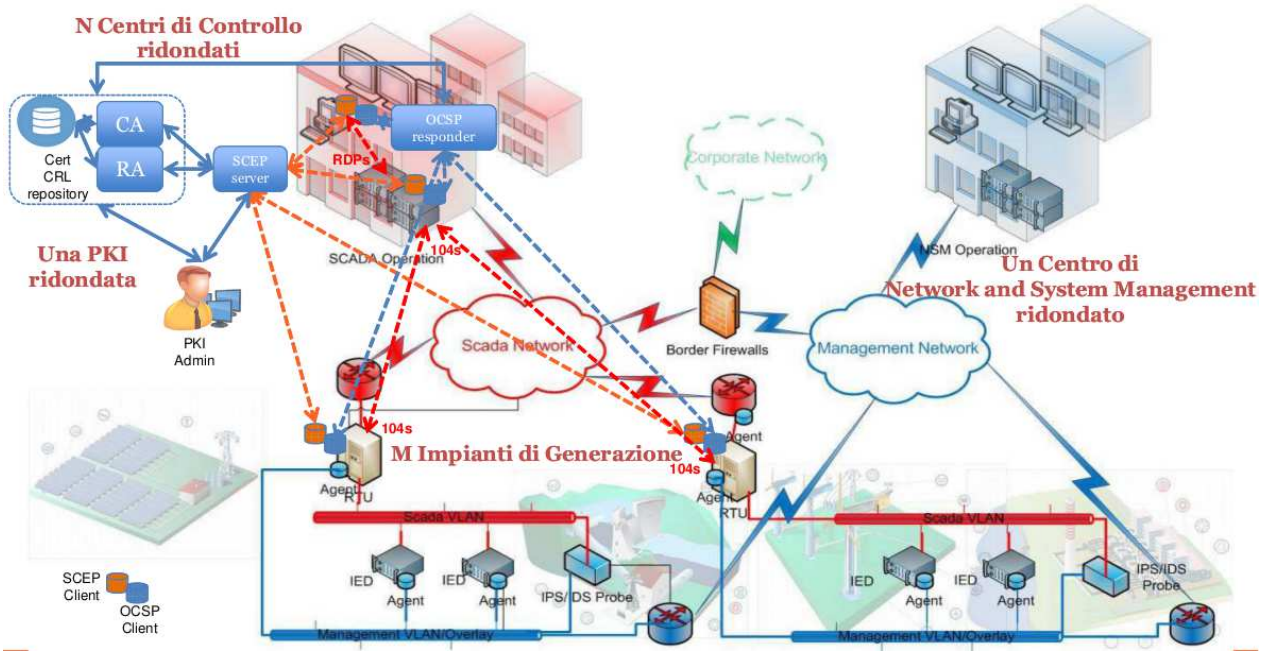

Figura 4 - Il sistema di Telecontrollo basato su IEC 60870-5-104 con IEC 62351

Questa separazione realizza il principio secondo il quale un sistema elettrico è affidabile se lo è il suo sistema di controllo. Per raggiungere un elevato livello di disponibilità le parti infrastrutturali del sistema di controllo, cioè rete di Telecomunicazioni e sistema di Telecontrollo, devono essere separatamente monitorate e gestite. Infatti avere in un unico sistema il controllo del sistema elettrico e della infrastruttura del sistema di controllo stesso può nascondere agli operatori problemi del sistema di controllo stesso.

Si tratta in sostanza dell'applicazione del principio del controllo ridondato indipendente su parti di un sistema (già ad alta affidabilità) particolarmente critiche per disponibilità delle sue funzioni vitali (si pensi ad esempio ai *watchdog* su parti hardware o software, in qualche modo NSM è il concetto generalizzato del watchdog applicator all'intero sistema di controllo).

Sul nostro sistema, che ha *N* Centri di Controllo per gli *M* impianti di Generazione che il Gruppo Enel che gestisce in Italia, le funzionalità NSM sono implementate mediante un prodotto di Network Management commerciale basato su scambio d'informazioni che utilizza il protocollo SNMP, secondo quanto descritto nella memoria del 2013[2]. Un sistema su cui operano più unità operative secondo viste e ruoli diversi: esercizio della rete di telecomunicazioni (NOC Network Operations Center), esercizio del sistema di apparati di sicurezza informatica (SOC Security Operations Center) e esercizio del sistema di Telecontrollo (che per analogia indichiamo con TOC Telecontrol Operations Center).

A questa infrastruttura classica si aggiunge un nuovo elemento infrastrutturale, la PKI (Public Key Infrastructure) il cui scopo è di dare tutta una serie di servizi crittografici atti a:

- assicurare l'autenticità della sorgente dati,

- assicurare che l'accesso ai dati sia autorizzato
- assicurare l'integrità dei dati
- prevenire l'accesso indebito a dati confidenziali
- prevenire il ripudio di un'azione o la legittima attribuzione di responsabilità per l'azione stessa
- prevenire la perdita di servizi essenziali e quindi garantire la loro disponibilità.

Per meglio capire il significato di questi aspetti nei paragrafi seguenti illustreremo alcuni principi e meccanismi basati sulla crittografia.

3.1 L'infrastruttura di chiave pubblica PKI (Public Key Infrastructure)

Nella Figura 5 - Elementi e meccanismi base dell'Infrastruttura di Chiave Pubblica o PKIFigura 5 sono rappresentati i componenti base di una Infrastruttura di Chiave Pubblica o *Public Key Infrastructure* (PKI) secondo quanto definito nel documento "Internet X.509 PKI and CRL Profile" [4].

Prima di descrivere i componenti della PKI dobbiamo dare la definizione di certificato digitale o semplicemente certificato: è un documento digitale che prova (certifica) il possesso di una coppia di chiavi pubblica - privata da parte di una entità (*Entity:* persona, macchina o componente di sistema digitale), nel certificato sono descritte l'identità del possessore delle chiavi, la scadenza del certificato e altre informazioni che dipendono dall'uso del certificato, il certificato è firmato digitalmente da una Autorità riconosciuta dagli utilizzatori della CA.

La firma digitale sul certificato della CA garantisce l'autenticità del certificato, come la firma autografa e riconoscibile in calce ad un documento cartaceo garantisce che quel documento è stato rilasciato da chi l'ha firmato.

Descriveremo nel paragrafo seguente un esempio per capire come la coppia delle chiavi e alcuni algoritmi crittografici costituiscano il meccanismo di firma digitale nel senso appena descritto.

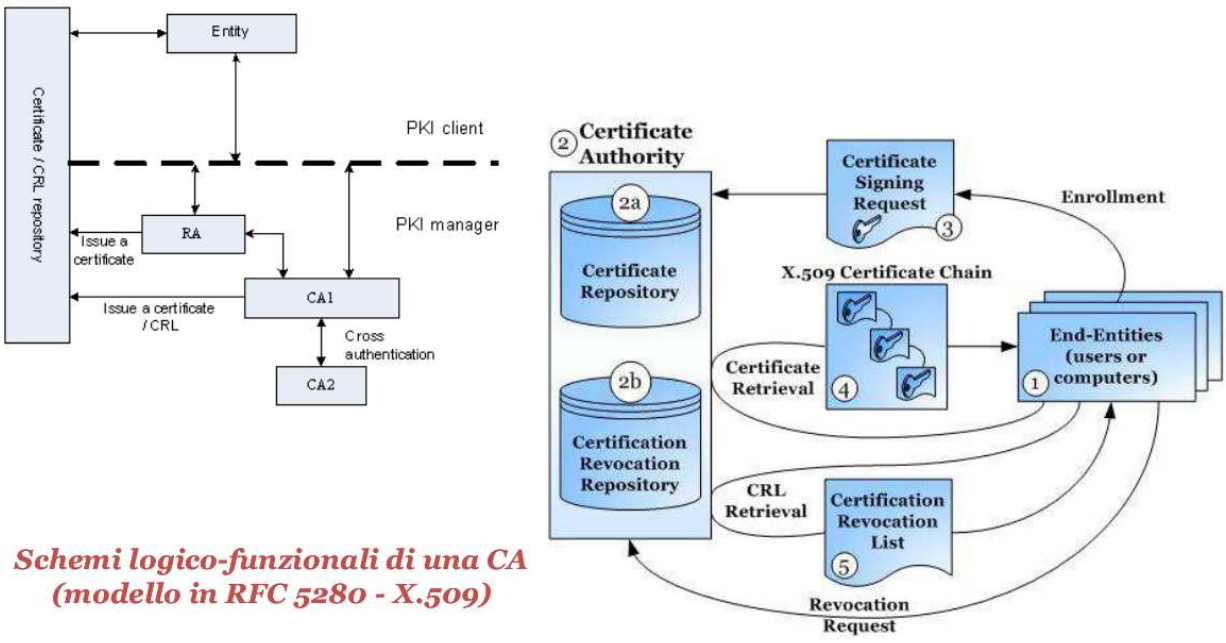

Figura 5 - Elementi e meccanismi base dell'Infrastruttura di Chiave Pubblica o PKI

La PKI è costituita un archivio (*repository*) di certificati e da una *Certification Authority* (CA) che assicura con le sue funzioni la corretta gestione dell'archivio dei certificati.
L'archivio dei certificati è organizzato in da due "liste" di certificati: la prima è la lista dei certificati validi e la seconda è la lista dei certificati revocati (*Certificate Revocation List* CRL), cioè certificati che sono stati ritirati e da considerare non più validi.
La CA può delegare alcune funzioni durante il processo d'inserimento di un nuovo certificato nell'archivio ad un componente denominato *Registration Authority* (RA).
Una entità che vuole verificare se è in contatto con una entità riconosciuta dalla CA verifica che sia in possesso da un certificato valido (la cui data di scadenza non sia trascorsa) emesso dalla CA non inserito nella CRL.
Nello schema di sinistra di Figura 5 sono rappresentate due CA (CA1, CA2) ad indicare che vi può essere un dialogo fra CA in modo da costituire una relazione di fiducia (*trust*) fra CA. C'è solitamente una relazione gerarchica fra CA.
C'è una CA di vertice che certifica altre CA figlie con lo stesso meccanismo di certificazione delle entità descritto sopra. Cioè una CA è identificata da un certificato firmato dalla CA madre contenente la sua chiave pubblica e le sue caratteristiche.
Senza entrare in altri dettagli diciamo che la CA attraverso la corretta gestione dell'archivio dei certificati e la CRL garantisce l'identità dei soggetti per cui ha emesso i certificati. In altre parole possiamo dire che ogni entità del nostro sistema può accertarsi di scambiare informazioni con un'altra entità di cui può verificare l'identità presso la CA.

3.2 Esempio d'uso delle chiavi crittografiche in ambienti con PKI

In questo paragrafo in modo molto semplificato vogliamo esporre un esempio in cui descrivere le tecniche crittografiche normalmente impiegate.
Prima di descrivere l'esempio definiamo cosa è una chiave crittografica o semplicemente chiave. Le chiavi sono essenzialmente di due tipi: chiavi simmetriche e chiavi asimmetriche.
Entrambe le chiavi consentono di codificare un messaggio (cioè trasformarlo attraverso un algoritmo che impiega quella chiave) modificando un contenuto in chiaro in una forma che può essere decodificata solo attraverso la chiave di cifratura. Per questo ci si riferisce a operazioni di cifratura e decifratura.
La chiave quindi non è altro che un numero da usare nell'algoritmo di cifratura. La lunghezza (numero di cifre) della chiave influenza, insieme al tipo di algoritmo, la "robustezza" della cifratura, ma richiede un numero proporzionale (a volte in modo non lineare) di risorse di calcolo necessarie ad implementare l'algoritmo di cifratura e decifratura.
Nel sistema a chiave simmetrica lo stesso numero (chiave) viene utilizzato sia per cifrare che per decifrare il messaggio scambiato fra le due entità. In questo caso si parla anche di segreto condiviso (la chiave di cifratura) fra le entità in comunicazione.
Nel sistema a chiave asimmetrica una coppia di numeri, detti chiave privata e chiave pubblica, vengono impiegati in modo asimmetrico per cifrare decifrare in messaggio scambiato fra due entità. Vale a dire che

il messaggio cifrato dall'entità sorgente mediante la chiave pubblica del destinatario può essere decifrato solo dall'entità destinataria mediante la sua chiave privata.

La coppia di chiavi che costituisce la chiave asimmetrica è in sostanza una coppia di due grandi numeri ottenuti impiegando un generatore di numeri casuali. Ciò implica che l'algoritmo di cifratura e decifratura asimmetrico è più pesante in termini di risorse di calcolo rispetto ad un algoritmo simmetrico di analoga robustezza. In altre parole, a parità di risorse di calcolo, l'algoritmo asimmetrico è più lento di quello simmetrico.

L'enorme vantaggio dell'impiego di tecniche di crittografia asimmetrica risiede nel fatto che non è necessario che ogni coppia di entità abbia una sua "speciale" chiave condivisa, cosa che comporterebbe una crescita di ordine quadratico nel numero delle chiavi al crescere del numero dei partecipanti: basta una coppia di chiavi (una privata e una pubblica) per ciascun partecipante.

Per combinare i vantaggi di entrambi gli schemi (simmetrico e asimmetrico) si adotta uno scambio con cifratura asimmetrica per scambiare chiavi di cifratura simmetrica generate al momento e usate per sessioni limitate, per esempio per un singolo documento (per questo spesso chiamate chiavi di sessione). Dopo un breve e più pesante (in termini computazionali) scambio asimmetrico l'entità sorgente e quella destinataria passano ad usare uno schema di cifratura simmetrica più leggero e quindi meno penalizzante per le prestazioni.

In Figura 6 sono esemplificate le varie fasi di uno scambio cifrato e mutuamente autenticato in un tipico ambiente applicativo *client – server*. Immaginate che il server sia una RTU di un impianto che espone il servizio per protocollo IEC 60870-5-104 ed il client sia l'istanza master dello stesso protocollo sullo SCADA da cui si conduce l'impianto.

Di seguito viene descritta in modo semplificato ciascuna delle operazioni indicate con carattere alfa-numerico cerchiato:

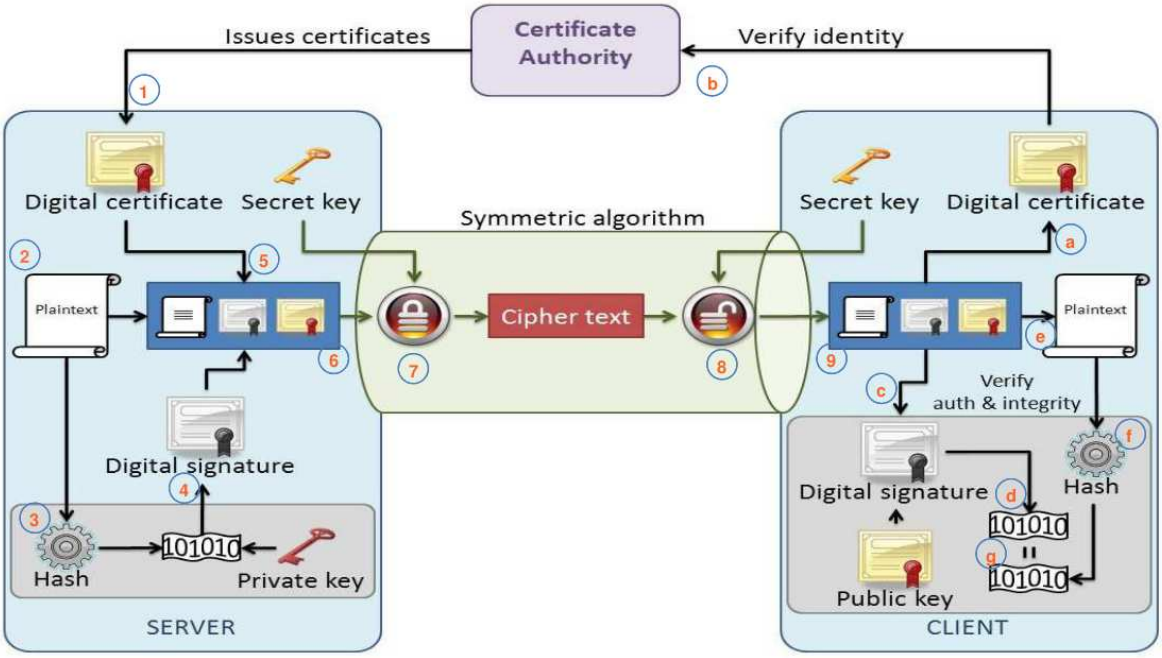

Figura 6 - Esempio d'impiego delle chiavi crittografiche

1. Nella fase di *enrollment* (vedi dopo) il dispositivo (RTU) server riceve un certificato di identità (*Digital certificate*) dalla CA (*Certificate Authority*)
2. Ogni volta che il server deve scambiare con il client un messaggio (*Plaintext*)
3. Ne calcola mediante un opportuno algoritmo un codice hashing (*Hash*), l'equivalente del CRC dei tradizionali protocolli seriali
4. Con l'algoritmo di cifratura asimmetrica, impiegando la chiave privata del *Server* (*Private key*), da *Hash* si ottiene la firma digitale (*Digital signature*)
5. Combinando *Plaintext, Hash, Digital signature*
6. e *Digital certificate* si ottiene l'intero messaggio da inviare al destinatario (*Client*)
7. Il messaggio viene cifrato con un algoritmo simmetrico (*Symmetric algorithm*) che impiega una chiave di sessione (*Secret key*) (vedi sopra)
8. Il messaggio viene trasportato sul canale di comunicazione cifrato (*Cipher text*) e in arrivo sul *client* (processo 104 master sullo SCADA) viene decifrato mediante algoritmo simmetrico impiegante la *Secret key* (chiave di sessione tra *Client* e *Server*)
9. Il messaggio decifrato viene avviato al processo per la verifica di autenticità e integrità (*Verify auth & integrity*)

a. La verifica di identità si avvia estraendo il certificato del *server* dal messaggio (*Digital certificate*)
b. Si chiede alla CA se *Digital certificate* è valido (non revocato) e se non è scaduto e corrisponde all'entità (RTU) attesa si procede
c. Estraendo la *Digital signature*
d. tramite la chiave pubblica del *server* contenuta nel suo certificato si ottiene lo Hash che deve coincidere con calcolato a partire
e. dal *Plaintext* estratto anch'esso dal messaggio in arrivo mediante
f. l'algoritmo di hashing,
g. se *Hash* estratto e *Hash* calcolato all'arrivo sul *Client* coincidono il messaggio ricevuto è autentico e integro, in particolare lo è il suo contenuto informativo (*Plaintext*),.

L'esempio non ha nessuna pretesa di essere una illustrazione completa ed esaustiva delle tecniche necessarie a realizzare la messa in sicurezza anche solo per il protocollo IEC 60870-5-104 atte a rendendolo conforme a IEC 62351. Ma vuole solo far capire quali sono gli strumenti da mettere in gioco per ottenere la messa in sicurezza oggetto di IEC 62351.

3.3 Nuovi processi sono richiesti per gestire chiavi e certificati

La PKI è quindi una infrastruttura essenziale, strutturale ai fini di realizzare un sistema di telecontrollo conforme alla norma IEC 62351. Di conseguenza oltre a realizzare i componenti descritti in 3.1 è necessario attivare una serie di processi organizzativi (e le relative procedure operative) necessari alla gestione dei certificati digitali che vanno a identificare univocamente le varie entità del sistema di telecontrollo.

Il primo documento organizzativo necessario è la *Certificate Security Policy* come indicato in IEC 62351-9 con riferimento ad una raccomandazione IETF RFC 3647[5].

Questa Policy all'interno dell'Azienda deve definire procedure, criteri, parametri e responsabilità sulla gestione dei Certificati Digitali, in particolare deve trovare posto un capitolo specifico per l'uso dei certificati nei sistemi industriali (*Industrial Control System* ICS).

Di seguito elenchiamo e descriviamo alcuni di questi processi ancora una volta senza la pretesa di essere esaustivi, ma per indicare la tipologia di processi da attivare per un sistema di telecontrollo che voglia essere conforme a IEC 62351.

La descrizione dei processi organizzativi necessari per gestire certificati e chiavi legati agli apparati e agli utenti del Sistema di telecontrollo, che sono le entità dei paragrafi precedenti, è necessariamente semplificata. Nell'implementazione in campo abbiamo adottato alcune semplificazioni iniziali, la più significativa è quella di rinunciare, in prima istanza, ai certificati utente di ogni operatore per assegnare certificati solo agli apparati in impianto e a quelli del centro di controllo (al quale è demandato il controllo che agiscano gli operatori autorizzati). Questo facilita il passaggio alla versione di protocollo IEC 60870-5-104 conforme a IEC 62351 rendendo più affrontabile lo sforza di portare l'infrastruttura PKI in campo.

Figura 7 - Processi di gestione dei Certificati

Si farà cenno agli elementi necessari per completare un disegno completo e robusto nello più ampio spirito della norma IEC 62351, ma è importante sottolineare che la norma stessa consente varie implementazioni tutte egualmente conformi quello che cambia è il grado di resilienza agli attacchi o guasti che possono compromettere sicurezza e disponibilità del sistema di Telecontrollo.

In Figura 7 sono riassunti i processi "minimi" necessari alla gestione dei certificati in relazione alla lo associazione ai dispositivi di campo.

Ora attraverso due esemplificazioni illustriamo alcuni elementi base dei processi di gestione dei certificati.

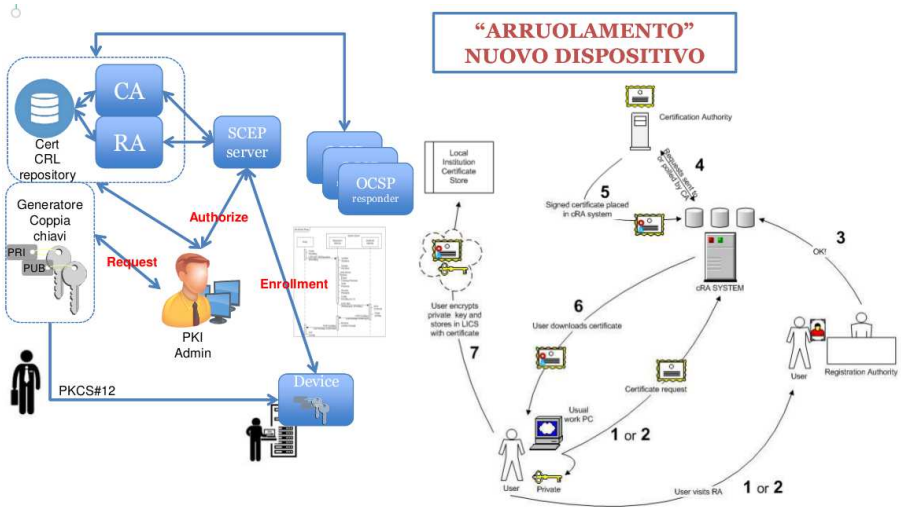

Figura 8 - Enrollment "arruolamento" di un nuovo dispositivo

Nella Figura 8 è illustrato il processo di *enrollment* cioè quel processo che consente di dichiarare alla PKI un nuovo dispositivo a cui rilascerà il suo certificato di identità. Un modulo controllato dall'amministrazione della CA genera la coppia di chiavi privata-pubblica (vedi sopra) la "imbusta" in un contenitore (file di formato PKCS#12[6]) cifrato con un segreto reso noto

all'operatore che va presso il dispositivo (SCADA o RTU, ad esempio) e lo rende disponibile al *client SCEP* del dispositivo. Il dispositivo mediante il protocollo SCEP[7], con l'autorizzazione dell'amministratore della PKI, "arruola" il dispositivo tramite la CA che rilascia il certificato che crea l'associazione unica tra dispositivo e la sua chiave privata che viene opportuna memorizzata nel dispositivo, copia viene conservata in un opportuno LICS (*Local Institution Certificate Store*).

La scelta di generare (per ora) la coppia di chiavi all'esterno del dispositivo finale deriva dalla temporanea necessità di aggirare possibili limiti del dispositivo titolare del certificato. La soluzione ideale infatti è quella che il dispositivo generi la coppia pubblica-privata di chiavi, e custodisca la chiave privata senza mai farla circolare anche su reti fidate e protette. Questa seconda opzione richiede certamente una nuova generazione di dispositivi.

La sicurezza con cui viene conservata la chiave privata e le sue copie è peraltro la parte più delicata e sensibile del meccanismo su cui si basa l'infrastruttura PKI. Quindi vanno adottate le misure di sicurezza adatte a questo scopo (quali ad esempio l'uso di *smartcard* e *HSM*).

In Figura 9 sono riportate altre due operazioni che si eseguono attraverso la PKI. La prima operazione è quella che viene richiesta ogni qualvolta sia necessario impiegare il certificato di un'altra entità: cioè l'operazione che porta ad appurare l'autentica identità di un dispositivo nel nostro caso. Proprio perché questa operazione può essere frequente ci si avvale di un *OCSP responder*[8]. Un server che si trova "vicino" ai dispositivi che devono richiedere lo stato dei certificati, hanno una funzione di gateway nei confronti della CA a riguardo delle operazioni di verifica dello stato dei certificati. Il server *OCSP responder* si aggiorna con la CA su richiesta o con ciclo dell'ordine delle 24h che è il periodo di solito indicato per l'aggiornamento della CRL della CA.

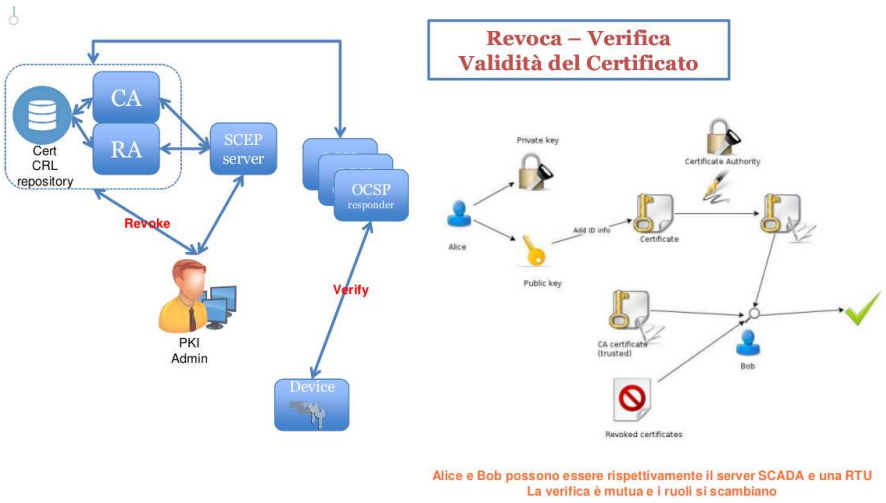

Figura 9 - Verifica e Revoca di un Certificato

Nella parte destra della figura è indicato il processo di verifica in termini semplificati e logici. L'entità *Bob* verifica l'identità dell'entità *Alice*: Il certificato di Alice firmato dalla CA arriva a Bob, il quale verifica che sia stato firmato da una *CA trusted* (fidata), di cui possiede il certificato e mediante il quale può operare questa verifica. Ora se il certificato è in vigore (entro i termini di validità inseriti nel certificato) e non è stato revocato è valido e Bob può impiegarlo per le sue operazioni crittografiche che riguardano Alice.

La revoca è una operazione amministrativa che può essere decisa dall'amministratore perché il dispositivo a cui è associato è stato, ad esempio, demolito o rubato. Si opera attraverso lo *SCEP server* di cui abbiamo parlato sopra.

Il ciclo completo di vita delle chiavi crittografiche e i relativi certificati è cosa assai complessa.

In Figura 10 è riportato il diagramma inserito in IEC 62351-9 per indicare tutte le fasi in cui chiavi e certificati entrano nella "vita" di un dispositivo, dalla fase di progetto, di produzione, di esercizio fino alla sua dismissione.

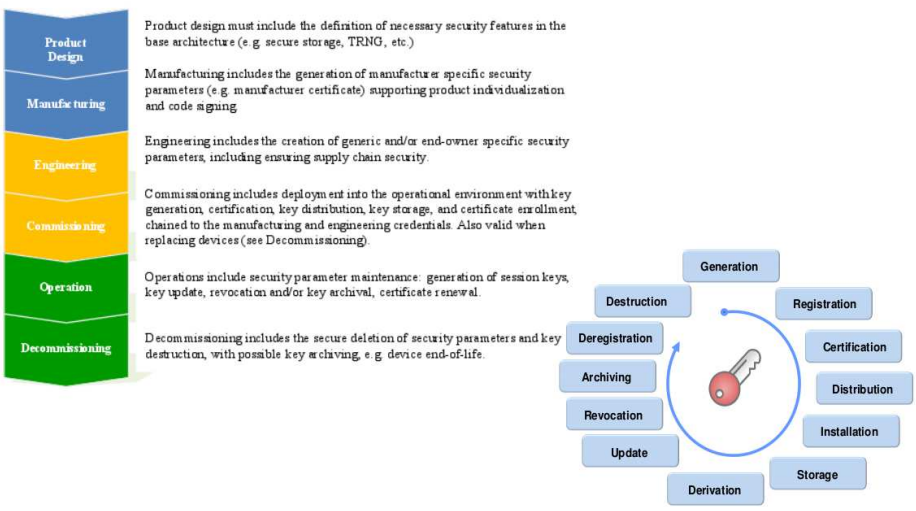

Figura 10 - Ciclo di vita delle Chiavi e dei Certificati associati

In questa memoria non ci addentriamo qui in altri dettagli perché non è negli scopi che ci siamo dati per questo documento.

3.4 Inserimento dello stack IEC 62351 nel driver del protocollo IEC 60870-5-104

In questo paragrafo si descrive brevemente l'implementazione in uno SCADA di un driver per protocollo IEC 60870-5-104 conforme a IEC 62351, cioè l'inserimento del TLS richiesto da IEC 62351-3 e la mutua autenticazione richiesta da IEC 62351-5 con le modifiche da questo indotte nello specifico nostro protocollo e definite da IEC 60870-5-7[9].

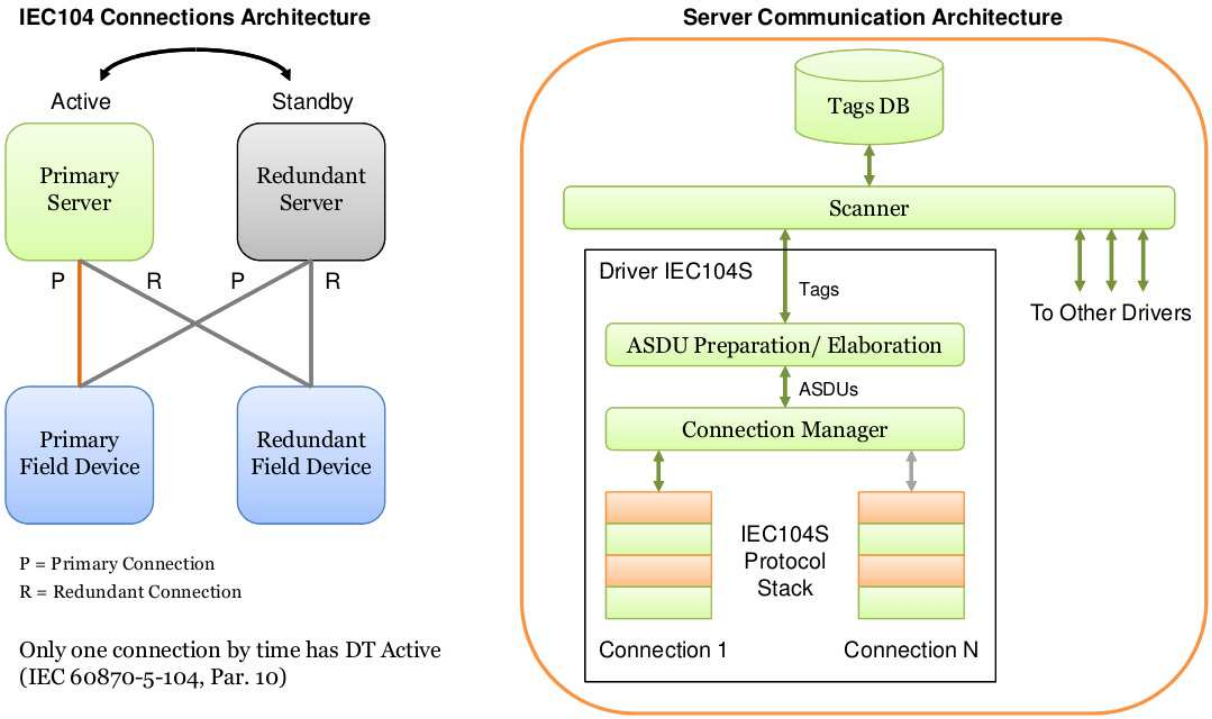

Figura 11 - Architettura di un driver per protocollo IEC 60870-5-104

In Figura 11 è riportata l'architettura di un driver per protocollo IEC 60870-5-104[10]. Lo SCADA gestisce la ridondanza tra due o più server, un solo server alla volta ha il controllo sul campo.

Ogni server gestisce più istanze IEC104 Master, ognuna con 1 o 2 connessioni IEC104 gestite in conformità alla specifica IEC 60870-5-104, Par. 10. Ogni server gestisce più istanze IEC104 Slave, ognuna con connessioni multiple verso stazioni master.

Rispetto all'implementazione "non – sicura", nella versione che recepisce la norma IEC 62351 (che in seguito indicheremo con IEC104s) sono stati inseriti due strati (*layers*) aggiuntivi rispettivamente per la implementazione della parte IEC 62351-5 e IEC 62351-3 (TLS 1.2). Ogni *layer* lavora in modo indipendente e senza conoscere le operazioni svolte dagli altri *layers*, il collegamento avviene mediante code di messaggi. Attivare il modo sicuro (IEC 104s) o non sicuro (IEC 104) significa inoltrare un messaggio su una coda piuttosto che un'altra. Quindi la compatibilità contemporanea del driver fra modo sicuro e non sicuro, richiesta da IEC 62351, è ottenuta attraverso uno commutatore che avvia i pacchetti verso la coda IEC 104 o IEC 104s (vedi Figura 12).

Tutte le funzioni di crittografia e di key management in generale richiesta da IEC 62351 sono realizzate in una libreria (CSA) (vedi Figura 13).

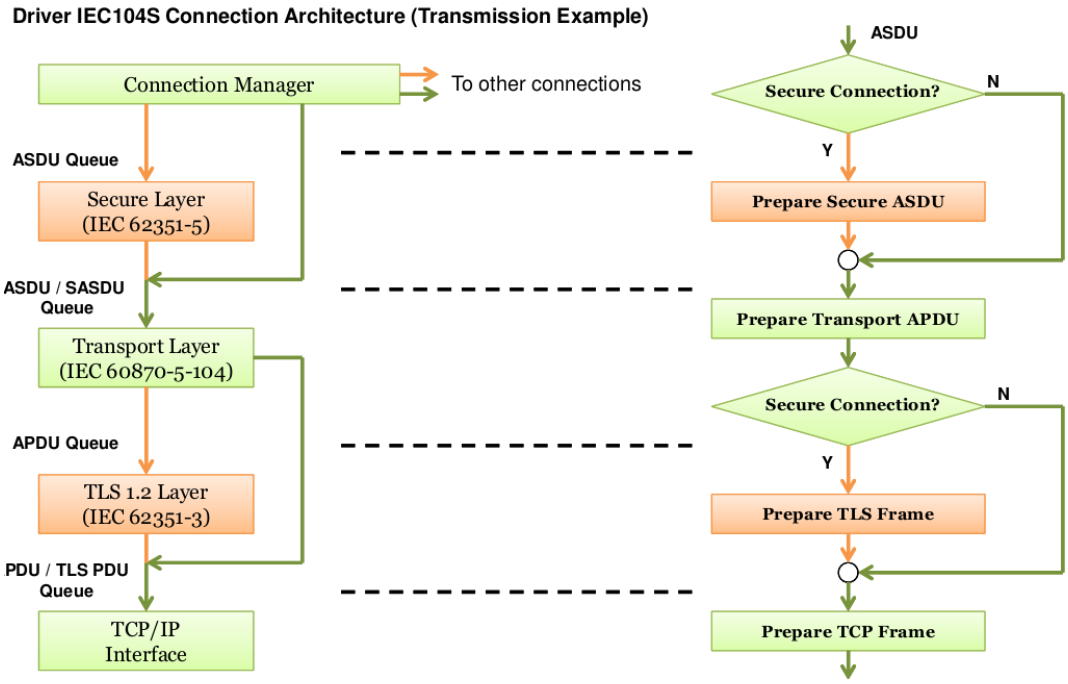

Figura 12 - Layers del driver IEC 104s con switch per compatibilità IEC 104

Queste *Common Libraries*, contengono tutte le funzioni necessarie per la gestione di connessioni SSL/TLS, gli algoritmi per l'autenticazione delle informazioni e per la generazioni delle chiavi di sessione (62351-5) nonché quelle per il *Certificates Management* (*Enrollment* e *Verification*) verso una PKI.

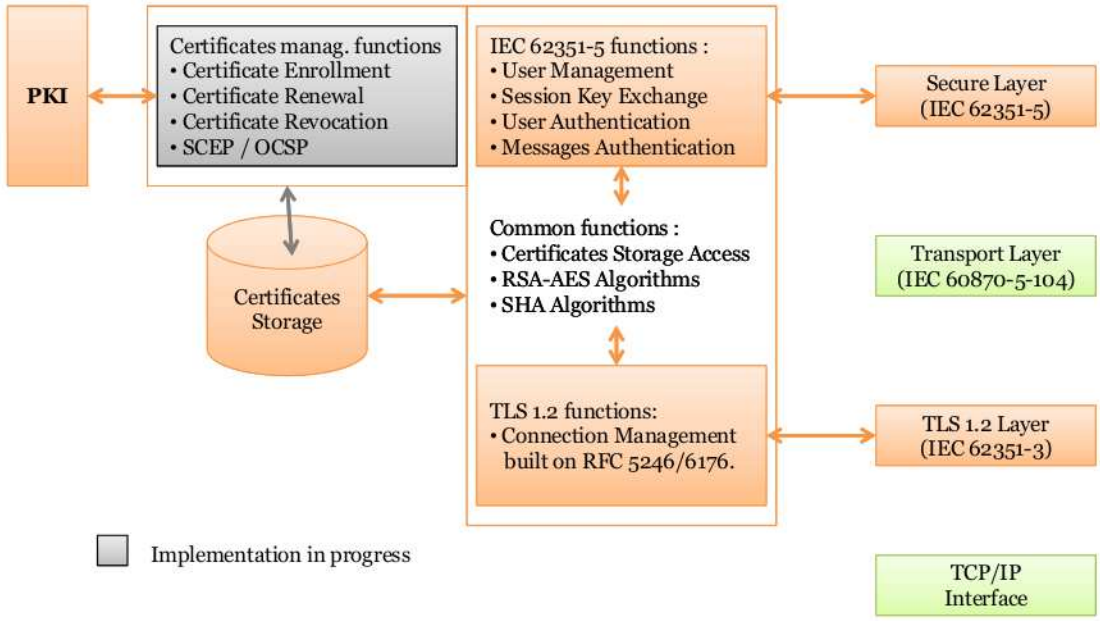

Figura 13 - Common Security Architecture library (CSA)

L'implementazione è completa tranne per le parti ombreggiate che sono in realizzazione. La realizzazione completa del driver IEC 104s a partire dalla versione non sicura ha richiesto circa sei mesi.

3.5 Il monitoraggio del traffico in presenza di canali cifrati

Chi opera tutti i giorni su un sistema di Telecontrollo sa che non si può farlo bene senza un adeguato strumento di monitoraggio del traffico che consenta di analizzare nel dettaglio lo scambio dati di una connessione IEC 60870-5-104.

A fronte di una situazione anomala si deve poter entrare nel dettaglio delle strutture dati del protocollo (*Deep Packet Inspection)* a tutti i livelli analizzabili del modello ISO-OSI (da L2 a L7) per capire cosa non va.

In ambiente IEC 104s il classico strumento di cattura e analisi del traffico (sonda – *Probe*) non è in grado di lavorare perché il traffico è cifrato. Per non perdere lo strumento di analisi bisogna consentire alla sonda di decifrare il traffico, ma perché questo non diventi un punto di debolezza, è necessario che la sonda stessa, che si pone fra i due attori della connessione IEC 104s, sia una parte riconosciuta e autorizzata.

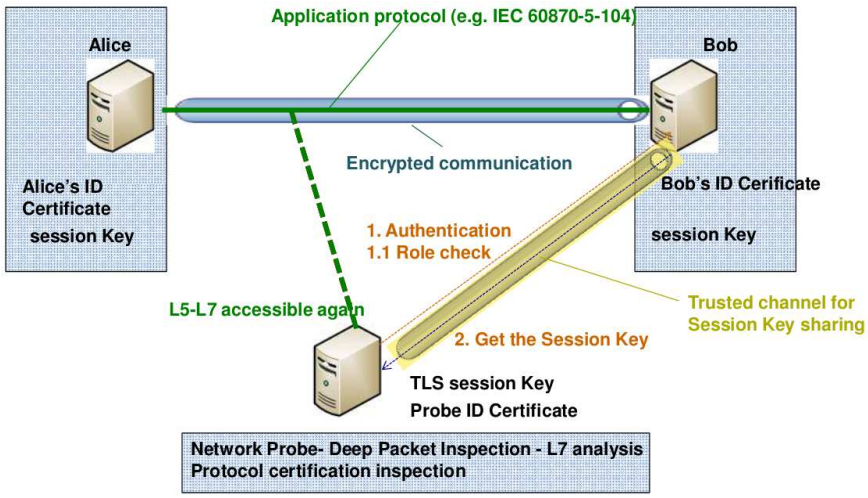

Figura 14 - Analisi del traffico cifrato con un modulo di analisi autorizzato

In Figura 14 è illustrata una proposta che abbiamo portato al IEC TC57 WG15[11] come una delle possibili soluzioni a cui lavoreremo per mantenere l'importante funzione di monitoraggio descritta sopra nel nostro sistema di Telecontrollo.

Una chiave di sessione (per cifratura simmetrica), di cui si è accennato in 3.2, viene rinnovata con periodo che può essere di pochi minuti (il minimo tempo di rinnovo consigliato in IEC 62351-9 è 2 minuti primi). L'idea è di modificare il meccanismo in cui s'instaura la sessione TLS per condividere la chiave di sessione non solo fra i due attori della connessione IEC 104s (i soliti Bob e Alice, che possono rappresentare RTU e SCADA di una connessione di campo), ma anche con la sonda. Quando questa si presenta da uno dei due attori (Bob nel nostro esempio), si fa riconoscere con il suo certificato (*Probe Certificate ID*), se Bob la riconosce come strumento autorizzato gli condivide la chiave di sessione.

Si può avere una versione in cui si rafforza la sicurezza di questa "intromissione" da parte della sonda: Bob gli condivide la chiave di sessione solo al termine del periodo (2 minuti) di validità. Il monitoraggio è comunque garantito, se lo strumento memorizza il traffico del periodo in cui è stata valida la chiave di sessione, ma non avrà alcuna possibilità di usarla in modo attivo perché quando ne viene in possesso la chiave di sessione è scaduta.

4 Conclusioni

Nella memoria abbiamo analizzato cosa significhi trasformare un sistema di Telecontrollo, basato su protocollo IEC 60870-5-104, in modo che risulti conforme alla norma IEC 62351. Norma IEC per la messa in sicurezza secondo, moderni criteri di cyber security, dei sistemi di controllo nel campo energetico.

Abbiamo illustrato in modo semplificato le tecniche adottate nella norma IEC e come trasformare l'infrastruttura di Telecontrollo classica per ottenere la conformità ai principi di sicurezza enunciati dalla norma stessa. Sono stati analizzati i nuovi processi organizzativi che sono da mettere in campo per gestire l'infrastruttura di chiave pubblica (PKI) necessaria a rendere possibile la messa in sicurezza. Infine abbiamo brevemente descritto gli interventi necessari sui moduli specifici del protocollo IEC 60870-5-104 (*driver*) per passare alla versione sicura (IEC 104s).

L'esperienza del nostro progetto ci dice che la norma IEC 62351 è sufficientemente matura per essere compitamente implementata sui sistemi in esercizio basati su protocollo IEC 60870-5-104. La prima versione mono Fornitore è già funzionante, prevediamo di eseguire i primi test di interoperabilità con l'implementazione di un altro Fornitore entro la fine di questo 2015. L'impatto dell'inserimento dello stack di sicurezza non è stato diverso da quello provocato da una comune significativa release di prodotto.

Entro il primo semestre 2016 è programmata la messa in campo della PKI dedicata al sistema di Telecontrollo e l'attivazione delle prime connessioni IEC 104s fra centri di controllo ed impianti.

Per giungere a una significativa diffusione di Sistemi di Telecontrollo messi in sicurezza mediante implementazione di IEC 62351 è necessario che parallelamente:

1. Utility e Fornitori facciano la loro parte sul tavolo IEC per far convergere la norma IEC 62351 ad un completo IS e sappiano trovare le opportunità per applicarla;
2. Gli enti regolatori prevedano un progressivo ma obbligatorio percorso per la messa in sicurezza dello scambio dati fra gli operatori del mercato elettrico.

I TSO (Transmission System Operator), che si trovano ad essere interlocutori degli enti regolatori e degli attori del mercato elettrico, potrebbero favorire l'introduzione di una PKI per il sistema elettrico che agirebbe come infrastruttura abilitante alla realizzazione di sistemi basati su IEC 62351. Una tale PKI potrebbe essere la radice del sistema di trust fra PKI descritto sopra (vedi par. 3.1).

Ringraziamenti

Ringraziamo tutti i colleghi che in Enel ed ABB hanno consentito la stesura di questa memoria leggendo pazientemente queste pagine e dandoci consigli e ritorni utili ad una più esatta e completa descrizione dei temi trattati.

Bibliografia e documenti di riferimento

[1] **Sicurezza informatica nei sistemi di telecontrollo per impianti di produzione da fonte rinnovabile**; F. Bellio, L. Cicognani, S. Doga – Atti del Forum Telecontrollo 2011

[2] **IEC TS 62351 nei sistemi di controllo per la Generazione del Gruppo Enel**; G.L. Pugni, F. Bellio – Atti del Forum Telecontrollo 2013

[3] **IEC 62351: Power systems management and associated information exchange – Data and communication security**; Parti da 1 a 13 – edizioni IEC - International Electrotechnical Commission

[4] **Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile – RFC 5280**; Internet Engineering Task Force (IETF)

[5] **Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework – RFC 3647;** Internet Engineering Task Force (IETF)

[6] **PUBLIC-KEY CRYPTOGRAPHY STANDARDS (PKCS)**; RSA Laboratories

[7] **Simple Certificate Enrollment Protocol (SCEP) - draft-nourse-scep-23;** Internet Engineering Task Force (IETF)

[8] **X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol (OCSP) – RFC 6960 ;** Internet Engineering Task Force (IETF)

[9] **IEC 60870-5-7 TS: Telecontrol equipment and systems – Part 5-7: Security extensions to IEC 60870-5-101 and IEC 60870-5-104 protocols (IEC 62351-5 secure authentication)** – edizioni IEC - International Electrotechnical Commission

[10] **IEC 60870-5-104 Second edition - Telecontrol equipment and systems – Part 5-104: Transmission protocols – Network access for IEC 60870-5-101 using standard transport profiles** – edizioni IEC - International Electrotechnical Commission

[11] **IEC TC57 WG15**: The Working Group 15 undertake the development of standards for security of the communication protocols defined by the IEC TC 57, specifically the IEC 60870-5 series, the IEC 60870-6 series, the IEC 61850 series, the IEC 61970 series, and the IEC 61968 series.

Undertake the development of standards and/or technical reports on end-to-end security issues – la definizione è presa dal sito di documentazione del IEC TC57 WG15 (http://iectc57.ucaiug.org/wg15public/default.aspx), il WG cura lo sviluppo di IEC 62351.