

ANIE
AUTOMAZIONE



IEC 62351 implementazione nei sistemi di telecontrollo per la Generazione Italia di Enel



Federico Bellio, Enel Produzione – Generazione Italia
Gian Luigi Pagni, Enel Italia – Information & Communication Technology
Marco Biancardi ABB Power Systems Division
Mauro Casalini, ABB Power Systems Division



Power and productivity
for a better world™



Indice della presentazione

Introduzione:

Le puntate precedenti su IEC62351

IEC62351 - la struttura della norma

IEC TC57 WG15 Architecture of Information Standard

Il Sistema di Telecontrollo:

Struttura duale SCADA-NSM secondo IEC62351-7

Relazione tra SCADA-RTU in connessione sicura e PKI

L'infrastruttura di chiave pubblica PKI

Nuovi processi sono richiesti per gestire chiavi/certificati

Implementazione SCADA:

Driver IEC 60870-5-104 con stack 62351

Il monitoraggio del traffico dati:

Il problema che si crea per l'inserimento della cifratura

Una possibile soluzione con traffico cifrato

Introduzione

Le puntate precedenti su IEC62351

IEC 62351: requisiti e minacce



- **Requisiti di sicurezza fondamentali:**
 - **Riservatezza (Confidentiality):** prevenire accesso non autorizzato informazioni;
 - **Integrità (Integrity):** prevenire modifica non autorizzata e furto informazioni;
 - **Disponibilità (Availability):** prevenire provocate indisponibilità servizi vitali e accesso autorizzato informazioni;
 - **Non-ripudiabilità o responsabilità (Non-repudiation or accountability):** prevenire rifiuto azione avvenuta o rivendicazione di un'azione non avvenuta.



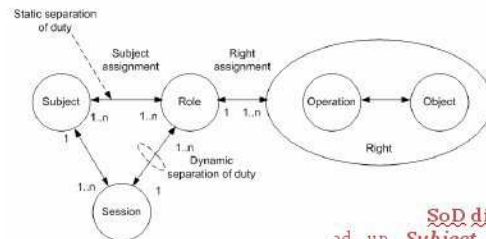
• M



RBAC Process Model

Diagramma RBAC

SoD statica
ad un **Subject** posso associare più **Role**, un **Role** si può assegnare a più **Subject**, ad ogni **Role** sono assegnati più **Right** (facoltà di esercitare un **Operation** su un **Object**)



SoD dinamica
ad un **Subject** posso associare più **Session**, ad ogni **Session** posso associare più **Role**, ad ogni **Role** sono assegnati più **Right**

«Competitività e Sostenibilità. Progetti e tecnologie al servizio delle reti di pubblica utilità» Bologna, 6-7 novembre 2013



Data Object Model

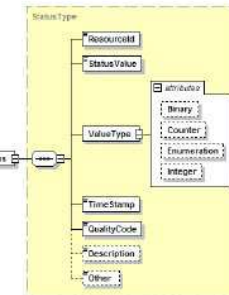
Per ottenere il monitoraggio integrato delle entità coinvolte nell'ambito dei sistemi di telecontrollo la norma 62351-7 utilizza un modello ad oggetti di tipo astratto, che possono essere di tipo semplice, cioè associati ad esempio ad un valore booleano o numerico, e più frequentemente oggetti strutturati che sono costituiti in modo ricorsivo da oggetti semplici o da ulteriori strutture:

- L"ID" della risorsa da monitorare
- Il "nome dell'oggetto", che rappresenta l'identità del "data object"
- Indicatore di qualità del data value
- Il timestamp di cambiamento.

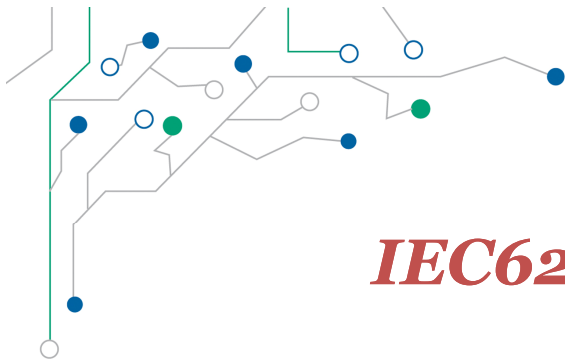
Gli oggetti possono essere in sola lettura o anche scrivibili.

La norma introduce alcune categorie di oggetti organizzati in tre livelli principali:

- "Networks and Protocols"
- "End Systems"
- "Intrusion Detection"



«Competitività e Sostenibilità. Progetti e tecnologie al servizio delle reti di pubblica utilità» Bologna, 6-7 novembre 2013

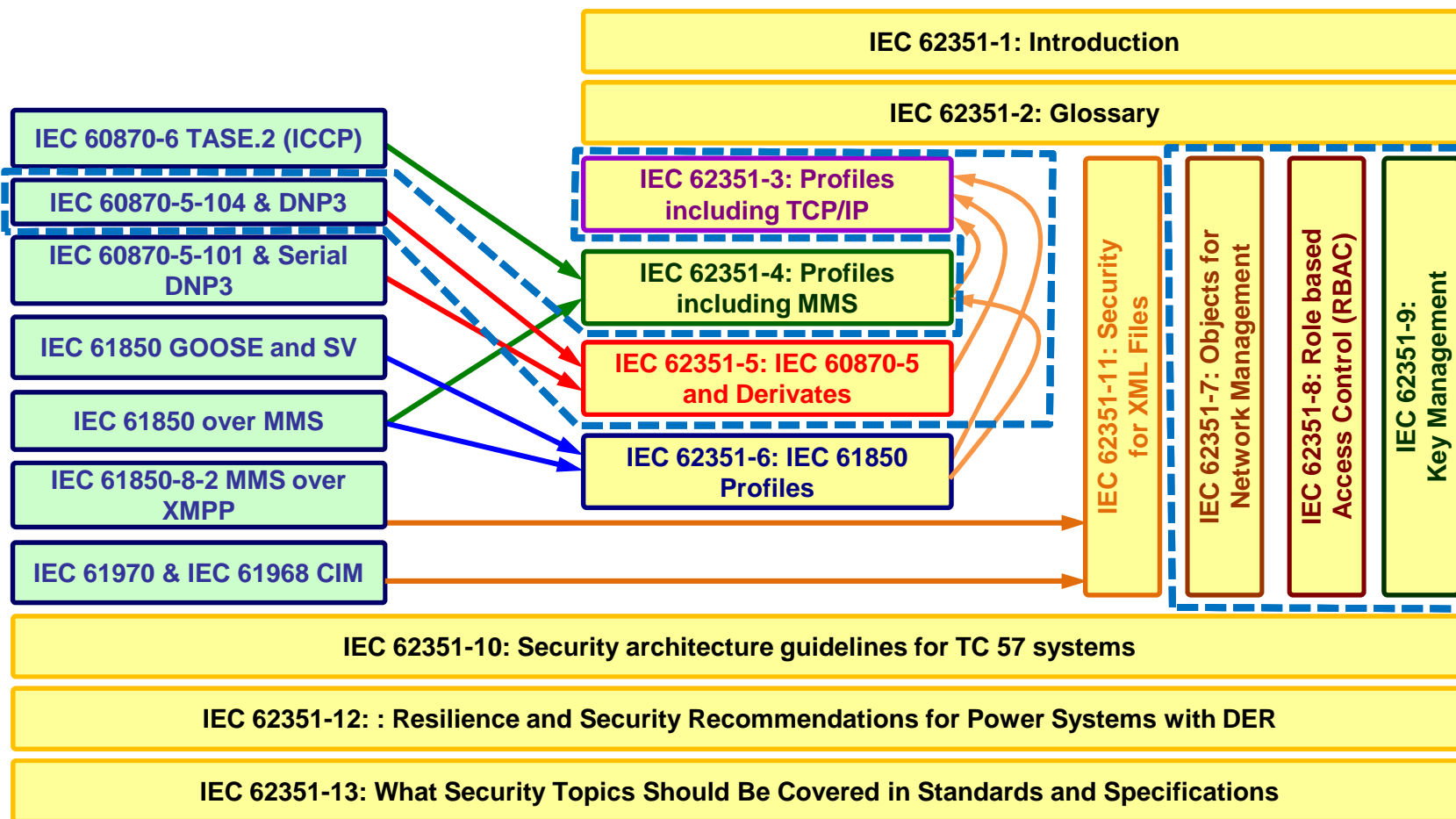


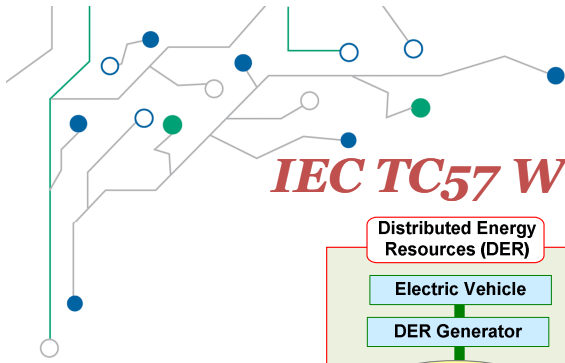
Introduzione

IEC62351 la struttura della norma

IEC TC57 Communication Standards

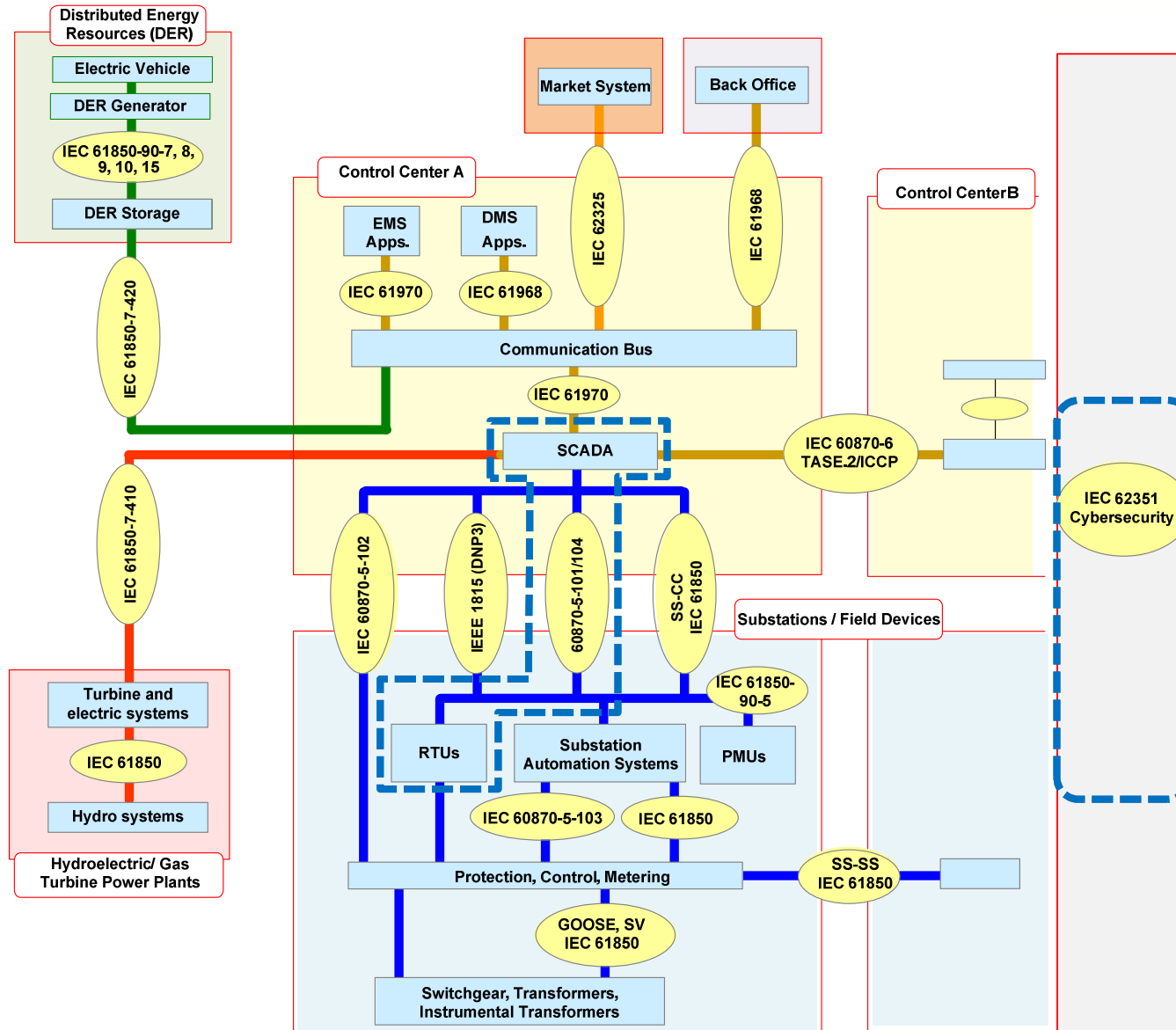
IEC 62351 Security Standards





Introduzione

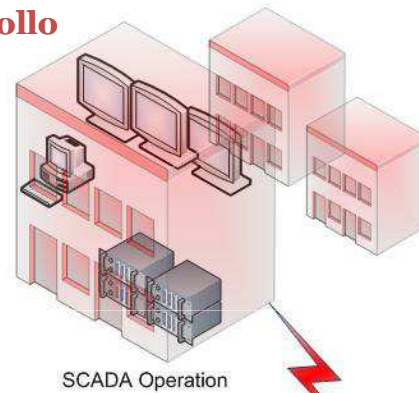
IEC TC57 WG15 Architecture of Information Standard



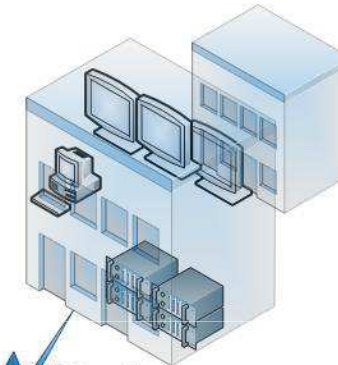
Il Sistema di Telecontrollo

Struttura duale SCADA-NSM secondo IEC62351-7

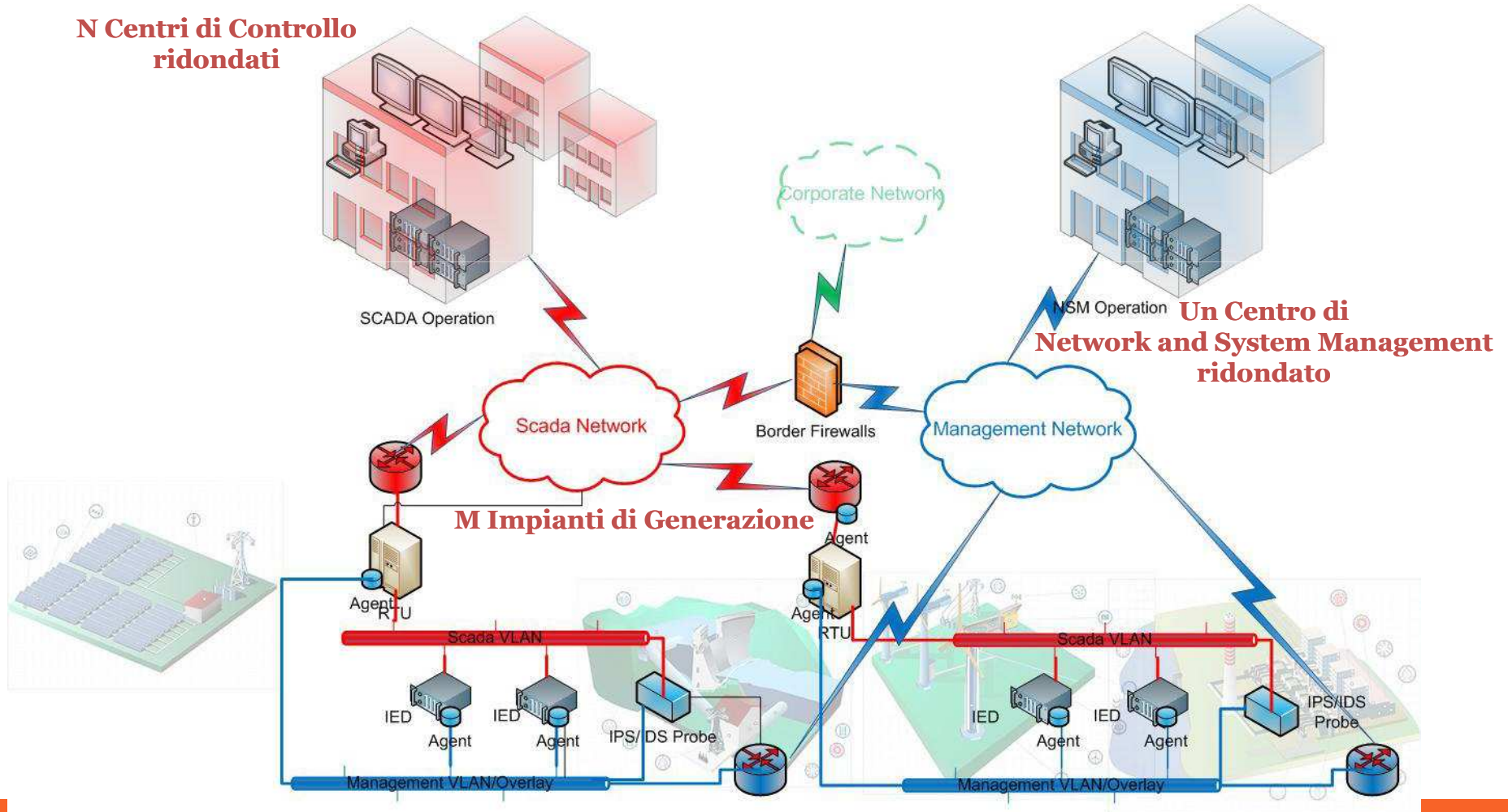
**N Centri di Controllo
ridondati**



SCADA Operation

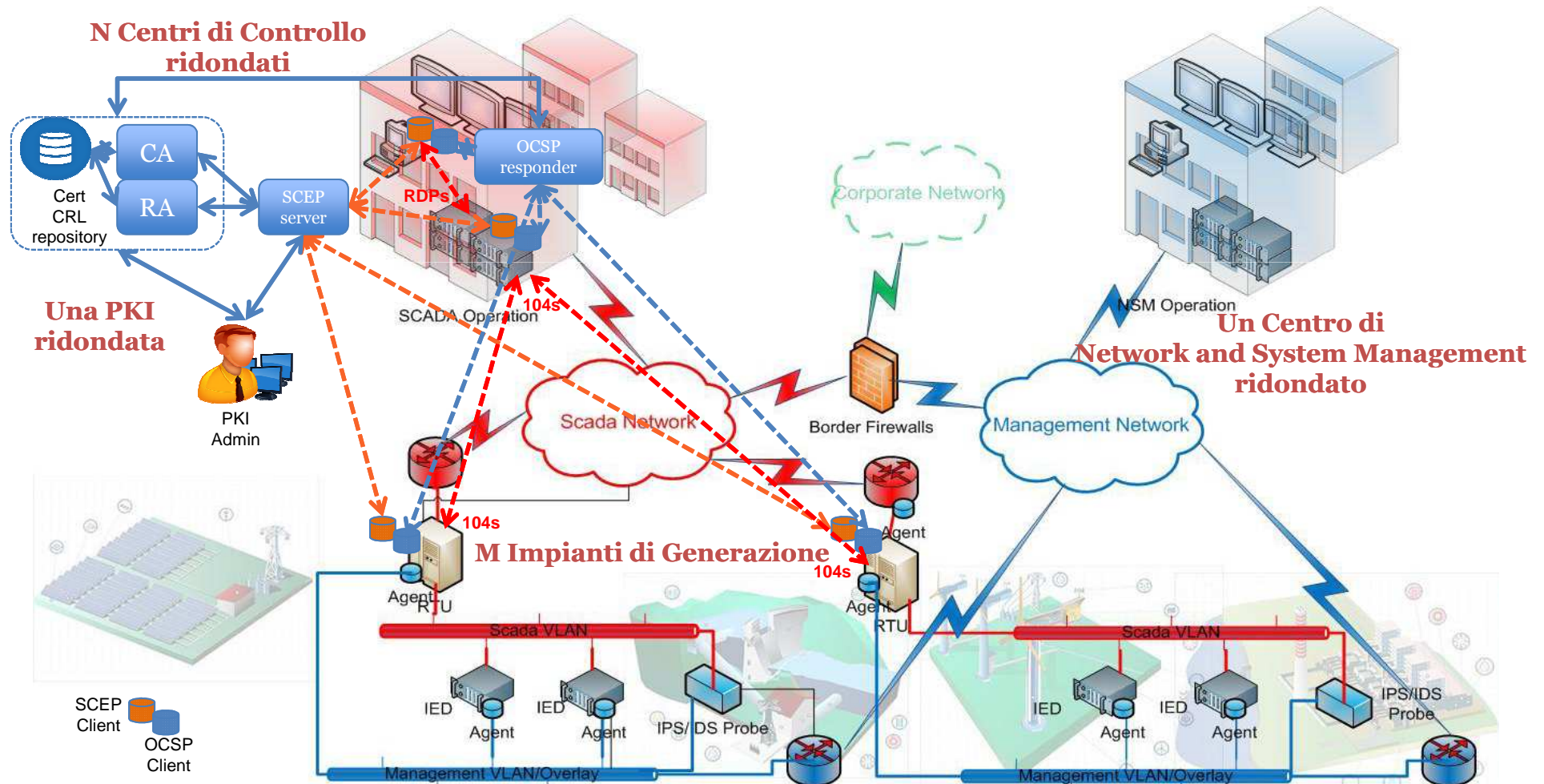


**Un Centro di
Network and System Management
ridondato**



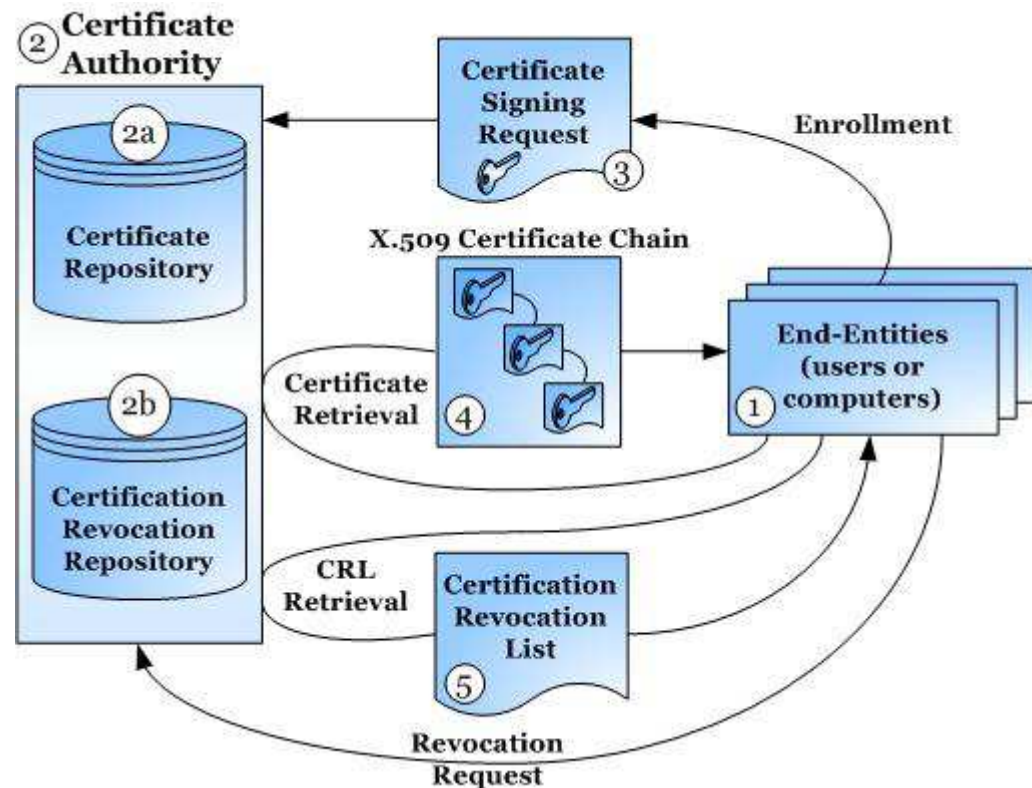
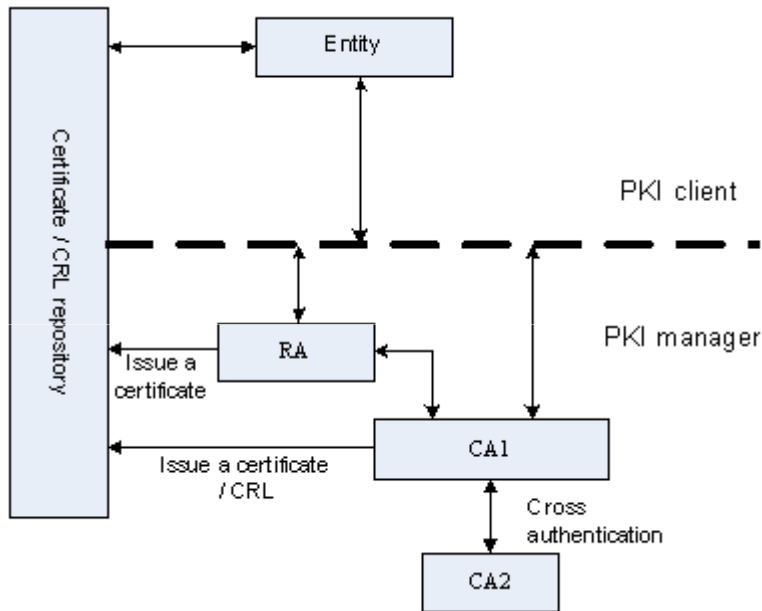
Il Sistema di Telecontrollo

Relazione tra SCADA-RTU in connessione sicura e PKI



Il Sistema di Telecontrollo

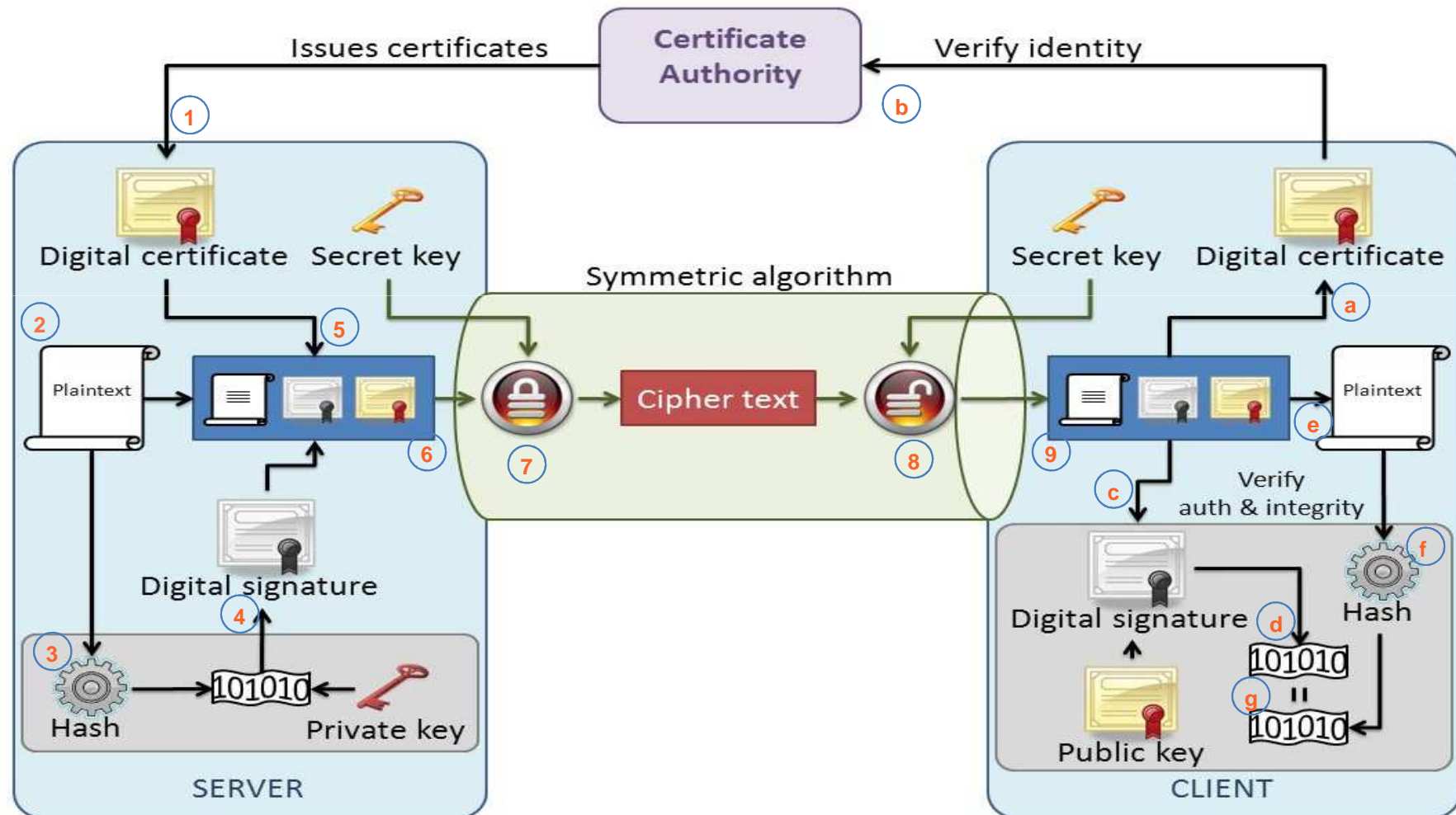
L'infrastruttura di chiave pubblica PKI (Public Key Infrastructure)

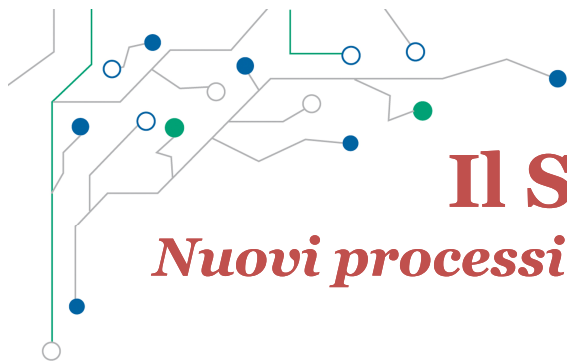


**Schemi logico-funzionali di una CA
(modello in RFC 5280 - X.509)**

Il sistema di telecontrollo

L'infrastruttura di chiave pubblica PKI (uso delle chiavi crittografiche)





Il Sistema di Telecontrollo

Nuovi processi sono richiesti per gestire chiavi/certificati

INSERIMENTO NUOVO DISPOSITIVO

- Emissione certificato
- Enrollment nella CA

SCADENZA - RINNOVO CERTIFICATO

- Verifica certificato
- Rinnovo certificato

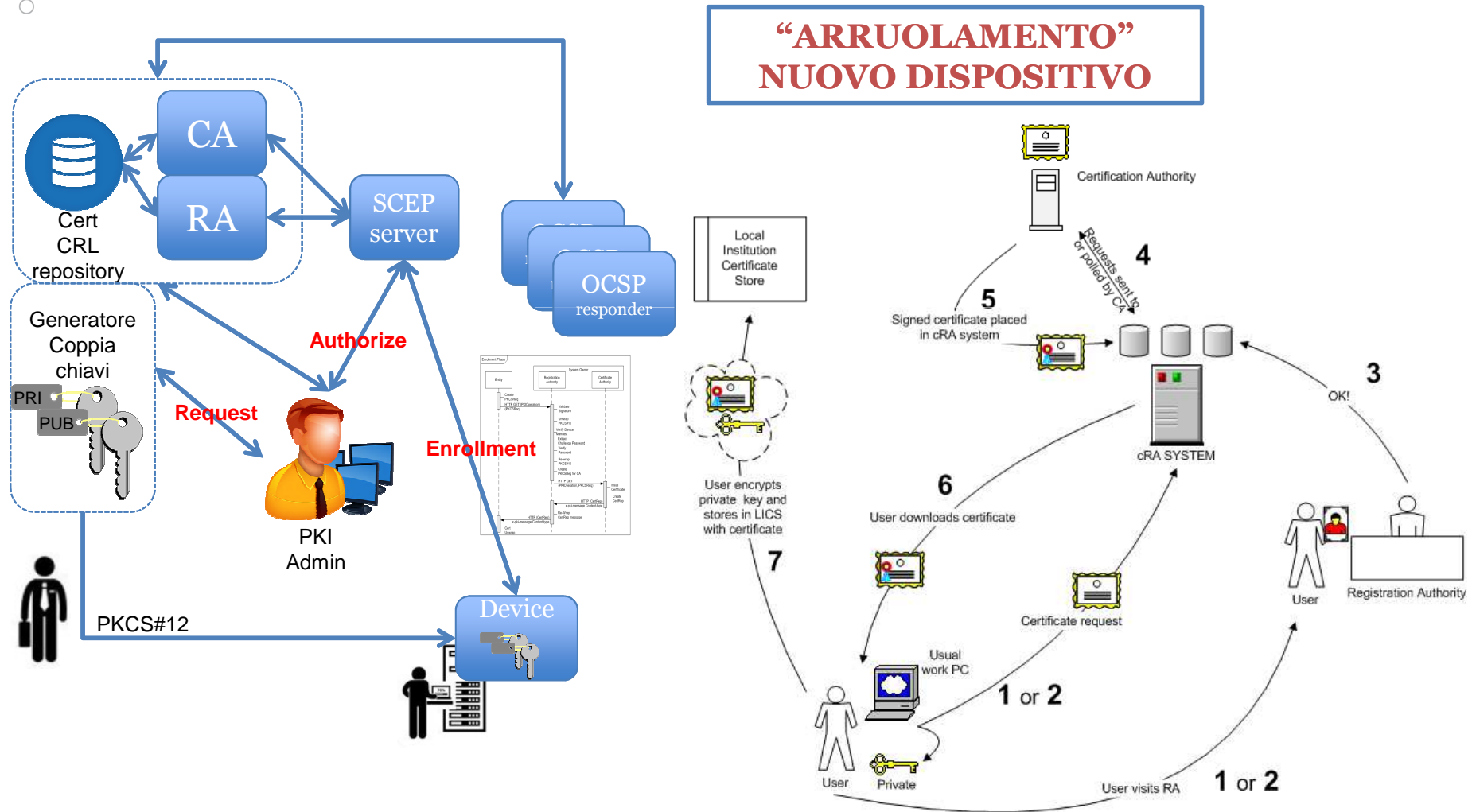
DECADENZA - REVOCA CERTIFICATO

- Verifica certificato
- Inutilizzabilità del certificato



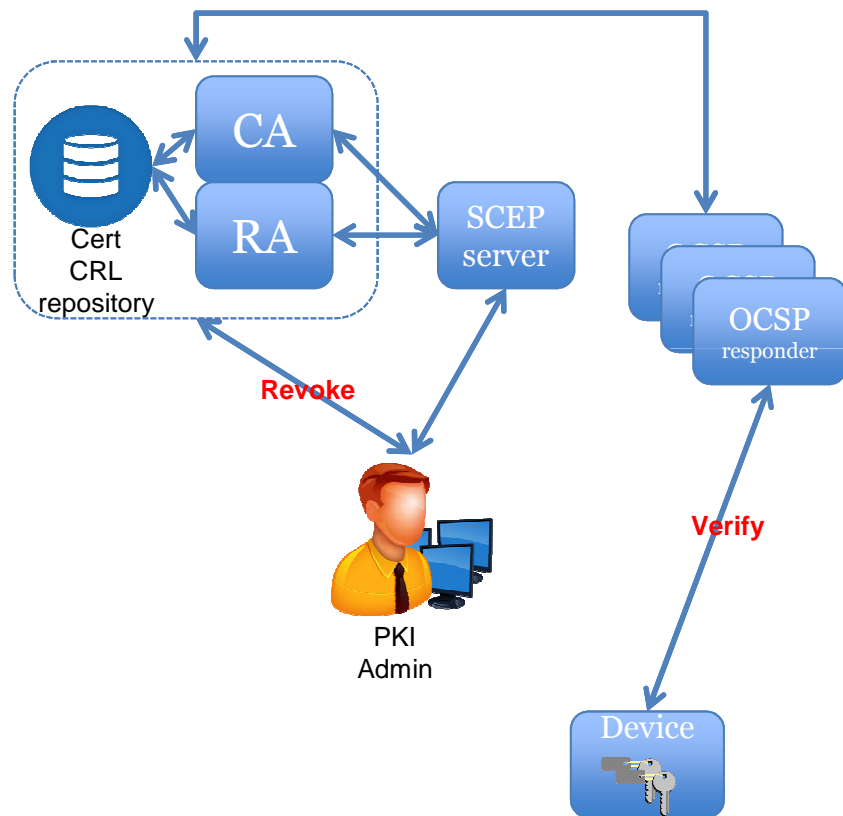
Il Sistema di Telecontrollo

Nuovi processi sono richiesti per gestire chiavi/certificati

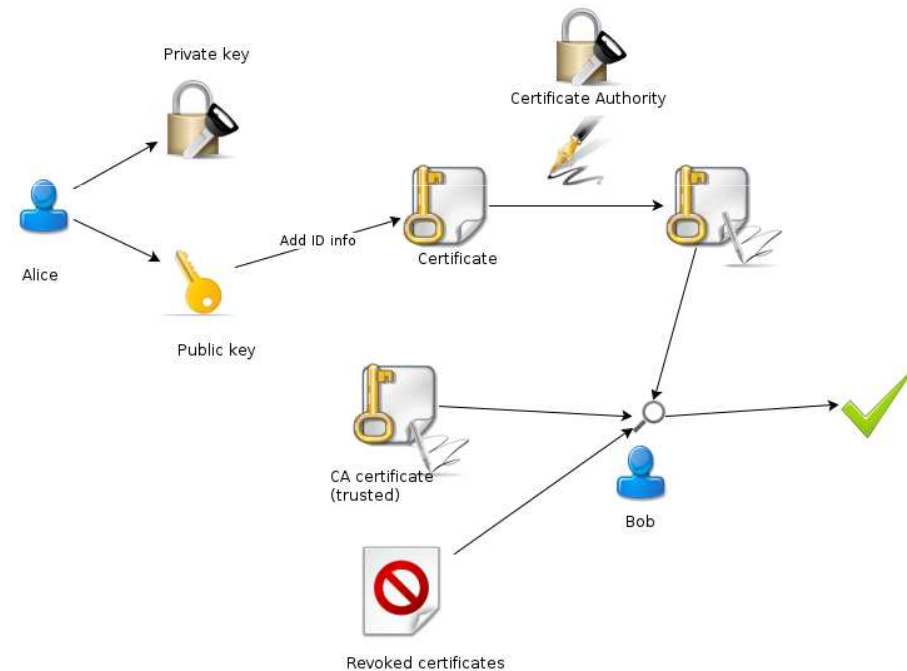


Il sistema di telecontrollo

Nuovi processi sono richiesti per gestire chiavi/certificati



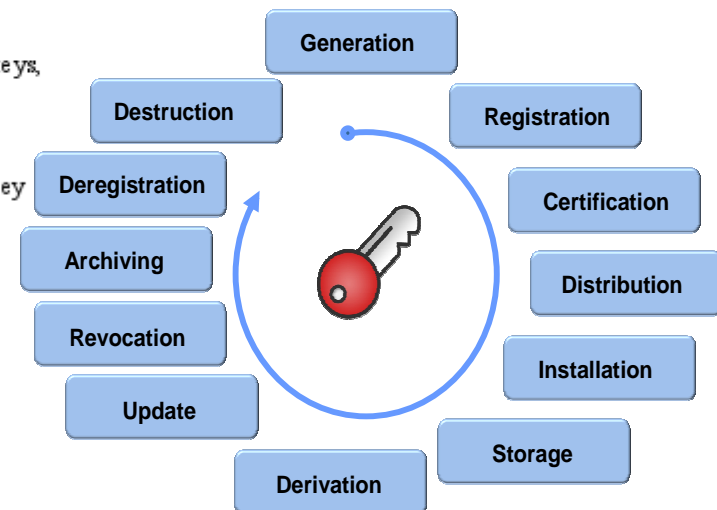
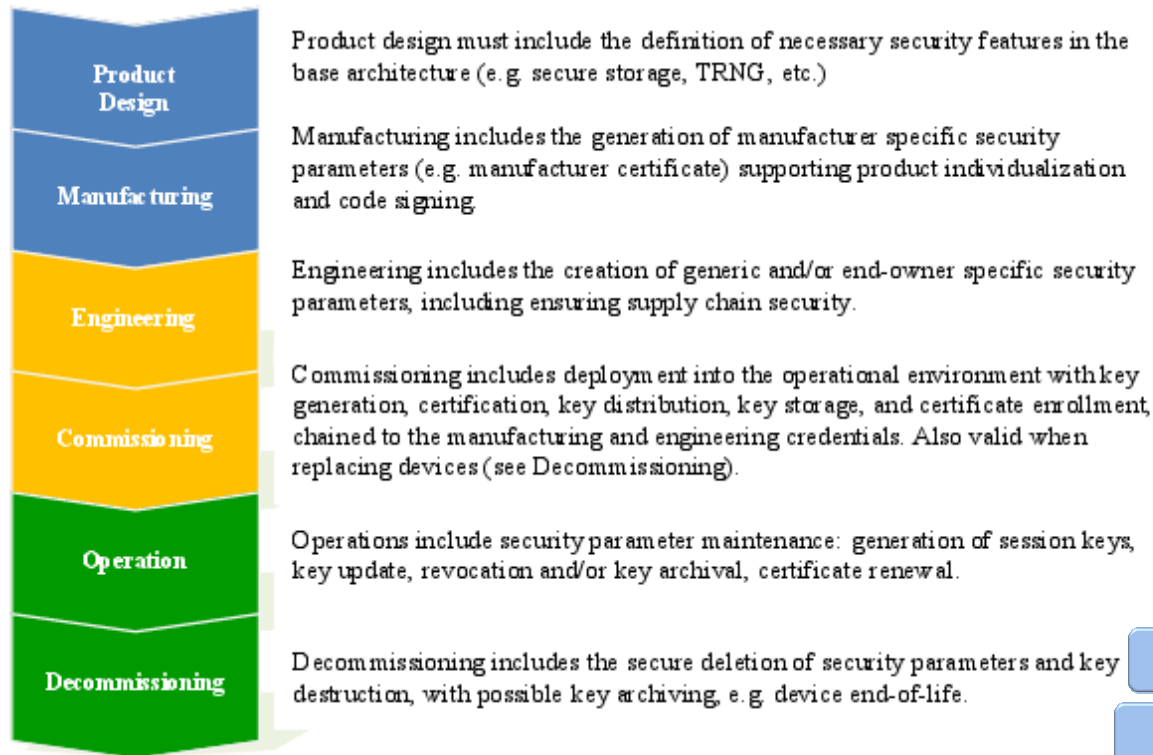
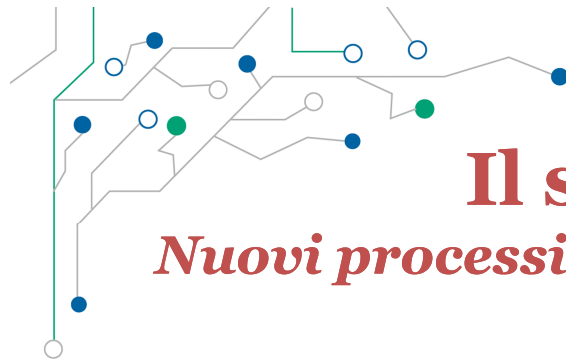
Revoca – Verifica Validità del Certificato



Alice e Bob possono essere rispettivamente il server SCADA e una RTU
La verifica è mutua e i ruoli si scambiano

Il sistema di telecontrollo

Nuovi processi sono richiesti per gestire chiavi/certificati

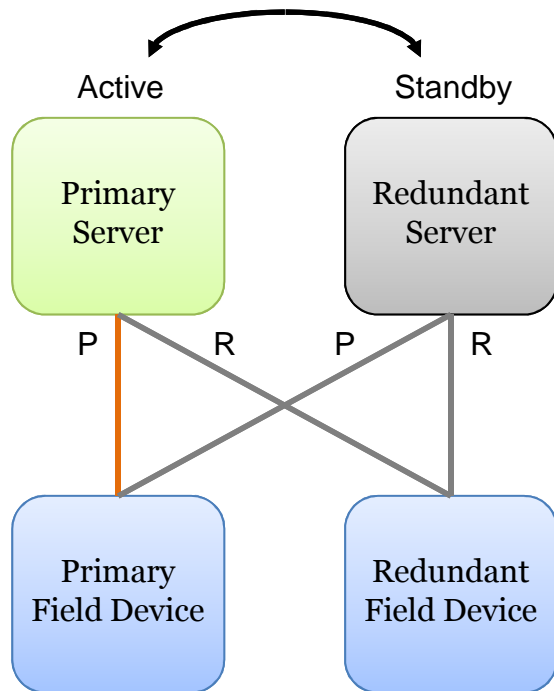




Implementazione SCADA

Driver IEC 60870-5-104 con stack 62351

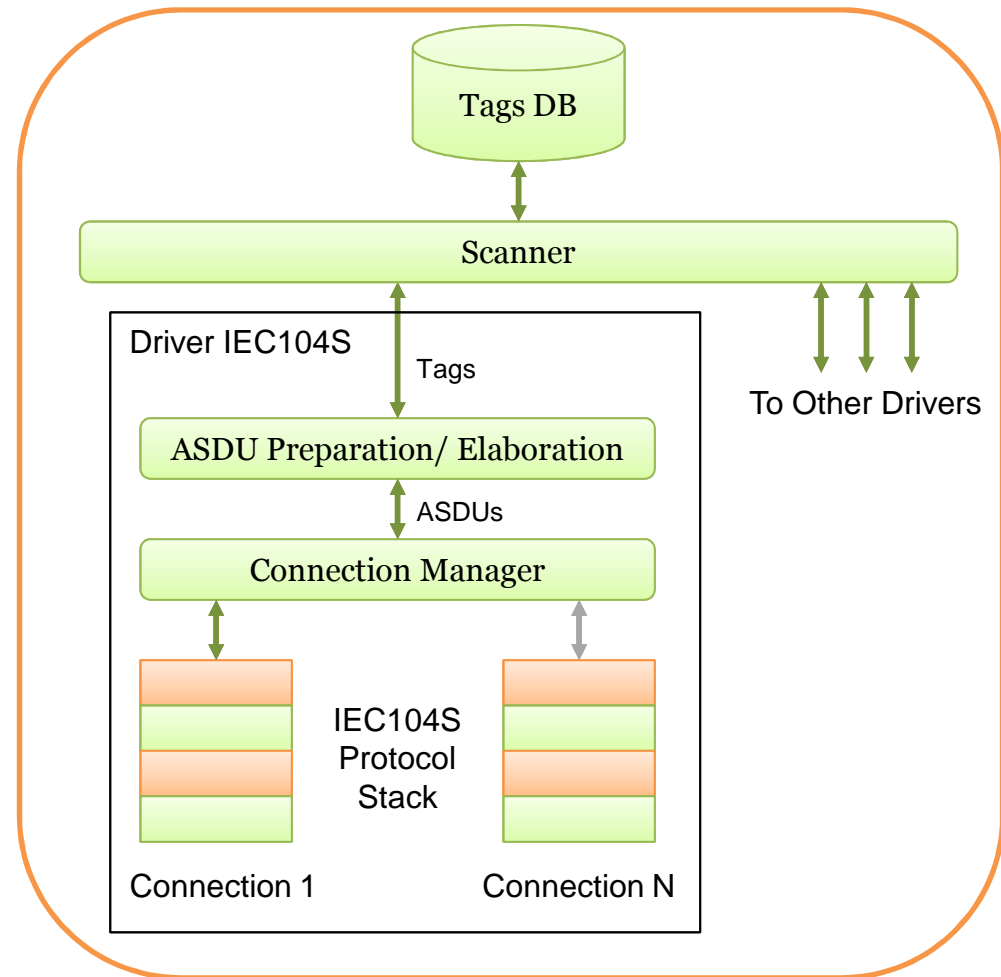
IEC104 Connections Architecture



P = Primary Connection
R = Redundant Connection

Only one connection by time has DT Active
(IEC 60870-5-104, Par. 10)

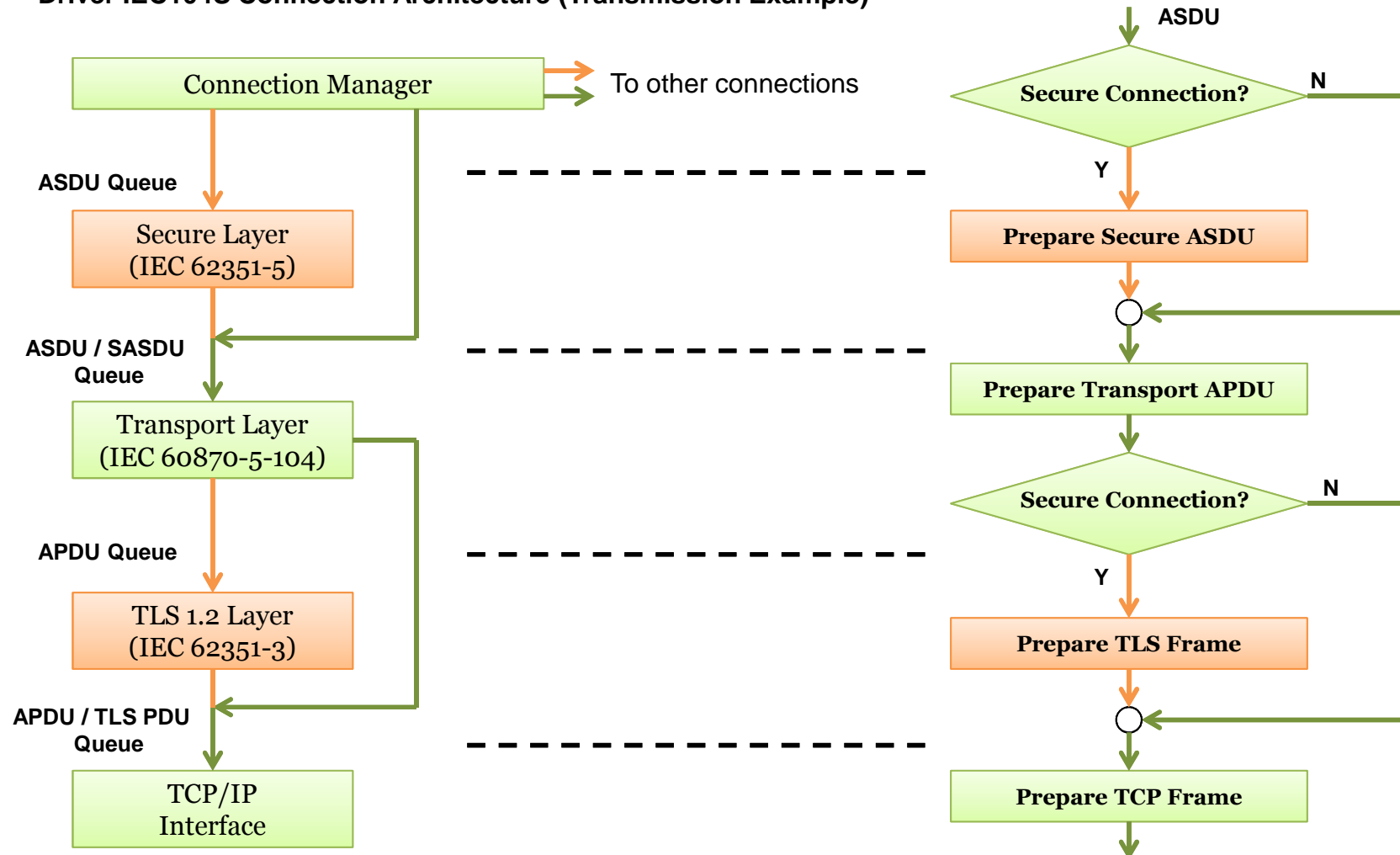
Server Communication Architecture



Implementazione SCADA

Driver IEC 60870-5-104 con stack 62351

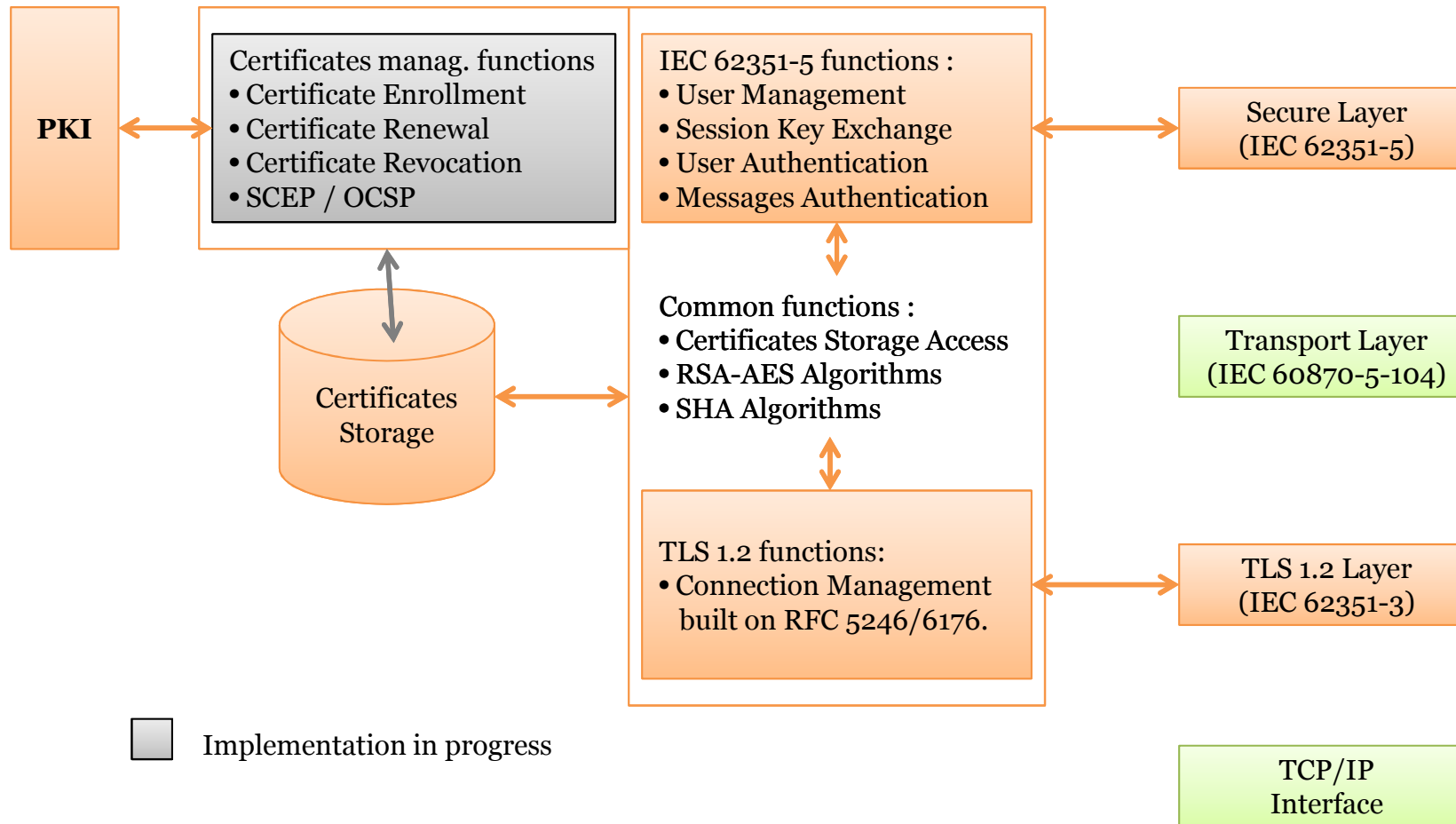
Driver IEC104S Connection Architecture (Transmission Example)



Implementazione SCADA

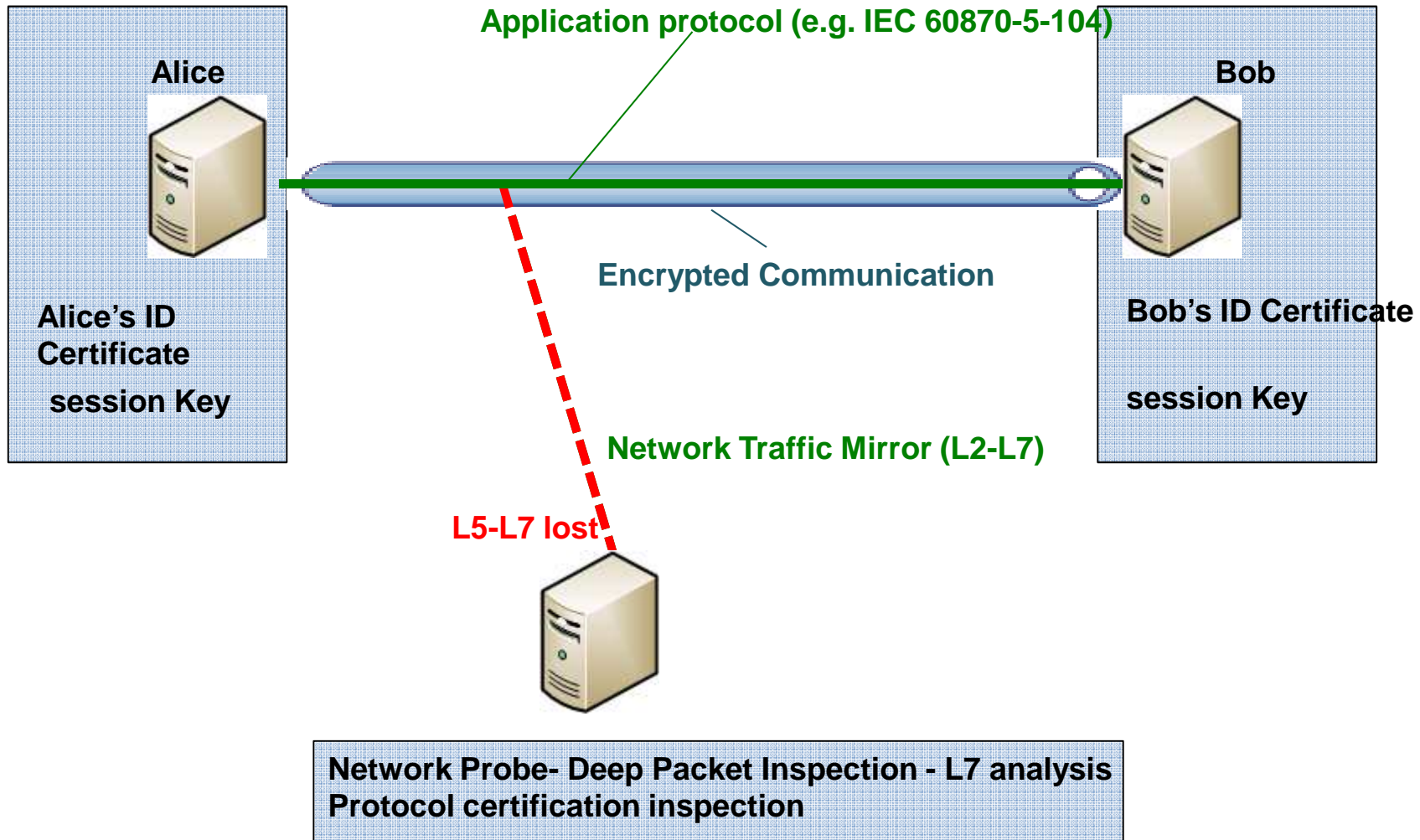
Driver IEC 60870-5-104 con stack 62351

ABB CSA (Common Security Architecture) library



Il monitoraggio del traffico dati

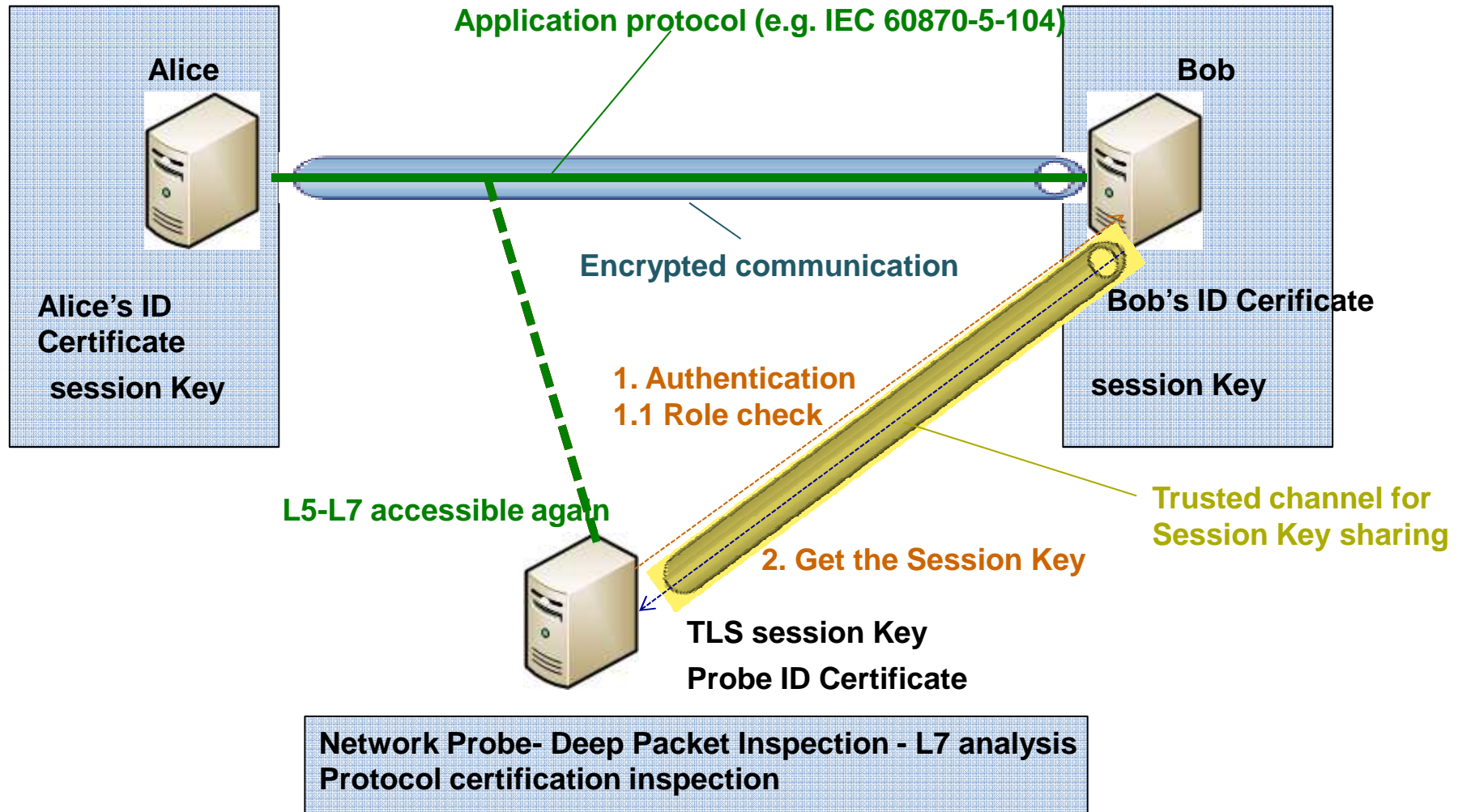
Il problema che si crea per l'inserimento della cifratura



Issuing Owner/Unit | Reclassified as by .The information contained in this document is the property of Enel SpA and must be used by the recipient only for the purposes for which it was intended. It is not to be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of Enel SpA.

Il monitoraggio del traffico dati

Una possibile soluzione con traffico cifrato



Issuing Owner/Unit | Reclassified as by .The information contained in this document is the property of Enel SpA and must be used by the recipient only for the purposes for which it was intended. It is not to be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of Enel SpA.



Conclusioni

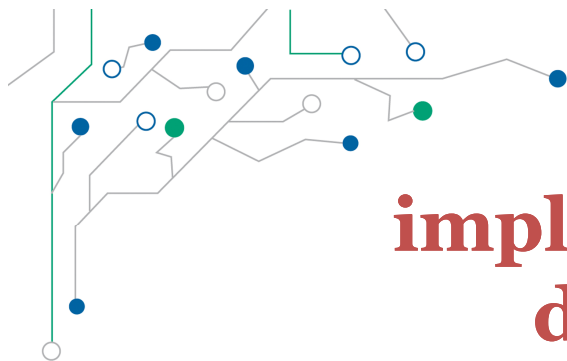


L'esperienza del nostro progetto ci dice che la norma IEC 62351 è sufficientemente matura per essere compitamente implementata sui sistemi in esercizio basati su IEC 60870-5-104.

L'impatto dell'inserimento dello stack di sicurezza non è diverso da quello provocato da una comune significativa release di prodotto.

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 nel 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*



IEC 62351 implementazione nei sistemi di telecontrollo per la Generazione Italia di Enel



Grazie per l'attenzione



Federico Bellio, Enel Produzione – Generazione Italia:

Gian Luigi Pagni, Enel Italia – Information & Communication Technology:

Marco Biancardi, ABB Power Systems Division:

Mauro Casalini, ABB Power Systems Division:

federico.bellio@enel.com

gianluigi.pagni@enel.com

marco.biancardi@it.abb.com

mauro.casalini@it.abb.com



ABB

Power and productivity
for a better world™