Rilheva IoT Platform

Procedure di sicurezza adottate

SISTEMA DI TELECONTROLLO RILHEVA GPRS - 3G (CARATTERISTICHE DEL VETTORE GPRS - 3G E SICUREZZE ADOTTATE)

Abstract: Sicurezza del Sistema di Telecontrollo Rilheva

Xeo4 ha progettato e sviluppato il sistema di telecontrollo Rilheva tenendo presente oltre agli aspetti di affidabilità, funzionalità e facilità di uso anche gli aspetti relativi alla sicurezza di accesso degli operatori abilitati dei Committenti ed a quelli relativi ad intrusione da parte di terzi.

In particolare sono state adottate tutte le protezioni hardware e software attualmente disponibili ed aggiornate continuamente per la prevenzione e la protezione del sistema di telecontrollo Rilheva.

I tipi di protezione adottati sono i seguenti:

- crittografia sulla infrastruttura trasmissiva dei dati tra le stazioni remote Rilheva ed il centro di telecontrollo;
- sicurezza e protezione fisica ed informatica lato centro di telecontrollo Xeo4;
- interfaccia web utilizzabile dagli operatori dei Committenti protetta da SSL (128 bit);
- gestione accessi con autenticazione e registrazione di tutte le operazioni eseguite dagli operatori abilitati dei Committenti (auditing);
- crittografia dei dati trasmessi dal centro di telecontrollo Xeo4 ai sistemi informativi aziendali dei Committenti.

Xeo4 Srl
www.xeo4.it
info@xeo4.it
+39.0523.498721

Vengono di seguito descritte le tipologie di sicurezza adottate per i punti sopra riportati.

Crittografia sulla infrastruttura trasmissiva tra le stazioni remote Rilheva e il centro di telecontrollo

Xeo4 utilizza principalmente per la trasmissione dei dati tra le stazioni remote RILHEVA ed il centro di telecontrollo web server le reti telefoniche cellulari **GPRS e 3G,** che sono un' estensione della rete telefonica **GSM.**

L'adozione della rete cellulare **GPRS – 3G** rappresenta una soluzione ottimale costi/benefici per la trasmissione dei dati tra le stazioni remote RILHEVA ed il centro di telecontrollo Xeo4, quando devono essere gestiti un elevato numero di stazioni remote con un volume contenuto dei dati da trasmettere.

Poiché è molto complesso riuscire ad identificare ogni stazione remota collegata alla rete pubblica internet a causa della limitata disponibilità di indirizzi IP a livello mondiale, Xeo4 ha messo a punto, a seguito di una impegnativa attività di ricerca e di sviluppo durata diversi anni, una soluzione che supera il limite degli indirizzi della rete **GPRS – 3G** identificando ogni stazione remota collegata al server indipendentemente dalla posizione geografica in cui sono installate, dal tipo di operatore telefonico impiegato, dalle funzionalità e dalle restrizioni della rete IP dell'operatore stesso.

L'impiego del vettore **GPRS – 3G**, con l'ottimizzazione della trasmissione mediante opportuni algoritmi di compressione e dal tipo di identificazione realizzata da Xeo4, consente di:

- avere una buona velocità di trasmissione e di gestire agevolmente il volume di dati da trasmettere;
- disporre di un canale di comunicazione sempre aperto (**ALWAYS ON)** permettendo in pratica una gestione "in tempo reale" di tutte le stazioni remote RILHEVA da parte del centro di telecontrollo web server di Xeo4;
- ottenere la **contemporaneità e la bidirezionalità** delle connessioni tra le stazioni remote ed il centro di telecontrollo;
- gestire contemporaneamente più gestori telefonici in caso di mancata copertura totale di un unico gestore per avere la copertura radio totale dell'area in cui viene effettuato il telecontrollo degli impianti dei Committenti;

Le caratteristiche sopra citate relative alla comunicazione **GPRS – 3G** sono prerogative proprie dell'architettura Rilheva e non frutto di accordi particolari con determinati operatori telefonici. Pertanto, in qualsiasi momento, i Committenti hanno la possibilità di passare ad un altro operatore di telefonia mobile in grado di fornire un analogo servizio di connettività **GPRS – 3G** a condizioni più vantaggiose.

Per realizzare la comunicazione tra le stazioni remote Rilheva ed il centro di telecontrollo Xeo4 è necessario utilizzare le comuni schede SIM GSM. Sono comunque consigliate le schede **SIM CARD GSM M2M** ("machine to machine" per il solo traffico dei dati **GPRS – 3G** e non predisposte della funzione di fonia per cui sono esenti dal canone governativo). E' consentito l'uso **contemporaneo** di SIM di più operatori telefonici nazionali come TIM – VODAFONE – WIND – TRE per la comunicazione delle stazioni remote **RILHEVA** con il centro di telecontrollo Xeo4 previa verifica della copertura radio nell'area di installazione delle stazioni remote.

La comunicazione tra le stazioni remote ed il centro di telecontrollo Xeo4 è una funzione ampiamente **utilizzata, collaudata e consolidata** dai Committenti che si avvalgono dei servizi forniti da Xeo4 e **non è vincolata** ad una infrastruttura telefonica creata "ad hoc".
La rete di comunicazione tra le stazioni remote ed il centro di telecontrollo Rilheva è basata su protocollo IP che utilizza l'infrastruttura GPRS – 3G del provider di telefonia prescelto (es. TIM, VODAFONE, WIND, ..).
Poiché il protocollo GPRS – 3G è una estensione della rete pubblica digitale GSM, i dati sono nativamente protetti tramite algoritmo di crittografia A5, il quale si basa su una chiave di sessione a 64 bit. Le recenti reti utilizzano l'estensione A5/3 che garantisce un ulteriore livello di sicurezza.
L'implementazione del meccanismo di protezione per comunicazioni GPRS – 3G prende il nome di GEA3[1], ed è uno standard pubblico emesso dall'ente ETSI[2].

Xeo4 Srl
www.xeo4.it
info@xeo4.it
+39.0523.498721

Sicurezza e protezione fisica ed informatica lato centro di telecontrollo Xeo4;

Le apparecchiature del centro di telecontrollo Xeo4 (server, router,..) sono alloggiate presso una serverfarm dotata dei più avanzati sistemi di sicurezza (sorveglianza armata, telecamere CCTV) e di sistemi di intrusione hardware ed informatici al fine di garantire:

- Backup della connettività Internet;
- SLA (continuità del servizio) del 99,9%
- Livelli di sicurezza informatica, grazie all'utilizzo tecnologie Firewall e Antivirus dell'ultima generazione;
- Presidio continuo di personale tecnico specializzato presso il centro di telecontrollo;
- Backup dell'alimentazione elettrica per mezzo di adeguati gruppi di continuità e gruppi elettrogeni;
- Climatizzazione a temperatura e umidità controllate dei locali in cui è installato il centro di telecontrollo;
- Sistemi di controllo di intrusione fisica;
- Backup dei dati acquisiti dalle stazioni remote Rilheva;

Il centro di telecontrollo è protetto da componenti firewall dell'ultima generazione che bloccano accessi non autorizzati e segnalano all'Amministratore di sistema Xeo4 eventuali tentativi di intrusione e penetrazione al centro di telecontrollo da parte di terzi.
La base dati utilizza tecniche di crittografia per la memorizzazione dei dati sensibili (es. password degli utenti). Sono inoltre implementati meccanismi automatici di backup che garantiscono, in caso di guasto hardware, il ripristino del database in tempi brevi con una minima perdita di dati.

Xeo4 Srl
www.xeo4.it
info@xeo4.it
+39.0523.498721

Il personale Xeo4 monitora costantemente lo stato dei propri server per minimizzare e per prevenire anomalie e fuori servizio del sistema di telecontrollo anche in giorni o orari non lavorativi. Inoltre, al fine di poter garantire una pronta risposta in caso di malfunzionamenti del sistema di telecontrollo, Xeo4 ha installato appositi software e opportuni controlli (watchdog) che controllano, automaticamente ed in continuo, il buon funzionamento di tutte le funzioni del sistema di telecontrollo, inviando le opportune segnalazioni al personale reperibile Xeo4 per assicurare interventi rapidi ed efficaci garantendo nell'arco dell'anno una continuità di esercizio pari al 99,9 %.

Interfaccia Web protetta da SSL 128 bit

Gli operatori dei Committenti, operando dalle rispettive sedi operative o da altre sedi, possono accedere al portale Rilheva mediante l'impiego di personal computer fissi e/o portatili dotati di normale browser Internet.

Sono disponibili diversi tipi di accessi: ad esempio per gli amministratori del sistema dei Committenti, per gli operatori destinati alla configurazione, per operatori adibiti alla sola visualizzazione dei dati e per i clienti dei Committenti.

Per aumentare il grado di protezione durante la navigazione, è stato adottato il protocollo SSL4 (Secure Socket Layer) a 128 bit che consente, grazie all'impiego di tecniche crittografiche, il trasferimento dei dati tramite la rete Internet in modo sicuro. Il suo funzionamento è basato su un sistema a doppia chiave e ai certificati digitali. In pratica esistono due chiavi: una per cifrare i dati inviati, l'altra per decifrarli. La seconda è conosciuta solamente da chi riceve i dati.

La protezione SSL 128 bit è sempre visualizzata nel monitor del personal computer con la visualizzazione di un "**lucchetto"** e con il prefisso **https** che identifica sia la validità e sia la tipologia di protezione adottata. La protezione SSL a 128 bit non presenta alcuna complicazione per i Committenti garantendo la crittografia dei dati con il più elevato grado di protezione attualmente disponibile

Tale protocollo, supportato da tutti i browser presenti sul mercato, è diventato lo standard di riferimento utilizzato da tutti i sistemi Home-Banking e per altre applicazioni critiche.

L'interfaccia web messa a disposizione da Xeo4 garantisce agli utilizzatori dei Committenti:

- riservatezza. Solo gli utenti abilitati possono accedere alle informazioni presenti nel centro di telecontrollo in base al profilo di pertinenza;
- integrità. Viene assicurata l'accuratezza complessiva delle informazioni acquisite da parte delle stazioni remote nei confronti della strumentazione del campo con la trasmissione delle stesse al centro di telecontrollo;
- disponibilità. Gli utenti autorizzati hanno accesso in tempo reale alle informazioni presenti nel centro di telecontrollo.

Gestione accessi e tracking

L'accesso al portale Rilheva web di Xeo4 è vincolato da una fase iniziale di autenticazione (login) in cui gli utenti dei Committenti devono inserire le proprie credenziali (codice azienda, nome utente e password) per accedere al sistema di telecontrollo Xeo4.

In questo modo ogni utente può essere riconosciuto ed abilitato ad accedere ai livelli di servizio legati al proprio profilo.

Il profilo utente definisce l'ambito in cui ciascun utente ha la facoltà di operare all'interno delle funzioni messe a disposizione del sistema di telecontrollo. Sono previsti **4 profili standard** che operano sull'intero parco delle stazioni remote installate che sono sufficienti a soddisfare le esigenze dei Committenti.

Un profilo personalizzato è caratterizzato da un insieme di privilegi in relazione a uno o più ambiti di utilizzo.

Ogni accesso ed ogni operazione effettuata nel sistema di telecontrollo viene registrato in un apposito log di sistema per permettere di risalite a tutti gli accessi ed operazioni effettuati, rilevando in questo modo la responsabilità di eventuali manomissioni.

Sicurezza dei dati trasmessi dal centro di telecontrollo Xeo4 ai sistemi informativi aziendali dei Committenti.

Il sistema di telecontrollo Xeo4 permette l'esportazione automatica dei dati memorizzati nei server del centro di telecontrollo Xeo4 ai sistemi informativi aziendali dei Committenti.

Sono disponibili due differenti modalità per esportare i dati:

- esportazione automatica XML
- esportazione automatica FTP

L'esportazione automatica XML permette di disporre nel sito web dei Committenti dei dati in tempo reale residenti nel database del centro di telecontrollo Xeo4. Questa funzione è molto utile se si desidera pubblicare sul proprio sito web informazioni di pubblico dominio (es. portata dei canali o temperatura dell'acqua).

La prerogativa di questa funzione consiste nel fatto che i Committenti non devono implementare nessun database sul proprio sito web, in quanto sfruttando la rete internet, possono estrarre, in maniera sicura, i dati dal server del centro di telecontrollo aggiornando i campi della propria pagina web o del proprio applicativo.

L'esportazione automatica FTP permette di generare, con cadenza prefissata, file contenenti la quota parte temporale dei dati di ogni stazione remota (nel formato .csv). Questa funzione è utilizzata dai Committenti che vogliono importare nei Sistemi Informativi Aziendali i dati ritenuti particolarmente importanti al fine di consentire successive elaborazioni. I Committenti potranno disporre, ad esempio giornalmente, dei dati riepilogativi del funzionamento degli impianti.

Le sicurezze adottate per il trasferimento dei dati sono:

- L'autenticazione è inoltre assicurata da hash MD5 per prevenire la visibilità delle credenziali di accesso logico ai dati.
- per i dati FTP non è adottato nessun algoritmo di crittografia in quanto è un protocollo in chiaro. E' tuttavia garantito l'accesso sicuro mediante l'autenticazione alla propria area FTP con user e password. In aggiunta è possibile aumentare il grado di sicurezza mediante accesso in tunnelling VPN con la rete Rilheva