Sicurezza
delle
Unità Locali Intelligenti
WIT

Descrizione Tecnica e Funzionale

V1.0 – 01/2019

+39 011 95 90 256
+39 011 95 90 177 - hot-line@wit-italia.com
10098 Rivoli (To)
wit@wit-italia.com
www.wit-italia.com
www.wit-square.it

1. SOMMARIO

2. INTRODUZIONE

La sicurezza è sempre stata un tema importante per gli impianti tecnici degli edifici, e lo è ancora di più negli ultimi anni.

Questo documento ha lo scopo di fornire una descrizione esaustiva e concisa della sicurezza delle Unità Locali Intelligenti WIT e ulteriori raccomandazioni complementari.

La sicurezza delle Unità Locali Intelligenti (ULI) è costituita da tre insiemi:

La sicurezza degli accessi

L'accesso al sistema deve essere protetto dagli intrusi e deve assegnare le autorizzazioni agli utenti in base ai suoi diritti.

La sicurezza dei dati

I dati costituiscono il cuore di ogni Unità Locale Intelligente. Il loro accesso e la loro integrità nel tempo durata devono essere garantiti.

La sicurezza funzionale

Base e prerequisito essenziali per i due precedenti: la sicurezza funzionale garantisce un funzionamento adeguato in ogni situazione.

Questo simbolo presenta delle raccomandazioni di sicurezza complementari ai prodotti.

La sicurezza dei sistemi WIT è in costante evoluzione.
Questo simbolo presenta le evoluzioni presenti nel nostro piano di miglioramento della sicurezza.

3. LA SICUREZZA DEGLI ACCESSI

3.1 Codici di accesso

L'accesso alle ULI è reso sicuro dalla richiesta di autenticazione a due parametri:

- Un nome utente.
- Una password.

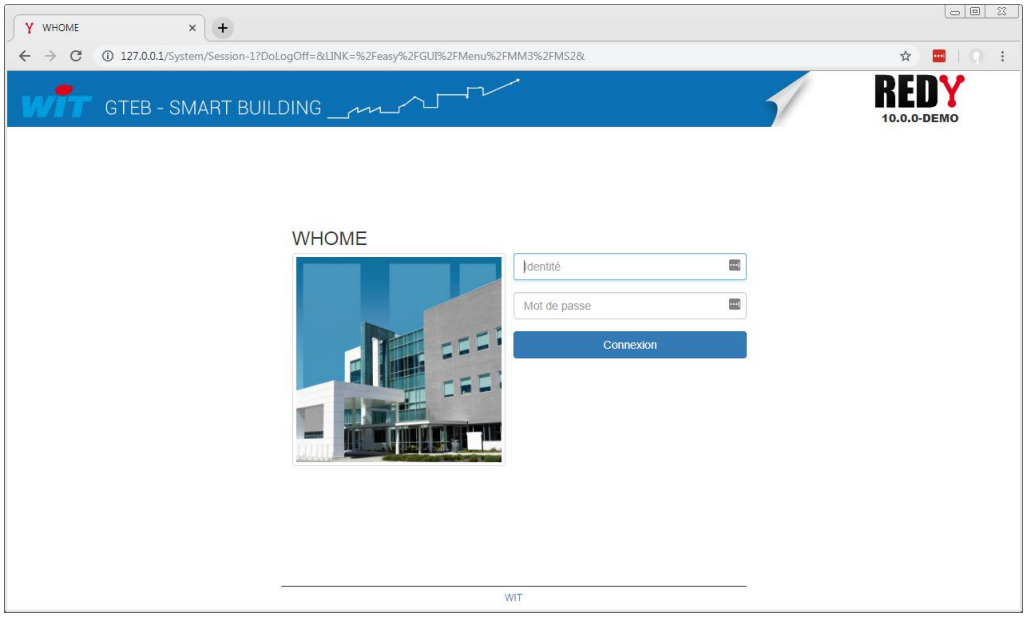

Fig.1 - Pagina di accesso del REDY

Nome utente

- Ogni nome utente è univoco.
  Un controllo automatico dell'unicità viene eseguito ogni volta che un nuovo utente viene creato.
- Un nome utente può contenere da 1 a 65 caratteri.
  Lettere, numeri e/o caratteri speciali.

Password

- Una password può contenere da 1 a 15 caratteri
  Lettere, numeri e/o caratteri speciali.
- Case sensitive: tiene conto del maiuscolo o minuscolo.

Utente predefinito

L'ULI presenta degli account predefiniti che è vivamente consigliato modificare.
Gli account predefiniti sono indicati nella documentazione tecnica di messa in servizio.
Questi sono i primi account utilizzati per tentare di accedere al sistema.

Piano di evoluzione

- Al primo accesso, la password predefinita deve obbligatoriamente essere cambiata.
- Delle regole possono essere applicate durante l'inserimento della password: nr. di caratteri minimo, lettere e cifre, almeno un carattere speciale, almeno una lettera maiuscola, elenco delle password vietate.

3.2 Disconnessione automatica

Quando la sessione di un utente è inattiva per un determinato periodo di tempo, viene chiusa automaticamente. Questo permette di ridurre il rischio che la sessione venga utilizzata da un'altra persona in modo indesiderato.

Il tempo di sessione (30 minuti per impostazione predefinita) può essere personalizzato per ogni utente,

3.3 Giornale delle sessioni

Le sessioni degli utenti (connessioni, sconnessioni e azioni) sono registrate con timestamp in un registro chiamato: giornale delle sessioni.

Il giornale delle sessioni può essere attivato/disattivato per ogni utente.

```
20190206104537  Connessione     Mauro              :System.User.U00002
20190206104552  Creare          Variabile analogica     :easy.RESS.R00024
20190206104604  Interruzione
```

Fig.2 – Esempio semplificato di un giornale di sessione

Piano di evoluzione

- Il giornale delle sessioni è destinano a trasformarsi in un giornale con formato Syslog.
- Questo registro permetterà di tener traccia dei tentativi di accesso errati: nome utente e / o password non validi e l'indirizzo IP di tutte le connessioni.

3.4 Firewall

Le Unità Locali Intelligenti (ULI) WIT sono dotate di un firewall nativo. Il firewall blocca tutte le connessioni sulle porte IP non autorizzate.

Piano di evoluzione

- Gestione di un elenco di indirizzi IP autorizzati che blocca qualsiasi connessione ad indirizzi IP diversi da quelli presenti in questo elenco.
- Gestione di un elenco di indirizzi IP non autorizzati (blacklist) blocca qualsiasi tentativo di connessione proveniente dagli indirizzi IP presenti in questo elenco.

3.5 Accesso fisico

La protezione dall'accesso fisico alle Unità Locali Intelligenti (ULI) deve essere presa in conto nell'ottica della sicurezza generale dell'installazione.

La protezione può essere messa in atto attraverso metodi tradizionali (porte dotate di serratura) o attraverso metodi più moderni: controllo accessi con identificazione delle persone (lettore di badge + serrature elettriche o senza fili). Questa seconda soluzione offre anche il vantaggio di poter monitorare l'accesso ai locali tecnici.

Il rilevamento delle intrusioni nei locali tecnici è un modo efficace per migliorare la sicurezza dell'accesso fisico poiché permette un allerta immediata per ogni accesso non autorizzato. Per questo l'ULI WIT dispone di ingressi che possono ospitare sensori a loop bilanciato che permettono, oltre al rilevamento delle intrusioni, il rilevamento di manomissioni come la messa in corto-circuito del sensore (loop chiuso), la sezione del cavo (loop aperto) e l'apertura o il deterioramento del sensore (loop sbilanciato).

4. SICUREZZA DEI DATI

4.1 Crittografia

La crittografia è il componente basilare della sicurezza dei dati e il modo più semplice e più importante per garantire che le informazioni presenti nell'Unità Locale Intelligente (ULI) non vengano sottratti da qualcuno che desideri utilizzarli per scopi fraudolenti o al di fuori delle leggi.

La crittografia è la conversione dei dati da un formato leggibile a un formato codificato che può essere letto o elaborato solo dopo la loro decodifica.

I principio della crittografia si basa sulla nozioni di algoritmo di codifica e di «chiave». Quando l'informazione viene inviata, viene crittografata utilizzando un algoritmo e può essere decodificata solo utilizzando la chiave appropriata.

Le ULI dispongono di funzioni di crittografia per le tre principali comunicazioni:

- HTTPS — Hyper Text Transfert Protocole Secure
  Protocollo usato per l'accesso al server web della ULI e alle sue API oltre che nelle comunicazioni inter-ULI (eShare) e per l'accesso alle applicazioni RIA.
- FTPS — File Transfert Protocole Secure
  Protocollo utilizzato per il trasferimento di file da e verso le ULI.
- SMTPS — Simple Mail Transfert Protocole Secure
  Protocollo utilizzato per l'invio di e-mail.

La versione del TLS (Transport Layer Security) utilizzata è la 1.2.

Il certificato utilizzato per la comunicazione può essere generato dalla ULI (auto-certificazione) o da un certificatore terzo.

Per maggiori informazioni, è possibile consultare il «Manuele di comunicazione sicura».
http://www.wit-italia.com/download/18867/

HTTPS

HTTPS permette di rendere sicura la connessione e gli scambi HTTP grazie ad un certificato di autenticazione emesso da un'autorità terza, considerata affidabile. Garantisce la confidenzialità e l'integrità dei dati inviati dall'utente (in particolare le informazioni inserite nei formulari) e ricevuti dal server (ULI).

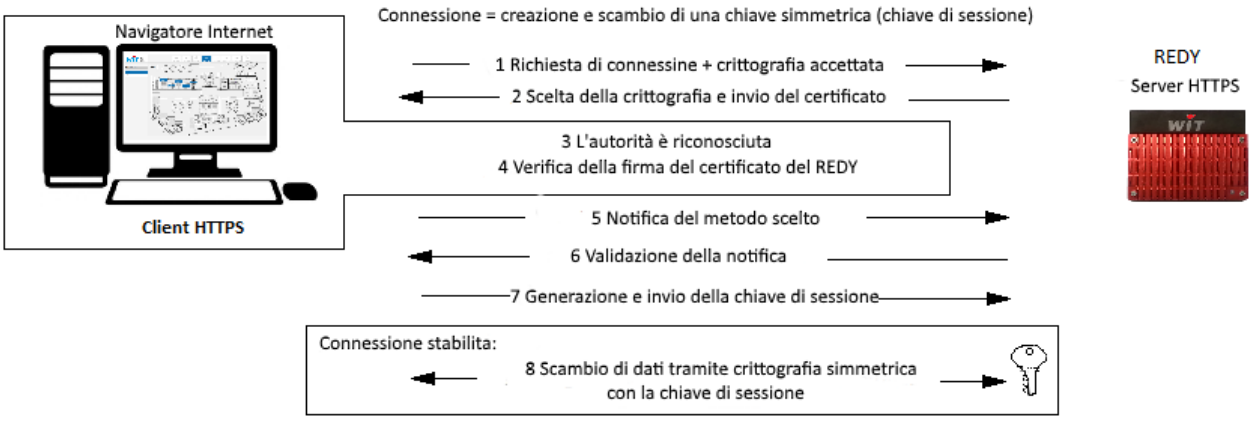

Fig.3 – Principio del HTTPS

FTPS

Il File Transfer Protocol Secure, abbreviato in FTPS, è un protocollo di comunicazione destinato allo scambio di file sulla rete TCP/IP, variante del FTP, reso sicuro dal protocollo SSL o TLS. Consente al visitatore di verificare l'identità del server a cui accede tramite un certificato di autenticazione. Permette anche di crittografare la comunicazione.

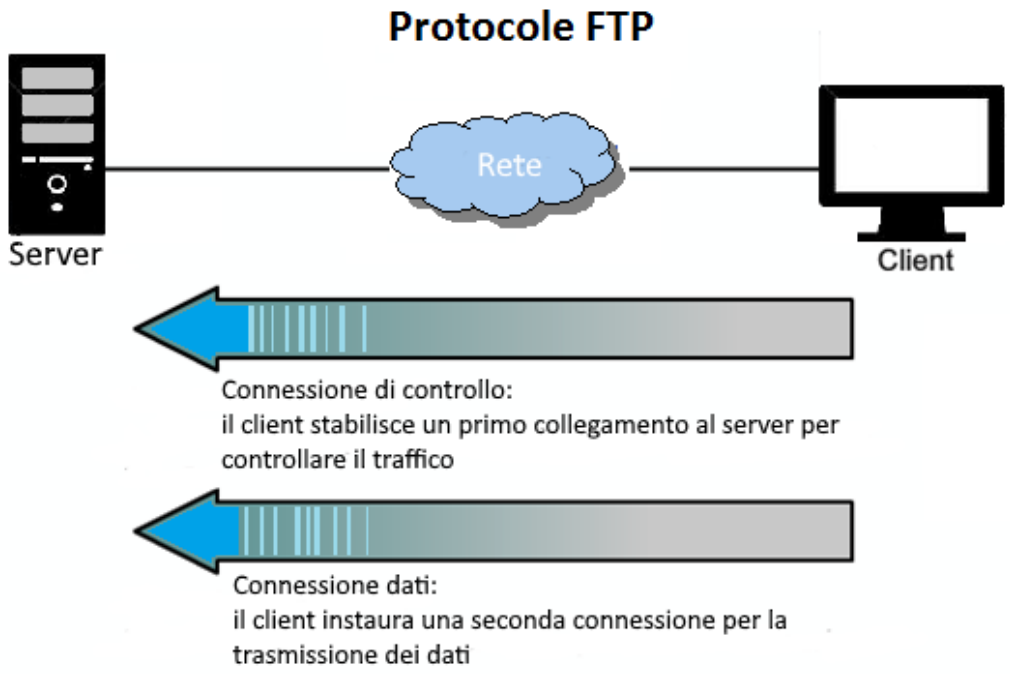

Fig.4 – Principio del FTPS

Esistono due metodi per invocare la crittografia SSL/TLS in FTP: «esplicito» o «implicito». Le Unità Locali Intelligenti (ULI) WIT utilizzano il modo «**implicito**».

Implicito: lo scambio è criptato da quando la connessione client / server è stabilita.
Esplicito: la connessione viene effettuata in chiaro e lo scambio dati è criptato dopo l'autenticazione.

SMTPS

Il Simple Mail Transfer Protocol Secure (SMTPS) è un metodo che permette di rendere sicuro il protocollo SMTP (invio d'e-mail) attraverso la sicurezza fornita dal layer di trasporto. E' destinato ad assicurare l'autentificazione dei partner di comunicazione oltre che la confidenzialità e l'integrità dei dati.

Esistono due modi per invocare la codifica SSL/TLS in SMTP: «esplicito» o «implicito». Le Unità Locali Intelligenti (ULI) WIT utilizzano il modo «**implicito**».

Implicito: lo scambio è criptato da quando la connessione client / server è stabilita.
Esplicito: la connessione viene effettuata in chiaro e lo scambio dati è criptato dopo l'autenticazione.

4.2 Livello utilizzatorore

Ogni utente è associato a un "livello utente" che consente o meno determinate funzionalità. Le ULI WIT permettono **quattro livelli**:

- Livello 1 - Invitato — sola lettura.
- Livello 2 - Utilizzatore — lettura e comando dei parametri di funzionamento. (consegne, planning, ecc.)
- Livello 3 - Installatore — modifica della parametrizzazione, delle schermate grafiche.
- Livello 4 - Amministratore — accesso all'intero sistema.

Ogni livello riprende le autorizzazioni del livello precedente.

4.3 Profili utilizzaztore

L'accesso ad ogni dato (misura, consegna, processo, …) può essere personalizzato in consultazione e/o modifica per ogni utente attraverso dei profili (gruppi) d'utilizzatore.

I profili assicurano sia la sicurezza dei dati che la semplificazione della loro consultazione.

Il numero di profili può arrivare a 1000 per Unità Locale Intelligente.

4.4 Salvataggio dei dati

I dati vengono salvati in una memoria permanente. Questa memoria mantiene tutti i dati in caso di interruzione di corrente e riavvio del sistema.

I dati possono essere esportati in diversi formati in modo che possano essere salvati su supporti esterni, elaborati da software / servizi di terze parti e / o reimportati secondo necessità.

5. SICUREZZA FUNZIONALE

La sicurezza funzionale è la capacità di un sistema di continuare a funzionare e di allertare in caso di malfunzionamento minore e di ripristinarne automaticamente il funzionamento in caso di un severo malfunzionamento.

5.1 Controllo dell'integrità dei file

Prima di essere importati nella ULI, i file sono sottoposti ad una verifica di integrità per verificare che non siano causa di un'alterazione del suo funzionamento.

I file principali interessati da questo controllo di integrità sono:

- Il firmware: Sistema Operativo, firmware UC, firmware PLUG.
- Parametrizzazione: totale o parziale (WKx).

Inoltre un controllo di compatibilità viene realizzato tra l'OS e il firmware in caso di aggiornamento.

5.2 Autodiagnostica

Le Unità Locali Intelligenti WIT eseguono un monitoraggio continuo del loro stato operativo e delle loro periferiche:

- Presenza tensione
- Tensione batteria
- Tensione UC
- Memoria restante (%)
- Tempo di ciclo minimo, massimo e medio (ms.)
- Stato del bus di comunicazione
- Statistiche sui frame emessi e ricevuti
- Data e ora dell'ultima inizializzazione della CPU

Quando lo stato di un parametro monitorato viene diagnosticato come anomalo, l'ULI è in grado di trasmettere un avviso e, se necessario, passare in uno stato di fallback.

5.3 Watchdog

Un watchdog è una funzione che garantisce il ripristino dell'Unità Locale Intelligente WIT quando supera un tempo di risposta del sistema insolitamente lungo. Questa situazione si può presentare quando l'esecuzione di uno Script crea un loop permanente.

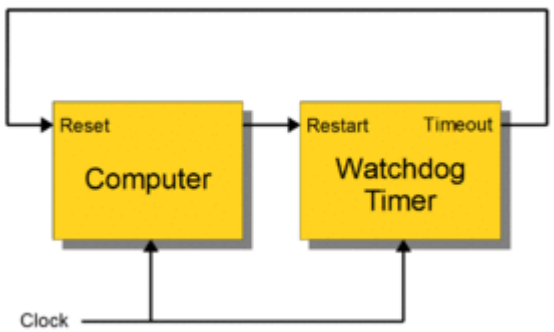

Fig.5 – Principio di funzionamento di un Watchdog

5.4 Stato di fallback

Quando la comunicazione tra l'Unità Centrale e gli ingressi/uscite dell'ULI viene interrotta (bus sezionato, perdita di potenza o riavvio dell'UC), è possibile configurare uno stato di fallback per ciascuna uscita (Digitale e Analogica).

Questa funzione viene utilizzata per definire lo stato operativo degradato (stato di fallback) dell'apparecchiatura in queste situazioni. Esempio: illuminazione, apertura o chiusura accessi, ecc.

5.5 Alimentazione di soccorso

L'alimentatore di backup consente di mantenere temporaneamente in funzione l'ULI in caso di interruzione dell'alimentazione principale. Le ULI WIT dispongono di un proprio sistema per ricaricare e monitorare lo stato della loro alimentazione di emergenza (batteria); ciò contribuisce all'ottimizzazione del budget dell'installazione, riduce al minimo le dimensioni dei quadri elettrici e migliora la manutenzione preventiva e correttiva.

5.6 Diffusione di allarmi

In caso di malfunzionamento, è essenziale essere avvisati in tempo reale per agire in modo reattivo. Le Unità Locali Intelligenti WIT possono allertare utilizzando diversi mezzi di comunicazione:

- SMS
- e-mail
- SIA su IP (monitoraggio remoto)
- Flussi RSS [1]
- PC di supervisione, locale o remoto
- EMI-UCP
- ESPA 4.4.4
- Messaggi vocali[2]
- Stampante (tipo EPSON LX 300+)

[1] via Script. [2] Tramite tele-trasmettitore.

La diffusione di avvisi può essere personalizzata in base ad una pianificazione propria a ciascun utente.