Ripartitori di costi per riscaldamento ad onde radio: sistemi proprietari e sistemi "OMS"

Cerchiamo di fare chiarezza!

Alcune aziende in materia di contabilizzazione del calore stanno offrendo cosiddetti sistemi ad onde radio "OMS", **proponendolo come sistema che permette di scegliere liberamente l'azienda di servizi che effettua le letture**. Esiste una grande confusione in merito a che cosa realmente è un sistema di comunicazione radio "OMS", in gergo spesso impropriamente chiamato anche "aperto". Cerchiamo di fare chiarezza.

Le specifiche "OMS" sono pubblicate dal OMS-Group e devono garantire l'intercomunicabilità tra diversi dispositivi anche di produttori diversi.

Riassumendo, in Italia, un dispositivo marchiato "certificato OMS" **deve**:

- **Comunicare a una frequenza radio definita (868,95 MHz)**
- **Garantire la protezione dei dati con crittografia AES-128**

Chi non è in possesso di questa chiave AES-128 programmata nel ripartitore, **non può leggere via radio in chiaro i dati, cioè i consumi rilevati dal ripartitore**.

Conseguentemente, se l'offerta commerciale propone "letture in chiaro OMS", chi installa i dispositivi deve fornire:

La lista completa dei numeri di serie dei dispositivi installati (es. contatori per acqua e ripartitori) con le relative chiavi AES-128! Inoltre, deve fornire eventuali password impostate per l'accesso al dispositivo per permettere un'eventuale manutenzione.

Consigliamo di diffidare di qualsiasi offerta per sistemi "OMS" dove il fornitore non s'impegna rigorosamente a questa condizione senza la quale il sistema non è "aperto", dove con *aperto* si intende che il cliente è libero di scegliere l'azienda di servizi per le letture. L'installazione del sistema non può essere considerato completato!

Anche se siamo convintissimi che altri sistemi ad onde radio, come il nostro bidirezionale TMS 566, diano INNUMEREVOLI vantaggi sia tecnici che commerciali al cliente, noi ci impegniamo fin da ora, qualora il cliente volesse scegliere di passare al sistema OMS-TMS 868, a garantire l'immediata ottemperanza alla condizione sopra descritta. Anzi! Offriamo addirittura una chiave AES-128 personalizzata per ogni condominio. Solo questo garantisce una sicura protezione in riferimento alle leggi sulla privacy!

Approfondimenti

Ripartitori di costi per riscaldamento ad onde radio: sistemi proprietari e sistemi *aperti* (*"*OMS")

Cerchiamo di fare chiarezza!

Prima di tutto una definizione:

Cosa è l'OMS (Open Metering System) Standard? Con la specifica Open Metering System il Gruppo OMS ha sviluppato uno standard, impropriamente chiamato *aperto,* per l'interfaccia di comunicazione; è quindi indipendente dal produttore, con alcuni requisiti di base. Applicando questo standard, si garantisce l'interoperatività della comunicazione dati per calore, acqua, elettricità e gas. In pratica l'OMS permette di integrare in un unico sistema le letture tutti questi contatori e richiede che venga assicurata un'alta protezione dei dati mediante crittografia.

Ma questo cosa significa per quanto riguarda il rilevamento e la trasmissione dei dati di consumo in ambito condominiale?

I dispositivi, come contatori per calore e acqua e ripartitori, venduti e installati con il sigillo "OMS", devono garantire di trasmettere i dati con frequenza di 868 MHz seguendo il protocollo previsto; devono inoltre garantire che la trasmissione dei dati sia sicura, sia per la correttezza dei dati trasmessi (Data security) che per la protezione del contenuto degli stessi (Data Privacy). Ricordiamo che i dati di consumo riconducibili ad una persona sono "dati personali" nel senso del GDPR.
Solitamente la protezione dei dati avviene tramite una chiave AES a 128bit [1)]. La specifica "OMS" prevede ESPLICITAMENTE che, se un sistema è dichiarato conforme all'OMS standard, questa chiave deve essere prevista dal sistema, poiché altrimenti chiunque può avere accesso ai singoli dati di consumo, e DEVE essere comunicata al cliente/utilizzatore.

Nel mio condominio hanno offerto l'installazione di un sistema "OMS". Cosa significa quindi?

Significa che, avendo a disposizione *le chiavi di cifratura AES, che devono essermi state* consegnate in seguito all'installazione del sistema, potrei acquistare una qualsiasi centralina/router/ripetitore purché funzionante a 868 MHz "OMS" e leggere i dati di consumo dei dispositivi installati.

Questo, in teoria, fornisce l'apparente vantaggio che alla scadenza del contratto di servizio con l'azienda incaricata per le letture, posso facilmente decidere di incaricare un'altra, lasciando i dispositivi installati così come sono.

Perché "apparente"?

Perché ci sono sistemi OMS, ad es. con ripartitori, dove ogni singolo dispositivo ha la sua chiave AES "personale". In questo caso devo programmare nella centralina tutte le chiavi di tutti i dispositivi è una banalità. Ci sono anche sistemi che lavorano con un'unica chiave AES. In questo caso però c'è il rischio che programmando con la chiave AES comunicatami la centralina per la lettura, questa legga anche i dati di eventuali condomini vicini. È ovvio che questo crea grossi problemi in merito alla sicurezza dei dati.

E i sistemi con comunicazione dei dati "proprietari"?

La comunicazione in questi sistemi funziona con protocolli, frequenza e crittografie decise dal produttore del dispositivo. Non essendo "OMS", le chiavi non devono essere comunicate al cliente/utilizzatore. Senza queste chiavi, è impossibile leggere i dati comunicati via onde radio.

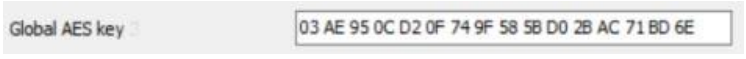
Ma allora, per il cliente finale, è sicuramente consigliabile acquistare un sistema "OMS"?

No! A parte il grosso problema della sicurezza dei dati in alcuni sistemi, come sopra menzionato, ci possono essere tanti grossi vantaggi nel decidere di acquistare un sistema di comunicazione "proprietario". Cerchiamo di spiegarlo facendo riferimento a 2 modelli di ripartitori dello stesso produttore, uno "OMS" e l'altro "proprietario".

A. **Ripartitore per costi di riscaldamento tipo TMS 868 OMS [2]:**
   Questo ripartitore funziona in modo unidirezionale, cioè manda i dati via radio in automatico ogni 5 minuti. Unidirezionale significa che il ripartitore non può essere contattato dall'esterno. Con la chiave AES, che deve essere comunicata al cliente, questi ripartitori possono essere letti con qualsiasi centralina certificata "OMS" a 868 MHZ o con opportuna antenna nel caso di letture "walk-by".

B. **Ripartitore per costi di riscaldamento tipo TMS 566 [2]:**
   Funziona in modo **bi**direzionale con frequenza 433MHz, con protocolli proprietari. Bidirezionale significa che in questo caso significa si può comunicare con il dispositivo dall'esterno, non accedendo all'appartamento. Inoltre i ripartitori trasmettono i dati solo con frequenza programmata (es. una volta al mese). Nel resto del tempo rimangono quiescenti. È quindi possibile riprogrammare tutti i parametri (ad es. cambiare le date di memorizzazione; aggiornare i valori "K", se necessario; ecc.). Questa possibilità costituisce un grandissimo vantaggio tecnico ed economico nel caso di manutenzioni necessarie. Vantaggio che, per quanto sappiamo, nessun altro ripartitore offre.
   Inoltre non ci sono problemi nel caso in cui il condominio decida, alla scadenza del contratto, di cambiare l'azienda di servizi che effettua le letture e le ripartizioni. La Oilcontrol offre di togliere le chiavi AES proprietarie oppure addirittura di sostituirle con una chiave personale, scelta dal cliente/condominio, risolvendo così elegantemente la questione relativa alla protezione dei dati. Questo cambio di chiavi si può fare dall'esterno, senza dovere accedere direttamente ai dispositivi facilitando notevolmente l'operazione.
   L'unica differenza rispetto al sistema "OMS" è che in questo caso è necessario acquistare una centralina TMS a 433 MHz oppure, per le letture walk-by, un'antenna TMS a 466 MHz. Se il sistema installato è già provvisto di centralina, non serve acquistare nulla; se però si vogliono programmare i dispositivi allora occorre il software TMS.

In conclusione, l'offerta di un sistema "OMS", definito impropriamente *aperto,* è spesso esclusivamente una scelta commerciale che nasconde gli indiscutibili vantaggi di altri sistemi. Qualora doveste optare per un sistema "OMS", vi consigliamo vivamente di esigere immediatamente la chiave AES di crittografia e di farvi comunicare in modo ufficiale la frequenza di trasmissione dei consumi via radio.

[1] Esempio di chiave AES : 

[2] I ripartitori TMS 868 e TMS 566 sono prodotti dalla Sontex Svizzera – www.sontex.it