

HSM Supervisor

Gestione e monitoraggio di apparecchiature HSM installate a distanza.

HSM SUPERVISOR è un sistema realizzato da Trittico Srl per la gestione e il monitoraggio remoto di apparecchiature HSM Thales, in grado di eseguire comandi console e inviare messaggi Host, connettendo fino a 128 HSM (Hardware Security Module) locali e remote contemporaneamente.

E' un prodotto realizzato per il funzionamento in ambiente Windows.

La porta console delle HSM viene connessa tramite cavo seriale ad un dispositivo hardware che trasforma la trasmissione da seriale a TCP/IP permettendo la connessione in rete. Tale dispositivo hardware è disponibile in configurazioni da 1 a 128 porte.

Il funzionamento come console permette di eseguire tutti i comandi previsti dalla HSM, è inoltre prevista una funzione per la verifica dello stato (ONLINE, OFFLINE, SECURE) di tutte le HSM connesse con segnalazione in caso di anomalie.

La verifica del corretto funzionamento della HSM può essere ripetuta periodicamente in forma automatica dal sistema, con la periodicità del tempo di verifica impostata dall'utente.

HSM SUPERVISOR permette l'invio di messaggi Host alle HSM connesse in rete, i comandi previsti sono i seguenti:

- Test di connessione alla HSM
- Cancellazione dello stato autorizzativo
- Generazione di chiavi DES
- Generazione e stampa dalla HSM di componenti di chiavi DES
- Formazione di chiavi da più componenti
- Import di chiavi cifrate sotto ZMK
- Export di chiavi da cifrare sotto ZMK
- Traduzione di chiavi da vecchia a nuova LMK
- Rimozione della vecchia LMK dalla memoria della HSM
- Cifratura / Decifratura file
- Generazione di coppie di chiavi RSA
- Export di chiavi cifrate sotto una chiave pubblica RSA
- Import di chiavi cifrate sotto una chiave pubblica RSA
- Calcolo dell'HASH
- Firma
- Verifica della firma
- Richiesta di certificati
- Analisi di certificati
- Derivazione di INITIAL KEY per terminali POS

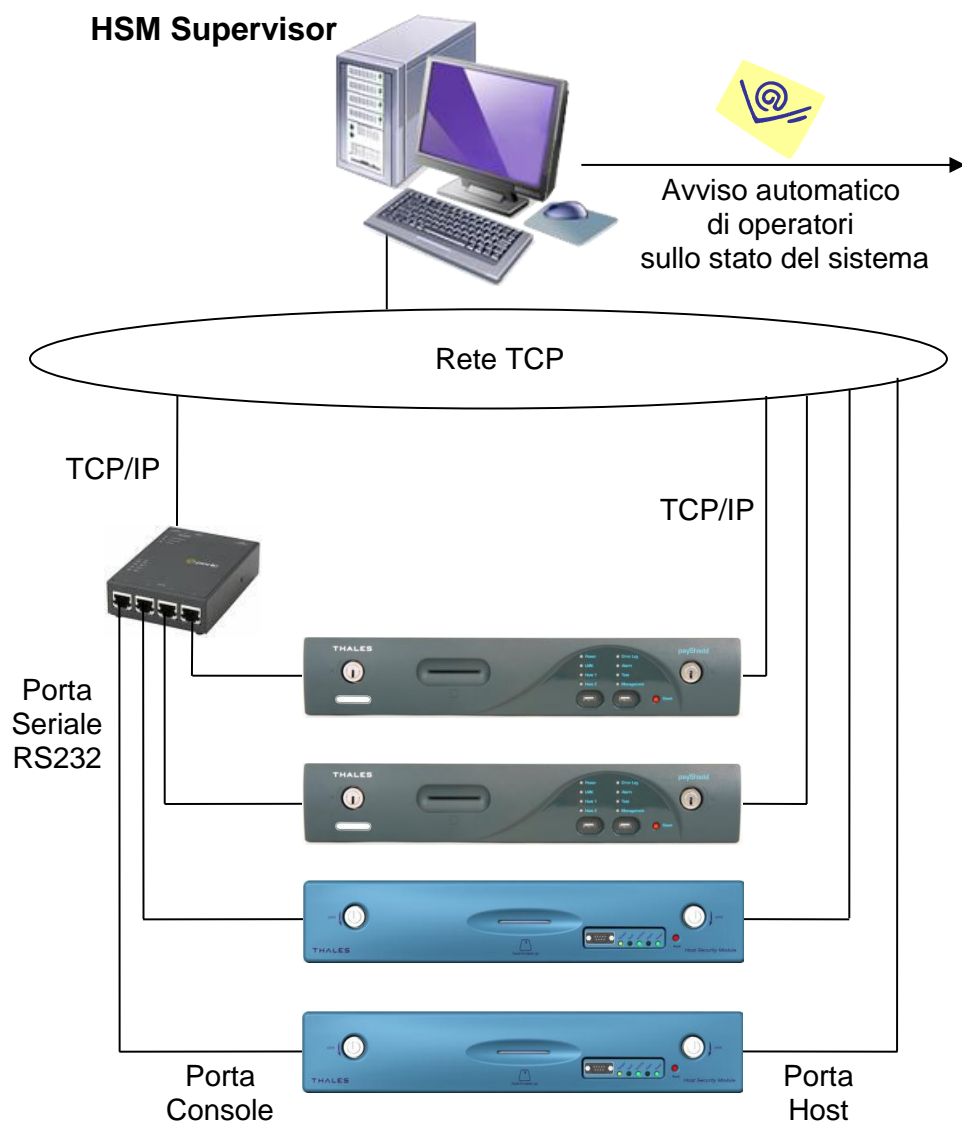
HSM Supervisor viene installato su un PC, che in questo modo funziona da console remota della macchina HSM connessa a distanza. La porta console della HSM si collega con un cavo seriale al dispositivo che permette la trasformazione da seriale a TCP/IP.

L'applicazione funziona inoltre da Host permettendo di eseguire una numerosa serie di comandi come ad esempio generazioni di chiavi DES ed RSA, firma e verifica di documenti, ecc.

Il sistema, abbinato all'utilizzo delle nuove HSM Thales payShield 9000, permette di eseguire un'ulteriore serie di funzioni di monitoraggio remoto:

- verifica del carico di lavoro di ogni singola apparecchiatura;
- procedura di audit sulle macchine, controllando le operazioni e i comandi che sono stati eseguiti su di esse.

Nell'immagine seguente è rappresentato lo schema funzionale del software HSM Supervisor.



Il software HSM Supervisor è personalizzabile, Trittico Srl è disponibile a effettuare modifiche in relazione alle esigenze dei Clienti.