SIGLA Terminal Services Edition[1]

Considerazioni generali

SIGLA controlla l'ambiente operativo nel quale viene eseguito e nel caso in cui rilevi di essere utilizzato in una sessione Windows Terminal Services (nel seguito WTS) utilizza un nuovo meccanismo di attribuzione delle licenze. Per tutti gli altri sistemi operativi Microsoft viene utilizzato l'usuale meccanismo di protezione senza alcuna modifica. Questo documento illustra il principio di funzionamento in questo ambiente operativo (WTS) e costituisce una appendice alla documentazione utente del pacchetto.

Il sistema di gestione delle licenze in ambiente WTS si basa su un unico dispositivo di protezione hardware fornito nella sola versione USB. A partire dal rilascio della versione **3.23/4.6** viene commercializzato un nuovo dispositivo, denominato **Sentinel Hasp**[2] (Figura 1), che sostituisce quello commercializzato in precedenza denominato **Eutronsec SmartKey** (Figura 2).

Il dispositivo di protezione deve essere installato sull'Application Server (server che esegue il servizio Terminal Services) ed è corredato di specifico software (la procedura d'installazione è descritta più avanti in questo documento). SIGLA opererà in versione dimostrativa, con le note limitazioni sulla dimensione massima degli archivi, nel caso in cui sia eseguito in ambiente WTS senza la presenza del nuovo dispositivo hardware. Come configurazione alternativa è possibile non installare il dispositivo sull'Application Server (nel seguito AS) ma installarlo su una qualunque altra macchina della rete locale (workstation o server) purché dotata si sistema operativo Windows Xp o superiore (la procedura d'installazione del software necessario è esattamente la stessa descritta per l'AS).

L'attribuzione della licenza è eseguita fornendo a SIGLA l'elenco dei moduli che possono essere abilitati sulla base dell'identificativo dell'utente utilizzato per connettersi al server (utente del sistema operativo). Questa operazione è eseguita utilizzando un apposito programma descritto più avanti in questo documento.

Soltanto un utente potrà essere autorizzato all'esecuzione della procedura di Configurazione di SIGLA, e in ogni caso ne potrà essere eseguita una sola istanza alla volta.

Ogni istanza dell'applicativo eseguita in una sessione remota distinta impegna una licenza per ogni modulo che richiede. Nel caso in cui il numero delle licenze disponibili per uno dei moduli richiesti sia stato esaurito da altri utenti, il modulo richiesto non sarà abilitato. Naturalmente se il numero complessivo delle istanze di SIGLA in esecuzione supera il numero totale delle licenze acquistate, sarà inibita l'esecuzione dell'applicativo.

Tutte le istanze eseguite nella stessa sessione remota *condividono la stessa licenza*, impegnano, cioè, la licenza per i vari moduli richiesti una sola volta (nella stessa sessione remota l'utente può eseguire più volte SIGLA utilizzando sempre una singola licenza e condividendo pertanto le autorizzazioni per i singoli moduli richiesti). Al fine di avere la certezza che non vengano impegnate ulteriori licenze è necessario attendere che la prima

[1] Data ultimo aggiornamento: 21 novembre 2013.
[2] A partire dalla versione **3.23/4.6** viene commercializzato questo nuovo dispositivo ma per compatibilità con le versioni precedenti è possibile utilizzare anche il precedente dispositivo hardware (Eutronsec SmartKey).

istanza di SIGLA abbia completato la fase di inizializzazione prima di eseguire ulteriori istanze dell'applicazione[3].

Per l'esecuzione di SIGLA in ambiente WTS non deve essere installato alcun driver software o dispositivo hardware nel client (eccetto il "Terminal Services Client"/"Remote Desktop Connection" se il sistema operativo non è WinXp) e neppure SIGLA stesso. Naturalmente nel client può essere comunque installato SIGLA che in questo caso sarà eseguito nella modalità client/server standard ed ovviamente richiederà la presenza del relativo dispositivo hardware di protezione e driver software.

La versione 4 di SIGLA invece può utilizzare anche in questa situazione lo stesso dispositivo Sentinel Hasp lavorando in modalità licenze concorrenti (a tal proposito si veda l'apposita documentazione).

Figura 1 - Sentinel Hasp

Figura 2 - Eutronsec SmartKey

Attribuzione delle licenze

In ambiente operativo WTS è utilizzato il meccanismo delle *licenze concorrenti*, nel senso che è fissato il numero massimo di istanze di SIGLA che possono essere eseguite contemporaneamente dagli utenti collegati in sessioni remote distinte (è opportuno osservare che due istanze di SIGLA eseguite nella stessa sessione remota non impegnano due licenze ma una sola e pertanto condividono le autorizzazioni sui vari moduli richiesti).

Ricordiamo, inoltre, che i moduli richiesti saranno effettivamente disponibili solo se realmente presenti nella licenza. Uno specifico messaggio di avvertimento, mostrato in Figura 3, indicherà all'utente se non sono disponibili licenze per tutti i moduli richiesti; i dettagli sui moduli richiesti ma non attivati possono essere ottenuti attraverso la funzione 'Info Moduli' che mostrerà in rosso, nella sezione dei moduli disponibili, i moduli richiesti ma non disponibili (Figura 4).

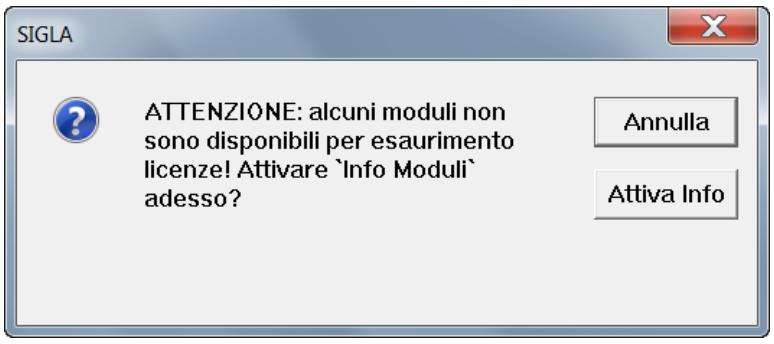

Figura 3

[3] La fase di inizializzazione può considerarsi conclusa nel momento in cui scompare l'immagine con il logo del programma.

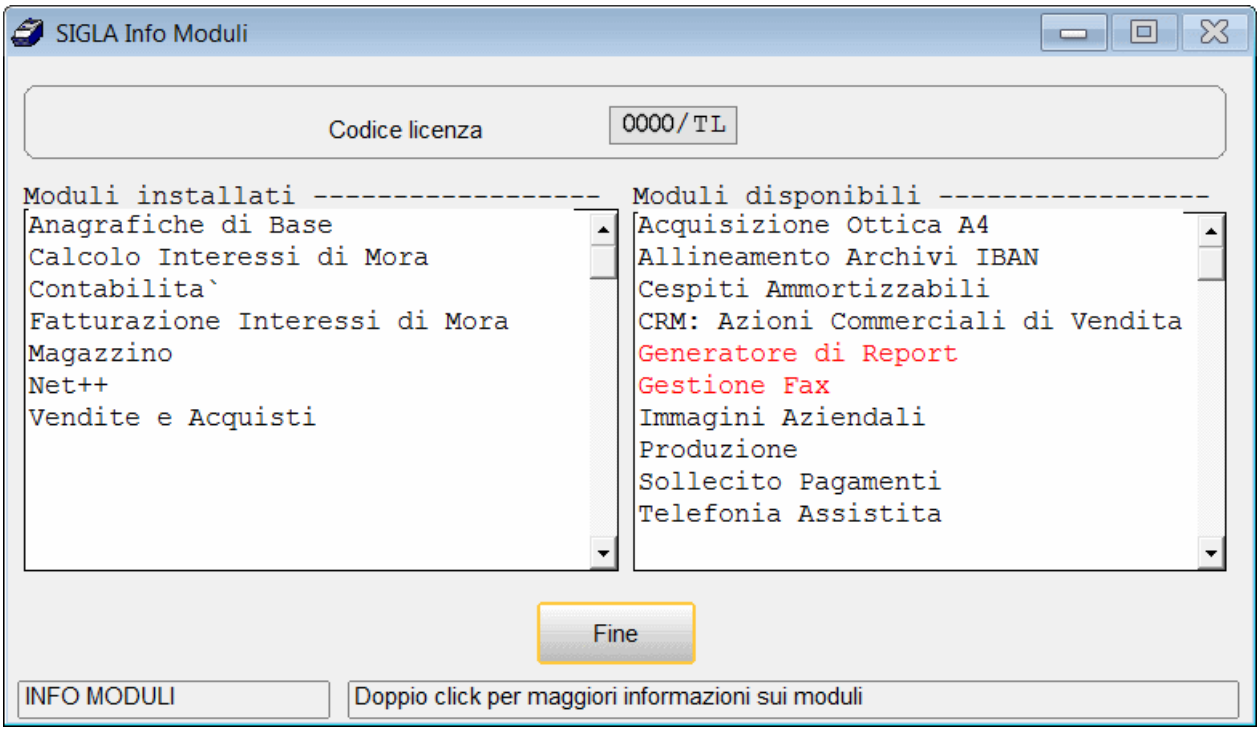

Figura 4

Per chiarezza ricordiamo che un modulo richiesto può non essere attribuito se è stato raggiunto il numero massimo di licenze acquisite oppure se il modulo stesso non fa parte della licenza complessiva.

In ambiente WTS il codice della licenza è costituito dal solo serial number, mentre il progressivo della chiave, significativo in ambiente client/server, viene sostituito dalla stringa fissa "TL" nel caso in cui sia utilizzato il dispositivo Sentinel Hasp o "TS" nel caso in cui sia utilizzato il dispositivo Eutronsec Smartkey.

Al fine di illustrare la nuova filosofia di gestione delle licenze si considerino gli esempi illustrati nel seguito.

Composizione della licenza

Licenza XYZ per un totale di 3 posti di lavoro così composti:

Modulo	***Numero di licenze***
Modulo Base (MBASE) [4]	3
Contabilità (CONT)	1
Magazzino (MAGA)	2
Vend./Acq. (V/A)	1

Esempio 1

Distribuzione dei moduli tra gli utenti:

ID Utente	***MBASE***	***CONT***	***MAGA***	***V/A***
USER01	Si	Si	No	No
USER02	Si	Si	No	No
USER03	Si	Si	No	No

Supponendo, in questo caso, che la sequenza temporale di esecuzione di SIGLA da parte dei tre utenti corrisponda allo stesso ordine con cui sono elencati nella tabella precedente, per gli

[4] Il numero delle licenze del modulo base corrisponde al numero di licenze complessive disponibili dato che questo modulo è l'unico necessario.

utenti USER02 e USER03 SIGLA funzionerebbe come se per le loro postazioni di lavoro fosse stato acquistato solo il modulo base.

In definitiva l'utente che per primo esegue SIGLA potrà utilizzare le funzioni del modulo contabile, mentre gli altri disporranno soltanto delle funzioni presenti nel modulo base.

Esempio 2

Distribuzione dei moduli tra gli utenti:

ID Utente	*MBASE*	*CONT*	*MAGA*	*V/A*
USER01	Si	Si	No	No
USER02	Si	Si	Si	Si
USER03	Si	No	Si	No

Supponendo, in questo caso, che la sequenza temporale di esecuzione di SIGLA da parte dei tre utenti corrisponda allo stesso ordine con cui sono elencati nella tabella precedente, per l'utente USER02 non è disponibile il modulo contabile, sempre che non esegua SIGLA prima dell'utente USER01 (nel qual caso per quest'ultimo sarebbe disponibile solo il modulo base) e solo in questo caso USER02 potrà disporre di tutti i moduli.

Naturalmente ciascun utente può eseguire più istanze dell'applicativo mantenendo lo stesso insieme di moduli già ottenuti alla prima esecuzione del programma e senza impegnare ulteriori licenze.

Esempio 3

Distribuzione dei moduli tra gli utenti:

ID Utente	*MBASE*	*CONT*	*MAGA*	*V/A*
USER01	Si	Si	No	No
USER02	Si	No	Si	Si
USER03	Si	No	Si	No

In questo caso i tre utenti avrebbero sempre disponibili tutti i moduli richiesti indipendentemente dal momento in cui eseguono SIGLA.

Esempio 4

Distribuzione dei moduli tra gli utenti:

ID Utente	*MBASE*	*CONT*	*MAGA*	*V/A*
USER01	Si	Si	No	No
USER02	Si	No	Si	Si
USER03	Si	No	Si	No
USER04	Si	Si	Si	Si

In questo caso solo tre utenti possono eseguire contemporaneamente SIGLA e la sequenza temporale di esecuzione dell'applicativo determina quale utente non può lavorare (il criterio segue il principio del "primo arrivato meglio servito"). Ad esempio, supponendo che il primo ad eseguire SIGLA sia l'utente USER01, in seguito l'utente USER04 e poi USER02, l'utente USER03 non potrà eseguire SIGLA ed inoltre per l'utente USER02 non sarà disponibile il modulo Vendite\Acquisti.

Dispositivo Sentinel Hasp

A partire dalla versione 3.23 di SIGLA e 4.6 di SIGLA Ultimate e Start Edition in ambiente WTS viene utilizzato il nuovo dispositivo di protezione Sentinel Hasp (Figura 1 - Sentinel HaspFigura 1). Si precisa che è comunque possibile utilizzare il precedente dispositivo Eutronsec Smartkey (Figura 2) in modo perfettamente compatibile con le precedenti versioni.

Installazione del software del dispositivo Sentinel Hasp

Per utilizzare il nuovo dispositivo hardware di protezione è necessario installare il software a corredo (driver della periferica e servizio di gestione). Il dispositivo, come già indicato, è fornito nella sola versione USB.

Come già accennato sono possibili due tipologie di installazione, la prima (da preferire) prevede di installare il dispositivo di protezione sull'AS mentre la seconda prevede l'installazione del dispositivo in una delle workstation o su uno degli altri server presenti nella rete locale[5]. Nell'AS **è sempre necessario** installare il software di gestione indipendentemente dalla tipologia di installazione che si intende utilizzare.

La procedura di installazione del software di gestione del dispositivo hardware deve essere eseguita da un utente dotato di diritti amministrativi sulla macchina (deve cioè appartenere al gruppo *Administrators*) ed è illustrata nelle figure che seguono. L'installazione del software si attua eseguendo il pacchetto di setup HASPUserSetup.exe.

Per prima cosa viene visualizzata la schermata di benvenuto nell'applicazione di installazione (Figura 5), e successivamente quella relativa alla licenza del prodotto (Figura 6).

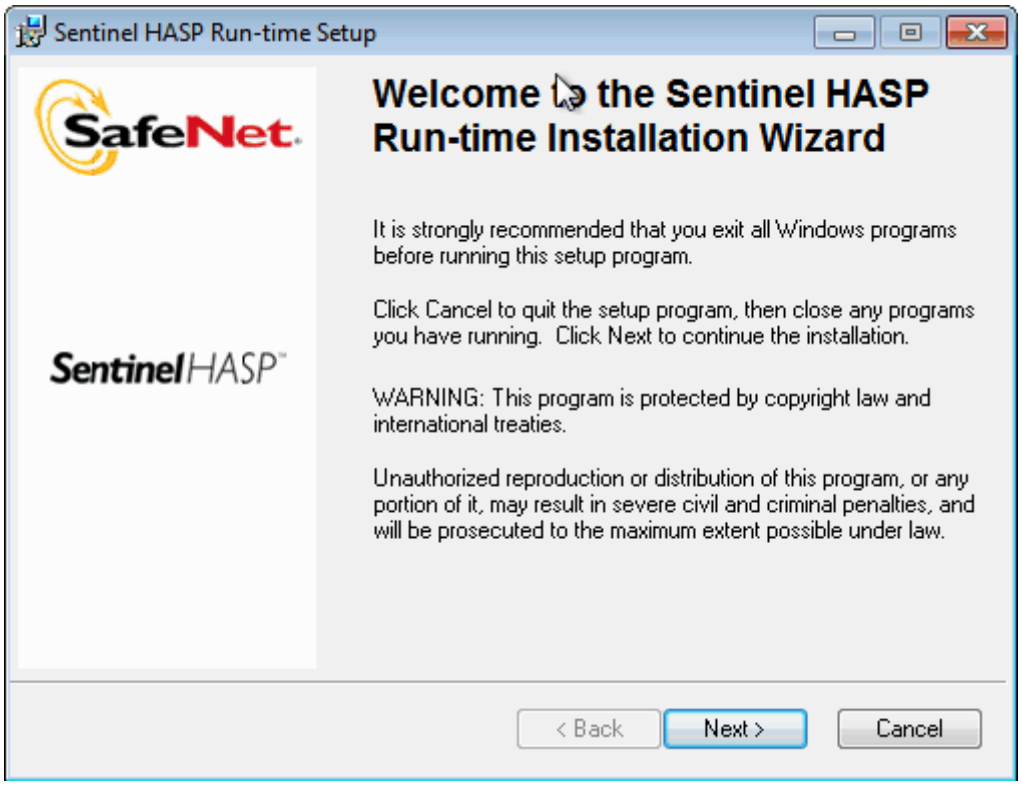

Figura 5

[5] La macchina deve essere dotata di sistema operativo deve essere Windows Xp o superiore e preferibilmente di un indirizzo IP statico.

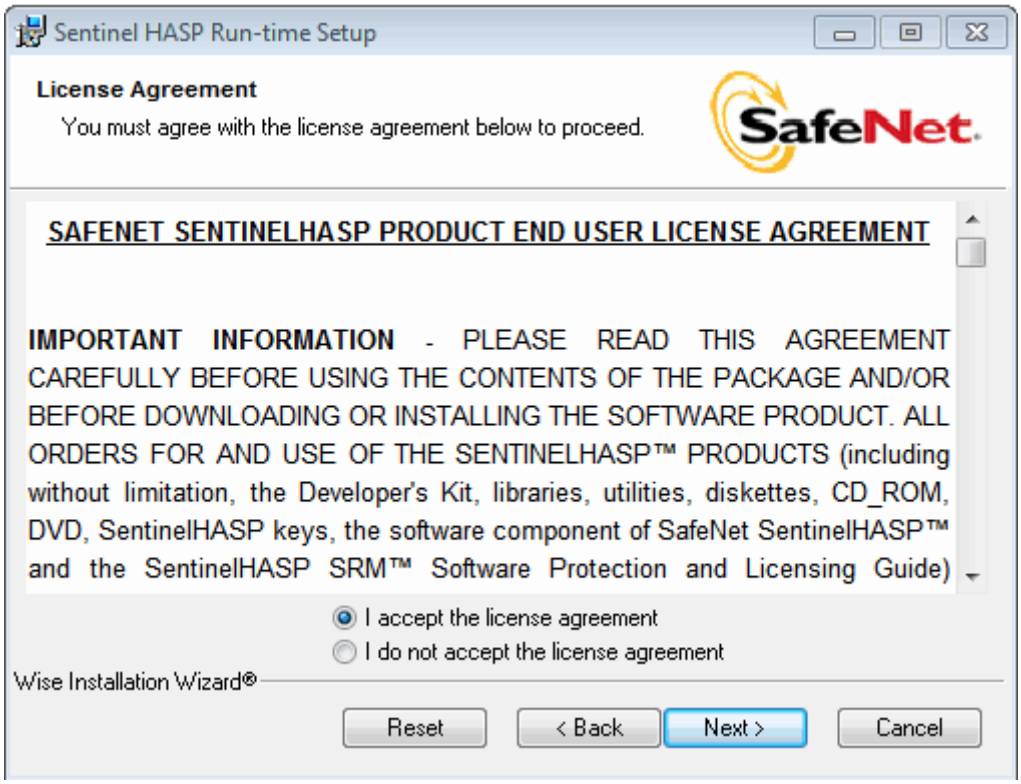

Figura 6

Accettata la licenza del prodotto viene abilitato il bottone *Next*, che consente di passare alla schermata di effettiva conferma dell'installazione stessa (Figura 7) dalla quale l'ulteriore pressione del bottone *Next* produrrà l'installazione del software.

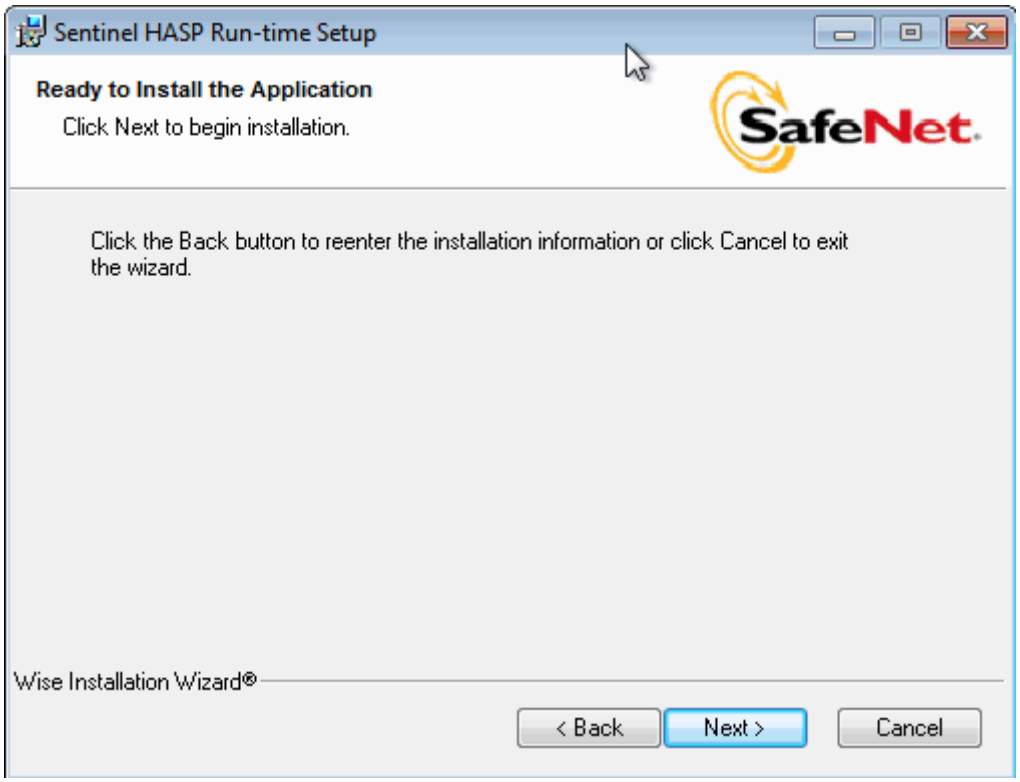

Figura 7

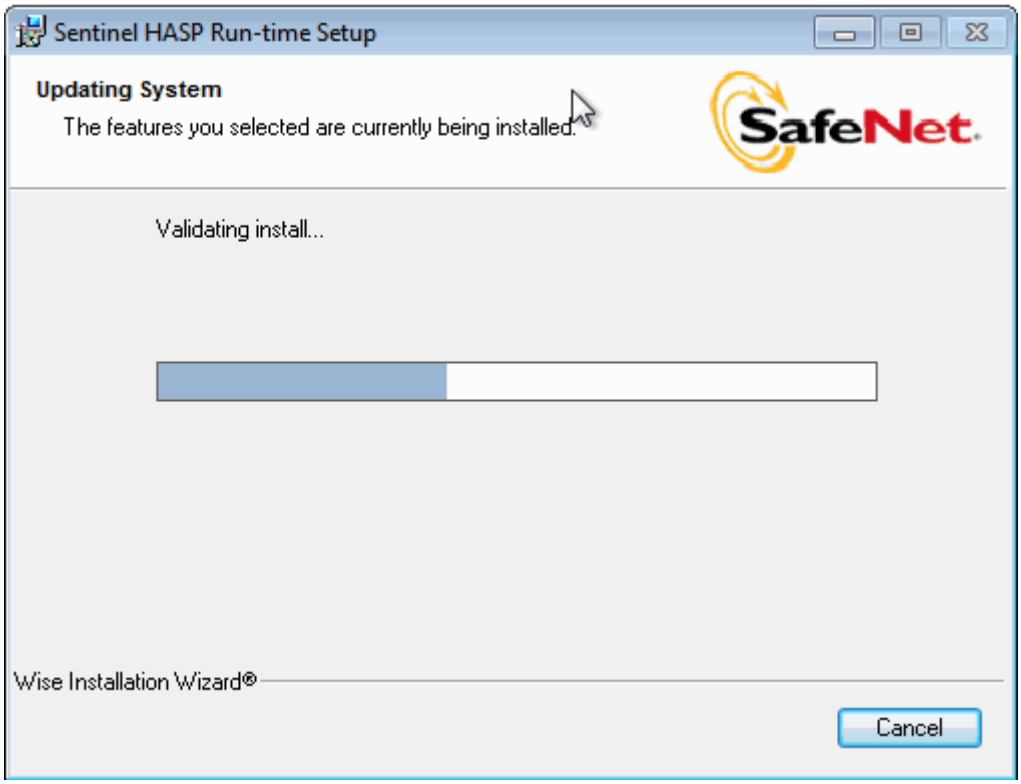

Figura 8

Il software di gestione del dispositivo utilizza la porta 1947 per la comunicazione locale con gli applicativi e per la comunicazione con gli eventuali componenti remoti (come nel caso in cui il dispositivo di protezione **non** sia installato in una porta USB dell'AS), è pertanto necessario accertarsi che eventuali firewall non blocchino il traffico su tale porta (come ricordato anche al termine della procedura di installazione, Figura 9).

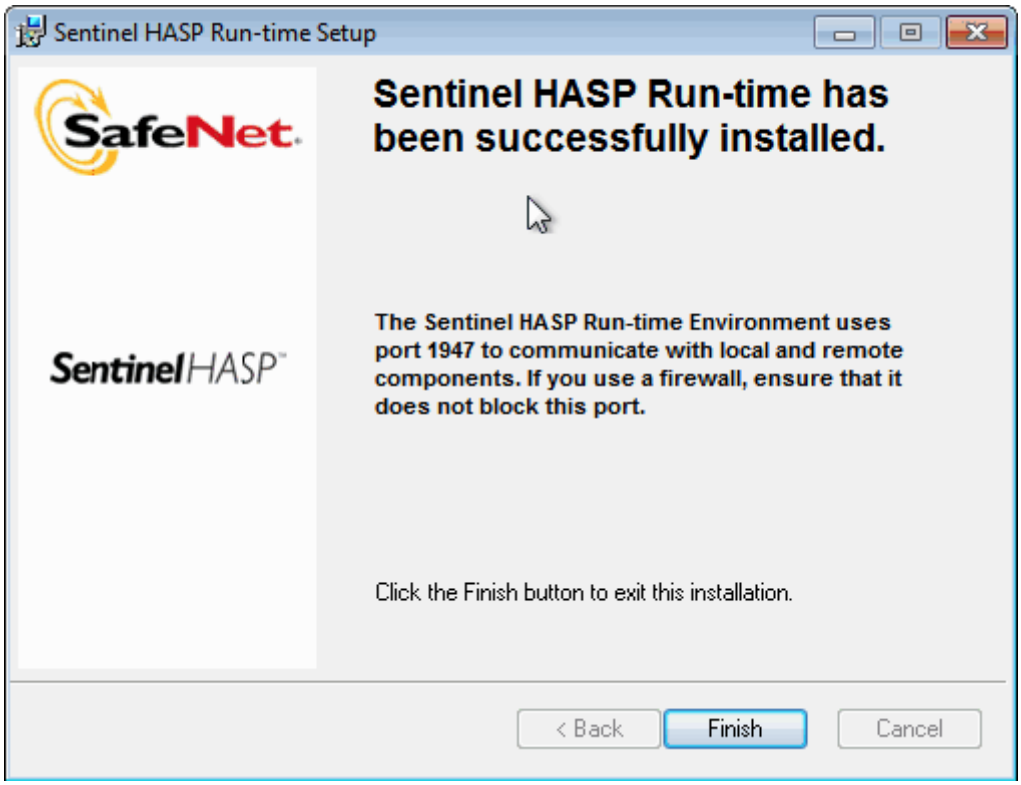

Figura 9

Nel caso di installazione del dispositivo hardware presso un altro PC della rete è necessario eseguire la stessa procedura di installazione del software di gestione anche in tale PC ricordando ci controllare la configurazione dell'eventuale firewall.

Programma di distribuzione delle licenze (per Sentinel Hasp)

La prima operazione da effettuare è quella di eseguire l'apposito programma SIGLATSE.EXE che provvederà a copiare i vari file nella cartella indicata. E' opportuno indicare una cartella non accessibile da parte dei normali utenti al fine di garantire il funzionamento dell'installazione secondo le specifiche imposte.

Prima di eseguire SIGLA in ambiente WTS è necessario associare a ciascun utente del server i moduli che devono essere attivati. Per portare a termine questa operazione è disponibile il programma SPPLic4.exe mostrato in Figura 10[6].

Il programma richiede, per essere eseguito su sistemi operativi con User Account Control (UAC) attivo, dei diritti di amministrazione, pena il fallimento delle operazioni avviate. Pertanto in Windows 2008 Server con UAC attivo, al momento dell'esecuzione del programma SPPLic4.exe il sistema chiede le credenziali dell'amministratore o la conferma, se l'utente è amministratore, per procedere con l'elevazione dei diritti.

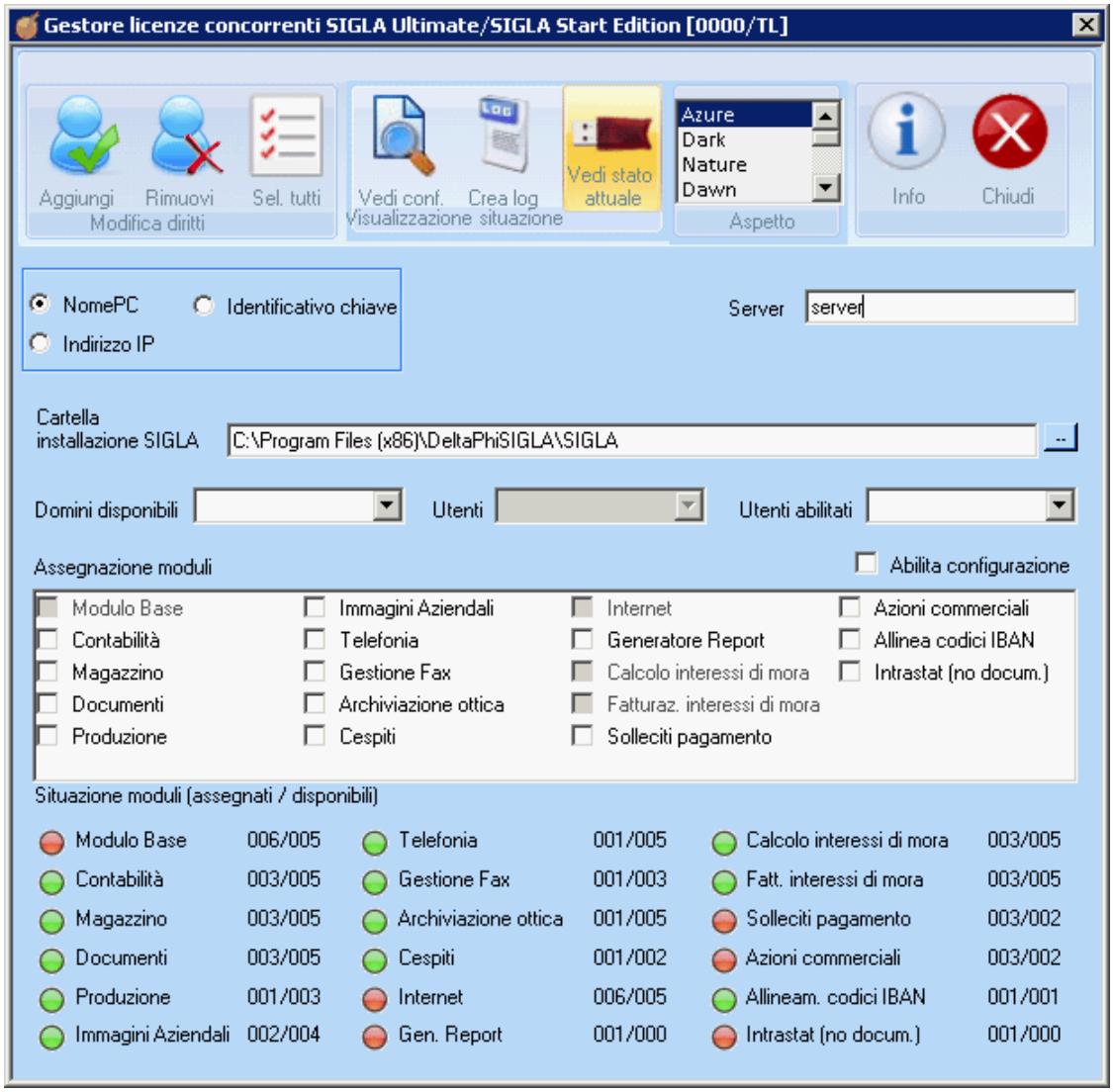

Figura 10

[6] Il programma SPPLic4.exe è stato realizzato utilizzando **Microsoft .Net Framework 2.0** che pertanto deve essere presente nel server, in caso contrario il modo migliore per installarlo è quello di utilizzare il servizio Windows Update di Microsoft.

La prima informazione da indicare è l'indirizzo del server dove è fisicamente installato il dispositivo di protezione. L'indirizzo del server può essere specificato con il nome o con l'indirizzo numerico, in base alla selezione dell'apposito radio button. Come valore di default è utilizzata l'opzione *NomePC* e *localhost* come indirizzo del server. Se il dispositivo di protezione è fisicamente presente in una porta USB dell'AS come indirizzo del server delle licenze è sufficiente utilizzare l'indirizzo di loopback *localhost* o *127.0.0.1*. Al contrario, se il dispositivo è installato presso un altro PC della rete[7] è necessario indicare il nome di tale PC oppure il suo indirizzo IP.

La successiva informazione da fornire è la cartella d'installazione di SIGLA, necessaria per salvare il file con la distribuzione delle licenze; premendo l'apposito bottone è possibile cercare la cartella nell'albero delle cartelle del disco locale.

Dopo aver scelto il dominio (se necessario, altrimenti si opera con gli utenti locali del server), l'utente (tra quelli mostrati nella lista ricavata dal dominio) e selezionato i moduli da attivare è necessario premere il bottone *Aggiungi*. Le stesse operazioni devono essere eseguite per tutti gli utenti abilitati alla connessione.

Il modulo base è automaticamente attribuito a tutti gli utenti in quanto è obbligatorio. E' possibile assegnare i moduli senza alcun vincolo particolare, anche indipendentemente dalla programmazione del dispositivo hardware[8]. Naturalmente i moduli effettivamente abilitati dipenderanno da quelli associati alla licenza acquisita.

L'opzione *Abilita configurazione* può essere selezionata soltanto per un utente e permette l'esecuzione del programma di Configurazione.

Il bottone *Sel. tutti i moduli* permette di selezionare tutti i moduli, il bottone *Vedi conf.* mostra un report in formato PDF con le informazioni di configurazione inserite ed il bottone *Situaz. attuale* interroga il servizio di gestione delle licenze, proponendo la situazione attuale delle licenze disponibili ed impegnate, così come riportato direttamente dal software di gestione del dispositivo.

Le informazioni sono salvate nel file SPPLIC.INI nella cartella d'installazione di SIGLA.

Viene anche mostrata la situazione dei moduli assegnati e disponibili in base alla programmazione del dispositivo di protezione. L'indicatore rosso evidenzia i moduli per i quali tutte le licenze disponibili sono state assegnate ed anche quelli per i quali nessuna licenza è stata acquisita.

Attraverso la combobox *Utenti abilitati* è possibile richiamare i dati relativi ad un utente già inserito ed eventualmente cancellarlo mediante il bottone *Rimuovi*.

Il bottone *Crea Log* crea un file di log in formato PDF con informazioni utili per una eventuale analisi da parte del supporto tecnico di Delta Phi SIGLA srl[9].

Messaggi di errore (Sentinel Hasp)

La tabella seguente descrive i messaggi di errore mostrati all'avvio di SIGLA nel caso in cui ne venga negata l'esecuzione.

E' stato raggiunto il numero massimo di licenze simultaneamente attive. Impossibile procedere!	Indica che non sono disponibili ulteriori licenze per l'esecuzione del programma.
Non si dispone dell'autorizzazione all'esecuzione del programma. Impossibile procedere!	Indica che l'utente utilizzato per la connessione a WTS non è stato inserito tra gli utenti abilitati all'esecuzione del programma. In sostanza l'utente non è presente nel file di attribuzione delle licenze creato dal programma spplic4.exe.

[7] In questo caso **è necessario** prestare attenzione alla configurazione di eventuali firewall in modo da non bloccare la comunicazione, che avviene sulla porta TCP 1947, tra SIGLA e il servizio di gestione delle licenze.
[8] Opportuni messaggi di avvertimento segnalano quando viene superato il numero delle licenze effettivamente disponibili.
[9] Il file di log viene creato nella sottocartella "DeltaPhiSIGLA\SPPLic4" creata nella cartella "Dati applicazioni" di tutti gli utenti.

Impossibile convalidare la licenza! Codice errore …	Errore generico di accesso alla chiave, il codice numerico specifica la natura dell'errore stesso. Due casi comuni possono essere: **50** il server indicato non dispone della chiave (indirizzo del server errato) **40** errore di comunicazione tra il license manager locale e quello remoto (si potrebbe riscontrare solo se il dispositivo è installato su un PC della rete diverso dal server) **31** il modulo richiesto non è disponibile (si può riscontrare se la chiave non è master e si esegue il programma di configurazione)

In presenza di firewall con configurazioni complesse l'errore "Impossibile convalidare la licenza! Codice errore 50" potrebbe essere imputabile al filtro del firewall sul traffico broadcast. In questo caso si può risolvere l'inconveniente senza variare la configurazione del firewall agendo su un parametro di configurazione del software di gestione della chiave.

Operando sull'AS, collegandosi all'indirizzo http://localhost:1947 attraverso il browser web si può accedere al *Centro di controllo* del *License Manager (LM)*. La funzione *Configuration/Configurazione* permette di impostare alcune opzioni di configurazione del LM (Figura 11).

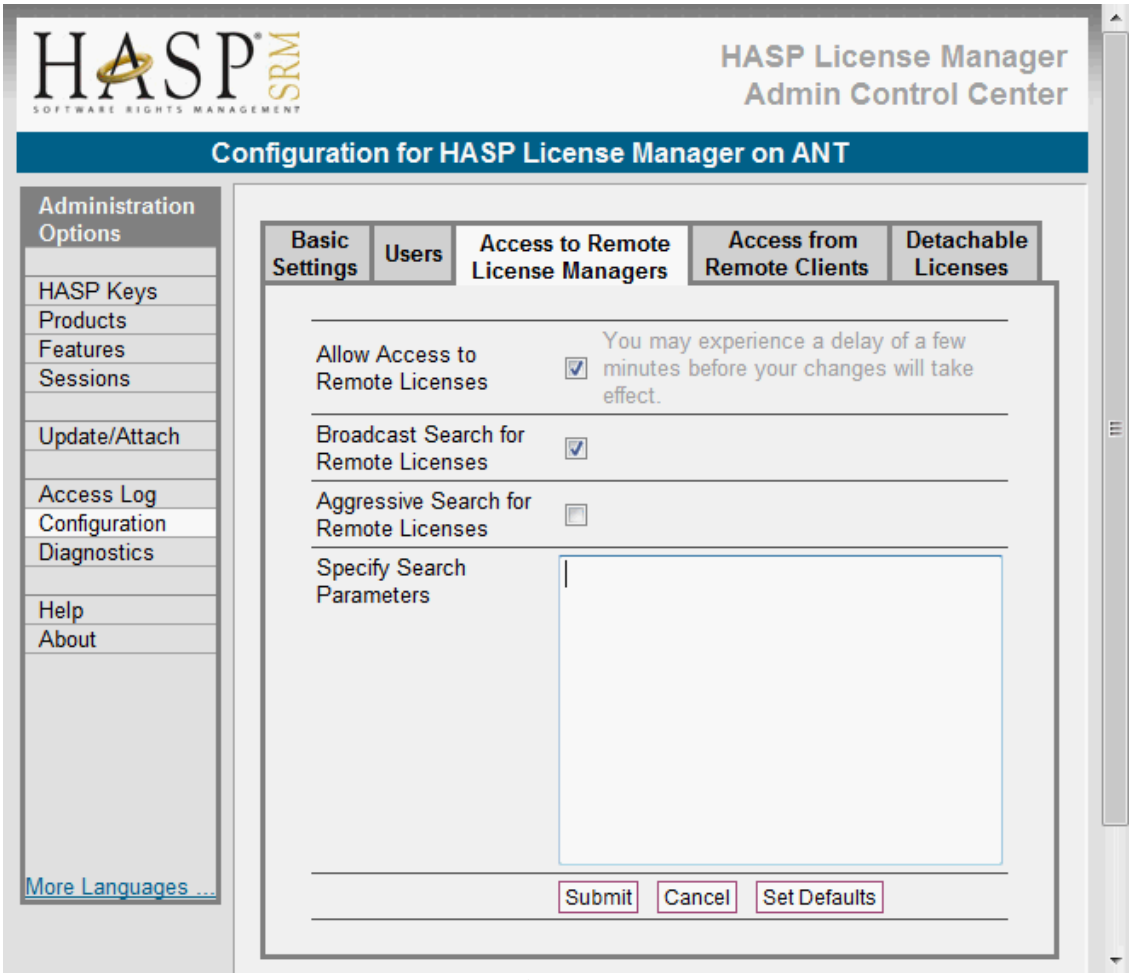

Figura 11

Per evitare i messaggi broadcast di ricerca dei server remoti da parte del LM è necessario accedere alla scheda *Access to Remote License Manager/Accesso ai License Manager remoti* e specificare l'indirizzo IP del PC nel quale è installato il dispositivo di protezione nella sezione

Specify Search Parameters/Specifica i parametri di ricerca e premere il bottone *Submit/Applica*.

ATTENZIONE: l'utilizzo del *Centro di Controllo del License Manager* è consigliato solo a persone **esperte** poiché applicare modifiche alla configurazione del LM in modo superficiale e senza approfondire il significato delle varie opzioni potrebbe compromettere il funzionamento di SIGLA.

Dispositivo Eutronsec SmartKey

Il dispositivo Eutronsec Smartkey **continua ad essere utilizzato anche dalla versione 3.23/4.6 e successive** per compatibilità con le versioni precedenti dell'applicativo. Nel seguito sono descritte la procedura di installazione del driver.

Tutte le componenti software relative al dispositivo Eutronsec SmartKey descritte sono contenute nel pacchetto SPP3WTS.EXE. Consigliamo di copiare le varie procedure in cartelle non accessibili da parte degli utenti collegati in sessioni remote al fine di garantire il funzionamento dell'installazione secondo le specifiche imposte.

Installazione del driver del dispositivo Eutronsec SmartKey

Per utilizzare il nuovo dispositivo hardware di protezione è necessario installare il driver della periferica e il servizio di gestione. Il dispositivo, come già indicato, è fornito nella sola versione USB.

Come già accennato sono possibili due tipologie di installazione, la prima (da preferire) prevede di installare il dispositivo di protezione sull'Application Server (AS) mentre la seconda prevede l'installazione del dispositivo in una delle workstation o degli altri server presenti nella rete locale[10].

Installazione nell'Application Server

La prima operazione da effettuare è quella di eseguire l'apposito programma SPP3WTS.EXE che provvederà a copiare i vari file nella cartella indicata. Consigliamo di copiare le varie procedure in cartelle non accessibili da parte degli utenti collegati in sessioni remote al fine di garantire il funzionamento dell'installazione secondo le specifiche imposte.

L'installazione del driver del dispositivo e del servizio di gestione può essere eseguito in forma automatica attraverso lo script INSTALL.CMD oppure manualmente lanciando i vari programmi in sequenza come indicato più avanti.

Installazione automatica con script (consigliata)

Assicurarsi che il dispositivo di protezione non sia già inserito in una porta USB[11], eseguire lo script INSTALL.CMD (che ovviamente deve essere avviato connettendosi al server con un utente del gruppo Administrators) ed inserire il dispositivo solo quando viene richiesto. Questo script provvede ad installare il driver della periferica, ad installare e configurare il servizio di gestione del sistema di attribuzione delle licenze e configura le opzioni necessarie a SIGLA per comunicare via TCP/IP con il servizio stesso. Per la comunicazione viene utilizzata la porta 15999, che può essere cambiata semplicemente agendo sulle specifiche righe dello script stesso. In base allo script fornito SIGLA cerca il servizio utilizzando l'indirizzo di loopback (127.0.0.1) e quindi non dovrebbe interagire con un eventuale firewall presente sul server[12].

[10] La macchina deve essere dotata di sistema operativo deve essere Windows 2000 o superiore e preferibilmente di un indirizzo IP statico.
[11] In caso contrario la procedura di installazione fallisce e il driver del dispositivo non viene installato.
[12] Non è obbligatorio installare la chiave di protezione sull'application server ma si potrebbe utilizzare anche un'altra macchina della rete aziendale ed in questo caso **è necessario** prestare attenzione alla configurazione di eventuali firewall in modo da non bloccare la comunicazione, sia TCP che UDP, tra SIGLA e il servizio di gestione delle licenze.

Per disinstallare il driver della periferica ed il servizio di gestione viene fornito lo script UNINSTALL.CMD.

In appendice è descritta la procedura di installazione manuale da utilizzare nel caso in cui non si vogliano impiegare gli script forniti o nel caso in cui degli errori impediscano il completamento degli script stessi.

Installazione in una workstation (o in un server) della rete locale

Anche in questo caso la prima operazione da effettuare è quella di eseguire l'apposito programma SPP3WTS.EXE che provvederà a copiare i vari file nella cartella indicata. Come già indicato è necessario utilizzare una macchina dotata di sistema operativo Windows 2000 o superiore e preferibilmente con indirizzo IP statico. Anche se si utilizza un server DHCP per l'attribuzione degli indirizzi è comunque possibile procedere con l'installazione avendo cura di utilizzare il nome della macchina invece che l'indirizzo IP.

L'installazione del driver del dispositivo e del servizio di gestione può essere eseguito in forma automatica attraverso lo script INSTALL.CMD, **esattamente** come descritto nel paragrafo precedente, oppure manualmente lanciando i vari programmi in sequenza come indicato più avanti.

Dopo aver installato il driver del dispositivo e del servizio di gestione delle licenze sulla workstation/server è necessario installare alcune componenti software anche sull'AS. Anche in questo caso l'operazione da effettuare è quella di eseguire l'apposito programma SPP3WTS.EXE che provvederà a copiare i vari file nella cartella indicata. Consigliamo di copiare le varie procedure in cartelle non accessibili da parte degli utenti collegati in sessioni remote al fine di garantire il funzionamento dell'installazione secondo le specifiche imposte.

Per completare l'operazione può essere utilizzato lo script CFGAPSER.CMD che richiede come paramento l'indirizzo IP (nel caso di indirizzo statico) o il nome (nel caso di indirizzo dinamico attribuito dal server DHCP) della workstation/server dove è installato il dispositivo di protezione.

Configurazione automatica con script

Eseguire lo script CFGAPSER.CMD (che ovviamente deve essere avviato connettendosi al server con un utente del gruppo Administrators) che richiede come parametro l'indirizzo o il nome della macchina dove è installato il dispositivo di protezione[13]. Questo script configura le opzioni necessarie a SIGLA per comunicare via TCP/IP con il servizio di attribuzione delle licenze (che è stato precedentemente installato su una workstation/server della rete locale). Per la comunicazione viene utilizzata la porta 15999, che può essere cambiata semplicemente agendo sulle specifiche righe dello script stesso. Attenzione il numero della porta deve coincidere con quello utilizzato dal servizio di gestione delle licenze altrimenti l'installazione non potrà operare correttamente.

Programma di distribuzione delle licenze (per Eutronsec SmartKey)

Prima di eseguire SIGLA in ambiente WTS è necessario associare a ciascun utente del server i moduli che devono essere attivati. Per portare a termine questa operazione è disponibile il programma SPPLIC.EXE mostrato in Figura 12[14]. E' opportuno che anche questo programma sia installato in una cartella non accessibile da parte dei normali utenti in quanto un uso inesperto potrebbe imporre un funzionamento dell'installazione non rispondente alle esigenze del cliente.

[13] Alternativamente è possibile modificare lo script assegnando alla variabile host l'indirizzo IP o il nome della workstation/server dove è installato il dispositivo di protezione.
[14] Se eseguito in ambiente WTS lo sfondo del programma è grigio.

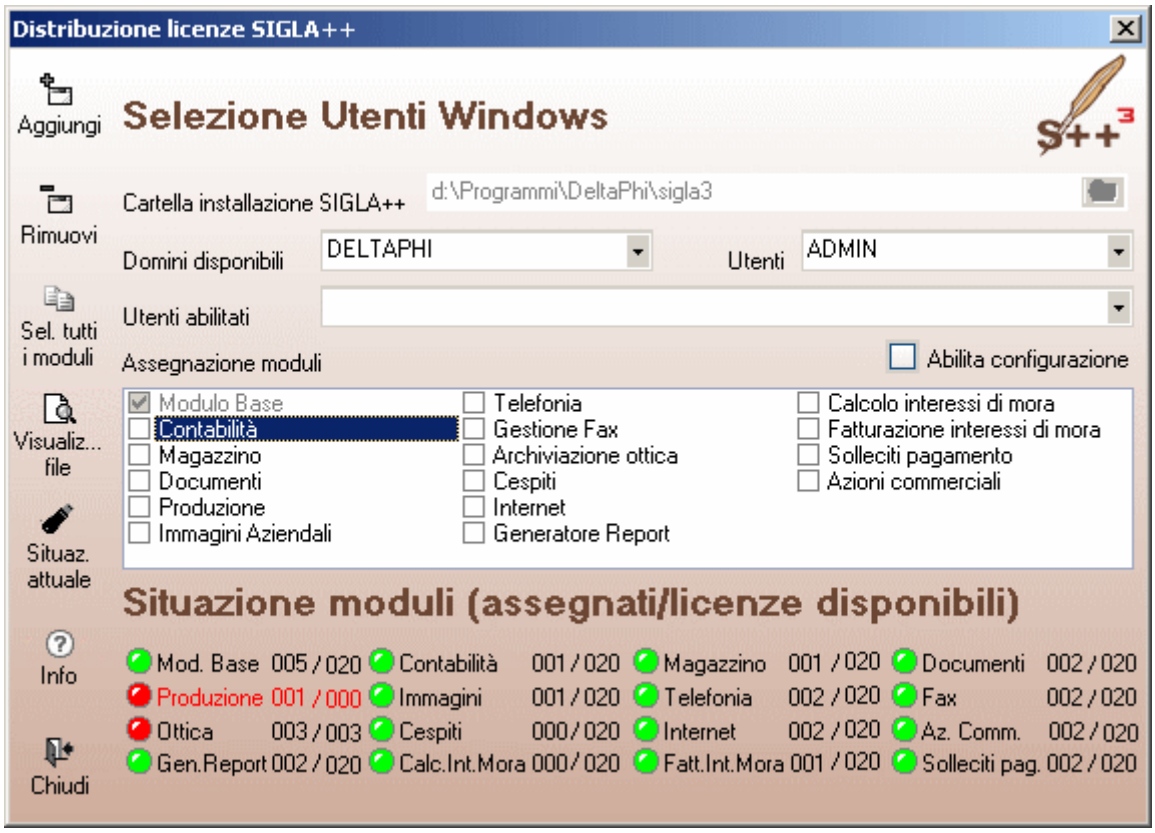

Figura 12

La prima informazione da fornire è la cartella d'installazione di SIGLA, necessaria per salvare il file con la distribuzione delle licenze; premendo l'apposito bottone è possibile cercare la cartella nell'albero delle cartelle del disco locale.

Dopo aver scelto il dominio (se necessario altrimenti si opera con gli utenti locali del server), l'utente (tra quelli mostrati nella lista ricavata dal dominio) e selezionato i moduli da attivare è necessario premere il bottone *Aggiungi*. Le stesse operazioni devono essere eseguite per tutti gli utenti abilitati alla connessione.

Il modulo base è automaticamente attribuito a tutti gli utenti in quanto è obbligatorio. E' possibile assegnare i moduli senza alcun vincolo particolare, anche indipendentemente dalla programmazione del dispositivo hardware[15]. Naturalmente i moduli effettivamente abilitatati dipenderanno da quelli associati alla licenza acquisita.

L'opzione *Abilita configurazione* può essere selezionata soltanto per un utente e permette l'esecuzione del programma di Configurazione.

Il bottone *Sel. tutti i moduli* permette di selezionare tutti i moduli, il bottone *Visualiz. file* mostra le informazioni in forma di report stampabile ed il bottone *Situaz. attuale* interroga il servizio di gestione delle licenze e mostra la situazione attuale delle licenze disponibili ed impegnate[16].

Le informazioni sono salvate nel file SPPLIC.INI nella cartella d'installazione di SIGLA e nella cartella d'installazione del programma di distribuzione delle licenze (SPPLIC.EXE) in modo da disporre di una copia di backup del file stesso.

Viene anche mostrata la situazione dei moduli assegnati e disponibili in base alla programmazione del dispositivo di protezione. L'indicatore rosso evidenzia i moduli per i quali tutte le licenze disponibili sono state assegnate ed anche quelli per i quali nessuna licenza è stata acquisita. Quando vengono assegnate più licenze di quelle disponibili anche la didascalia diventa rossa.

[15] Opportuni messaggi di avvertimento segnalano quando viene superato il numero delle licenze effettivamente disponibili.
[16] L'esecuzione di questa funzione richiede un certo tempo per essere completata.

Attraverso la combobox *Utenti abilitati* è possibile richiamare i dati relativi ad un utente già inserito ed eventualmente cancellarlo mediante il bottone *Rimuovi*.

Messaggi di errore (Eutronsec SmartKey)

La tabella seguente descrive i messaggi di errore mostrati all'avvio di SIGLA nel caso in cui ne venga negata l'esecuzione.

E' stato raggiunto il numero massimo di licenze simultaneamente attive. Impossibile procedere!	Indica che non sono disponibili ulteriori licenze per l'esecuzione del programma.
Non si dispone dell'autorizzazione all'esecuzione del programma. Impossibile procedere!	Indica che l'utente utilizzato per la connessione a WTS non è stato inserito tra gli utenti abilitati all'esecuzione del programma. In sostanza l'utente non è presente nel file di attribuzione delle licenze creato dal programma spplic.exe.
Parametri di configurazione del sistema di gestione delle licenze errati! Codice errore …	Indica che è presente un errore di configurazione, in particolare -1000 indica un errore di accesso al server delle licenze -1300 indica che non è stato trovato il file spplic.ini.
Impossibile convalidare la licenza! Codice errore …	Errore generico di accesso alla chiave, il codice numerico specifica la natura dell'errore stesso. Due casi comuni possono essere: **-5** errore di rete **-23** errore di inizializzazione del protocollo TCPIP

Installazione manuale del driver del dispositivo Eutronsec SmartKey

Questo paragrafo illustra le varie fasi dell'installazione del driver del dispositivo di protezione hardware e delle componenti software necessarie al corretto funzionamento del sistema. Lo script di installazione fornito esegue esattamente gli stessi passi descritti nel seguito. Se è già stata eseguita l'installazione dei vari componenti utilizzando lo script INSTALL.CMD non è ovviamente necessario procedere alla installazione manuale.

L'installazione del driver del dispositivo viene eseguita attraverso il programma SDI.EXE (che ovviamente deve essere avviato connettendosi al server con un utente del gruppo Administrators). La sequenza delle operazioni è mostrata nelle figure seguenti. Per prima cosa è necessario scegliere la pagina *USB*. Per prima cosa è necessario assicurarsi che il dispositivo non sia già inserito in una porta USB.

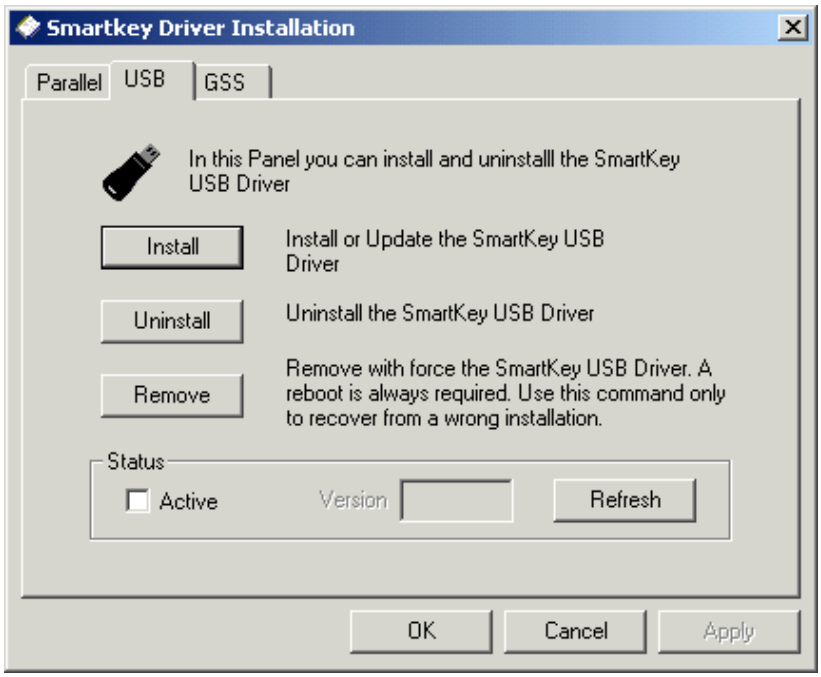

Figura 13

Per proseguire nell'installazione è necessario premere il bottone *Install*.

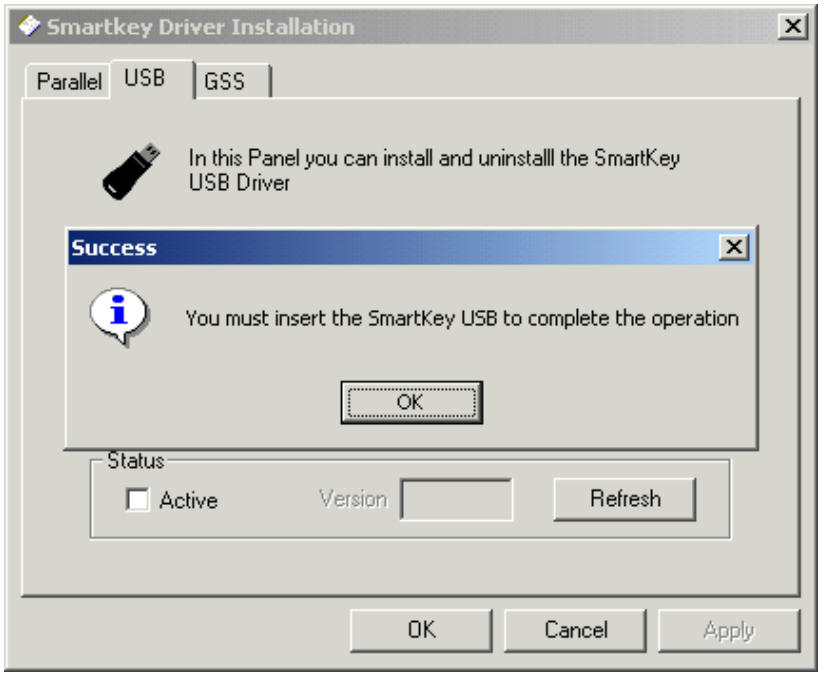

Figura 14

Inserire il dispositivo nella porta USB, premere il bottone *OK* e attendere il completamento dell'installazione come mostrato nelle figure seguenti.

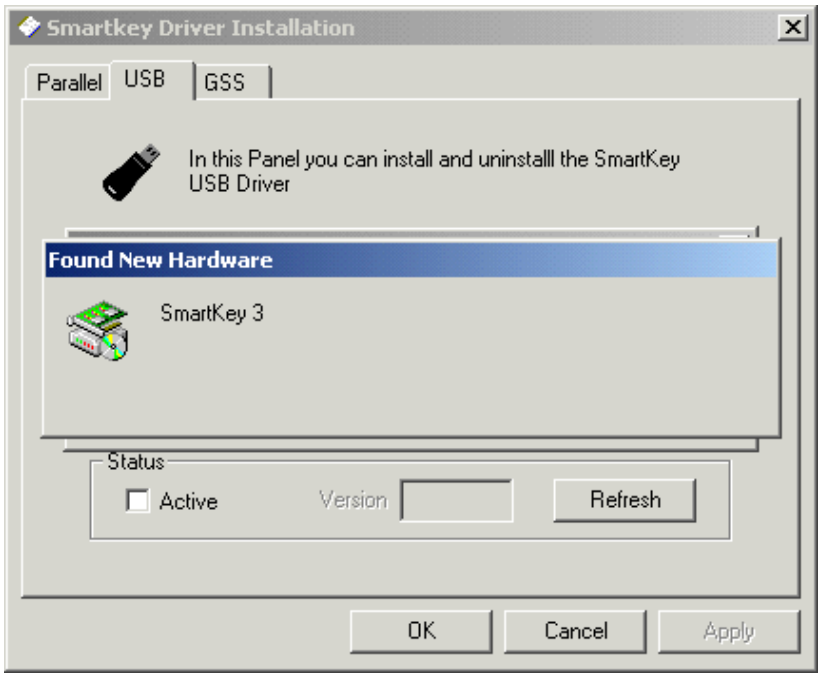

Figura 15

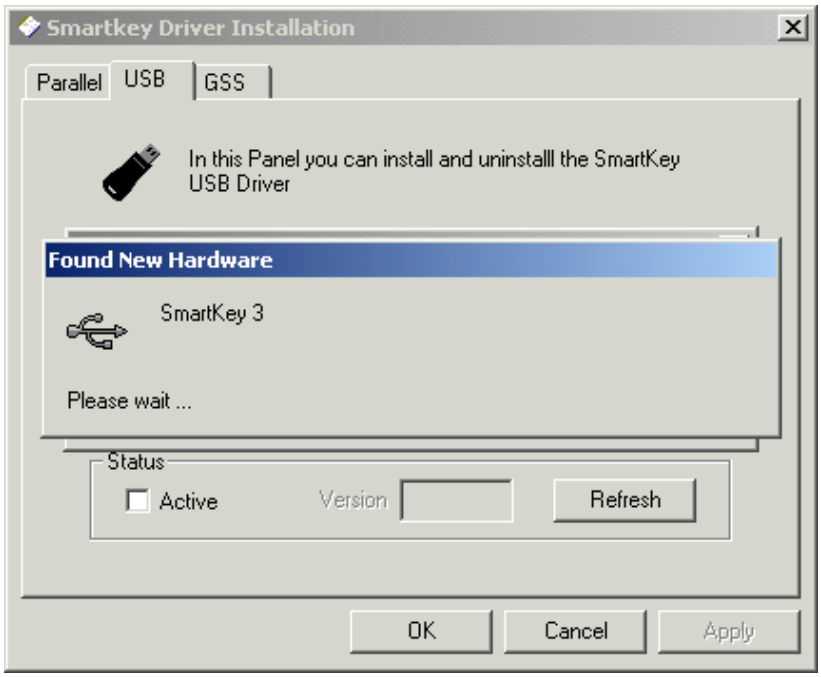

Figura 16

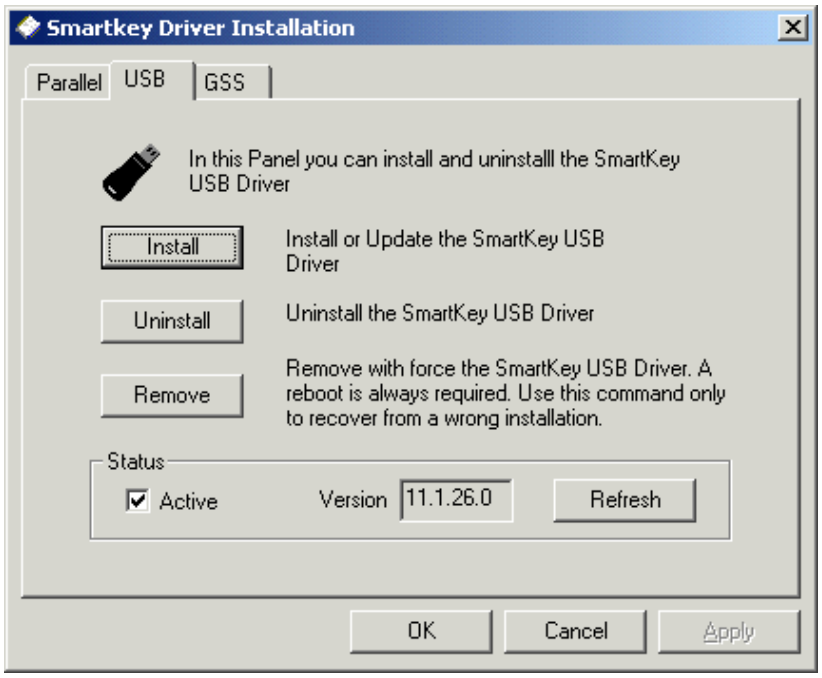

Figura 17

Ad installazione completata nel box *Status* si potrà vedere che il checkbox *Active* è selezionato ed il campo *Version* mostrerà la versione del driver.

A questo punto è necessario installare il servizio di gestione del dispositivo attraverso il programma d'utilità ASKEYADD.EXE al quale deve essere fornita unicamente la porta che sarà utilizzata per la comunicazione con i client (il servizio è in ascolto sulla porta indicata[17]), ad esempio può essere utilizzata la porta 15999. Dal prompt dei comandi emettere il comando mostrato in Figura 18, dopo essersi posizionati nella cartella indicata in fase di installazione del software.

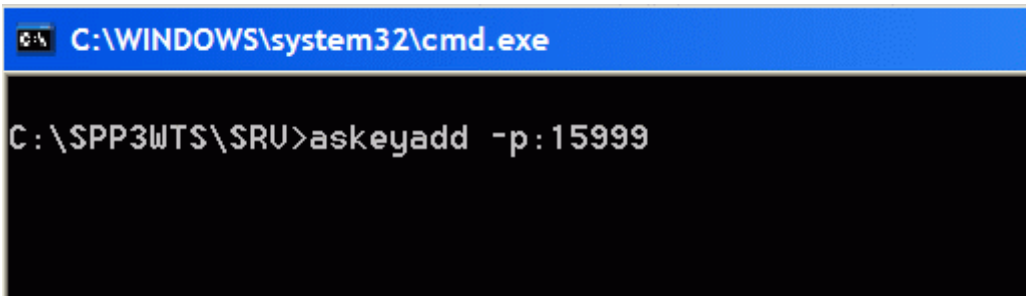

Figura 18

Il servizio inserisce vari messaggi nel registro degli eventi di sistema riservato alle applicazioni sia durante il normale utilizzo sia in caso d'errore. Il registro può essere consultato attraverso l'*Event Viewer* (*Visualizzatore Eventi*) di Windows.

Il programma ASKEYRM.EXE effettua anche la disinstallazione del servizio.

Il passo successivo consiste nella configurazione del client di connessione al servizio di gestione del dispositivo. L'operazione è eseguita dal programma CSKEYCFG.EXE la cui esecuzione (dal prompt dei comandi) è mostrata nella figura seguente. Il programma richiede come parametri il nome del server o il suo indirizzo IP (127.0.0.1 nell'esempio) e la porta sulla quale è in ascolto il servizio (15999 nell'esempio). Naturalmente è essenziale che queste due informazioni siano indicate in modo corretto altrimenti SIGLA non potrà essere eseguito (in particolare la porta deve corrispondere a quella indicata in fase d'installazione del servizio).

[17] La comunicazione avviene sull'indirizzo di loopback (127.0.0.1) e pertanto non dovrebbe essere influenzata dalla presenza di un eventuale firewall. In caso contrario è necessario procedere alle opportune modifiche alla configurazione del firewall in modo da non bloccare le comunicazioni, sia TCP che UDP, sulla porta specifica.

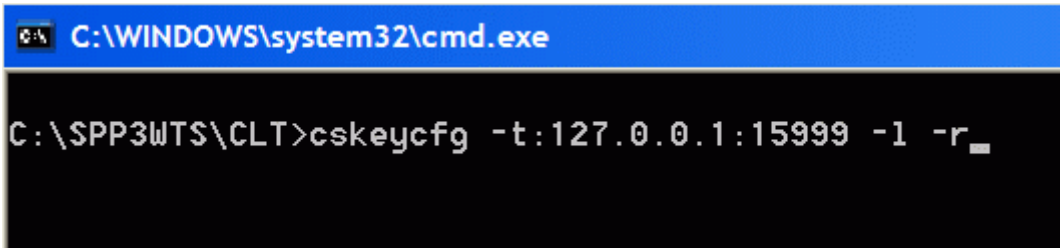

Figura 19

L'esecuzione di questo comando produce, al proprio termine, una schermata analoga a quella in Figura 20

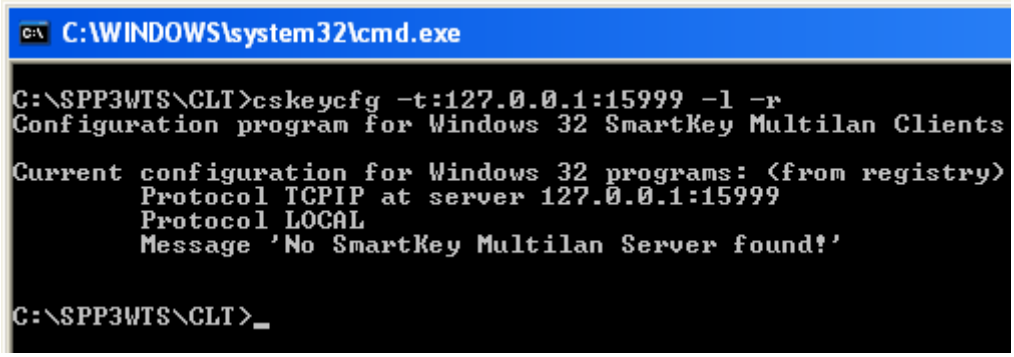

Figura 20

Dove il messaggio *'No SmartKey Multilan Server found!'* non indica il verificarsi di un errore, ma è il messaggio, salvato dall'installazione, che verrà usato in caso di chiave non trovata.

Tra le applicazioni fornite è disponibile anche il programma SKEYMON.EXE che fornisce in tempo reale le statistiche d'utilizzo del dispositivo di protezione. Questo programma deve essere utilizzato esclusivamente a fini diagnostici ed il suo utilizzo non è assolutamente necessario per il corretto funzionamento dell'installazione.