SAP Security

Seminario del corso: Elementi di Sicurezza Informatica

Davide Diosono

Università degli Studi di Perugia

25 Maggio 2010

Argomenti trattati

I Introduzione
- Sistemi informativi aziendali
- Sistemi E.R.P.
- SAP NetWeaver

II Modelli e strategie di sicurezza
- ABAP
  - Autenticazione degli utenti
  - Autorizzazione degli utenti
  - Livello trasporto

Il sistema informativo

Il sistema informativo di un'impresa è il complesso di elementi in grado di fornire le informazioni necessarie alle persone che lavorano a tutti i livelli dell'organizzazione.
E' composto da:

- un *patrimonio di dati*
- un *insieme di procedure*
- un *insieme di persone*
- un *insieme di mezzi e strumenti*
- un *insieme di principi generali e di idee di fondo*

Enterprise Resource Planning

Un **ERP** è un tipo di sistema informatico aziendale che pone particolare attenzione all'**ottimizzazione** dell'uso delle risorse disponibili in azienda.
Un sistema ERP può supportare i processi aziendali agendo su tre versanti attraverso:

- la *codifica del sapere comune*
- la *standardizzazione dei comportamenti*
- l'*integrazione dei flussi informativi*

... in tre lettere: S.A.P

SAP in cifre

Entrate totali	10,672 milioni di euro
Entrate da vendita software e servizi relativi al software	8,198 milioni di euro
n.ro impiegati	47,598 a tempo pieno
n.ro clienti	più di 95,000 in oltre 120 paesi
n.ro partner	più di 2,400 partner certificati

SAP NetWeaver

SAP NetWeaver è un insieme di strumenti SAP costruiti per consentire la **cooperazione** tra applicazioni, la **costruzione** di nuove sulla base di applicazioni esistenti, e l'abbassamento dei **costi d'acquisizione** delle stesse.
SAP NetWeaver si fonda su standard Internet quali **HTTP**, **XML** e **Web Services**.

Permette inoltre la realizzazione dell'architettura basata sui servizi **SOA**.

SAP NetWeaver

- *integrazione web* dei processi, tramite vari ed eterogenei sistemi, protocolli, banche dati e fonti.
- compatibile con il linguaggio di programmazione *ABAP*
- programmabile sia in *ABAP* che in *JAVA*

SAP NetWeaver

- *integrazione web* dei processi, tramite vari ed eterogenei sistemi, protocolli, banche dati e fonti.
- compatibile con il linguaggio di programmazione *ABAP*
- programmabile sia in *ABAP* che in *JAVA*

ABAP

Consente la creazione di transazioni interattive e reports; è oggi uno tra i maggiori linguaggi di programmazione usati al mondo.

SAP NetWeaver

- *integrazione web* dei processi, tramite vari ed eterogenei sistemi, protocolli, banche dati e fonti.
- compatibile con il linguaggio di programmazione *ABAP*
- programmabile sia in *ABAP* che in *JAVA*

J2EE

Java EE (J2EE) è la versione *enterprise* della piattaforma Java. E' una tra le più importanti piattaforme tecnologiche di sviluppo, soprattutto in ambiti in cui la sicurezza e la robustezza sono vincoli imprescindibili.

ABAP

Abbiamo diverse vulnerabilita in ogni **punto d'integrazione** dove vengono scambiati dati e informazioni.
La sicurezza deve quindi riguardare:

- **livello presentazione**: applicazioni front-end e client usate per accedere a SAP Web AS ABAP.
  - *autenticazione degli utenti*
- **livello applicazione**: logica applicativa all'interno del sistema AS ABAP.
  - *autorizzazione e gestione degli utenti*
- **livello trasporto** supportare le comunicazioni necessarie per l'intero sistema.
  - *protocolli di sicurezza delle comunicazioni*

Autenticazione degli utenti

L'autenticazione degli utenti consiste nella verifica dell'identità degli utenti, programmi, e servizi per garantire l'accesso al sistema soltanto in seguito ad un'autenticazione conclusasi con successo.

- SNC
- SSL
- User ID e password
- Certificati X.509
- SAP Logon Tickets e SSO

Secure Network Communication

SNC integra un prodotto di sicurezza esterno con il sistema SAP per fornire funzioni di sicurezza aggiuntive non originariamente disponibili.
SNC fornisce:

- diversi livelli di autenticazione,
  - autenticazione di sicurezza per la protezione della **comunicazione tra diversi client** e le componenti del server del sistema che usano `DIAG` o `RFC`.
  - autenticazione tra componenti server: `SAP Cryptographic Library`.
- protezione dell'integrità,
- protezione della privacy.

Secure Sockets Layer

Secure Sockets Layer (SSL) è un protocollo crittografico che fornisce una comunicazione sicura sopra la rete Internet.

SSL fornisce:

- criptazione dei dati,
- autenticazione lato server,
- autenticazione lato client,
- mutua autenticazione.

User ID e password

User ID e password è il meccanismo di autenticazione di default supportato da tutti i prodotti SAP NetWeaver.

La password deve rispettare sia le regole predefinite di SAP sia quelle che può aver aggiunto l'amministratore:

- `login/fails_to_user_lock`
- `login/fails_to_user_session_end`

Certificati X.509

Un certificato client X.509 è una digital identification card o chiave. Usando questo meccanismo di sicurezza, l'utente ha bisogno di avere il proprio certificato client X.509 inserito all'interno di una **PKI**.
L'utente che tenta di accedere al sistema AS ABAP:

I presenta un certificato valido al server usando il protocollo SSL,

II il server decripta la richiesta di log-on usando la sua chiave privata,

III l'autenticazione si svolge nel sottostante protocollo SSL. Non è necessario inserire user ID e password.

SAP Logon Tickets e SSO

L'utente si autentica una sola volta e il sistema emette un Ticket all'utente con in quale può accedere ad altri sistemi.
Requisiti:

- per l'autenticazione tra componenti server, entrambi i sistemi devono aver sincronizzati gli orologi di sistema.
- il sistema mittente deve possedere una **coppia di chiavi** affinché possa firmare il Ticket.
- il sistema accettante:
  - deve essere posto nello stesso **dominio DNS** del server mittente
  - deve avere un certificato di **chiave pubblica** del mittente per verificare il Ticket.

Configurazione:

- identificare un sistema deputato all'emissione dei ticket prima di configurare gli altri sistemi.
- sistema ABAP:
  - nel sistema AS ABAP mittente:
    `login/create_sso2_ticket` a 2.
  - nel sistema accettante:
    - installare **SAP Security Library** o **SAP Cryptographic Library**,
    - impostare il parametro `login/accept_sso2_ticket` a 1,
    - usando la transazione **SS02** (Single Sign-On Wizard) è possibile stabilire automaticamente la configurazione appropriata per il sistema accettante.

Logon Ticket da J2EE

- nell'engine J2EE occorre implementare la **SAP Cryptographic Library**
- impostare gli stessi elementi nel sistema AS ABAP
- importare manualmente il **certificato di chiave pubblica** nel **PSE** dell'engine J2EE usando la transazione **STRUST** o **STRUSTSS02** (Trust Manager).

Autorizzazione

I concetti riguardanti l'autorizzazione in SAP AS ABAP prevedono un approccio **basato sui ruoli**.

Quando un utente tenta di autenticarsi in un'applicazione SAP, il sistema autentica l'utente e imposta alcuni controlli di accesso controllando gli *authorization object* assegnati all'utente.

Per eseguire una transazione in SAP, l'utente necessita di una serie di *authorization objects* allocati nel suo **User Master Record**.

User Master Record

L'**User Master Record** memorizza tutta l'informazione riguardante un utente, incluse le sue autorizzazioni e altre impostazioni. Solo dopo che l'amministratore ha creato l'utente nell'user master record, l'utente può loggarsi nel sistema SAP e accedere alle funzionalità al suo interno in base alle autorizzazioni assegnate ai ruoli.

- **SU01** (Create/Mantain Users) - creazione di un nuovo utente
- **SU10** (Mass Mantain Users) - gestione di più utenti

Ruoli

Ciascun tipo di ruolo rappresenta una combinazione logica di transazioni SAP richieste per eseguire una funzione o un task.
E' possibile creare i ruoli usando la transazione **PFCG**.
Tipologie di ruolo:

ruolo singolo

Contiene i **dati di autorizzazione** e la **struttura del menu di log-on** composta dalle transazioni assegnate al ruolo.
Gli utenti assegnati al ruolo ereditano la struttura dei menu e le transazioni.

Ruoli

Ciascun tipo di ruolo rappresenta una combinazione logica di transazioni SAP richieste per eseguire una funzione o un task.
E' possibile creare i ruoli usando la transazione **PFCG**.
Tipologie di ruolo:

ruolo composto

Non contengono dati d'autorizzazione ma **raggruppano** ruoli singoli. Gli utenti assegnati ce vi sono assegnati vengono *automaticamente* assegnati ai corrispondenti ruoli.

Ruoli

Ciascun tipo di ruolo rappresenta una combinazione logica di transazioni SAP richieste per eseguire una funzione o un task.
E' possibile creare i ruoli usando la transazione **PFCG**.
Tipologie di ruolo:

ruolo derivato

Si riferisce a **ruoli già esistenti**; eredita la **struttura dei menu** e le **transazioni** dai ruoli referenziati. Possono essere passati i valori di default ma non quelli specifici all'organizzazione e gli assegnamenti agli utenti.

Authorization Objects e Field Values

Authorization Object

Un authorization object può raggruppare fino a 10 *authorization field* valutati secondo la relazione **AND**.

Authorization Fields

Gli authorization fields all'interno degli authorization objects sono considerati elementi del sistema da proteggere. L'authorization field può essere un valore numerico singolo oppure un intervallo di valori. Il sistema valuta questi insiemi di valori secondo la relazione **OR**.

Controlli per l'autorizzazione

I si verifica la presenza del codice della transazione nella tabella **TSTC**

II si controlla nella tabella se la transazione è stata bloccata dall'amministratore.

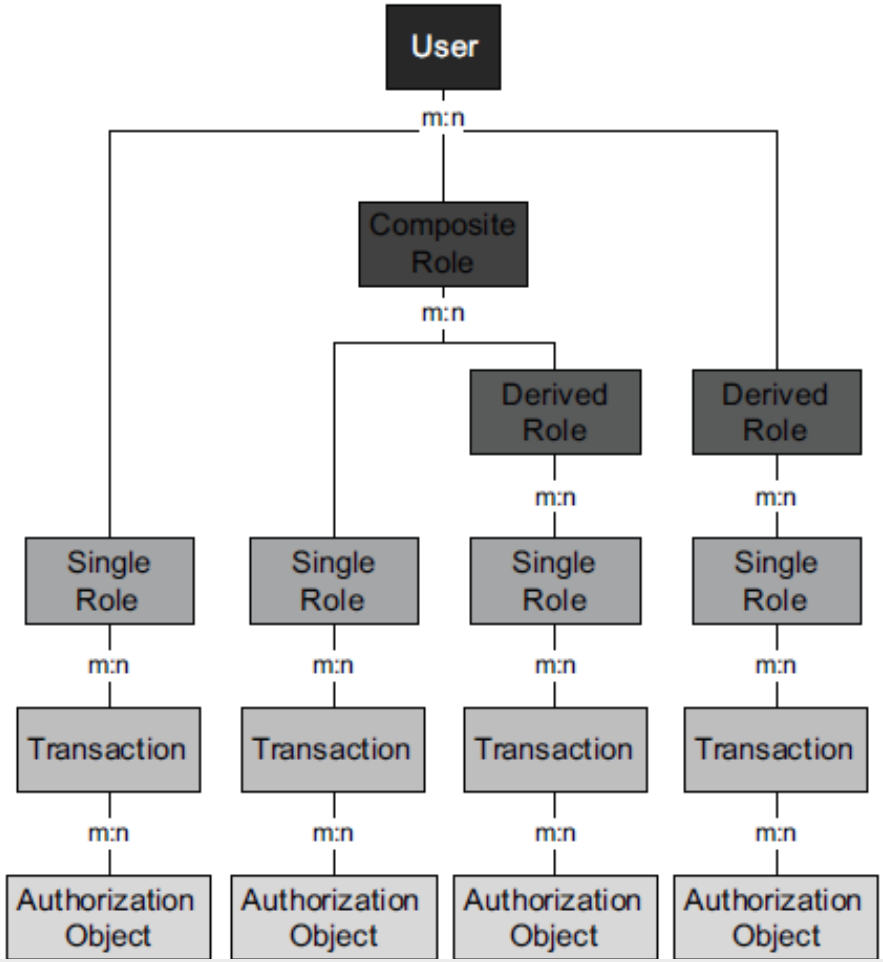
III si controlla se l'utente possiede le autorizzazioni necessarie.

- si controlla l'oggetto **S_TCODE**
- e il campo **TCD** (Transaction Code)

Occorre notare che il sistema non esegue alcun controllo nei seguenti casi:

- se è stato disattivato il check indicator dell'authorization object per la specifica transazione (transazione **SU24**).
- se il controllo è stato disattivato globalmente per gli authorization object di tutte le transazioni (transazione **SU24** o **SU25**).
- se il parametro `auth/no_check_in_some_cases` ha valore Y.

Riassumendo



Authorization Group

Authorization Group

Un authorization group può essere definito come un *authorization field* usato per proteggere **tabelle** e **programmi**.
Ad un authorization group possono essere assegnate una o più tabelle.
Una tabella può essere assegnata **solo** ad un authorization group specifico.

Authorization Group su tabelle

Per esempio, è possibile proteggere tabelle definendo un apposito gruppo nella tabella **TBRG** e assegnando i gruppi alle tabelle che si vogliono proteggere nella tabella **TDDAT**.

Con questo meccanismo di sicurezza, è possibile prevenire l'accesso alle tabelle usando transazioni come **SE16** (Display Table) e **SM30** (Table Maintenance).

Per accedere alle tabelle protette, l'utente richiede l'autorizzazione ad entrambi i gruppi definiti nella tabella **TDDAT** e all'authorization object **S_TABU_DIS** con l'authorization field **DICBERCLS** contenenti questo authorization group.

Authorization Group su programmi

E' inoltre possibile definire authorization group sui programmi nella tabella **TPGP** e assegnare i gruppi ai programmi che si vuole proteggere nella tabella **TPGPT**.

- Un gruppo può essere assegnato ad uno o più *programmi*.
- Un programma può essere assegnato solo ad un *authorization group*.

Gestione degli utenti

La gestione degli utenti è una funzionalità essenziale per il business e alcune considerazioni devono essere prese riguardo l'accesso all'informazione (*segregation of duties*).
Compiti:

- modifica dei diritti di accesso
- gestione di identità diverse in sistemi diversi collegate ad uno stesso utente

Gestione integrata degli utenti

In questo scenario tutti i dati di gestione degli utenti sono mantenuti centralmente in un unico sistema.

Vantaggi:

- amministrazione degli utenti più **semplice**,
- riduzione della **ridondanza** dei dati,
- riduzione degli **overhead** nella gestione,
- maggiore **trasparenza**,
- incremento della **privacy**.

Soluzioni

Nei sistemi SAP Web AS ABAP ci sono due opzioni tra cui scegliere:

- **CUA**: integra la gestione dei dati degli utenti di più sistemi basati su ABAP in un unico sistema.
- **LDAP**: integra la gestione dei dati relativi ad utenti di sistemi SAP e non-SAP in un unico sistema.

Central User Administration

Definizioni

Il sistema dove risiede CUA è chiamato **sistema centrale** e tutti gli altri sistemi a cui CUA distribuisce i dati sono definiti **sistemi figli**.

Schema di funzionamento:
qualsiasi cambiamento alle informazioni sono mantenuti nel sistema centralee distribuiti in modo asincrono ai sistemi figli applicando la tecnologia **ALE**.

Lightweight Directory Access Protocol Synchronization

Con Lightweight Directory Access Protocol (LDAP) syncronization, è possibile integrare la gestione degli utenti e consentire che sistemi diversi (SAP e non-SAP) possano sincronizzarsi con la directory di servizio di LDAP e ricavare le informazioni sugli utenti.

Il **processo di sincronizzazione** consente di scambiare informazioni sugli utenti da/verso la directory LDAP.
A seconda di come è stata configurata la directory LDAP, è possibile configurare la *direzione* del processo di sincronizzazione.

Configurare LDAP

Per comunicare tra un sistema AS ABAP e la directory LDAP occorre l'interfaccia `LDAP Connector`, che è una collezione di moduli usati per accedere ad una directory LDAP.

E' possibile abilitare l'interfaccia LDAP Connector creando una destinazione **RFC** chiamata `LDAP` e specificando le opportune impostazioni nella transazione **LDAP**.

Gestione degli utenti

Si usa la transazione **SU01** per gestire gli user master record. Le funzioni di questa transazione riguardano la capacità di:

- creare, modificare, copiare, cancellare e bloccare user ID.
- impostare, cambiare e generare password.
- assegnare ad un utente uno o più ruoli.
- gestire le impostazioni di default degli utenti.
- gestire altre impostazioni (tipo utente, indirizzo di posta elettronica).

Per gestire un grande numero di utenti in un sistema, è possibile utilizzare la transazione **SU10** (Mass User Changes).

Gestione dei ruoli

E' possibile utilizzare **PFCG** per la creazione, l'assegnamento e la cancellazione di ruoli.
Le funzioni contenute in questa transazione consentono di:

- creare, modificare, cancellare e trasportare *ruoli singoli*,
- creare una template di un ruolo,
- creare *ruoli compositi* e *ruoli derivati*,
- generare automaticamente profili di autorizzazioni per un ruolo,
- assegnare *authorization object* ad un ruolo,
- cambiare gli *authorization object* e gli *authorization values*.

Analizzare le autorizzazioni

Durante la creazione di nuovi ruoli, la gestione di ruoli esistenti, o la ricerca delle soluzioni per un errore di authorization denial error, è abbastanza utile invocare la transazione **SU53** per analizzare le autorizzazioni mancanti.

In alternativa si può usare la *system trace* eseguendo la transazione **ST01**, le cui informazioni riguardano l'intero sistema. Si può limitare la sessione di trace per user ID, transazione, o nome di profilo.

Logging e Monitoring permettono di individuare le debolezze e le vulnerabilità del sistema e il monitor pro-attivo di tutte le attività relative alla sicurezza.
Gli strumenti che si possano usare includono:

Security Audit Log

Le transazioni **SM19** e **SM20** monitorizzano e inseriscono nel log le informazioni riguardanti l'attività degli utenti, come:

- tentativi riusciti e falliti di log-on (Dialog e RFC)
- transazioni riuscite e fallite
- chiamate RFC a funzioni nei moduli
- modifiche agli user master record
- modifiche alla configurazione di audit

Logging e Monitoring permettono di individuare le debolezze e le vulnerabilità del sistema e il monitor pro-attivo di tutte le attività relative alla sicurezza.
Gli strumenti che si possano usare includono:

Audit Info System

Strumento di auditing che si può utilizzare per analizzare alcuni aspetti di sicurezza del sistema.
Si accede ad AIS tramite la transazione **SECR**.
Le funzioni disponibili riguardano:

- procedure di auditing e documentazione
- valutazioni di auditing
- download dei dati di auditing

Logging e Monitoring permettono di individuare le debolezze e le vulnerabilità del sistema e il monitor pro-attivo di tutte le attività relative alla sicurezza.
Gli strumenti che si possano usare includono:

Alert di sicurezza in CCMS

Quando il **Security Audit Log** registra un evento di sicurezza, è possibile propagare il un alert di sicurezza al monitor degli alert del CCMS.
Gli alert di sicurezza che sono stati creati corrispondono a classi di eventi di audit definite nel Security Audit Log.
Si può accedere agli alert CCMS usando la transazione **RZ20**.

User Information System

La transazione **SUIM** fornisce una visione completa sulle **autorizzazioni** e sugli **utenti** del sistema SAP.

Le liste di report che si possono produrre usando User Information System includono:

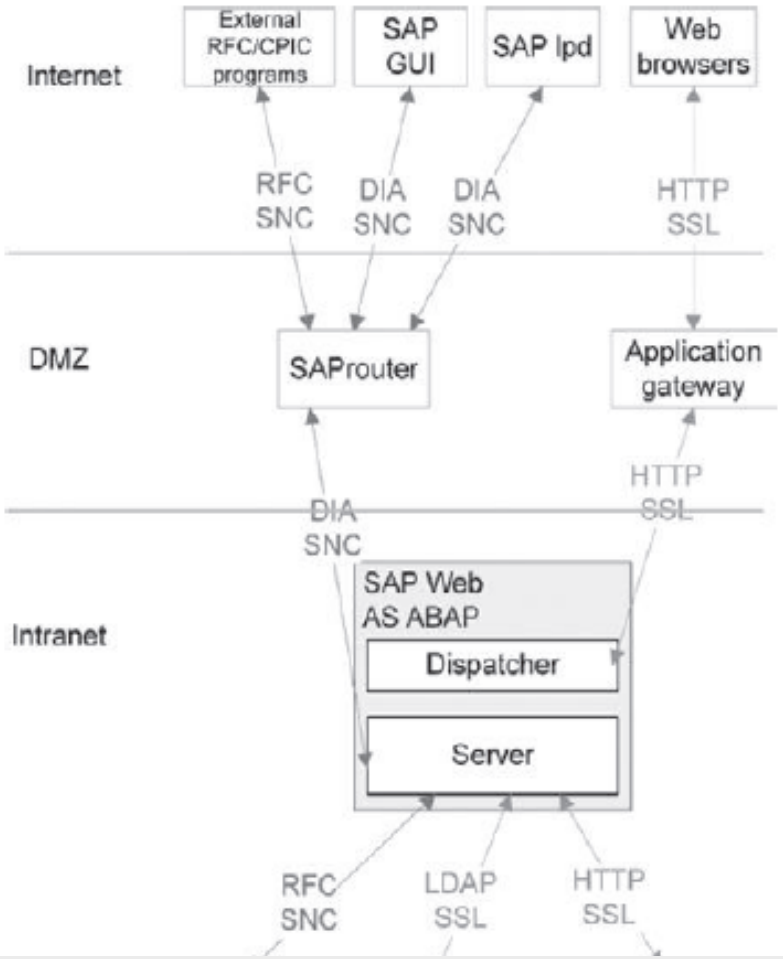
- visualizzazione degli utenti secondo criteri complessi,
- visualizzazione degli utenti per date di log-on e cambiamento della password,
- visualizzazione degli utenti secondo autorizzazioni critiche,
- visualizzazione dei ruoli e dei profili secondo criteri complessi,
- visualizzazione delle transazioni contenute all'interno di

Mettere in sicurezza il livello trasporto

Dal punto di vista dell'integrità dei dati e della privacy, è importante proteggere l'infrastruttura della rete visto che supporta le comunicazioni necessarie al tuo business.
Il meccanismo usato per la sicurezza del livello trasporto e per la crittografia dipende dal protocollo usato:

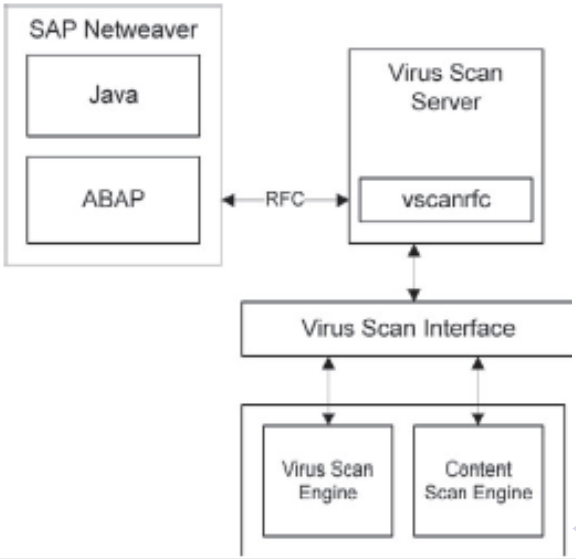
- Per i protocolli SAP, come **DIALOG** e **RFC**, si può usare **SNC**
- Per proteggere le comunicazioni con protocolli Internet, come **HTTP**, si può usare **SSL**.
- I protocolli di accesso alle directory, come **LDAP**, usano anch'essi **SSL**.

Uso di una DMZ

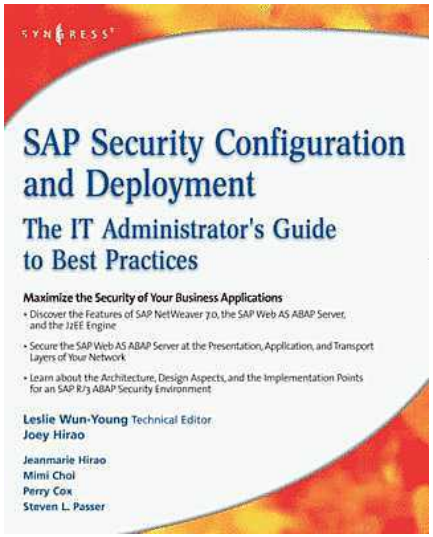


Virus Scan Interface

Con **VSI** è possibile incrementare la sicurezza del sistema scansionando files e documenti. Supporta sia AS ABAP che J2EE Engine.
La soluzione VSI consiste di **VSI** e di un **prodotto antivirus** di un venditore certificato.



Riferimenti



Grazie per l'attenzione