1

INTRODUZIONE

1.1 IL SISTEMA INFORMATIVO AZIENDALE

1.1.1 *Il sistema informativo*

Il sistema informativo in un'impresa deve essere visto come quel complesso di elementi in grado di fornire le informazioni necessarie alle persone che lavorano a tutti i livelli dell'organizzazione. Ogni struttura, nel cui interno sia necessario produrre o scambiare informazioni dispone di un proprio sistema informativo. Quando è possibile individuarlo in forma esplicita, esso risulta composto dai seguenti elementi:

- un **patrimonio di dati**: i dati rappresentano la materia prima con cui si producono le informazioni; in altri termini i dati sono una rappresentazione oggettiva della realtà, mentre le informazioni sono prodotte per un destinatario che ne ha bisogno per lo svolgimento delle proprie mansioni;
- un **insieme di procedure** per l'acquisizione e il trattamento di dati per la produzione di informazioni;
- un **insieme di persone** che sovrintendono a tali procedure (perché le svolgono di persona o le alimentano con i dati necessari, oppure perché gestiscono le apparecchiature che svolgono le procedure in modo automatico);
- un **insieme di mezzi e strumenti** necessari al trattamento, trasferimento, archiviazione, di dati e informazioni;
- un **insieme di principi generali di valori e di idee di fondo** che caratterizzano il sistema e ne determinano il comportamento.

In particolare i sistemi informativi, in quanto permettono di ridurre i costi e i tempi di acquisizione, raccolta e trasmissione delle informazioni, sono in grado di supportare l'impresa nel migliorare il proprio sistema informativo e le relazioni con i clienti.
Relativamente al *miglioramento del sistema operativo*, ad esempio, il sistema informativo permette all'impresa di ridurre il livello delle scorte ed i tempi di attraversamento in fabbrica.
Relativamente al *rafforzamento delle relazioni con il cliente*, ad esempio, il sistema informativo permette un'ampia visibilità sulle richieste dei clienti e sullo stato di avanzamento delle attività produttive ed amministrative. L'introduzione in azienda di un sistema informativo nasce come un cambiamento tecnico a livello proprio di sistemi informatici per poi espanderrsi all'interno dell'impresa arrivando a toccarne l'assetto strategico e

organizzativo.
A *livello organizzativo* può favorire una semplificazione della struttura e l'automazione dei compiti lavorativi routinali.
A *livello strategico* può favorire il riposizionamento dell'impresa e, soprattutto nel caso in cui si coinvolga più organizzazioni, anche una ridefinizione delle attività che l'impresa svolge al suo interno.

1.2 I SISTEMI ERP

Un tipo particolare di sistema informatico aziendale è il cosiddetto E.R.P. (dall'acronimo dell'espressione inglese *Enterprise Resource Planning*).
Definiamo ERP come quel tipo di sistema informatico aziendale che pone particolare attenzione all'ottimizzazione dell'uso delle risorse disponibili in azienda, e che quindi si occupa della gestione della produzione, della catena di approvvigionamento, della distribuzione, dei preventivi e degli ordini, oltre però a fornire comunque un sistema integrato di soluzioni alle più diverse problematiche aziendali, tra le quali di solito la gestione della contabilità, dei rapporti con la clientela e dei magazzini.
Un sistema ERP può supportare i processi aziendali agendo su tre versanti:

- attraverso la *codifica del sapere comune* e la *standardizzazione dei comportamenti*. Ciò facilità la comunicazione all'interno dell'impresa. La codifica rende trasparenti le informazioni richieste per ciascuna attività o fase di processo; la diffusione istantanea dell'informazione codificata in tutto il sistema rende continuamente le informazioni disponibili nei diversi punti dell'organizzazione.
  Inoltre la codifica delle attività le rende accessibili ad una più ampia schiera di operatori: si riduce il rischio, oggi assai frequente, che la mancanza di un operatore, unico conoscitore delle modalità di svolgimento delle attività, possa bloccare lo svolgimento di un intero processo.

- attraverso l'*integrazione dei flussi informativi*. La traduzione letterale di ERP sarebbe: sistemi per la pianificazione aziendale delle risorse, ma non è quella corretta. La traduzione nella nostra lingua più corretta anche se non letterale sarebbe: sistemi informativi integrati, a segnalare proprio la capacità di questi sistemi di integrare i diversi sottoinsiemi presenti in azienda. L'univocità dei dati presenti nel sistema e la diffusione istantanea delle informazioni consente di eliminare tutte quelle attività di reimissione dei dati tipica dei sistemi non integrati. In tal modo si liberano risorse precedentemente impegnate in attività a nessun valore aggiunto e, spesso, a scarso contenuto professionale e motivazionale.

1.3 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.

Possiamo individuare nell'integrazione delle persone, delle informazioni e dei processi le funzionalità principali di SAP NetWeaver. Integrare le persone significa unire le persone e aiutarle a lavorare di più e più efficientemente. Integrare informazione significa raccogliere l'informazione proveniente da diverse locazioni e dargli senso nelle operazioni di tutti i giorni. Integrare i processi significa coordinare il flusso di lavoro dei dipartimenti, divisioni, e compagnie.

SAP NetWeaver è progettato per:

- **consentire il cambiamento** attraverso un incremento della flessibilità del business e della sua adattabilità.
- **incrementare l'usabilità** rendendo semplice l'utilizzo dei sistemi per gli utenti finali, aumentando così l'adozione degli utenti, il risparmio, la produttività.
- **migliorare l'integrazione** facendo il possibile per far lavorare insieme le applicazioni dell'azienda.
- **consentire l'innovazione** permettendo che nuove applicazioni possano essere costruite a partire da applicazioni già esistenti.
- **risparmiare** riducendo le spese di acquisizione e manutenzione dei sistemi esistenti.

In pratica SAP NetWeaver viene utilizzato:

- nella *creazione di portali* che accorpano le funzionalità di diversi programmi e le presentano con un'interfaccia facile da usare.
- per la *creazione di versioni consistenti di dati vitali* che provengono da applicazioni diverse.
- per consentire che un processo iniziato in un'applicazione fornisca un'interfaccia affinché continui *attraverso altre applicazioni*, o sistemi di altre compagnie.

1.3.1 *La piattaforma aperta per le applicazioni e l'integrazione*

SAP NetWeaver si fonda sugli standard Internet quali HTTP, XML e Web Services, garantendo così la piena interoperabilità con Microsoft .NET e con gli ambienti J2EE come IBM WebSphere. Con SAP NetWeaver è quindi più facile costruire e trarre beneficio da soluzioni di business ritagliate sulle esigenze di ciascun cliente. Con SAP NetWeaver Software è possibile realizzare l'architettura basata sui servizi (Enterprise Service- Oriented Architecture) che combina i vantaggi delle applicazioni enterprise SAP con la flessibilità dei Web Services, per adeguarsi ai modelli di business più dinamici.

2

CONCETTI E MODELLI DI SICUREZZA

SAP NetWeaver è basato su standard di mercato con diverse tecnologie e mccanismi di sicurezza per la protezione della privacy dei dati commerciali e l'integrità degli stessi da accessi non autorizzati. In questo capitolo, esamineremo l'approccio tenuto da SAP per fornire soluzioni di sicurezza per le tecnologie di SAP NetWeaver quali SAP Web Applicaton Server (AS) ABAP, SAP Web AS J2EE e sistemi backend (basati su UNIX e Oracle). Scendendo nei dettagli, le prossime sezioni spiegheranno concetti e meccanismi di sicurezza disponibili per l'autenticazione dgli utenti, come user ID e password, Secure Network Communication (SNC), Secure Sockets Layer (SSL), certificati X.509 per le connessioni ad Internet, e SAP log-on tickets per soluzioni SSO (Single Sign-On).
In più questo capitolo racchiude la spiegazione di concetti sull'autorizzazione, vantaggi di controllo di accesso basato sui ruoli, l'importanza dell'integrazione nella gestione degli utenti, le opzioni nella gestione degli utenti e dei ruoli, ma anche altre misure disponibili nella protezione e crittografia nello scambio di dati per creare canali di comunicazione privati ed incrementare la sicurezza dei contenuti.

2.1 ABAP

Sono passati i tempi in cui la sicurezza nei sistemi SAP ABAP si rivolgeva esclusivamente al livello applicazione e l'implementazione di autorizzazioni e ruoli era sufficiente. Con l'introduzione della piattaforma tecnologica SAP NetWeaver, le soluzioni SAP sono ora basate su una architettura client/server più aperta, basata sul web e multilivello, che integra diversi componenti, applicazioni o sistemi attraversando i confini tecnologici e di business. I dati e le informazioni possono essere scambiate e integrate tra componenti, applicazioni e sistemi. Questo porta a problemi di vulnerabilità dei dati ad ogni punto di integrazione dove vengono scambiati dati e informazioni. Per questo la sicurezza deve riguardare i livelli presentazione, applicazione e trasporto; tutti gli aspetti di sicurezza sono basati sulla restrizione delle funzionalità di ogni livello in base alle autorizzazioni possedute dagli utenti e dai sistemi:

- il *livello presentazione* racchiude diverse applicazioni front-end (ad es., interfacce grafiche per SAP) e client (ad es., browser Web) usate per accedere a SAP Web AS ABAP.
  Siccome i dati sono scambiati sopra reti esposte (ad es. Internet), si presentano rischi per la sicurezza della comunicazione con il sistema AS ABAP. Per garantire la protezione della comunicazione, gli utenti devono autenticarsi con successo prima

di poter accedere al sistema; questo meccanismo è chiamato **autenticazione degli utenti**.

- il *livello applicazione* è costituito dalla logica applicativa all'interno del sistema AS ABAP. Poiché dati importanti e sensibili possono essere acceduti nel sistema AS ABAP, vengono introdotti rischi di business particolarmente significativi se il controllo di accesso non è opportunamente gestito. Per prevenire accessi non autorizzati, il controllo degli accessi è basato sul concetto dell'**autorizzazione** e della **gestione degli utenti**. Dati particolarmente sensibili possono essere ulteriormente protetti usando il meccanismo SSF (Secure Store and Forward).
- il *livello trasporto* supporta le comunicazioni necessarie per l'intero sistema. Dati che sono scambiati sopra reti non sicure innalzano i rischi per l'integrità dei dati e la protezione della privacy oltre ad altre minacce per la sicurezza. Per assicurare che i dati vengono comunicati in modo sicuro possono essere usati protocolli di sicurezza come SNC (Secure Network Communication) e SSL (Secure Sockets Layer).

2.1.1 *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.
Minacce alla sicurezza come virus, worms o furti di informazione o di identità possono essere sventati utilizzando appropriate procedure di autenticazione. Ciascuno di questi attacchi può causare ore di produttività persa in scansioni alla ricerca di virus o nell'installazione di patch.
L'autenticazione degli utenti protegge il *livello presentazione* del sistema SAP Web AS ABAP. Il tipico meccanismo con user ID e password è supportato da tutti i prodotti SAP NetWeaver. Siccome questo sistema non può completamente prevenire attacchi di sicurezza, il sistema deve essere protetto usando metodi di autenticazione più forti, come un prodotto di sicurezza esterno che supporti la criptazione o certificati firmati da una CA (Certificate Authority) fidata.

Secure Network Connection Secure Network Connection (SNC) integra un prodotto di sicurezza esterno con il sistema SAP per fornire funzioni di sicurezza aggiuntive non originariamente disponibili. Il prodotto di sicurezza esterno deve essere certificato dal *SAP Software Partner Program*. SNC può fornire diversi livelli di autenticazione (*verifica dell'identità*), *protezione dell'integrità* (ravvisare qualsiasi modifica dei dati che può essere avvenuta durante la comunicazione), e *protezione della privacy* (fornire la critpazione del messaggio). Si può usare SNC per avere un'autenticazione di sicurezza per la protezione della comunicazione tra diversi client e le componenti del server del sistema AS ABAP che usano Dialog (DIAG) e protocolli RFC (Remote Function Call). Per l'autenticazione tra componenti server (per esempio, connessioni tra sistemi ECC (ERP Central Component) e

BW (Business Warehouse)), il prodotto di sicurezza di default che si può usare è chiamato SAP Cryptographic Library (SAPCRYPTOLIB). Gli algoritmi crittografici garantiscono la privacy della comunicazione attraverso la criptazione.
Addizionali misure di sicurezza possono rendersi necessarie per determinati prodotti di sicurezza per assicurare che la sicurezza non venga compromessa. Per esempio, se il prodotto di sicurezza usa una tecnologia a chiave pubblica (per esempio, certificati client), allora è necessaria un'infrastruttura a chiave pubblica PKI (Public-Key Infrastructure). In questi casi, apposite procedure di sicurezza devono essere messe in atto per la generazione e la distribuzione delle chiavi e dei certificati per gli utenti e le componenti del sistema. Occorre anche assicurarsi che le chiavi private siano memorizzate in una locazione sicura, per mezzo di crypto box o smart card, e che la chiave pubblica sia firmata da una CA fidata.
E' inoltre importante notare come qualche paese ha restrizioni riguardanti l'uso della crittografia nelle applicazioni software.

Secure Sockets Layer Secure Sockets Layer (SSL) è un protocollo crittografico che fornisce una comunicazione sicura sopra la rete Internet. SSL può fornire la criptazione dei dati, l'autenticazione lato server (il server si identifica al client), autenticazione lato client (il client si identifica al server), e mutua autenticazione. Garantisce la condifenzialità dei dati sopra la rete. Il protocollo SSL usa un'infrastruttura a chiave pubblica per fornire questa protezione.
SSL viene usato per fornire connessioni HTTP sicure tra componenti client e server nel sistema SAP WEB AS ABAP.
Per l'autenticazione SSL, il server deve avere una coppia di chiave pubblica-privata e un certificato di chiave pubblica affinché possa identificarsi come componente server, e un altro coppia di chiavi e un certificato per identificarsi come componente client. Queste coppie di chiavi e certificati vengono memorizzati nel PSE (Personal Security Environment).

User ID e Password Come è stato menzionato, user ID e password è il meccanismo di autenticazione di default supportato da tutti i prodotti SAP NetWeaver. Per poter accedere al sistema, deve essere inserita la combinazione user ID e password corretta. Quando l'utente la immette, il sistema esegue alcuni controlli per vedere se l'utente può accedere con queste credenziali e la correttezza delle stesse.
Se la password è imposta ad initial, è scaduta o resettata dall'amministratore, l'utente deve impostare una nuova password. Questa password deve rispettare sia le regole predefinite di SAP sia quelle che può aver aggiunto l'amministratore. Per esempio, se l'utente immette una password non corretta, può ripetere la procedura un numero di pari non superiore al numero di tentativi concessi (impostata dal parametro di profilo *login/fails_to_user_lock* e *login/fails_to_user_session_end*). Quando uno dei due parametri viene raggiunto, allor l'user ID viene bloccato e la sessione termina.

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 un'infrastruttura a chiave pubblica (PKI).
L'utente che tenta di accedere al sistema AS ABAP ha bisogno di presentare un certificato valido al server usando il protocollo SSL. A quel punto il server decripta la richiesta di log-on usando la sua chiave privata; solo il server può decriptare questa richiesta.
L'autenticazione si svolge nel sottostante protocollo SSL. Quindi, non è necessario inserire user ID e password.
Per assicurare che questi certificati siano emessi da una sorgente fidata, è raccomandato l'uso di certificati firmati da una CA fidata. Questo comporta che una CA venga scelta come designata nel sistema AS ABAP (chiave privata) e che l'utente che accede al sistema AS ABAP debba possedere un certificato valido signato dalla CA scelta (chiave pubblica). La corrispondente chiave privata dell'utente deve essere memorizzata in una locazione sicura (per esempio, protetta da password o con smart card).
Oltre a proteggere il livello presentazione, questo meccanismo può anche essere usato per proteggere il *livello trasporto*, specificatamente per proteggere le connessioni HTTP tra componenti client e server nel sistema AS ABAP.

SAP Logon Tickets e Single Sign-on SAP Logon Ticket fornisce i meccanismi di autenticazione per proteggere la comunicazione tra componenti client e server nel sistema AS ABAP. L'utente viene autenticato usando il Logon Ticket con un token di autenticazione. L'utente si autentica una sola volta (per esempio, usando user ID e password) e il sistema emette un Logon Ticket all'utente. Con il Logon Ticket, l'utente può accedere ai sistemi senza il bisogno di re-inserire il suo user ID e password.
SAP Logon Tickets vengono usati in soluzioni SSO (Single Sign-On). Questo meccanismo di sicurezza beneficia molto dell'ambiente di SAP, caratterizzato dalla presenza di un buon numero di sistemi diversi, in cui ciascun utente può avere più password per accedere ad applicazioni diverse, e dove tener traccia delle password crea problemi facilmente previdibili (password dimenticate) che possono risultare in un numero maggiore di chiamate all'help desk e quindi ad un incremento dei costi di amministrazione.
Per l'autenticazione SAP Logon Ticket con componenti client (per esempio, SAP GUI per Windows), gli utenti devono avere lo stesso user ID in tutti i sistemi in cui devono accedere e i loro browser Web devono accettare i cookie.
Per l'autenticazione tra componenti server, sia il sistema accettante sia il server mittente devono aver sincronizzati gli orologi di sistema. Il sistema mittente deve possedere una coppia di chiavi pubblica e privata affinché possa firmare digitalmente il Logon Tickets. Il sistema accettante deve essere posto nello stesso dominio DNS (Domain Name Server) del server mittente e deve avere un certificato di chiave pubblica per verificare la firma digitale del ticket.
E' raccomandato identificare un sistema specifico deputato all'emissione dei ticket prima di configurare gli altri sistemi. Di default, il PSE (Personal Security Environment) viene usato per memorizzare i certificati. E' possibile configurare il sistema AS ABAP in modo

da fargli emettere i log-on ticket impostando il parametro *login/create_sso2_ticket* a 2.
Per poter accettare Logon Tickets da un altro sistema ABAP occorre installare SAP Security Library (o SAP Cryptographic Library), e impostare il parametro *login/accept_sso2_ticket* ad 1. Con la transazione **SS02** (Single Sign-On Wizard) è possibile stabilire automaticamente la configurazione appropriata per il sistema accettante.
Se il sistema AS ABAP deve essere configurato in modo tale da accettare Logon Tickets da J2EE, allora occorre implementare la SAP Cryptographic Library e impostare gli stessi parametri nel sistema AS ABAP. In più, occorre importare manualmente il certificato di chiave pubblica dell'engine J2EE nel PSE usando la transazione **STRUST** o **STRUSTSS02** (Trust Manager).

2.1.2 *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 objects assegnati all'utente.
In questo modo l'utente può eseguire soltanto le transazioni, i programmi e i servizi per i quali gli è stato concordato l'accesso.
Per eseguire una transazione in SAP, l'utente necessita di una serie di *authorization objects* allocati nel suo *user master record*. Una combinazione di questi ruoli, o *ruolo composto*, definisce l'accesso per una specifica posizione all'interno dell'organizzazione (ad esempio, amministrazione del personale).
I ruoli composti possono essere un gruppo di ruoli singoli o derivati oppure entrambi. I ruoli corrispondenti sono assegnati direttamente agli utenti nell'user master record. Il diagramma sottostante illustra la relazione gerarchica tra utenti, ruoli composti/singoli, transazioni, oggetti e campi d'autorizzazione.

User Master Record L'User Master Record memorizza tutta l'informazione riguardante un utente, incluse le sue autorizzazioni e altre impostazioni. Solo quando 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 assegnati ai ruoli. Puoi creare un nuovo utente usando la transazione **SU01** (Create/Mantain Users). Per gestire un ampio numero di utenti, si può usare la transazione **SU10** (Mass Mantain Users).

Ruoli e Profili 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 PFCF (il profile generator). Ci sono diversi tipi di ruoli, rispettivamente singoli, composti e derivati:

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

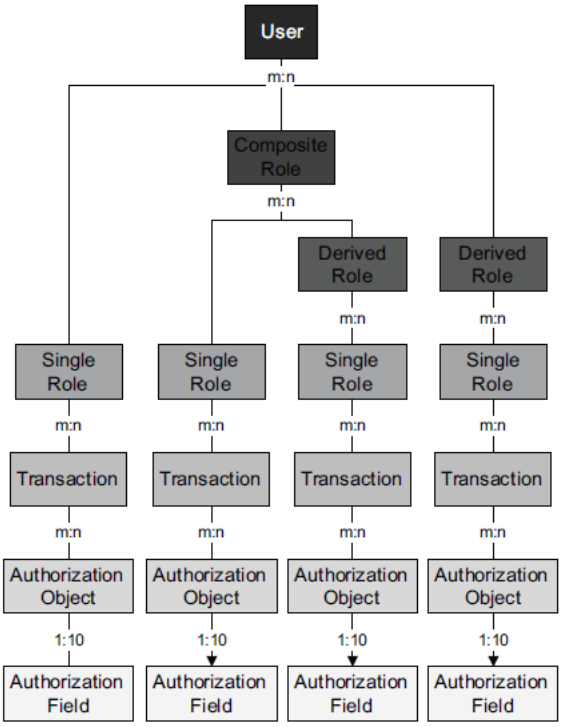

Figura 1: Relazione tra utenti, ruolo singoli/composti/derivati, transazioni, oggetti d'autorizzazione e campi d'autorizzazione

dei menu e le transazioni.

ruolo composto diversamente dai ruoli singoli, non contengono dati di autorizzazione. Il loro scopo è di raggruppare ruoli singoli. Gli utenti che sono assegnati a un ruolo composto sono automaticamente assegnati ai corrispondenti ruoli durante il confronto degli utenti.

ruolo derivato si riferisce a ruoli già esistenti; eredita la struttura dei menu e le transazioni dai ruoli referenziati. Possono essere passati valori di default ma non quelli specifici all'organizzazione e gli assegnamenti degli utenti. I ruoli derivati sono interessanti per la gestione dei ruoli in cui le funzionalità sono le stesse ma i livelli organizzativi possono essere differenti.

Authorization Objects e Field Values Un *authorization object* è ciò che usa SAP per assegnare autorizzazioni e consentire controlli complessi al fine di determinare quale tipo di accesso riservare agli utenti.
Un *authorization object* è formato da *authorization fields* e può raggruppare fino a 10 *authorization fields* valutati secondo la relazione AND.
Gli *authorization fields* all'interno degli *authorization objects* sono considerati elementi del sistema da proteggere che si riferiscono ad elementi memorizzati con l'ABAP Dictionary.
L'*authorization field* può essere un valore numerico singolo oppure un intervallo di valori.

Questi insiemi di valori sono chiamati *autorizzazioni*. E' possibile consentire tutti i valori oppure un valore nullo come valori legittimi. Il sistema valuta questi insiemi di valori secondo la relazione OR. Per fare in modo che un controllo sull'autorizzazione termini con successo, tutti i valori dei campi di un *authorization object* devono essere gestiti in modo appropriato nell'user master.
Per esempio, esaminiamo l'*authorization object* F_KNA1_BUK (Customer Authorization for Company Codes), che richiede gli *authorization field* ACTVT (Activity) e BURKS (Company Code). Per consentire la creazione di un customer master record, l'amministratore della sicurezza deve creare le autorizzazioni assegnando all'utente gli *authorization object* K_KNA1_BUK con l'*authorization field Activity* impostato a 01 e l'*authorization field Company Code* impostato a 3129.
Da un punto di vista operativo, l'autorizzazione può essere classificata in general authorization, functional authorization e organization authorization: una general authorization specifica la funzione che un utente può eseguire, che è, un authorization object F_KNA1_BUK è stato assegnato per creare customer master record. Il sistema cerca fra le autorizzazioni dell'utente se è presente quella per creare customer accounts (che è, Activity 01 in almeno un company code. In seguito il sistema controlla se all'utente è consentito creare account per un specifica unità organizzativa (Company Code 3129).

Controlli sull'autorizzazione Quando l'utente tenta di eseguire una transazione selezionata tramite il menu o con un comando, il sistema esegue alcuni controlli. Il primo fra questi verifica la presenza del codice della transazione nella tabella TSTC e controlla se la transazione è stata bloccata dall'amministratore. Il sistema poi controlla se l'utente possiede le autorizzazioni necessarie per eseguire la transazioni controllando l'oggetto S_TCODE e il campo TCD (Transaction Code) contenuto al suo interno. L'utente deve avere un'autorizzazione con il valore del codice della transazione selezionata.
Se viene creata una nuova transazione con la transazione SE93, è possibile assegnare più autorizzazioni alla transazione. Ciò è particolarmente utile quando è necessario proteggere una transazione con un'autorizzazione diversa. Per transazioni per cui sono state inserite autorizzazioni aggiuntive tramite la transazione SE93, l'utente richiede anche l'object authorization TSTA, memorizzato nella tabella TSTCA. In alternativa, è possibile considerare l'uso di altri metodi per proteggere la transazione, come un *level program* con il comando AUTHORITY-CHECKS.
Le transazioni invocate indirettamente non sono incluse in questo controllo iniziale. Per transazioni complesse che richiamano altre transazioni, vengono eseguiti altri controlli.
Terminata questa prima fase di analisi, il sistema controlla se la transazione selezionata è assegnata ad un authorization object. In caso affermativo, viene fatto un controllo per verificare se l'utente ha l'autorizzazione per questo authorization object. E' possibile usare la transazione **SU24** (Edit Authorization Object) e cliccare sul bottone *Check Indicator* per verificare gli authorization object assegnati alla transazione.
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 nella transazione SU24. Tieni a mente che non si può disattivare il *check indicator* per gli authorization object predefiniti nelle aree di SAP NetWeaver e HR (Human Resource).
- se hai disattivato globalmente gli authorization object per tutte le transazioni usando la transazione SU24 o SU25.
- se il parametro *auth/no_check_in_some_cases* ha valore Y.

L'utente può eseguire la transazione quando tutti i controlli sopra citati hanno riportato un successo; altrimenti il sistema terminerà visualizzando un messaggio appropriato.

Authorization Groups Un *authorization group* può essere definito come un *authorization field* usato per proteggere tabelle e programmi. 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. Ad un *authorization group* possono essere assegnate una o più tabelle. Una tabella può essere assegnata solo ad un *authorization group* specifico. Alternativamente, può essere usata la transazione **SE11** sotto Utilities | Table Maintenance Generator per gestire l'assegnazione delle tabelle ai gruppi. 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*. Ciò è particolarmente utile quando si vuole proteggere tabelle custom. Le tabelle SAP standard sono generalmente protette; comunque, se richiesto è possibile cambiare manualmente l'*authorization group*.
In maniera del tutto simile è 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*. In alternativa, è possibile assegnare il gruppo al programma usando SE38. Questo previene gli utenti dall'accesso al programma usando transazioni come **SE38** e **SA38** (Execute Program). Per accedere al programma protetto, l'utente richiede l'autorizzazione all'*authorization object* S_PROGRAM con l'*authorization field* P_GROUP contenente il gruppo.

Gestione degli utenti Un aspetto nella gestione degli utenti non banale riguarda il processo di modifica dei diritti di accesso che si può verificare quando un utente viene promosso o lascia la compagnia. Riducendo il tempo e la complessità delle operazioni necessarie, può ridurre il numero di chiamate all'help desk, incrementare la produttività degli impiegati e di frequente rappresenta una fonte di risparmio.
Siccome molte organizzazioni sentono la necessità di gestire singole identità degli utenti attraverso sistemi diversi, si presenta il rieschio di dover gestire più identità per lo stesso utente.

Per esempio, se un impiegato abbandona l'azienda, allora teoricamente tutti gli accessi al sistema dovrebbero essere revocati; comunque, c'è un elemento di rischo dove un amministratore può aver revocato l'accesso degli utenti al sistema SAP Enterprise Portal, in questo caso l'utente potrebbe ancora accedere al sistema. Il modo più semplice per mitigare il rischio è offerto da una gestione integrata degli utenti e da un archivio degli utenti centralizzato al quale gli altri sistemi si sincronizzano. Questo significa che se i diritti di accesso di un utente sono revocati in un sistema questo effetto viene propagato in tutti gli altri sistemi.

Gestione degli utenti integrata L'integrazione nella gestione degli utenti è il consolidamento dei dati relativi agli utenti e alle autorizzazioni inizialmente sparse in più sistemi in un unico archivio centralizzato. Tutti i dati di gestione degli utenti sono così mantenuti centralmente in un unico sistema. Questo non solo rende l'amministrazione degli utenti più semplice, ma riduce allo stesso tempo la ridondanza nei dati e gli overhead nella gestione, incrementa la trasparenza, e incrementa la privacy.
Nei sistemi SAP Web AS ABAP ci sono due opzioni di gestione degli utenti tra cui scegliere:

- Central User Administration (CUA) integra la gestione dei dati degli utenti di più sistemi basati su ABAP in un unico sistema.
- Lightweight Directory Access Protocol (LDAP) synchronization integra la gestione dei dati degli utenti di più sistemi (SAP e non-SAP) in un unico sistema.

Central User Administration Central User Administration (CUA) è una feature presente nei sistemi SAP AS ABAP, con la quale è possibile integrare la gestione degli utenti di più sistemi ABAP in un unico sistema. Il sistema dove risiede CUA è chiamato *sistema centrale* e tutti gli altri sistemi a cui CUA distribuisce i dati sono definiti *sistemi figli*.
Qualsiasi cambiamento alle informazioni (per esempio nome, indirizzo email, ruoli assegnati, dati di licenza) devono essere mantenuti nel sistema centrale, dopodiché i cambiamenti vengono distribuiti in modo asincrono ai sistemi figli usando Application Link Enabling (ALE).
L'implementazione di CUA rende più facile l'amministrazione degli utenti e dei diritti ad essi associati.

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. Per esempio, è possibile far uso delle informazioni riguardanti il personale dipendente memorizzate in una directory LDAP e copiare i dati (per esempio, indirizzo, numero di telefono, indirizzo email) in un sistema AS ABAP.

A seconda di come è stata configurata la directory LDAP, è possibile configurare la direzione del processo di sincronizzazione. Per esempio, se si vuole inviare indietro tutti gli aggiornamenti sui dati alla directory LDAP, la comunicazione tra il sistema AS ABAP e la directory LDAP usa il protocollo 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**.

E' possibile integrare un sistema centrale CUA con una directory LDAP. Tutto ciò è una buona idea se si vuole integrare i dati sugli utenti con una directory LDAP e si hanno molti sistemi AS ABAP, in quanto occorre sincronizzare soltanto una volta la directory LDAP con il sistema centrale CUA.

Manutenzione utenti La manutenzione degli utenti riguarda le operazioni di creazione, modifica, cancellazione, blocco degli user master record.
Si usa la transazione **SU01** per gestire gli user master record. Le funzioni di questa transazione rigurdano 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 come la stampante predefinita, i parametri di un utente, il fuso orario, etc.
- gestire altre impostazioni come il tipo di utente, l'indirizzo di posta elettronica, gruppo dell'utente, SNC, license data, etc.

Per gestire un grande numero di utenti in un sistema, è possibile utilizzare la transazione **SU10** (Mass User Changes), dove si può cambiare l'user master record relativo ai dati di log-on, le impostazioni predefinite, i parametri, ruoli e profili. Per sistemi dove è implementato CUA, la gestione degli utenti deve essere eseguita sul sistema centrale cosicché le modifiche sulle informazioni possano essere distribuite nella modalità stabilita nelle impostazioni della transazione **SCUM** ai sistemi figli.

Manutenzione dei ruoli La manutenzione dei ruoli riguarda la creazione, l'assegnamento, e la cancellazione di ruoli. E' possibile utilizzare la transazione **PFCG** (Profile Generator) per modificare i ruoli. Alcune funzioni di questa transazione includono la possibilità di:

- creare, modificare, cancellare, e trasportare *ruoli singoli*.
- creare una template di un ruolo.
- creare *ruoli composti* e *ruoli derivati*

- modificare la strutture di default del menu di un ruolo.
- generare automaticamente profili di autorizzazioni per un ruolo.
- assegnare *authorization objects* ad un ruolo.
- cambiare gli *authorization objects* e gli *authorization values*.
- assegnare una o più user ID al ruolo ed eseguire un confronto tra utenti per trasferire autorizzazioni all'user master record.

In termini di ruoli e responsabilità per quanto riguarda la funzionalità di *Role Maintenance*, l'amministratore della sicurezza di SAP tipicamente crea e gestisce i ruoli mentre l'amministratore degli utenti assegna i ruoli agli utenti, e qualche volta l'help desk resetta e cambia le password.

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. Per la generazione di un record occorre eseguire la transazione **SU53** o **/nSU53** direttamente dopo la visualizzazione dell'errore di `authorization denial error`. Ottenuto il report, si può analizzare quale *authorization object* era stato controllato per una specifica transazione. E' possibile utilizzare la transazione SU56 per visualizzare una lista di tutte le autorizzazioni nel proprio user master.
In alternativa, è possibile utilizzare la *system trace* eseguendo la transazione **ST01**. Prima di eseguire la sessione di trace bisogna accertarsi di aver selezionato il check box **Authorization**. Siccome fa una trace di tutto il sistema, le informazioni registrate nella trace riguardano tutto il sistema. Si può limitare la sessione di trace per user ID, transazione, o nome di profilo. Ricordati di disattivare la sessione di trace se non richiesta.

TIP Quando occorre assegnare autorizzazioni ai ruoli, si consiglia di usare l'approccio pragmatico *less is more*: si parte con soltanto gli *authorization objects* che si reputano indispensabili, si usa poi la *authorization trace* per trovare gli *authorization object* e gli *authorization values* necessari; si costruiscono poi i ruoli aggiungendo gradualmente gli *authorization object* necessari.

Logging e Monitoring 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, indirizzare ogni problema di sicurezza che può nascere e rafforzare le policies di sicurezza.
Gli strumenti che si possono usare includono `Security Audit Log`, `Audit Info System` (AIS), alert di sicurezza all'interno di CCMS e l'Users Information System (SUIM).

- Security Audit Log (transaction SM19 e SM20) viene usato per scopi di reporting e di audit. Monitorizza e inserisce 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 records
  - modifiche alla configurazione di audit

- Audit Info System (AIS) è uno 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 sono le seguenti:
  - procedure di auditing e documentazione
  - valutazioni di auditing
  - download dei dati di auditing

- Security Alerts in Computing Center Management System (CCMS) quando il `Security Audit Log` registra gli eventi di sicurezza, può propagare il corrispondente alert di sicurezza al monitor degli alert del `Computing Center Management System`. 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 è uno strumento di report e monitoraggio usato dagli amministratori della sicurezza per fonire una visione completa sulle autorizzazioni e sugli utenti del sistema SAP, ed è particolarmente utile quando colleziona informazioni per scopi di monitoring e audit.
  Per accedere all'`User Information System` occorre eseguire la transazione **SUIM** oppure tramite il menu SAP, scegliere **Tools | Administration | User Maintenance | Information System**. Le liste di report che si possono produrre usando User Information System includono:
  - la visualizzazione degli utenti secondo criteri complessi
  - la visualizzazione degli utenti mediante combinazioni critiche di autorizzazioni all'inizio della transazione
  - la visualizzazione degli utenti per data di log-on e cambiamento della password
  - la visualizzazione degli utenti secondo autorizzazioni critiche
  - la visualizzazione dei ruoli e dei profili secondo criteri complessi
  - il confronto di ruoli e utenti diversi
  - la visualizzazione delle transazioni contenute all'interno di un ruolo
  - la visualizzazione delle modifiche di un documento in base ad utente, ruolo, profilo e autorizzazioni
  - la creazione di liste where-used per ruoli, profili e autorizzazioni.

  Come alternativa, si può usare la transazione **SE16** per ricavare informazioni simili per scopi di monitoraggio e di audit.

2.1.3 *Mettere in sicurezza il livello di trasporto in SAP WEB AS ABAP*

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 business. SAP Web AS ABAP usa diversi protocolli per proteggere la comunicazione con i partner.
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 (Secure Network Communications). Usando SNC, si può rafforzare le comunicazioni verso il sistema SAP implementando misure di sicurezza aggiuntive che il sistema SAP non fornisce direttamente (come ad esempio, certificati client o autenticazione tramite smart card).
- per procolli Internet, come HTTP, si può usare SSL (Secure Sockets Layer) per proteggere la comunicazioni. Usando HTTPS (Hypertext Transport Protocol Secure) nella URL al posto di HTTP, si dirigono le comunicazioni verso un numero di porta sicura invece che alla solita porta 80. La sessione utente viene gestita dal protocollo SSL.
- I protocolli di accesso alle directory, come LDAP, usano anch'essi SSL. Così facendo si può assicurare che lo scambio dei dati (per esempio, user ID e password, user data) tra la directory e il sistema SAP sia sicuro.

Una topologia di rete ben definita può prevenire minacce di sicurezza quali virus, attacchi DOS, eavesdropping e il furto di informazioni aziendali. E' altamente consigliabile l'uso di una DMZ (demilitarized zone) per costituire un'infrastruttura di rete come mostrato in Figura 2. Una DMZ aggiunge un livello aggiuntivo di sicurezza nella LAN di un'organizzazione in modo tale che un attaccante esterno può solo accedere alle apparecchiature nella DMZ e non all'intera rete dell'organizzazione.
Questo significa piazzare il sistema SAP, come un sistema SAP Web AS ABAP (sia il database sia l'application server) nella Intranet zone. Dato che i sistemi sono all'interno di una LAN sicura che è protetta con un firewall, si può operare in sicurezza senza dover usare SNC (impostando il parametro *snc/r3int_rfc_secure* a 0).
Altri device come SAP Web dispatcher, Application gateway e SAProuter possono essere posizionati nella DMZ interna in modo da fornire l'accesso a Internet.

Secure Store and Forward E' importante proteggere dati sensibili memorizzati nei sistemi SAP e prevenirne l'accesso da accessi non autorizzati. Il sistema SAP WEB AS usa un meccanismo chiamato *Secure Store and Forward* per proteggere dati e documenti usando la firma digitale e digital envelopes. Ciò consente la protezione dei dati anche quando lasciano il sistema SAP, e quindi i dati possono essere trasmessi sopra i canali di comunicazione senza comprometterne la protezione.
Simile a ciò che la firma tradizionale è per un documento di carta, una firma digitale

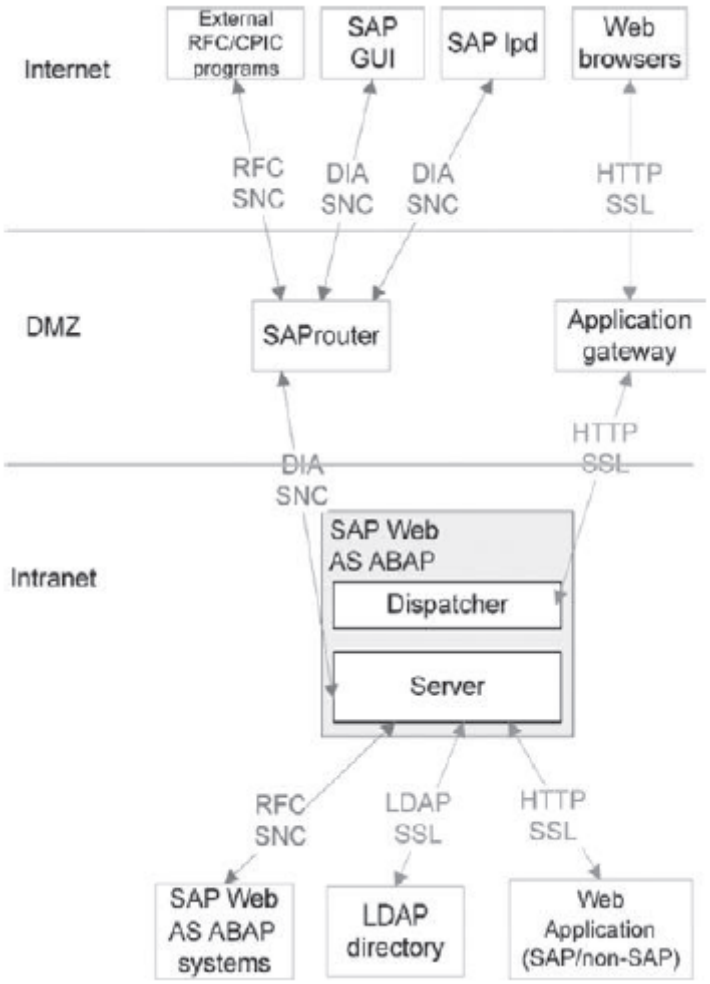

Figura 2: Sicurezza nel livello trasporto nei sistemi SAP Web AS ABAP

identifica univocamente l'individuo che firma il documento digitale e garantisce che l'individuo è realmente chi dice di essere. La firma digitale protegge anche l'integrità dei dati firmati e quindi se i dati vengono alterati in qualsiasi modo allora la firma non è più valida. Una digital envelope fa si che i contenuti dei dati siano visibili soltanto al destinatario voluto.
Di default, SAP Web AS ABAP già ha la SAP Security Library (or SAPSECULIB) per le firme digitali. In alternativa si può usare la SAP Cryptographic Library, che supporta le digital envelopes e crypto hardware, o un prodotto di sicurezza esterno certificato da SAP.
Ciascun partecipante che usa la firma digitale o le digital envelopes necessita di una propria coppia di chiavi (pubblica e privata). E' particolarmente importante che le misure di sicurezza siano in grado di proteggere le chiavi da accessi non autorizzati e abusi. La chiave privata deve essere memorizzata in una locazione sicura. Per la chiave pubblica, occorre assicurarsi che il certificato sia stato emesso da una sorgente fidata ed è stata segnata da una CA (Certification Authority) fidata. In maniera simile per il server AS ABAP, c'è una coppia di chiavi. La chiave privata è memorizzata nel sistema PSE (Personal Security Environment) in un file chiamato `SAPSYS.pse`, che si trova nella sottodirectory `sec` della directory specificata dal parametro `DIR-INSTANCE`. L'accesso a questa directory è possibile soltanto all'amministratore della sicurezza e deve essere messa in sicurezza per assicurare che la chiave privata non venga compromessa.

Virus Scan Interface Data la totale apertura della tecnologia SAP NetWeaver ogni volta che un file esterno viene caricato è presente il rischio di virus, trojan, adware, spyware, o altri attacchi malevoli. Per esempio i documenti dei fornitori che vengono caricati esternamente sono suscettibili a contenere virus, trojan e altri malware.
E' possibile usare il VSI (Virus Scan Interface) per incrementare la sicurezza del sistema scansionando files e documenti. Supporta sia AS ABAP che J2EE Engine come mostrato in Figura 3.

La soluzione VSI consiste di VSI e di un prodotto antivirus di un venditore certificato. Una lista di tutti i venditori certificati per l'interfaccia VSI è disponibile in SAP Service Marketplace.

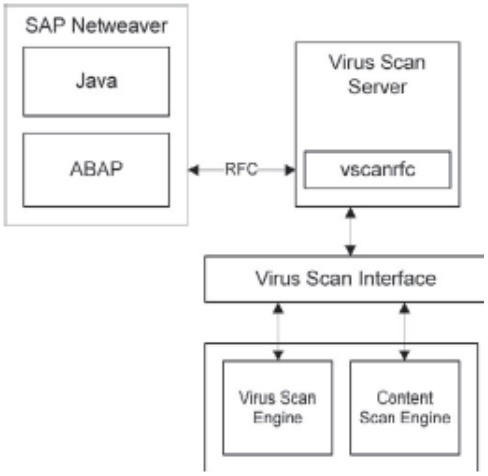

Figura 3: Proteggere la sicurezza dei contenuti con Virus Scan Interface