

Alessandro Faustini

Tivoli Security Specialist

**La soluzione IBM per la  
gestione delle Identità e del  
Controllo Logico degli  
Accessi**



# Agenda

Gestione delle identità

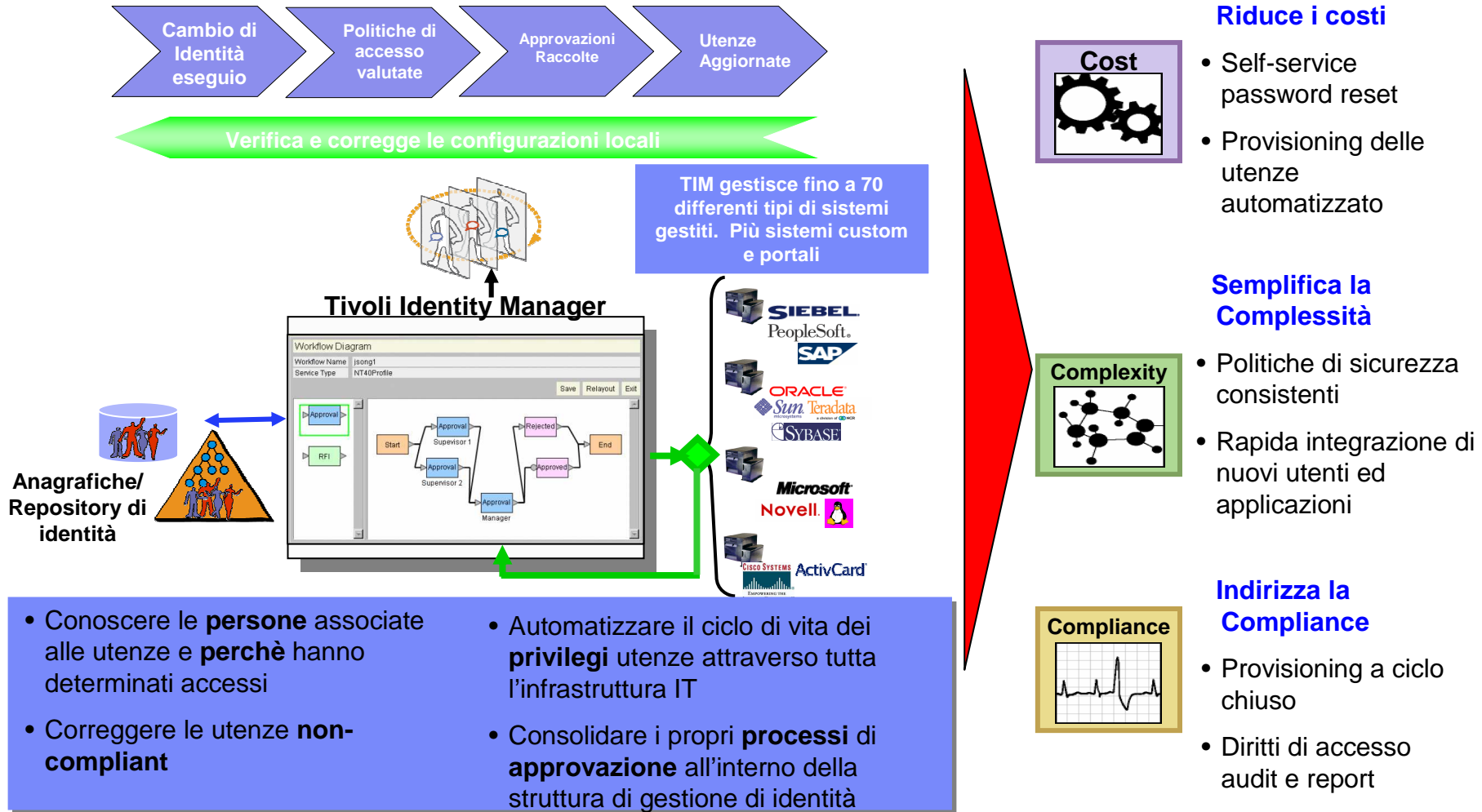
Soluzione Tivoli per l'Identity Management

Controllo degli accessi

Autenticazione, Autorizzazione e *Single Sign-On*

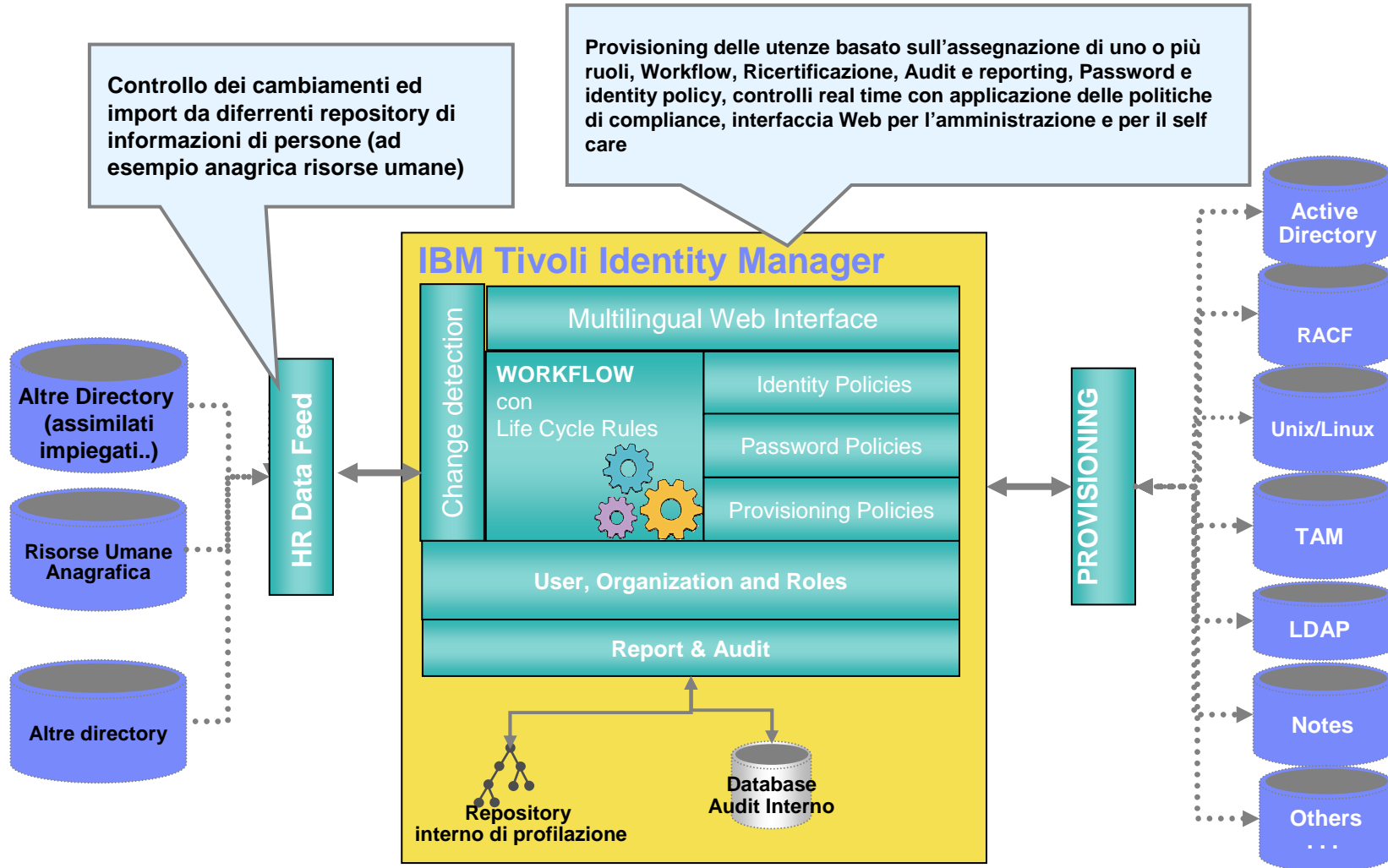


# Tivoli Identity Manager: automatizza la gestione del ciclo di vita delle identità





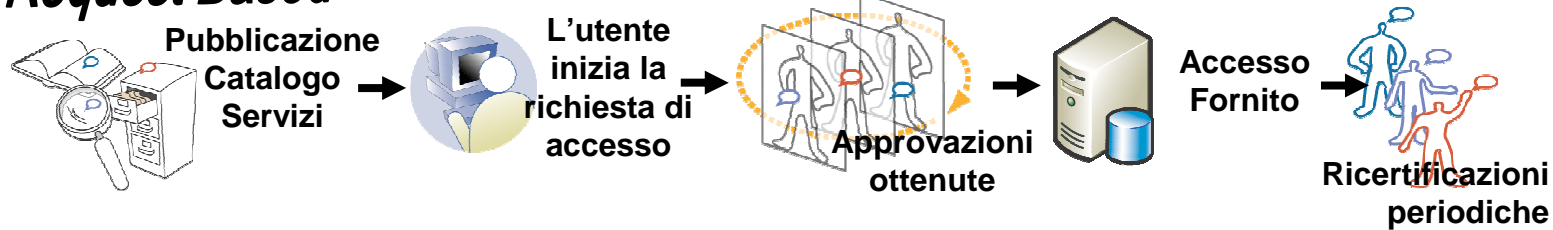
# Tivoli Identity Manager: Architettura Logica





Un approccio per fasi per automatizzare il provisioning delle utenze e fornisce miglioramenti in efficienza e controllo

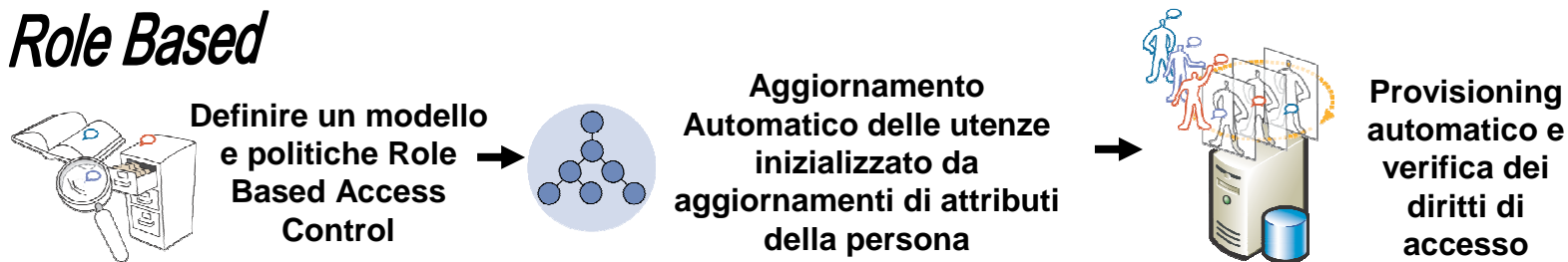
### *Request Based*



### *Hybrid Approach*



### *Role Based*



Investimenti

Operatività immediata

Automazione

Disegno politiche automatiche

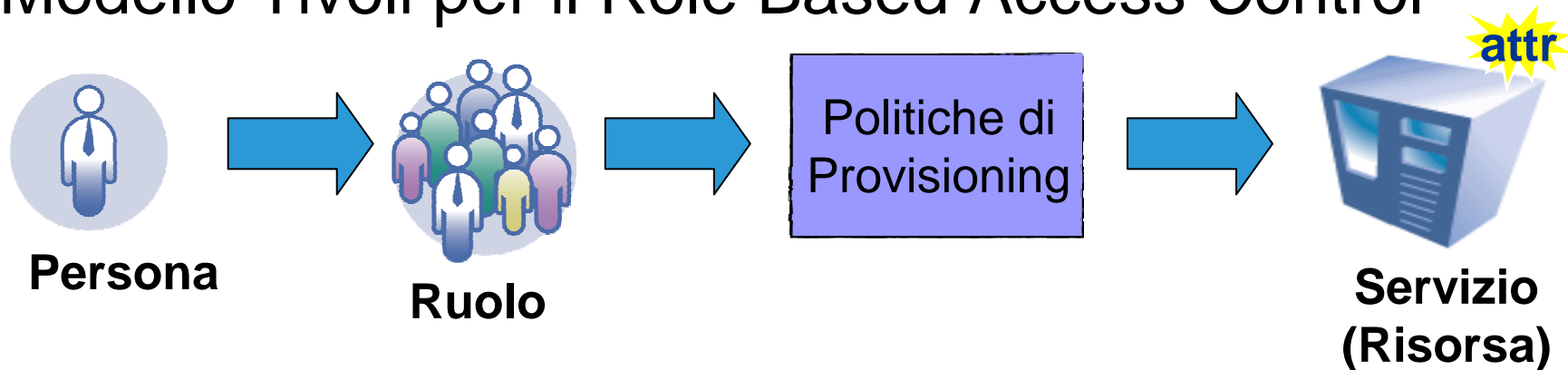


BASTA PARLARE INIZIAMO A FARE

© 2008 IBM Corporation



## Modello Tivoli per il Role Based Access Control

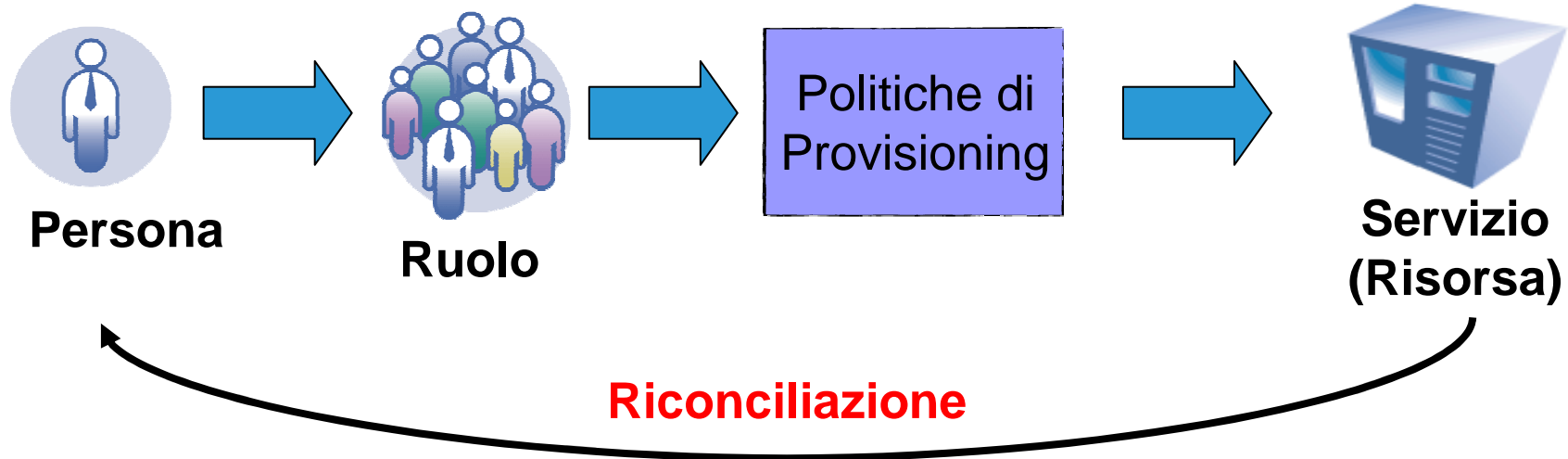


- Persone assegnate ai ruoli in funzione delle responsabilità
- Alle persone sono create/modificate utenze sulle risorse gestite in funzione dell'appartenza ai Ruoli attraverso le politiche di Provisioning
- Le Politiche di Provisioning definiscono anche gli attributi per le utenze



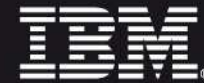


## Riconciliazione Confronta “Ciò che è” a “Ciò che Dovrebbe essere”



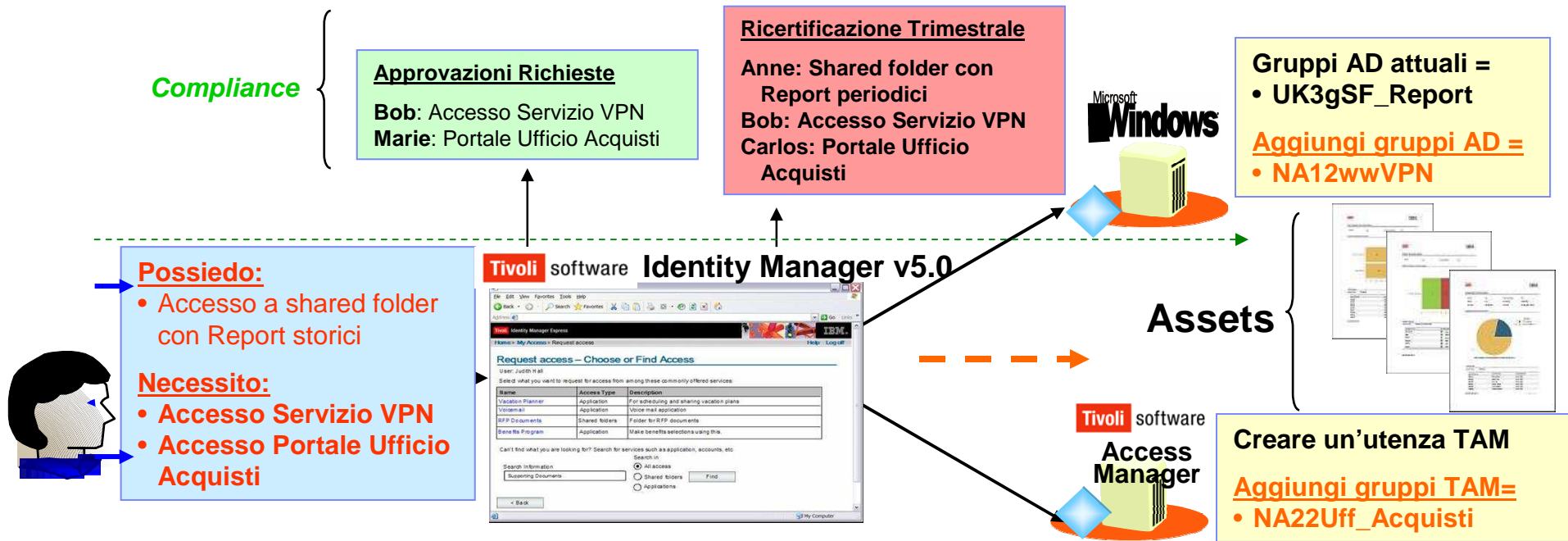
- Politiche “controllate” durante la **riconciliazione**
- TIM può “annullare” cambiamenti **non autorizzati** eseguiti dagli amministratori locali
- La Riconciliazione identifica gli account “**orfani**” (adopt, suspend, etc)





# Gestione degli Accessi ai Servizi, Non Solo utenze IT

## Access Entitlements: Flusso tipico semplificato (Esempio)



- Le persone richiedono accessi a servizi significativi, **non utenze IT-centriche** od utenze basate su parametri – è una **visione orientata al servizio offerto** esempio..”accesso al Portale XYZ Ufficio Acquisti”
- Workflow di Approvazione e Ricertificazione** può essere definito al livello dell’asset (accesso)
- Sono forniti in TIM report di audit orientati al **tracciamento degli accessi ai servizi**

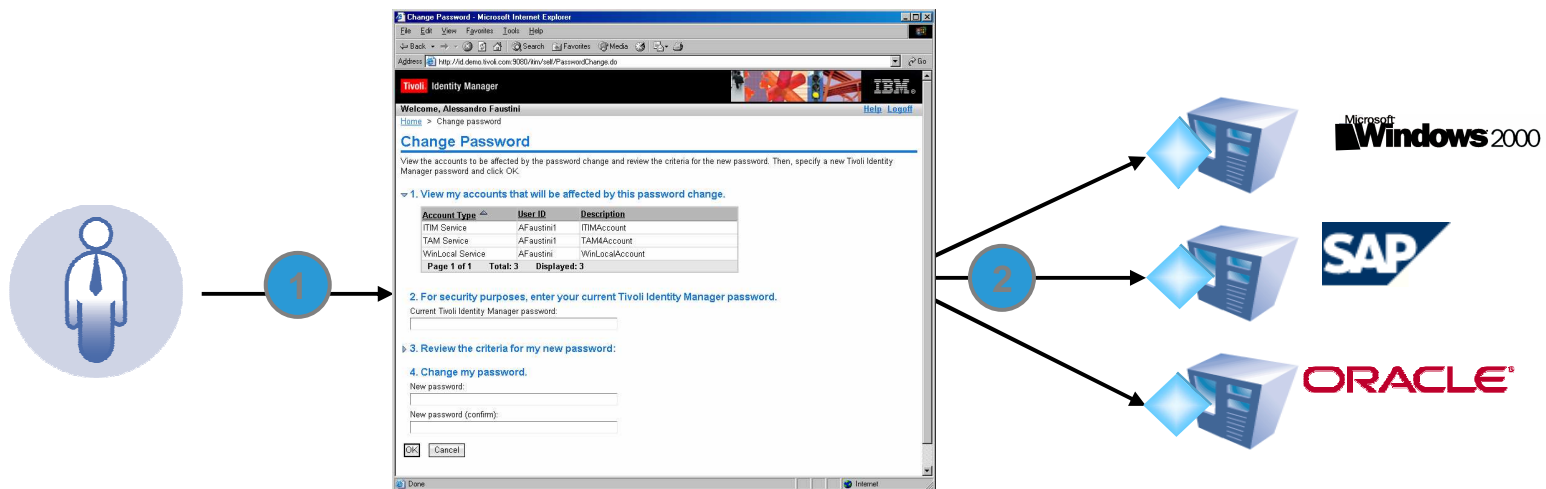






# Self Service: riduce le chiamate all' Help Desk

- Gli utenti possono (se autorizzati) editare le proprie informazioni personali
- I cambiamenti possono essere rivisti/approvati attraverso workflow di approvazione
- Challenge Response e Password Synchronization
- Reverse password synchronization per alcune piattaforme





# Funzionalità di Self-Care facilmente adattabili alle esigenze aziendali

**Web Interface per gli utenti finali** (esterna alla Web administration console)

Fornisce un **semplice**, ed **amichevole** interfaccia web; riducendo i costi di training per gli utenti finali



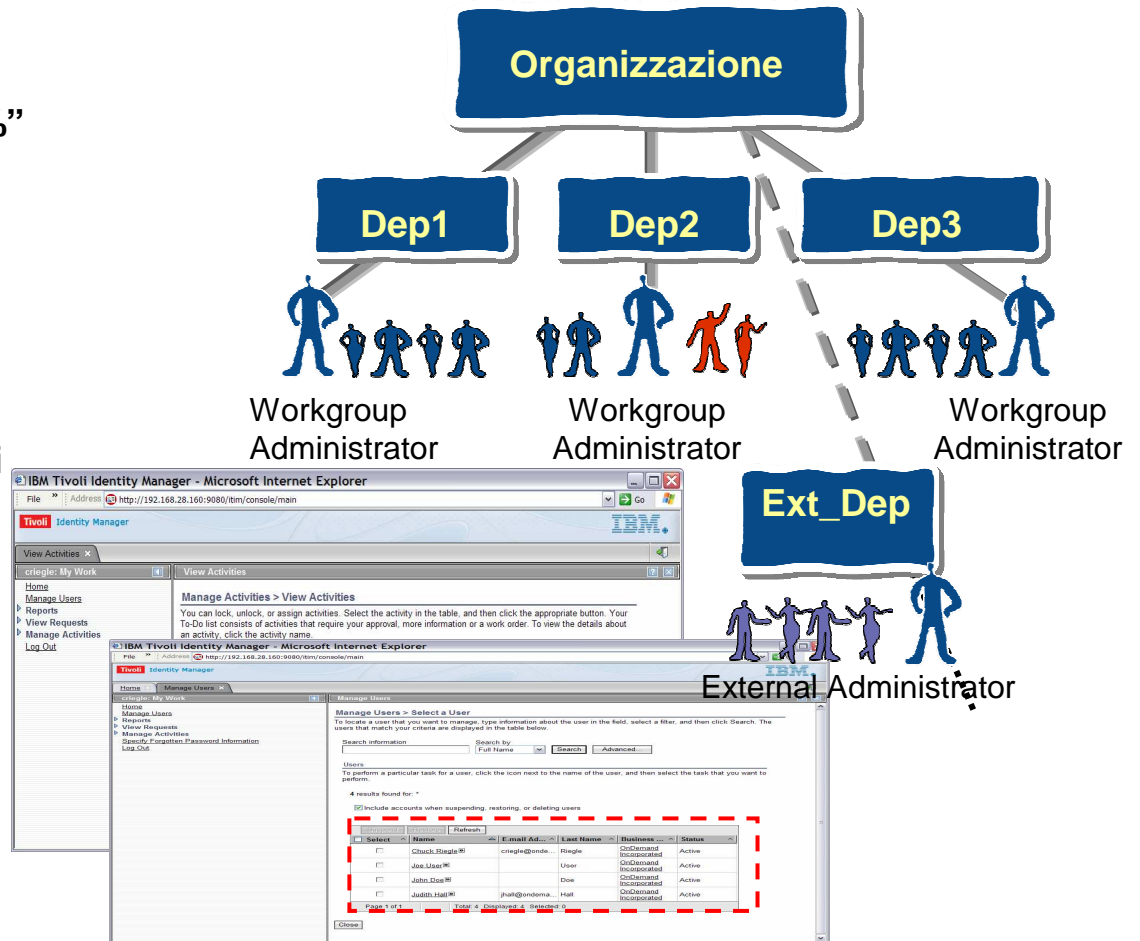
**BASTA PARLARE INIZIAMO A FARE**

© 2008 IBM Corporation



# L'Amministrazione delegata fornisce l'efficienza della centralizzazione mentre consente di mantenere il controllo nelle mani degli esperti

- **Centralizzare dove ha senso "circa l'80%"**
  - Politiche di sicurezza critiche
  - Task amministrativi ripetitivi
  
- **Muovere il controllo vicino ai decision maker**
  - La responsabilità deve rimanere presso i local manager i gli owner delle risorse
  - Migliorare la scalabilità
  - Aumentare la velocità
  
- **Distribuire il carico delle Approvazioni**
  - Bulk approve/reject
  - Task di lock o di delega





# TIM Console Web di Amministrazione – Viste Personalizzate

IBM Tivoli Identity Manager - Microsoft Internet Explorer

Address: http://192.168.28.160:9080/itim/console/main

Vista3 •Report

Home

jbenson: My Work

Home

Home

Reports

- Requests Reports
- User and Accounts Reports
- Services Reports
- Audit and Security Reports
- Custom Reports

View Requests

- View Pending Requests by User
- View All Requests by User
- View Pending Requests by Service
- View All Requests by Service
- View All Requests

Log Out

Welcome

Select your tasks from the table below

Common Tasks

<a href="#">Run User and Accounts Report</a>	Run various user and accounts reports.
<a href="#">Run Custom Report</a>	Run custom reports.
<a href="#">Run Services Report</a>	Run various reports for selected service or services.
<a href="#">Run Audit and Security Report</a>	Run audit and security related reports.
<a href="#">Run Requests Report</a>	Run various user requests reports.
<a href="#">View Pending Requests by Service</a>	View pending requests on selected service or services.
<a href="#">View All Requests</a>	View requests submitted to the system, pending or completed requests.





# Report con Tivoli Identity Manager

## Report Richieste (Account ed Access)

- Operazioni UtENZE
- Operazioni UtENZE eseguite da un individuo
- Approvazioni e Reject
- Report delle operazioni
- Approvazioni Pending
- Report approvazioni reject
- Report per Persone

## Report Persone ed utenze

- Report UtENZE / Accessi
- Report Ricertificazioni pending UtENZE/Accessi
- Accessi per un Individuo
- UtENZE per un Individuo
- UtENZE individuali su base ruolo
- Report per il change history di ricertificazione \*\*
- Individui sospesi

## Report di audit e di Sicurezza

- Access Control Information {ACIs} Access Report
- Eventi di Audit \*\*
- UtENZE dormienti
- Entitlements assegnato ad un individuo
- UtENZE non-Compliant
- UtENZE Orfane
- Politiche
- Politiche che governano un ruolo
- Report delle politiche di ricertificazione \*\*
- UtENZE Sospese

## Report sui Servizi (target gestiti)

- Statistiche di riconciliazione
- Riassunto delle utENZE per un servizio

**Recertification Change History Report**

Owner	Account ID	Service Name	Access Name	Recertifier	Recertification Date	Recertification Response	Action Taken	Justification
Jan Kirchauer	kirchauer	Accounting Application Server - WTN		Mike Stevens	30/08/2007 17:02	Reject	Suspend Success	contract expires on Sept. 1, 2007
Jan Kirchauer	kirchauer	Accounting Application Server - WTN		Mike Stevens	30/08/2007 17:15	Approve	Administrative Certify Success	Im's contract has been renewed.
Judith Hill	jhill	Accounting Application Server - WTN		James Smith	24/08/2007 07:45	Approve	Certify Success	

**Welcome**  
Select your tasks from the table below

**Common Tasks**

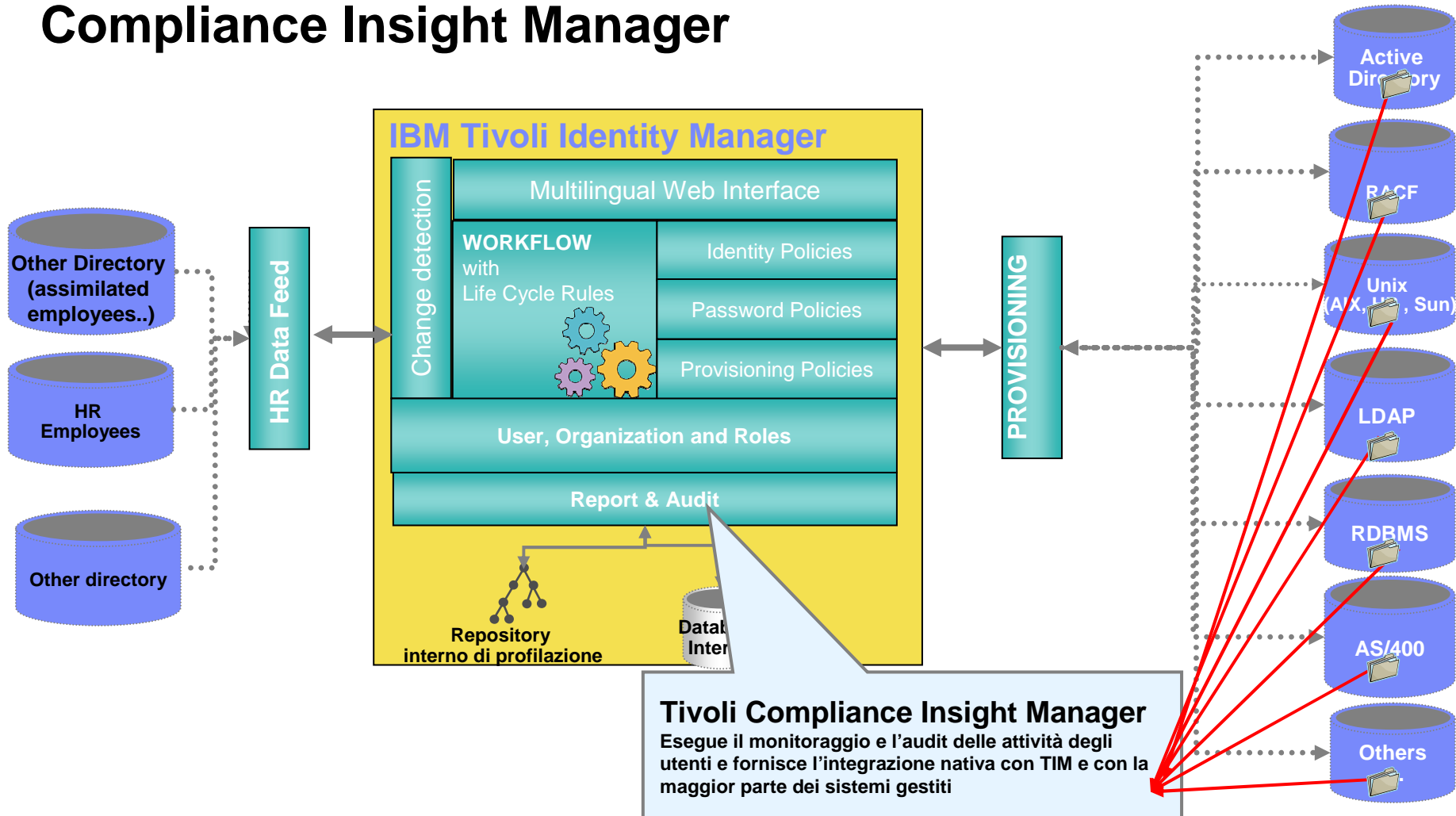
- [Run User and Accounts Report](#) - Run various user and accounts reports.
- [Run Custom Report](#) - Run custom reports.
- [Run Services Report](#) - Run various reports for selected service or services.
- [Run Audit and Security Report](#) - Run audit and security related reports.
- [Run Requests Report](#) - Run various user requests reports.
- [View Pending Requests by Service](#) - View pending requests on selected service or services.
- [View All Requests](#) - View requests submitted to the system, pending or completed requests.

**\*\* sia per informazioni di utenze ed accessi**





# Tivoli Identity Manager: Integrazione dell'Audit con Tivoli Compliance Insight Manager





# Agenda

Gestione delle identità

Soluzione Tivoli per l'Identity Management

Controllo degli accessi

Autenticazione, Autorizzazione e *Single Sign-On*



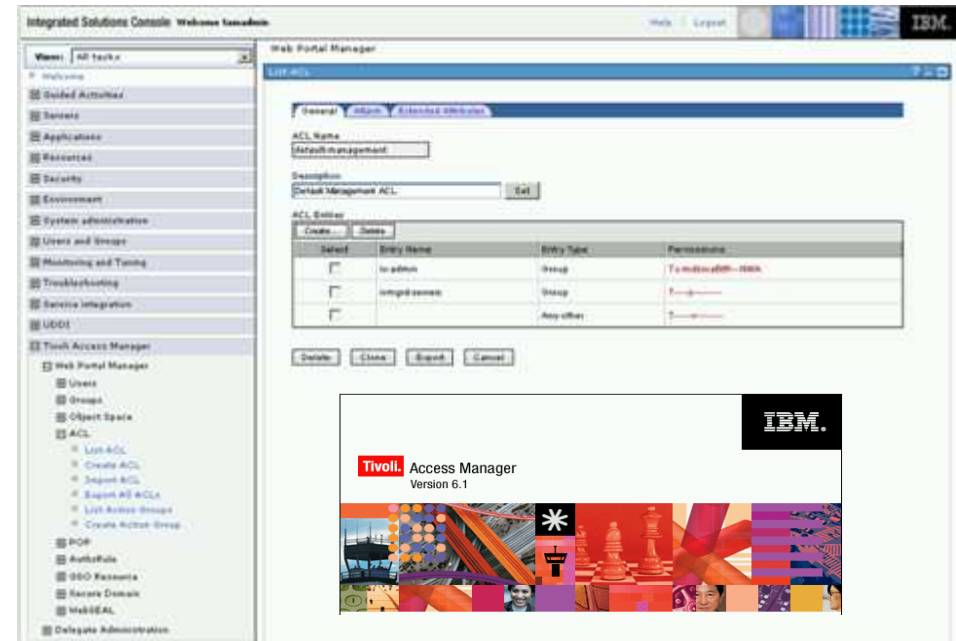


# Tivoli Access Manager

IBM Tivoli Access Manager è un software di sicurezza per il controllo accessi nativamente integrato con Tivoli Identity Manager, che consente di gestire centralmente le fasi di autenticazione e autorizzazione sfruttando il concetto di policy di sicurezza

## Caratteristiche principali

- Fornisce un servizio centrale di autenticazione e autorizzazione alle applicazioni aziendali
- Supporta ed è in grado di interagire con un'ampia varietà di ambienti eterogenei
- Supporta ed è a sua volta basato su tecnologie standard di mercato
- Consente elevata flessibilità nel disegno
- E' in grado di realizzare un sistema di controllo accessi basato sui ruoli
- Common Criteria certified



*Tivoli Access Manager for e-Business*

*Tivoli Access Manager for Enterprise Single Sign-On*

*Tivoli Access Manager for Operating Systems*



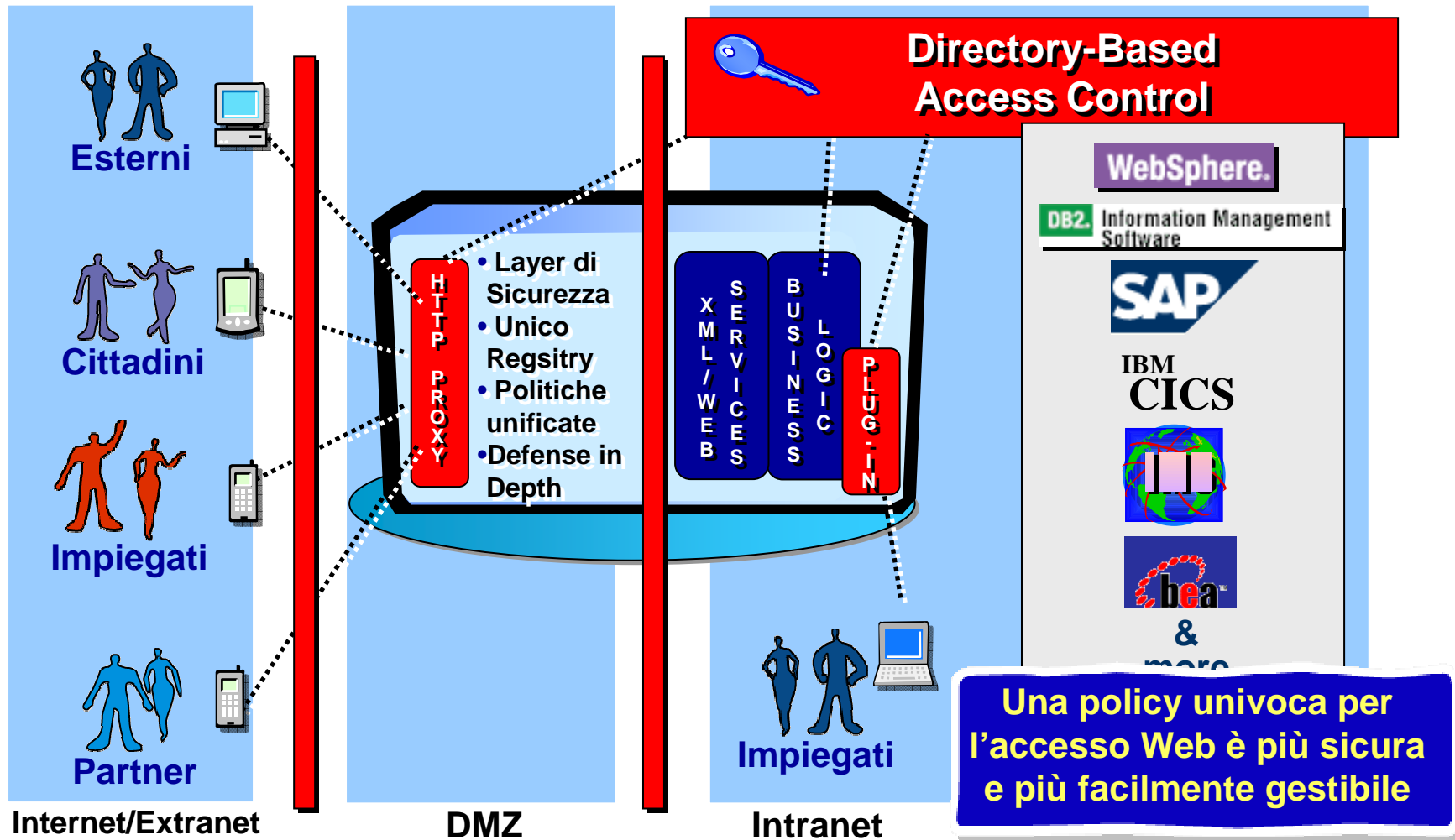
BASTA PARLARE **INIZIAMO A FARE**

© 2008 IBM Corporation

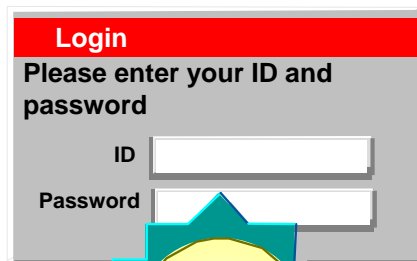




# Tivoli Access Manager for e-Business Overview



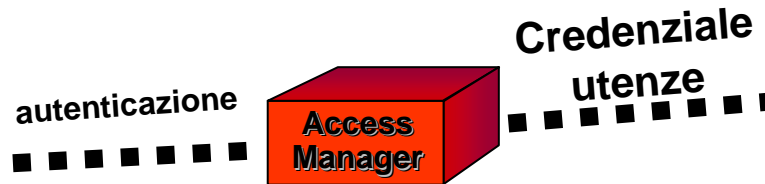
# Come è possibile autenticare un utente?



**Login**  
Please enter your ID and password

ID

Password



## ► Provare l'identità del chiamante

- Basic authentication
- Forms-based authentication
- X.509 Certificate
- Kerberos ticket
- RSA SecurID Token
- Mobile device
- Altre attraverso EAI (External Authentication Interface)

## ► Opzioni Avanzate

- Step-up authentication
- Forced re-authentication
- Switch user

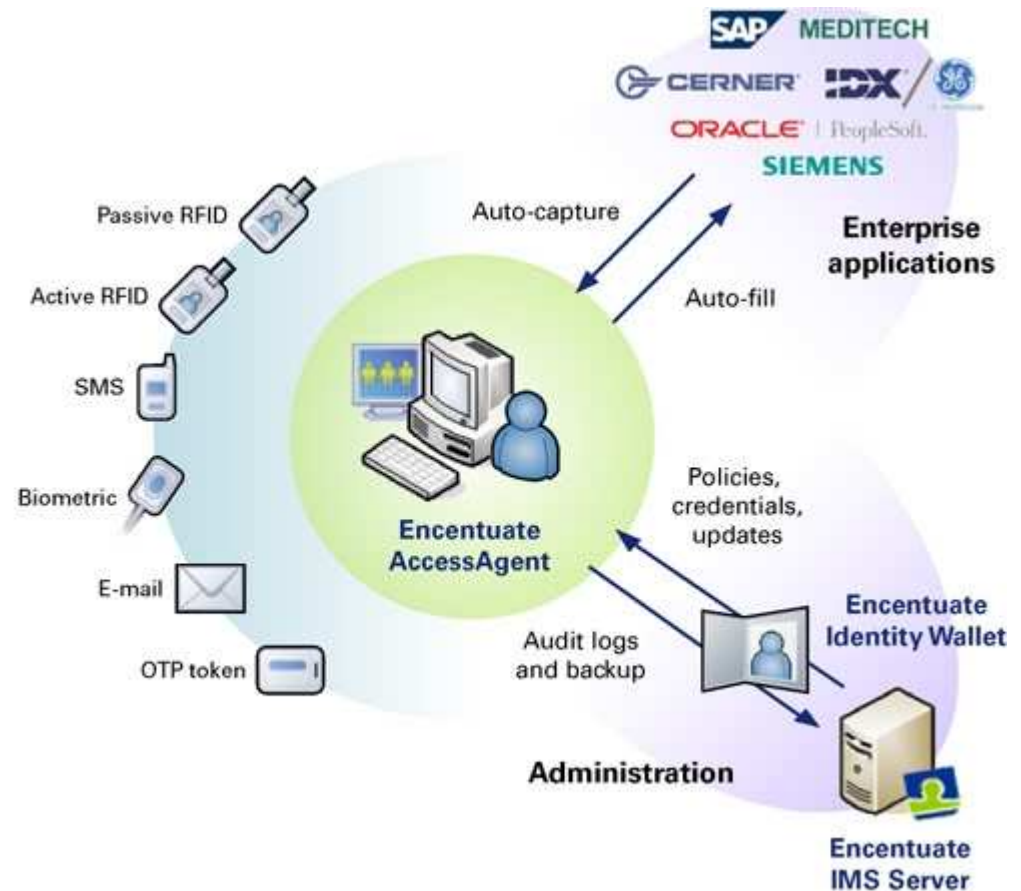




# Tivoli Access Manager for Enterprise Single Sign-On

- Enterprise Single Sign-On per tutte le tipologie di applicazioni client-server (emulatore di terminale, Windows, Java)
- Autenticazione Two-Factor e tracciamento dell'accesso utente
- Fast user switching
- Audit e Policy Management centralizzato
- Integrazione con Tivoli Identity Manager
- Nessuna modifica applicativa richiesta

Second factors

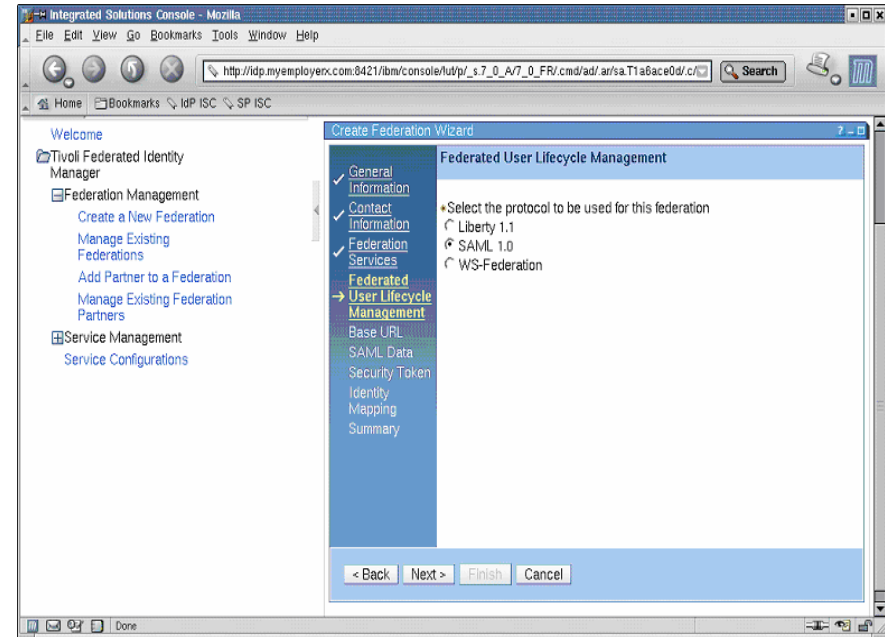




# IBM Tivoli Federated Identity Manager

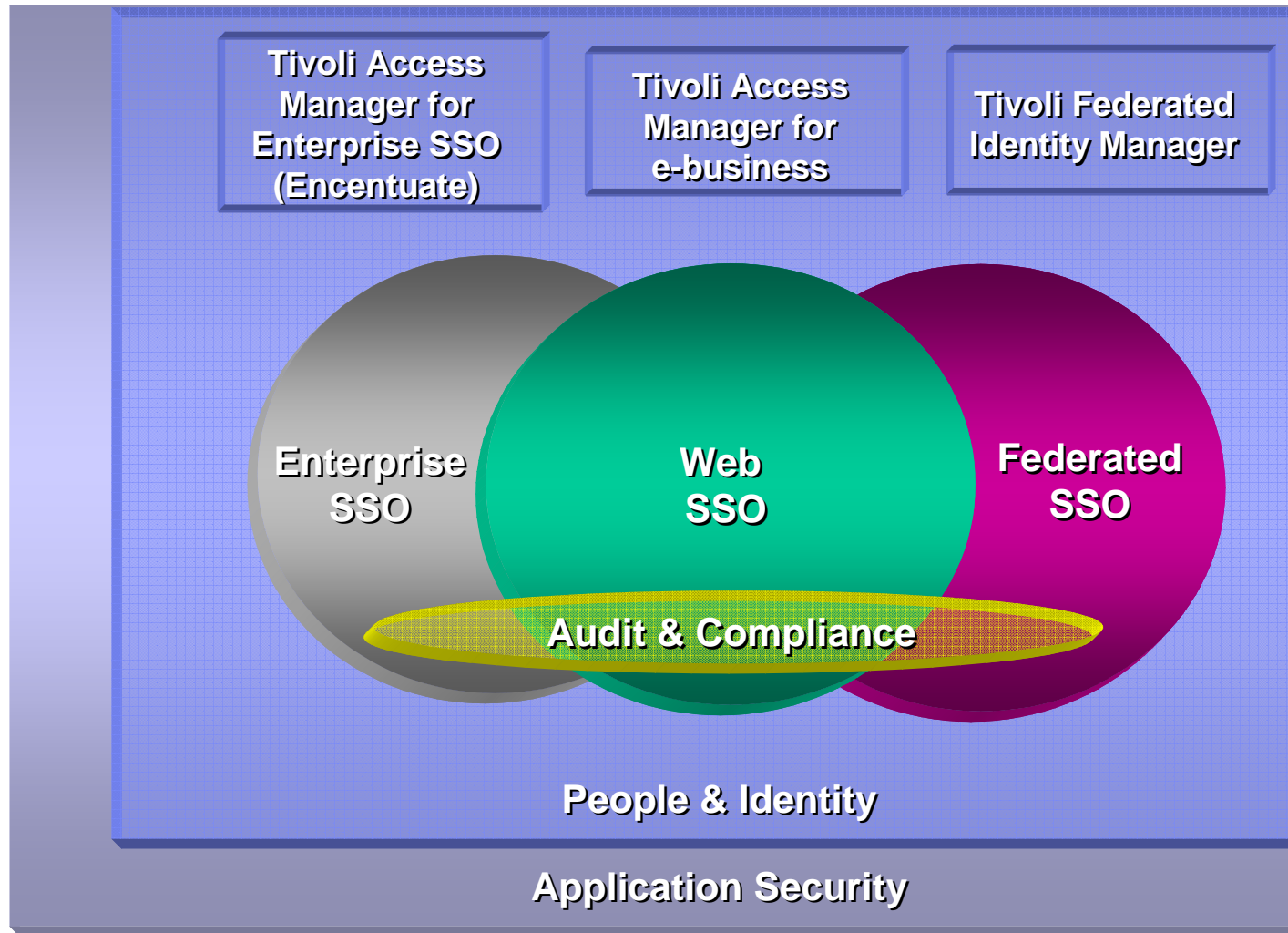
Il Tivoli Federated Identity Manager è una soluzione basata su standard per realizzare scenari di Federated Single Sign-On, relazioni di trust management e sicurezza in ambienti web services e SOA.

- **La più completa soluzione per il supporto di scenari di Federated SSO**
- **Supporta tutti i protocolli standard di federazione inclusi:**
  - **SAML 1.0, 1.1, 2.0, Liberty ID-FF 1.x (Compliant), WS-Federation**
- **Web Services & SOA Security Management**
  - **Supporto per complessi scenari di mediazione ed identity mapping**
- **Fornisce la sicurezza come servizio**
  - **autenticazione (WS-Federation & WS-Trust)**
  - **amministrazione (provisioning)**





# La soluzione completa per il Single Sign-On





# Tivoli - Certificazioni Common Criteria

## ▪ Tivoli Access Manager for e-Business

- Common Criteria EAL3+: BSI-DSZ-CC-0343-2007 [www.commoncriteriaportal.org](http://www.commoncriteriaportal.org)
- Certified with SAP

## ▪ Tivoli Identity Manager

- Common Criteria EAL3: BSI-DSZ-CC-0237-2006 [www.bsi.de](http://www.bsi.de)
- Certified with SAP

## ▪ Tivoli Directory Server

- Common Criteria EAL4+: BSI-DSZ-CC-0283-2006 [www.commoncriteriaportal.org](http://www.commoncriteriaportal.org)

## ▪ Tivoli Directory Server

- LDAP Certified v2 The Open Group [www.opengroup.org](http://www.opengroup.org)





# Grazie



BASTA PARLARE **INIZIAMO A FARE**

© 2008 IBM Corporation