IBM Software Group

Tivoli Security

- Tivoli Spring Update -

Tivoli software

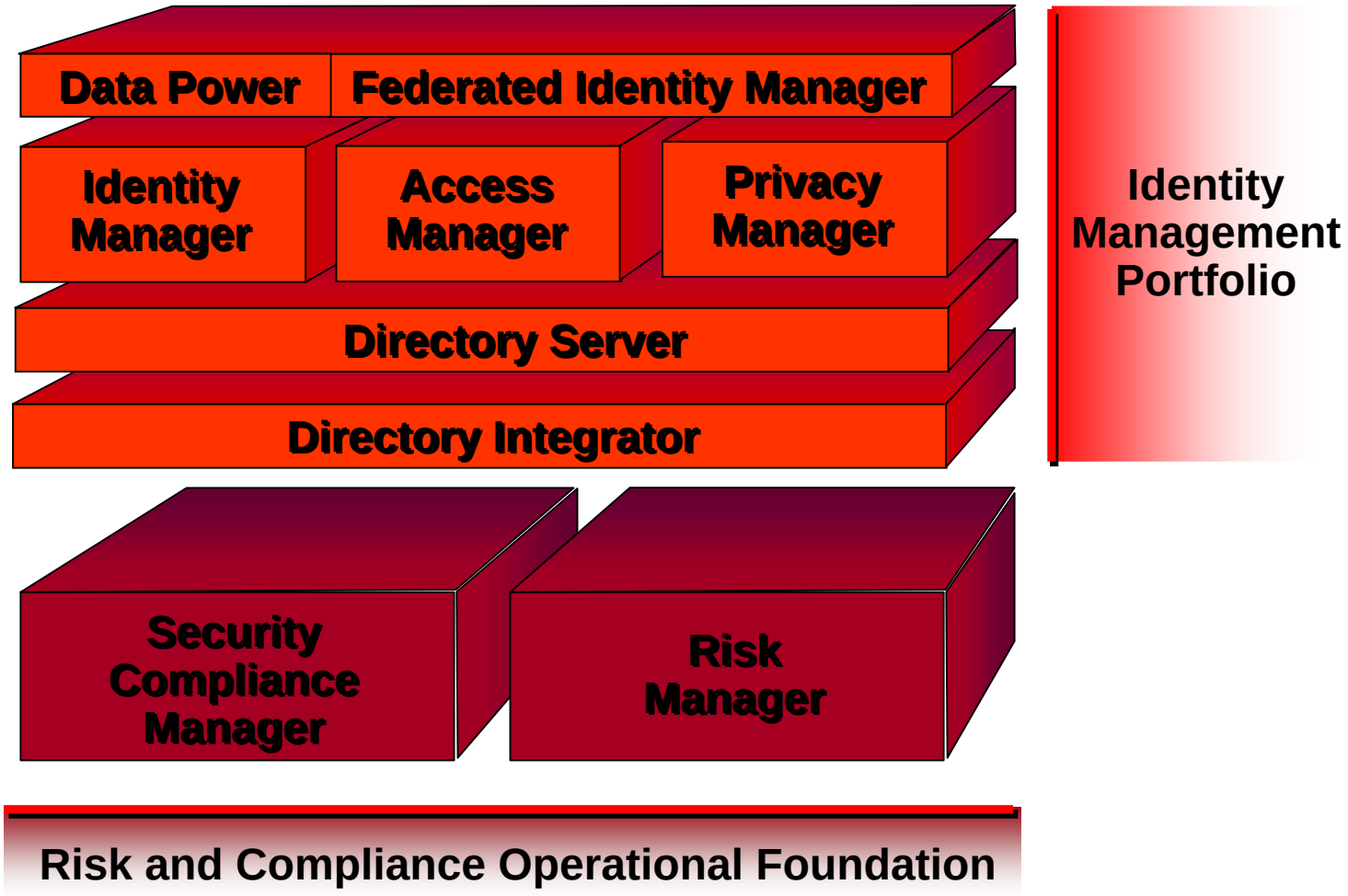
ON DEMAND BUSINESS

Pär Kidman
Certified Consulting IT Specialist
IBM Software Group
par.kidman@se.ibm.com

Agenda

- Lite kort om våra lösningar inom Tivoli Security
- Tivoli Identity Manager
- Tivoli Access Manager
- Tivoli Federated Identity Manager

Våra lösningar…



IBM Software Group

Tivoli Identity Manager

Tivoli software

ON DEMAND BUSINESS

Problemområden…

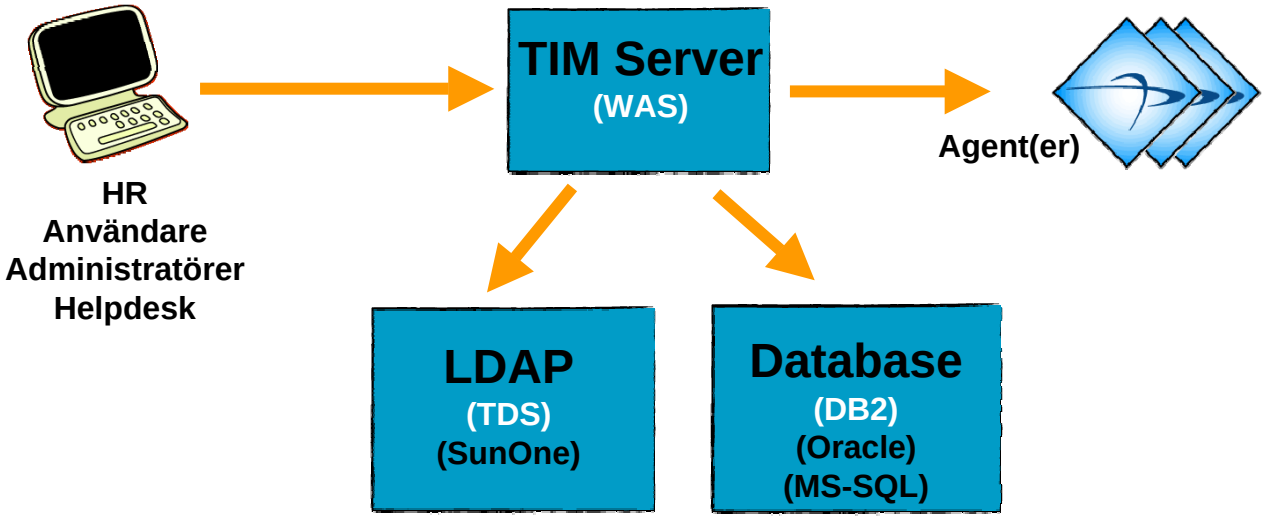
- **Behörighetstilldelning (provisioning)**
  - **Är alla konton giltiga på alla målsystem? – Ägarlösa konton m.m.**
  - **Har alla konton rätt behörigheter? - På alla system?**
  - **Hur ser man till att det förblir så?**
- **Produktivitet**
  - **Får användarna rätt konton och behörigheter på ett effektivt sätt?**
- **Kvalitet**
  - **Följer alltid man säkerhetspolicy och regelverk vid behörighetstilldening på alla applikationer och system?**
- **Spårbarhet / revision**
  - **Kan jag bevisa vad som har hänt vid en revision? - För alla behörighetsrelaterade transaktioner?**

Tivoli Automatiserar behörighetstilldelningen

- Gör det möjligt att validera behörigheter och åtkomster centralt
  - Säkerhetspolicy'n efterlevs
- Tilldelar effektivt nya konton och behörigheter
  - Automatisera godkännandeflöden (workflows)
- Hittar och korrigerar automatiskt felaktiga konton och behörigheter
  - "Closed-loop policy management"

Tivoli Identity Manager (TIM)

- **TIM servern styr alla delar:**
  - **Tilldelning av behörigheter, Arbetsflöden, Självbetjäning, Administration m.m.**
- **LDAP lagrar all person- och kontorelaterad information**
- **Databasen lagrar transaktioner som sker i systemet**
- **Agenterna utför åtgärder på målsystemen**



Några av våra agenter….

- IBM Access Manager
- IBM AIX
- IBM AS/400
- IBM Lotus Notes
- IBM RACF
- BMC Remedy
- Cisco ACS
- Computer Associates ACF/2
- Computer Associates Top Secret
- Documentum
- Hewlett Packard HP-UX
- Hewlett Packard Tru64 Unix
- Hewlett Packard VMS
- LDAP-X
- Linux
- Microsoft Exchange 5.5
- Microsoft SQL
- Windows NT 4.0
- Windows 2000 Server with Active Directory, Exchange 2000 (on Windows 2000), Windows 2003 Enterprise Edition and Exchange 2003 (on Windows 2003 Enterprise Edition)
- Windows 2000 Server with Active Directory and Windows 2003 Server with Active Directory
- Novell GroupWise
- Novell Netware NDS/eDirectory
- Oracle versions
- Oracle ERP
- PeopleSoft PeopleTools
- Peregrine ServiceCenter
- RSA ACE/Server
- SAP
- SUN Solaris
- Sybase Server
- IBM DB2 UDB
- Universal Provisioning Agent

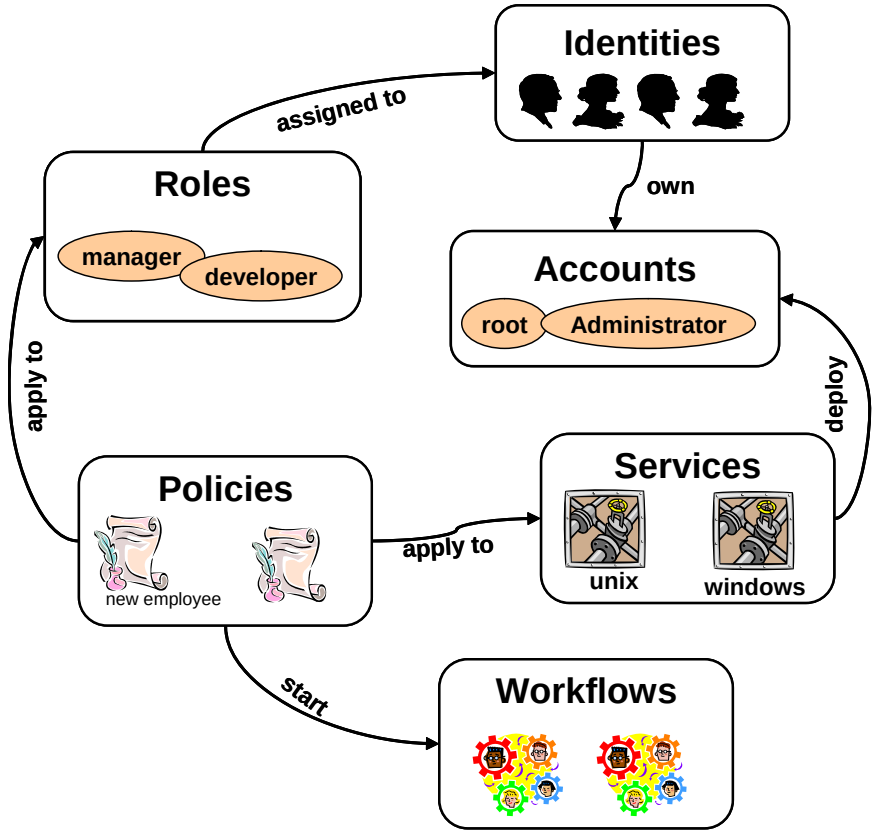
Det finns även ett antal agenter som säljs som en tjänst av IBM och våra partners (ex. Cisco CallManager)

Tivoli Directory Integrator – För att kunna skapa egna agenter

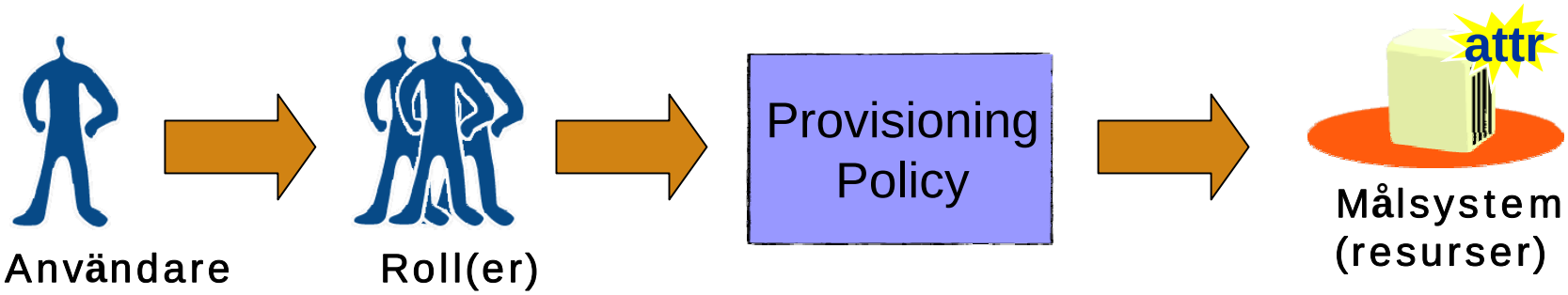
ITIM: automatisk, rollbaserad användarhantering

Automatiserar helt tilldelning och borttag av behörigheter

- **Behörigheter ändras automatiskt när man byter roll / tjänst**
- **Sammlar konton och behörigheter till rätt grupp av användare**
- **Minskar administrationen och ökar effektiviteten**
- **Tar automatiskt bort konton som inte längre behövs när användaren byter arbetsuppgifter eller slutar**

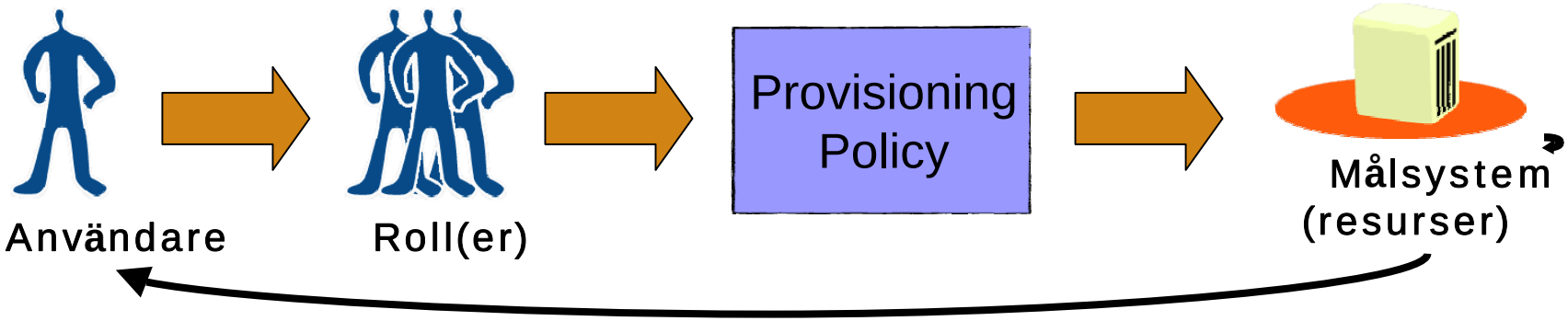


Modellen för tilldelning av behörigheter



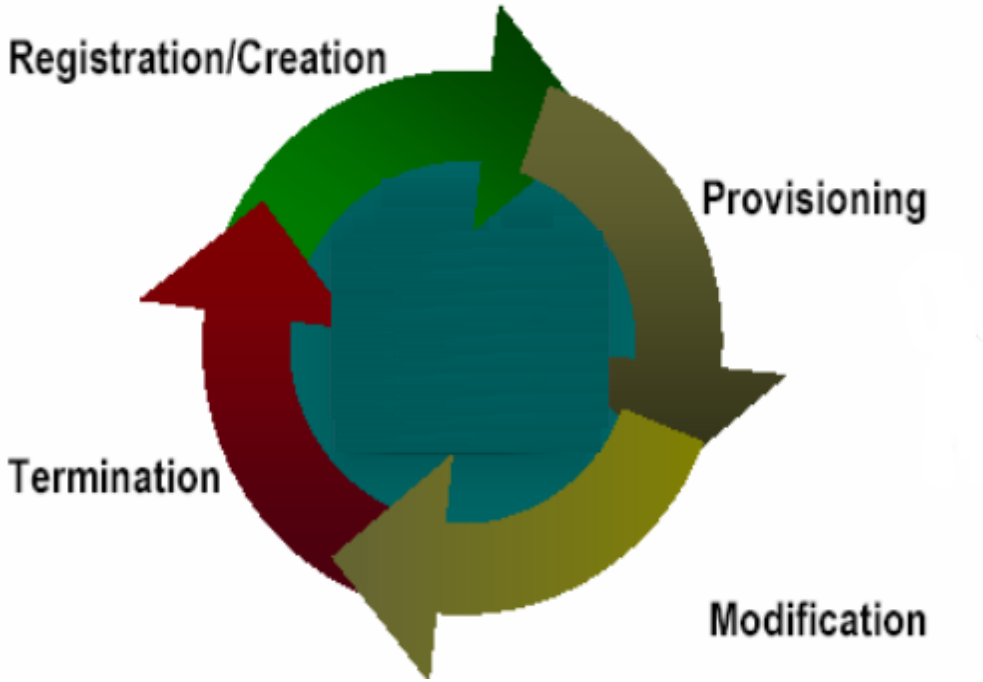
- **Användare tilldelas roller baserat på ansvarsområden**
- **Medlemmar i roller får tillgång till målsystem m.h.a. en “Provisioning Policy”**
- **“Provisioning Policies” kan även definiera de attribut ett konto skall ha (förnamn, efternamn, telefonnummer, grupptillhörighet, etc)**

“Reconciliation” jämför vad som finns med vad som borde finnas



- **Vid “reconciliation” kan TIM säkerställa att konton och rättigheter är enligt policy**
  - **TIM kan korrigera otillåtna förändringar gjorda lokalt på målsystemen (t.ex. av en lokal administratör)**
- **Reconciliation identifierar “herrelösa” konton (s.k. Orphan Accounts)**
  - **Kopplar konton till giltiga användare samt spärrar, aktiverar eller tar bort ogiltiga konton**

Lifecycle Management

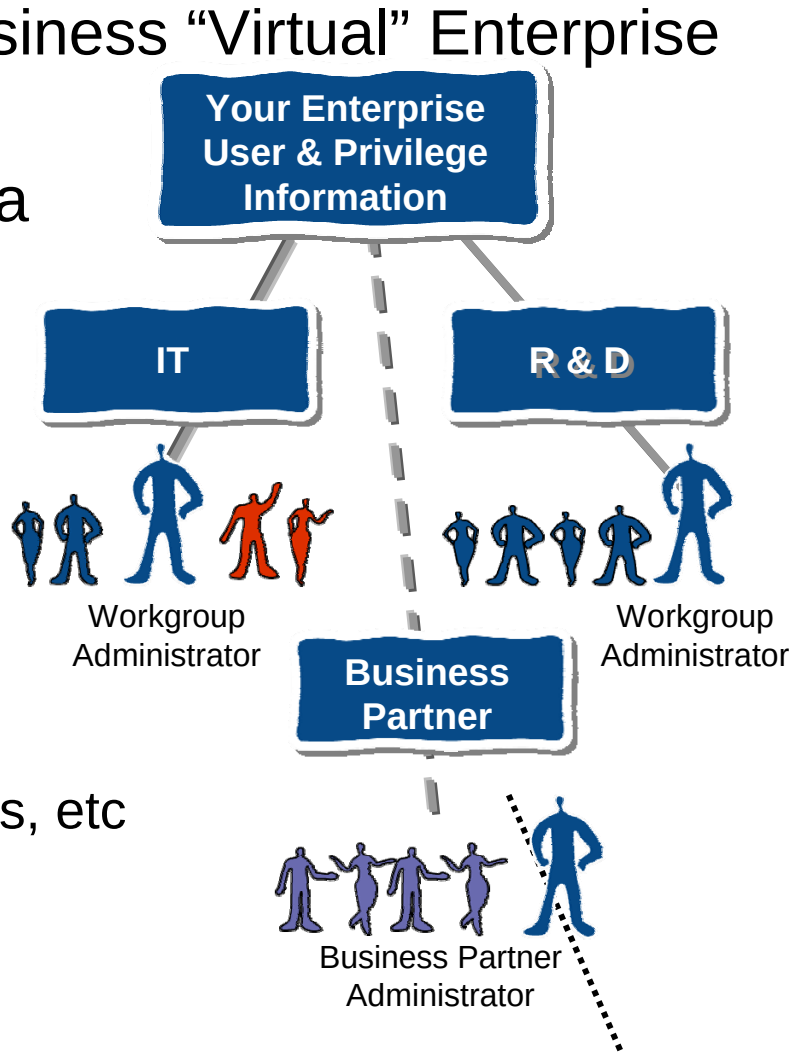


“Lifecycle Management” hanterar identiteter, konton och behörigheter från att de skapas, ändras och tas bort…

Exempel:
- **Självregistrering**
- **Flytt inom organisationen**
- **Omcertifiering av användare**

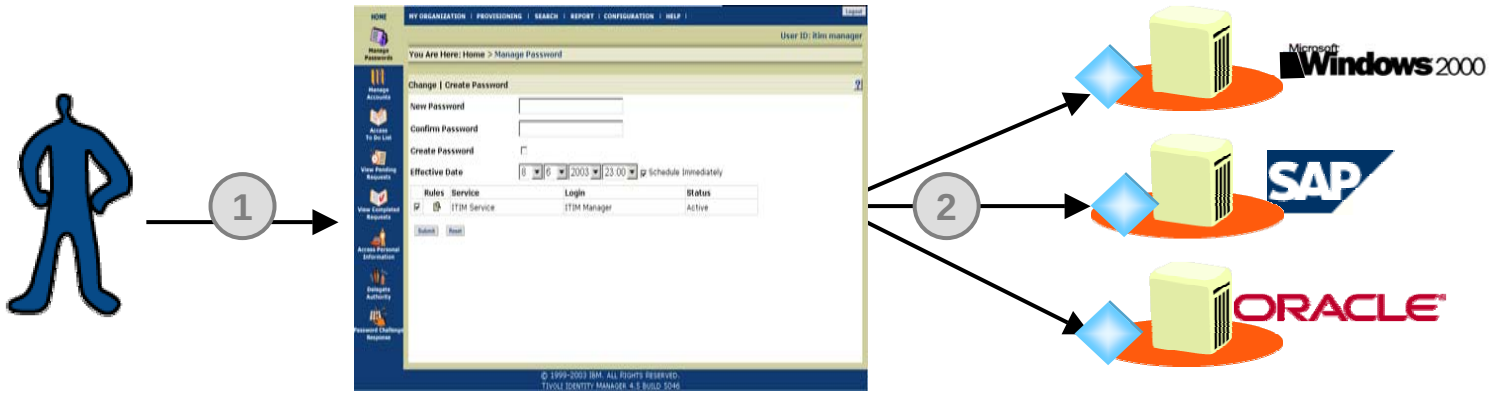
Delegering av administration

- "Junior" administratörer kan hantera användare och attribut
- Möjlighet att begränsa interna TIM resurser
  - Services, Provisioning Policies, Reports, etc



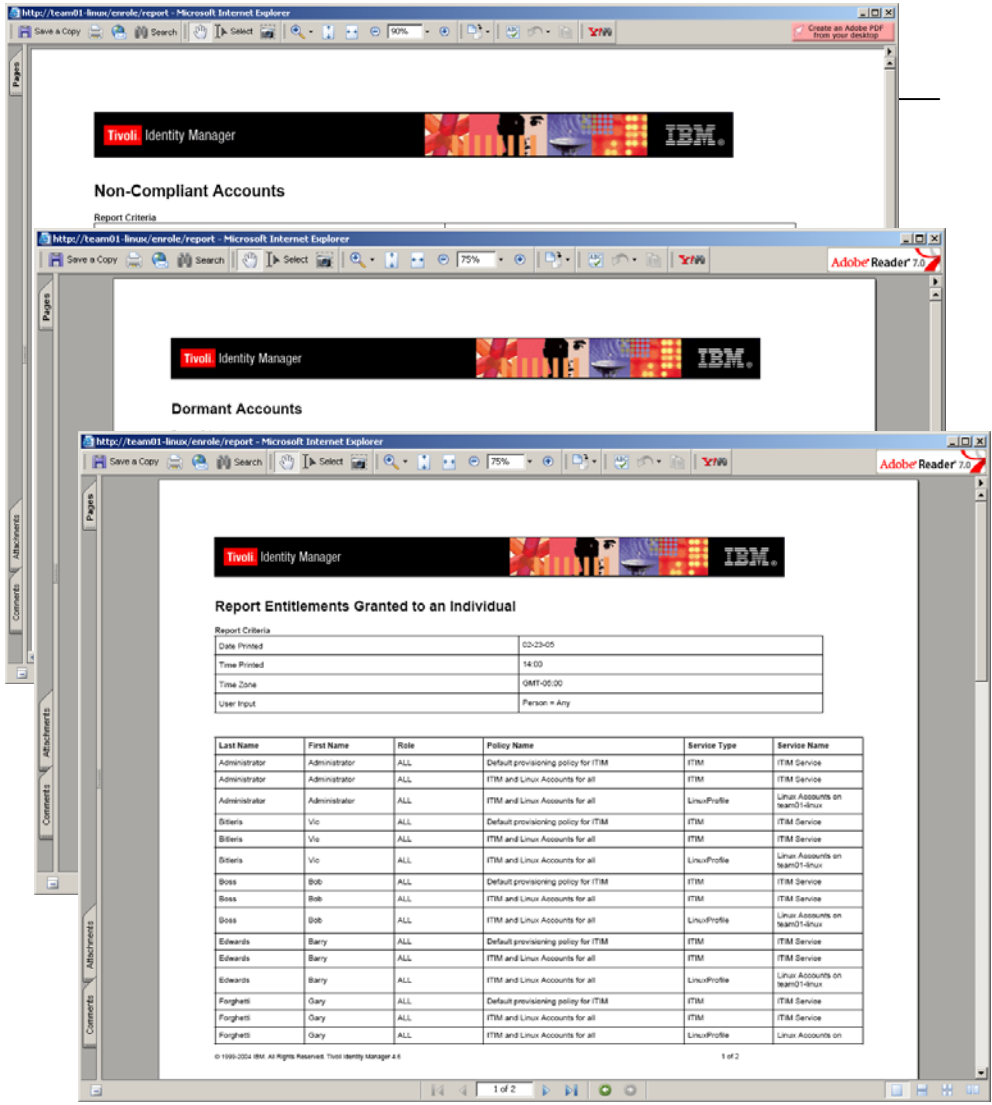
Självbetjäning / lösenordssynkronisering minskar antalet samtal till Help Desk

- Användare kan hantera egna attribut (address, titel, etc)
- “Challenge response” när man glömt sitt lösenord
- Förändringar kan verifieras och attesteras m.h.a. arbetsflöden
- Upphämntning av lösenord
- Lösenordssynkronisering mot alla målsystem
- Lösenordsbyten i AD, AIX, RACF och Tivoli Access Manager kan fångas upp av TIM och synkroniseras ut till alla målsystem



Integrerat rapporteringsvertyg

- 22 färdiga rapporter
- Möjlighet att anpassa och skapa egna rapporter
- Möjlighet att styra vem får se vilka rapporter
- Acrobat Format för att enkelt kunna se rapporter
- Kan exporteras I CSV format
- Stöd för Crystal Reports



IBM Software Group

Tivoli Identity Manager Express

Tivoli software

ON DEMAND BUSINESS

TIM Express i korthet

- Enkel att installera, implementera och administrera
- Innehåller grundläggande funktioner för användaradministration
- TIM Express kan användas för upp till 5000 användare

TIM Express funktionalitet – en överblick

- **Funktionalitet:**
  - **Request-baserad kontotilldelning med godkännandeflöden**
  - **Självbetjäning för slutanvändare**
  - **Färdigpaketerad med rapportering**
  - **Anpassade användargränssnitt**
  - **Förinstallerade/bundlade adaptrar**

TIM Express funktionalitet

- **Request-baserad kontotilldelning med godkännandeflöden**
  - **Förenklar processer avseende tilldelning, ändring, och borttagande av användarkonton, med inbyggd audit-funktionalitet. TIM Express automatiserar processer som t. ex. när användare begär access till en ny tjänst, då meddelas berörda chefer för godkännande, kompletterande information kan hämtas in och konton sätts upp i målsystemet. Systemägare, chefer eller administratörer kan direkt ta bort onödiga/felaktiga konon när användare byter jobb alternativt kräva om-certifiering med automatik.**

- **Självbetjäning för slutanvändare**
  - **Minska trycket på helpdesk genom att ge användarna tillgång till webinterface där de kan sköta sina lösenord och uppdatera personlig information. TIM Express låter även användarna synka sina lösenord på alla konton.**

TIM Express funktionalitet

- **Färdigpaketerad med rapportverktyg**
  - **Förenklar och spar tid/pengar vid revisioner och validering av konton. Rapporterna I TIM Express ger en konsoliderad vy över access rättigheter och loggade händelser inom användarhanteringen över samtliga system som omfattas.**
  - Följande rapporter ingår:
    - **Approval process report**
    - **Request report**
    - **Rejected requests report**
    - **Pending request report**
    - **Account report**
    - **Suspended person report**
    - **Dormant account report**
    - **Active account report**
    - **Services report**
    - **Reconciliation report**

TIM Express funktionalitet

- **Anpassade användargränssnitt**
  - **TIM Express har olika användargränssnitt för olika typanvändare, som bara visar den nödvändiga informationen för att respektive person skall kunna utföra sitt jobb. Det finns fem olika vyer, skräddarsydda för följande användartyper:**
  - **- Systemadministratörer**
  - **- Systemägare**
  - **- Helpdesk**
  - **- Chefer**
  - **- Slutanvändare**
  - **Man kan enkelt ändra på vad respektive användare tillåts göra I TIM Express. Olika funktioner kan enkelt slås på eller av genom att systemadministratören markerar eller avmarkerar funktioner I verktyget.**

TIM Express funktionalitet

- Förinstallerade/bundlade adaptrar
  - **TIM Express levereras med populära adaptrar för att göra den lätt att installera, implementera och förvalta. Vissa adaptrar installeras redan under TIM Express grundinstallation. Andra kommer bundlade med produkten.**
  - **TIM Express installerar vissa remote-adaptrar automatiskt (agentless). Fjärrkonfigurering (SSH) av dessa adaptrar med TIM Servern hjälper till att effektivisera implementationen. Följande adaptrar installeras med automatik:**

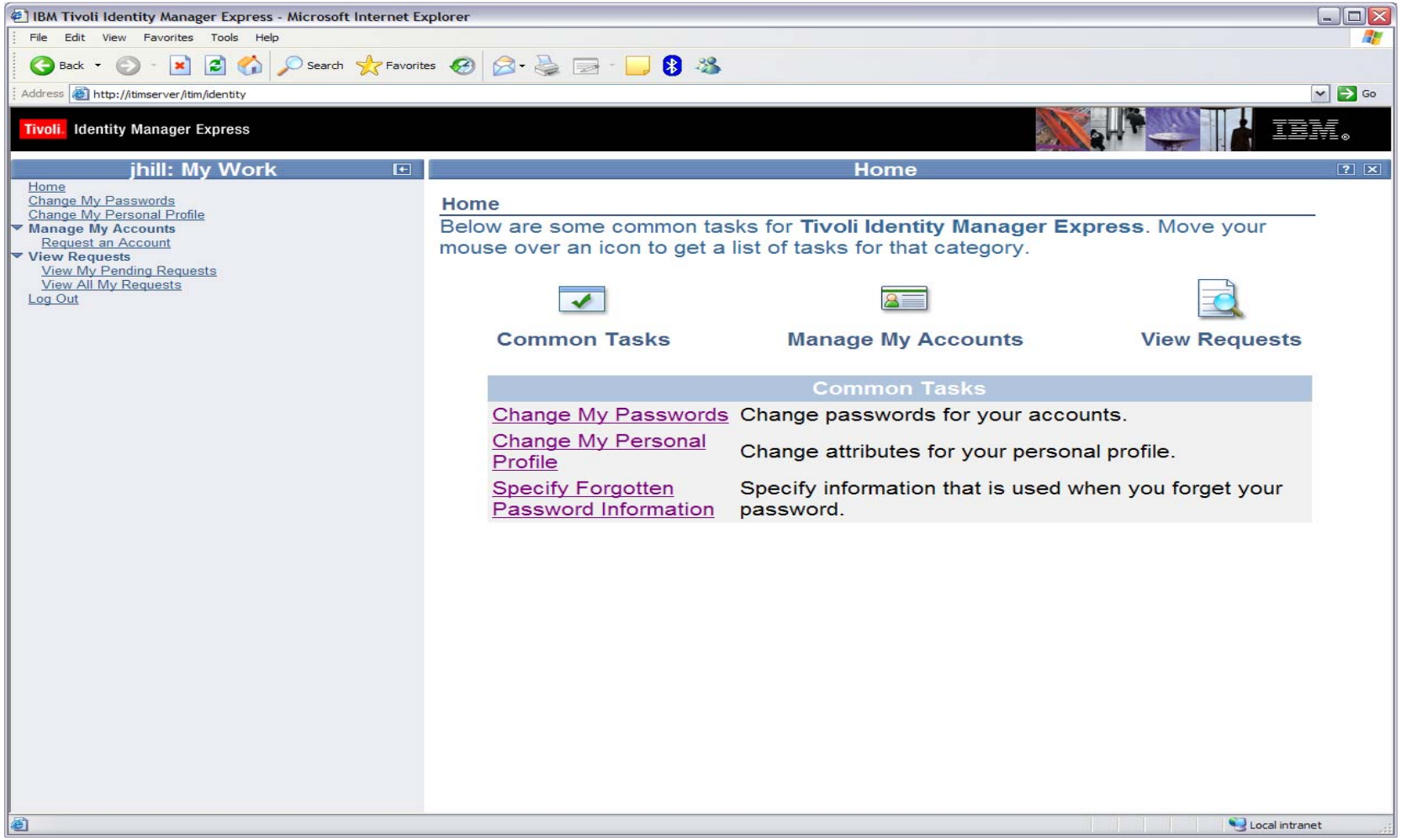
    LDAP, Solaris, AIX, RHEL, SuSe, HP/UX
  - **Några av de adaptrar som följer med i paketet är:**

    Active Directory, Tivoli Access Manager och Lotus Notes

TIM Express – Har anpassade vyer

- Systemadministratör
- Helpdesk
- Chefer
- Systemägare
- Slutanvändare

Exempel…


IBM Tivoli Identity Manager Express - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://itimserver/itim/identity
Go
Tivoli Identity Manager Express
IBM
jhill: My Work
Home
Change My Passwords
Change My Personal Profile
Manage My Accounts
Request an Account
View Requests
View My Pending Requests
View All My Requests
Log Out
Home
Home
Below are some common tasks for Tivoli Identity Manager Express. Move your mouse over an icon to get a list of tasks for that category.
Common Tasks
Manage My Accounts
View Requests
Common Tasks
Change My Passwords
Change passwords for your accounts.
Change My Personal Profile
Change attributes for your personal profile.
Specify Forgotten Password Information
Specify information that is used when you forget your password.
Local intranet

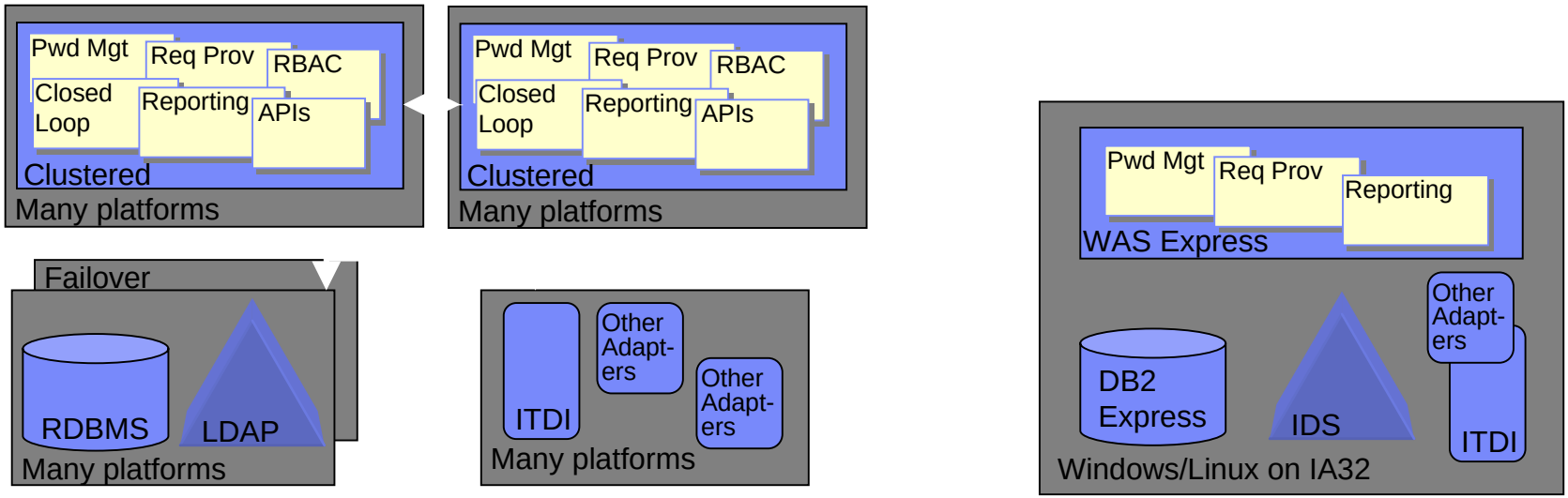
Skillnader mellan TIM och TIM Express

TIM

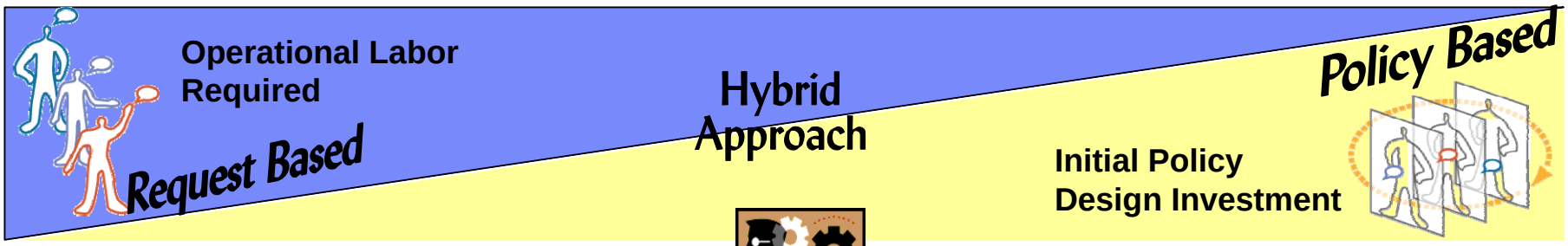
- Automated provisioning/de-provisioning
- Closed loop remediation, plus recertification
- Highly scalable, with high availability options
- Extensible workflow, reporting, and APIs
- For enterprise and medium sizes customers with advanced needs

TIM Express

- Request based provisioning
- Account recertification workflow
- All-in-one installer on single server
- Persona driven UI views and default settings
- For SMBs and departments/subsidiaries



När ska man välja TIM resp. TIM Express?



Manual

Profile: Primarily Knowledge Workers
Sample Industry: Computer Services
Sample Customer: IBM

Profile: Mixed Workforce
Sample Industry: Retail Banking
Sample Customer: ING

Automated

Profile: Primarily Homogeneous Workforce
Sample Industry: Distribution
Sample Customer: UPS

ITIM 4.6 with customization	ITIM 4.6
ITIM 4.6 Express	

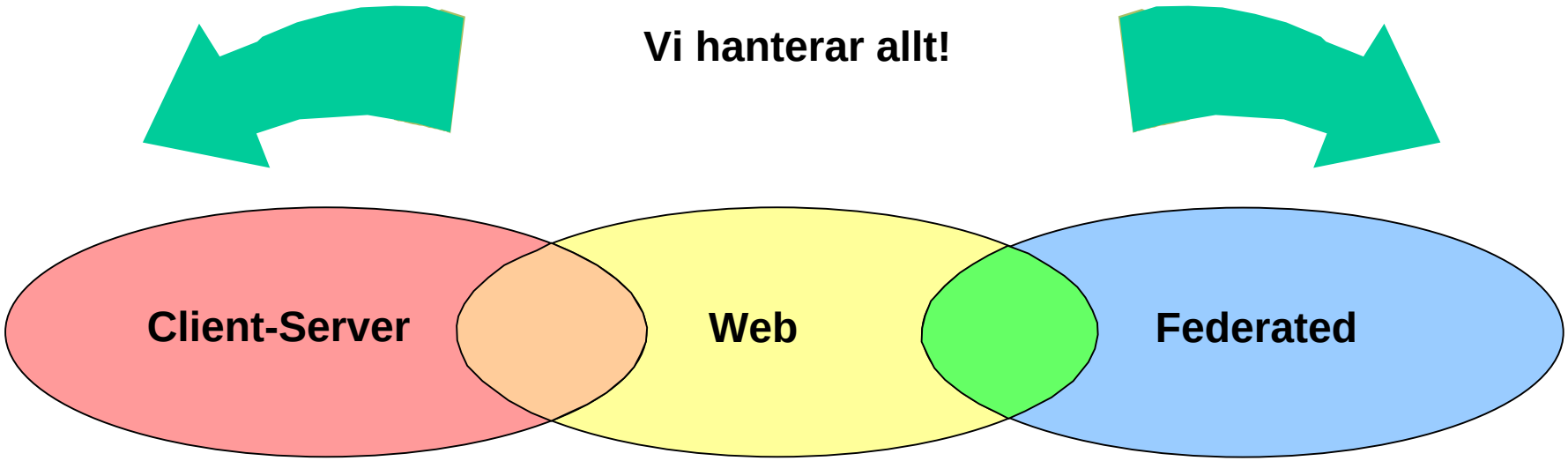
IBM Software Group

Tivoli Access Manager

Tivoli software

ON DEMAND BUSINESS

Ökad produktivitet: Single Sign-On

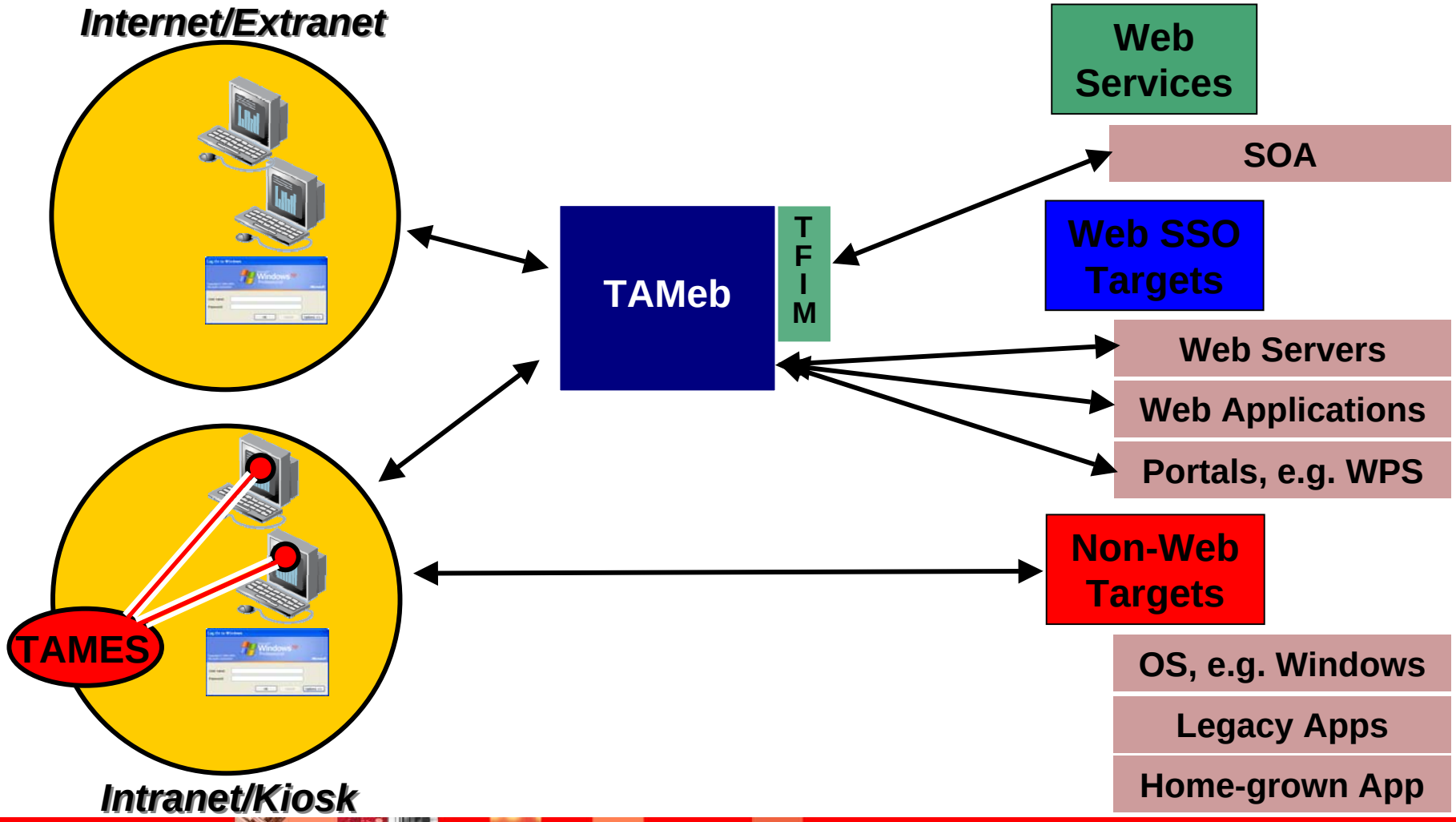


Tivoli Access Manager for e-business

Tivoli Access Mgr. for E-SSO

Tivoli Federated Identity Manager

Fullständig Single Sign-On



Tivoli Access Manager Familjen

- Tivoli Access Manager for e-business (TAMeb)
  - Web SSO, Centraliserad autentisering, auktorisering och spårbarhet
  - Common Criteria Certifierad
- Tivoli Access Manager for Enterprise Sign-On (TAMES)
  - Fullständig SSO baserad på OEM
- Tivoli Access Manager for Business Integration (TAMBI)
  - WebSphere MQ baserad åtkomskontroll, dataintegritet och säkerhet
- Tivoli Access Manager for Operating Systems (TAMOS)
  - Säkrar UNIX and Linux
  - Förväntad Common Criteria Certifiering våren/sommaren, 2006

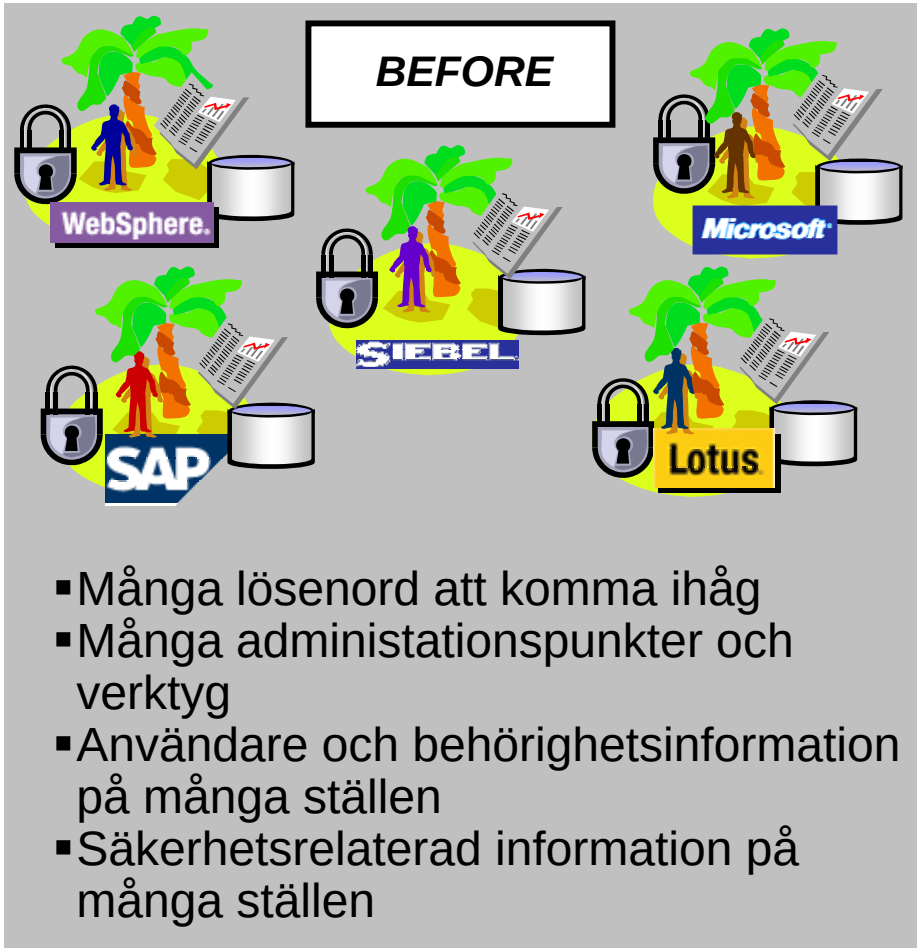
IBM Software Group

Tivoli Access Manager for e-Business

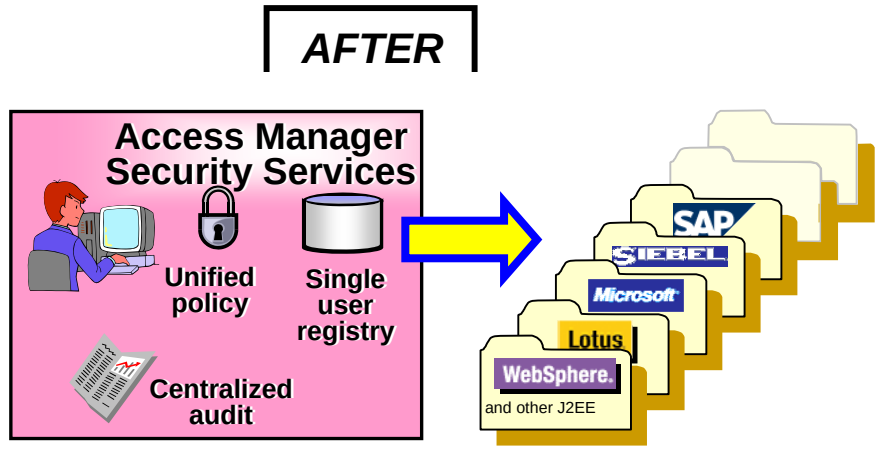
Tivoli software

ON DEMAND BUSINESS

Tivoli Access Manager for e-business



- Många lösenord att komma ihåg
- Många administationspunkter och verktyg
- Användare och behörighetsinformation på många ställen
- Säkerhetsrelaterad information på många ställen



- Web single sign-on
- Central administration eller delegering med ett verktyg
- Central hantering av användare och säkerhetsrelaterad
- Central Policy + Säkerhetsinformation => Revisionstålighet

= Säkerhets policy = Anv. & grupp info Information

TAMeb — Grundfunktionalitet

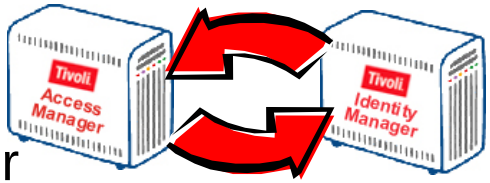
Dynamic Rules

- Ta åtkomstbeslut i realtid
- Minskar antalet grupper
- Baseras på standards (XSLT)

Desktop SSO

- Många kunder vill använda MS Kerberos SSO"….
- Kan MS hantera annat än MS? (WAS, WLS…etc)
- Vi löser detta med TAMeb!

TIM Linkage



- TAM agenter
- Gemensam lösenordspolicy
- Web SSO till TIM
- Självregistering / självbetjöning

Appl/Portal Integration

- Autentisering
- Web SSO
- IBM: WebSphere/Portal
- SAP, Siebel, PeopleSoft, . . . (more than 55 products)

TAMeb färdig integration

Ready for IBM Tivoli e-business software

IBM Integration factory

Application Single Sign-On

- Adexa collaboration products (9)
- Blockade ESconnect
- Broadvision One to One
- CA Siteminder
- Cash-U Pecan
- Centric Product Innovation (3)
- Citrix Metaframe / Nfuse XP
- Documentum Content Server/Webtop
- Documentum eRoom
- IBM Content Manager
- IBM Host on Demand
- IBM Host Publisher
- IBM Lotus Domino
- IBM Lotus iNotes
- IBM Lotus Quickplace
- IBM Lotus Sametime
- IBM Lotus Team Workplace
- Intelliden R-Series
- Interwoven TeamSite
- Kana Platform
- Kintana Suite (Mercury Interactive)
- Microsoft Exchange (OWA)
- Microsoft SharePoint Portal/Services
- OpenConnect WebConnect
- Oracle Application server
- PeopleSoft Enterprise Application
- PeopleSoft Enterprise PeopleTools
- Rocksteady Rocknet
- SAP Enterprise Portal
- SAP Internet Transaction Server
- Secur-IT C-Man
- Secur-IT D-Man
- Siebel
- Sourcefire ISM
- Sun Calendar Server*
- Sun Messenger Server*
- Vasco Digipass (via C-Man)

Desktop SSO

- ActivCard ActivClient
- Microsoft Kerberos (SPNEGO)
- Microsoft NTLM

Directory sync & virtualization

- Aelita Ent. Directory Manager
- IBM Tivoli Directory Integrator
- OctetString Virtual Directory
- Radiant Logic

Encryption, SSL & VPN

- Aventail EX-1500
- Eracom ProtectServer Orange
- IBM 4758
- IBM 4960
- Ingrian Secure Transaction Appliance
- nCipher nForce
- Neoteris IVE

Integration and Consulting

- Deloitte & Touche
- EDS
- IBM Global Services

Plus many others including local SIs
such as Secur-IT and Sena Systems

Messaging security

- IBM WebSphere BI Message Broker
- IBM WebSphere BI Event Broker
- IBM WebSphere MQ

Platform & Traffic Mgmt.

- Crossbeam Security Svcs. Switch
- F5 Networks BIG IP
- Sanctum AppShield

Strong Authentication

- ActivCard
- Aladdin Knowledge Systems
- Daon Engine (Biometrics)
- Entrust TruePass
- VeriSign
- RSA SecurID

UNIX Deployment Lockdown

- HP-UX
- IBM AIX
- IBM DB2
- IBM HTTP Server
- IBM WebSphere App. Server
- Oracle DB
- Red Hat Linux
- Sun Solaris
- SuSE Linux

User repository

- CA eTrust Directory
- IBM Tivoli Directory Server
- Microsoft Active Directory
- Novell eDirectory
- Siemens Nixdorf DirX Directory
- Sun ONE Directory Server
- Vasco Digipass

Web Server Plug-in

- Apache
- IBM HTTP Server
- IBM WebSphere Edge Server
- Microsoft IIS
- Sun ONE Web Server

Web Application Server

- BEA WebLogic Server
- IBM WebSphere App. Server (Any J2EE Platform)
- Microsoft .NET

Web Portal Server

- BEA WebLogic Portal (SSO)
- IBM WebSphere Portal
- Plumtree Portal*
- Sun ONE Portal Server (SSO)

XML and Web Services

- DataPower
- Digital Evolution / SOA Software
- Forum Systems
- Layer 7 SecureSpan Gateway
- Reactivity XML Firewall
- VordelSecure

* By request

IBM Software Group

Tivoli Access Manager for Operating Systems

Tivoli software

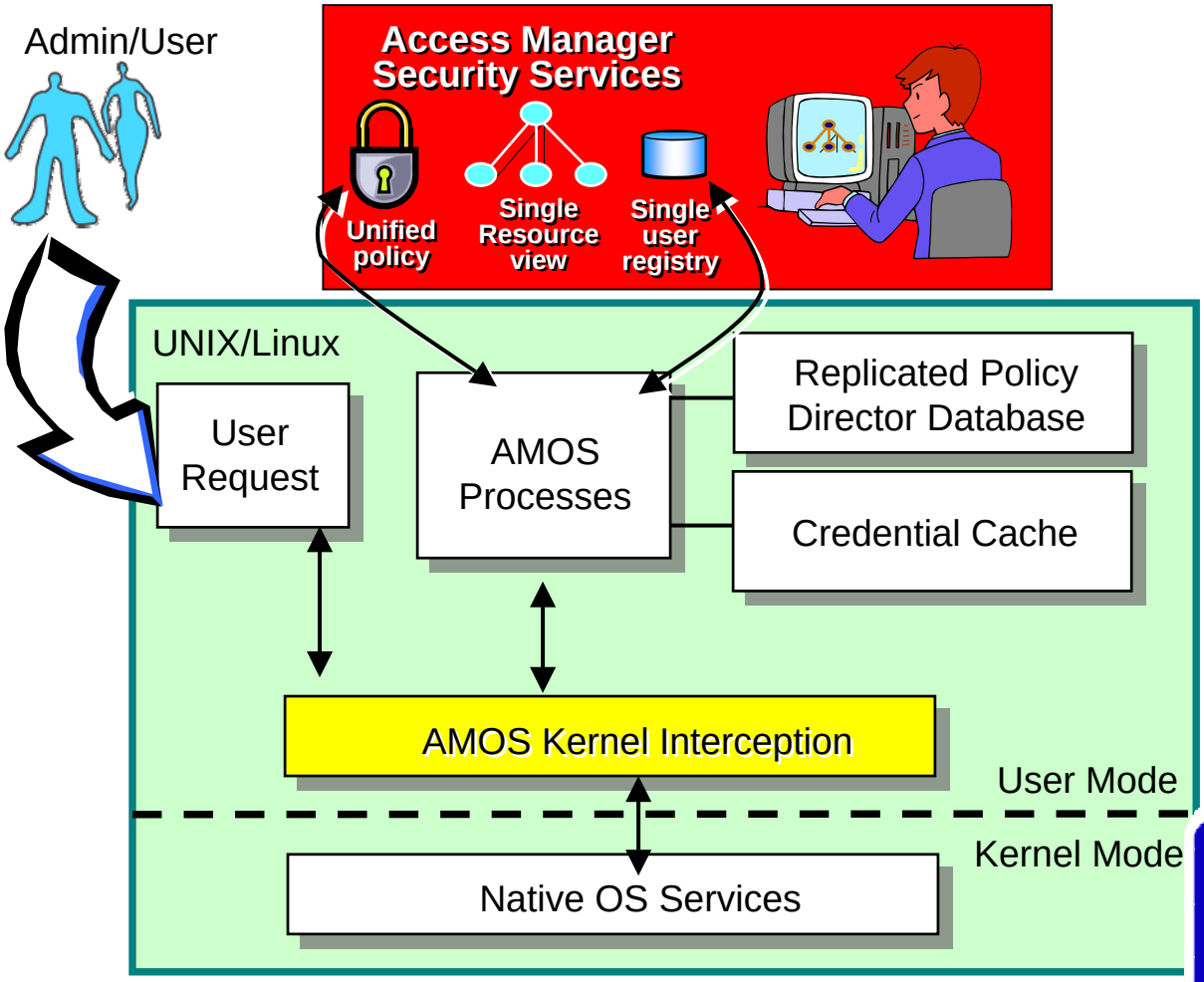
ON DEMAND BUSINESS

Vad är Access Manager for Operating Systems?

AMOS är en “brandvägg” för UNIX/Linux operativsystem

- Hanterar det största hotet – interna användare….
- Ökar säkerheten till “mainframe-nivå”
- Centraliserar säkerhetsrelaterad information och gör den mer lätt-tillgänglig vid revision
- Central policyhantering även för UNIX/Linux

Access Manager for Operating Systems



- **Skyddar:**
  - Filsystemet
  - Nätverkstjänster
  - Inloggning - när och varifrån
  - Ändringar av användare och grupper
  - m.m.

Starkare kontroll av root kontot och andra konton

IBM Software Group

TAM for Enterprise SSO

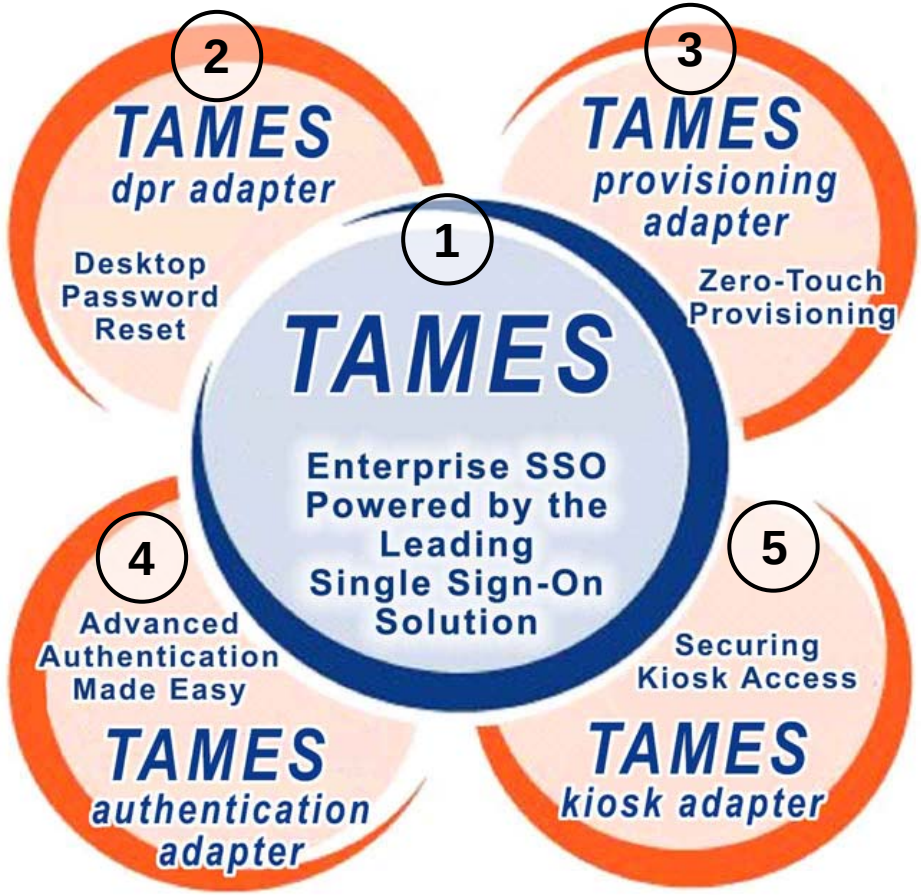
Tivoli software

ON DEMAND BUSINESS

TAMES: Tivoli Access Mgr. for Enterprise SSO

Komponenter i TAMES:

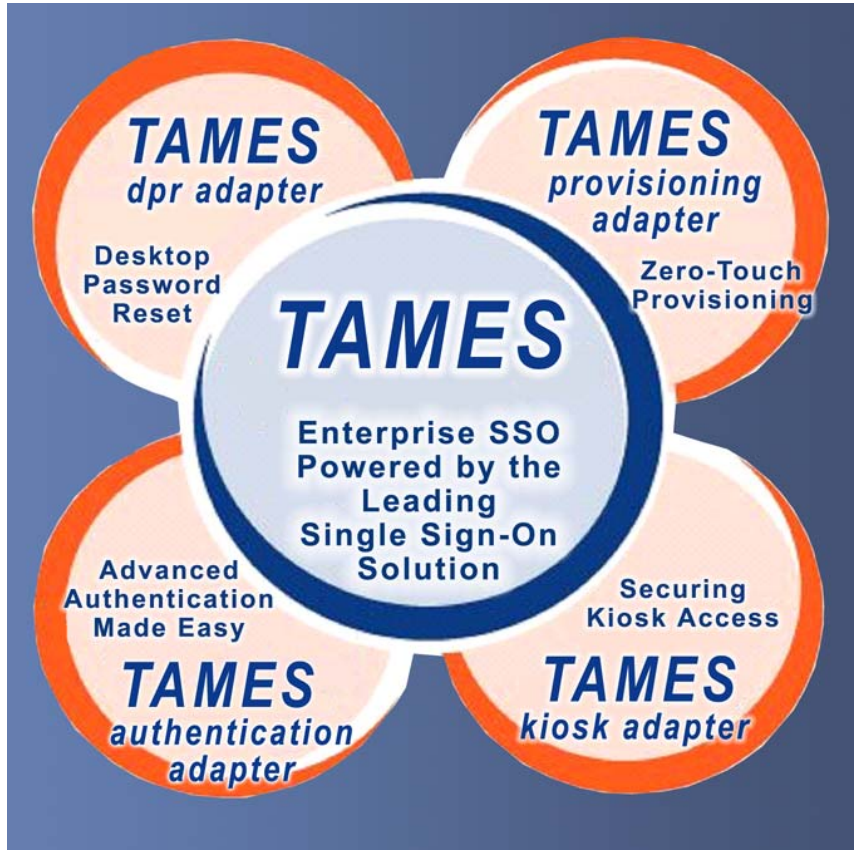
1. TAMES – basprodukten
2. DPR Adapter - Windows-baserad självbetjäning av lösenord
3. Provisioning Adapter - Integration med ITIM
4. Authentication Adapter – Flexibel Autentisering
5. Kiosk Adapter – Säker åtkomst till arbetsstationer som används av många användare



Komponenter i TAMES

- TAMES SSO eliminerar arbetet med att integrera applikationer så att man kan få SSO inom loppet av dagar och inte månader/år.

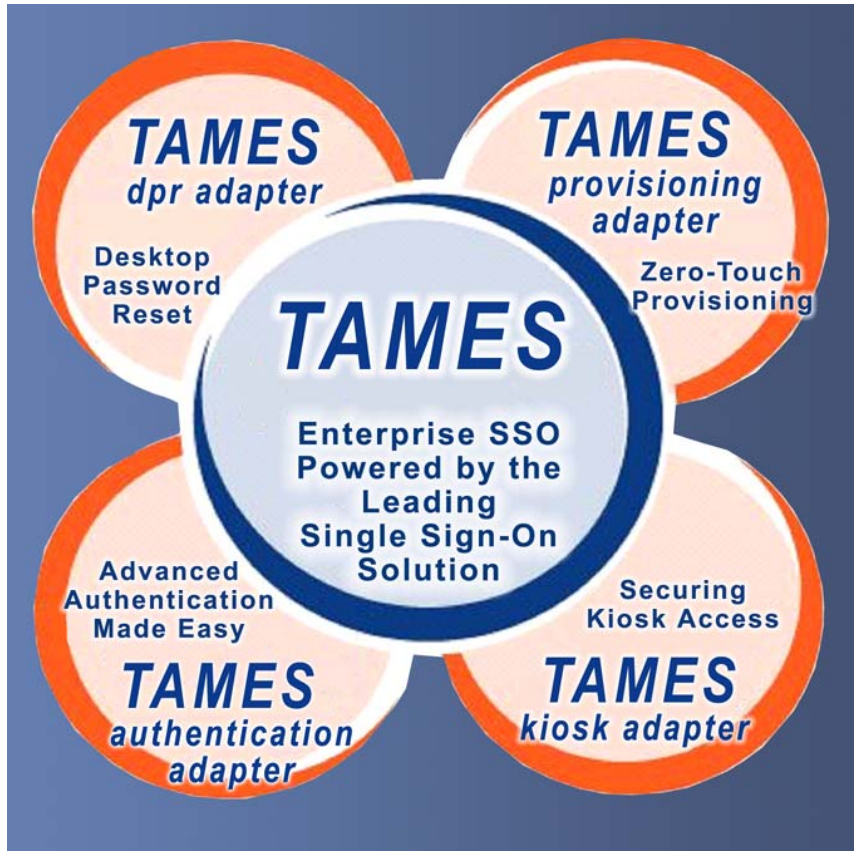
- TAMES DPRA gör det möjligt för användare att återställa sitt windowslösenord direkt från sin arbetsstation utan att behöva ringa helpdesk.



Komponenter i TAMES

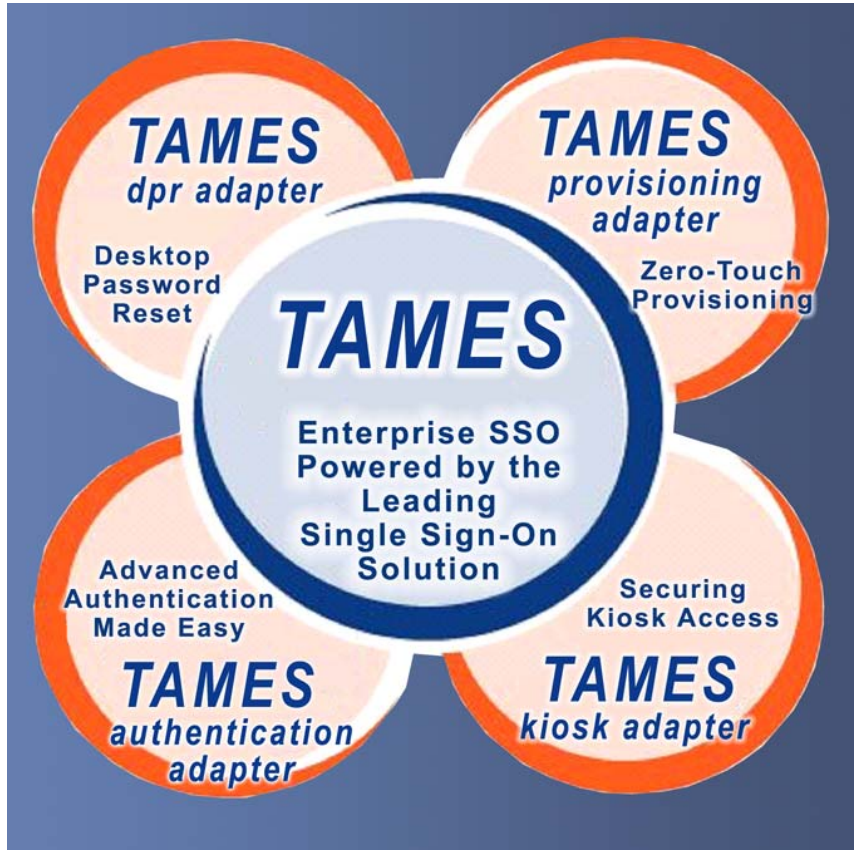
- TAMES AA gör det möjligt att använda vilken kombination av autentisering som helst (ex.vis. tokens, smart cards, biometri och lösenord) för att kontrollera åtkomst till applikationer.

- TAMES PA gör det möjligt att synka konton och lösenord från ITIM till TAMES.



Komponenter i TAMES

- TAMES KA gör det möjligt att bl.a. automatiskt avsluta inaktiva sessioner och stänga ner applikationer som körs på en delad arbetsstation.



Det tar inte lång tid att implementera TAMES!

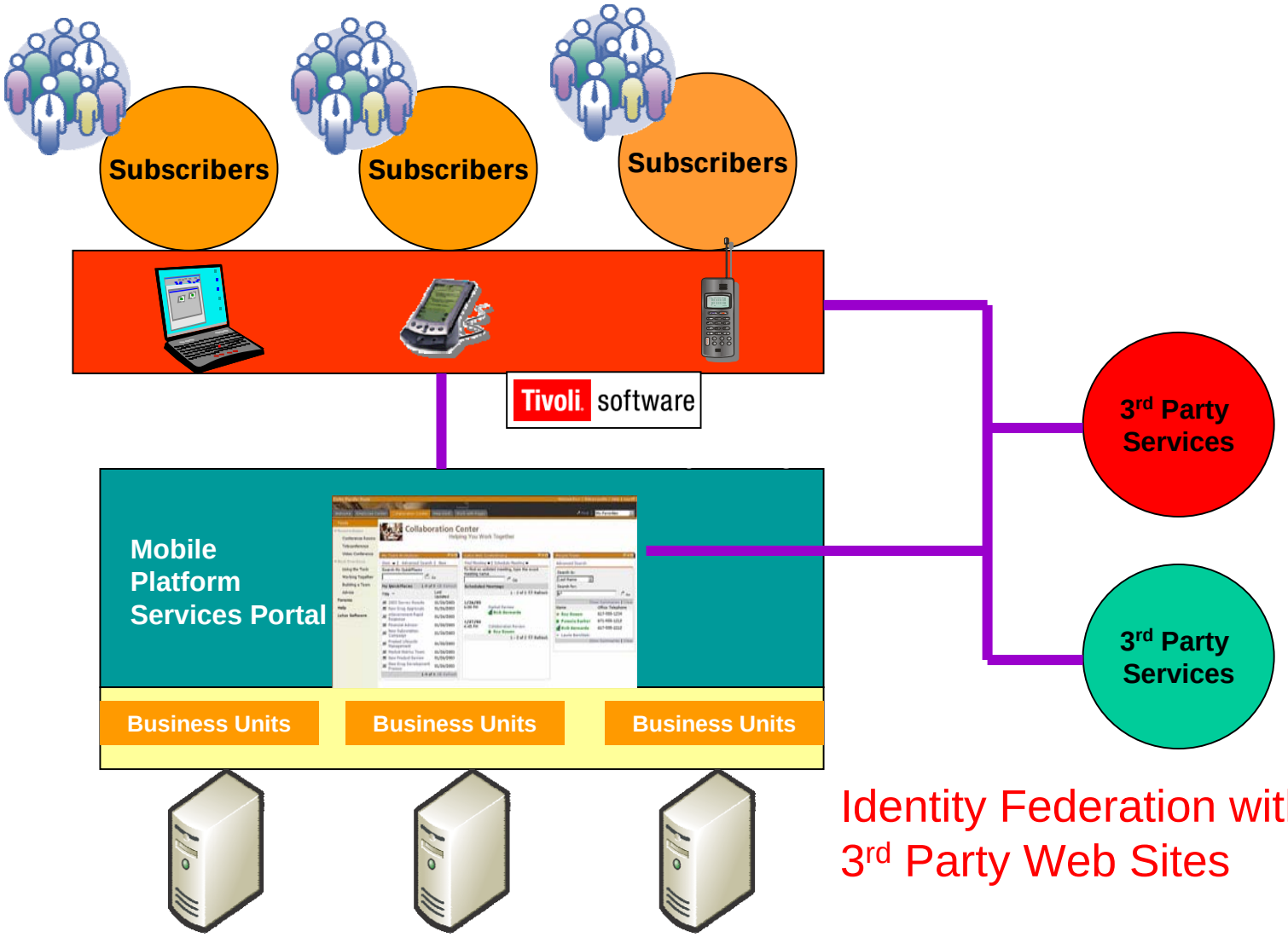
IBM Software Group

Tivoli Federated Identity Manager

Tivoli software

ON DEMAND BUSINESS

Orange: Integrerad portal för mobiltelefonabonnenter

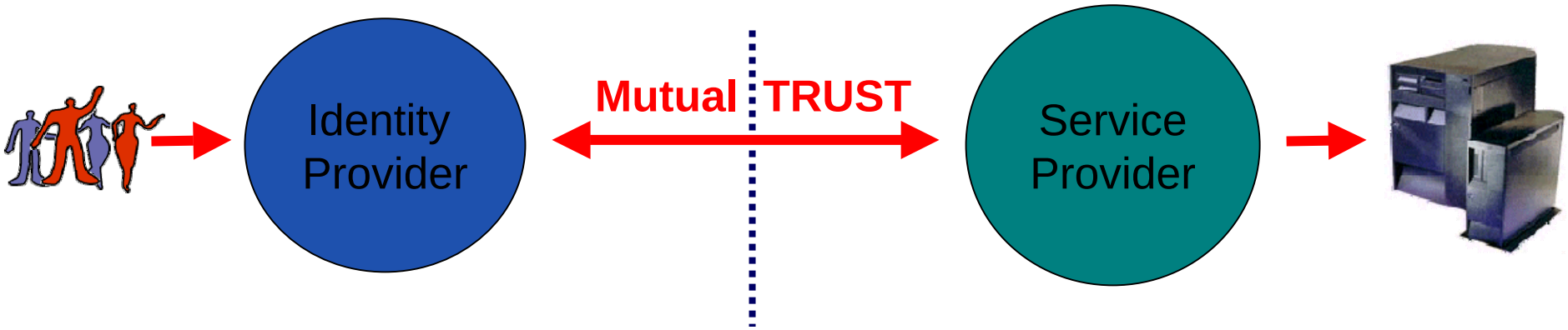


Identity Federation with 3rd Party Web Sites

Roller: Identity Provider and Service Provider

“Vouching” party in transaction

“Validation” party in transaction



1. Utfärdar “Network / Login credentials”
2. Administrerar användarkonton/id’n
3. Autentiserar användaren
4. “Borgar” för användarens identitet

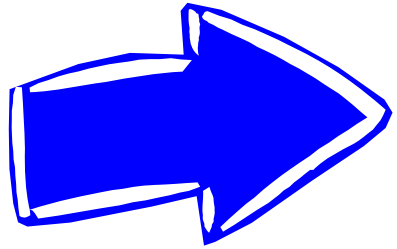
Tjänsteleverantören hanterar åtkomsten till sina tjänster

Den externa användaren har åtkomst till tjänsterna så länge federeringen är giltig

Hanterar endast användaregenskaper som är relevanta för tjänsteleverantören

FIM & Standards

FIM :
Hanterar de 3 stora protokollen för federerad identitetshantering



Web Services Security Management:
SOAP/HTTP

Assertions:
SAML,
UID/PW

Identity Federation Mgmt. (HTTP, Liberty)

SSO w/SAML, Liberty, WS-Federation tokens

HTTP SSO with SAML

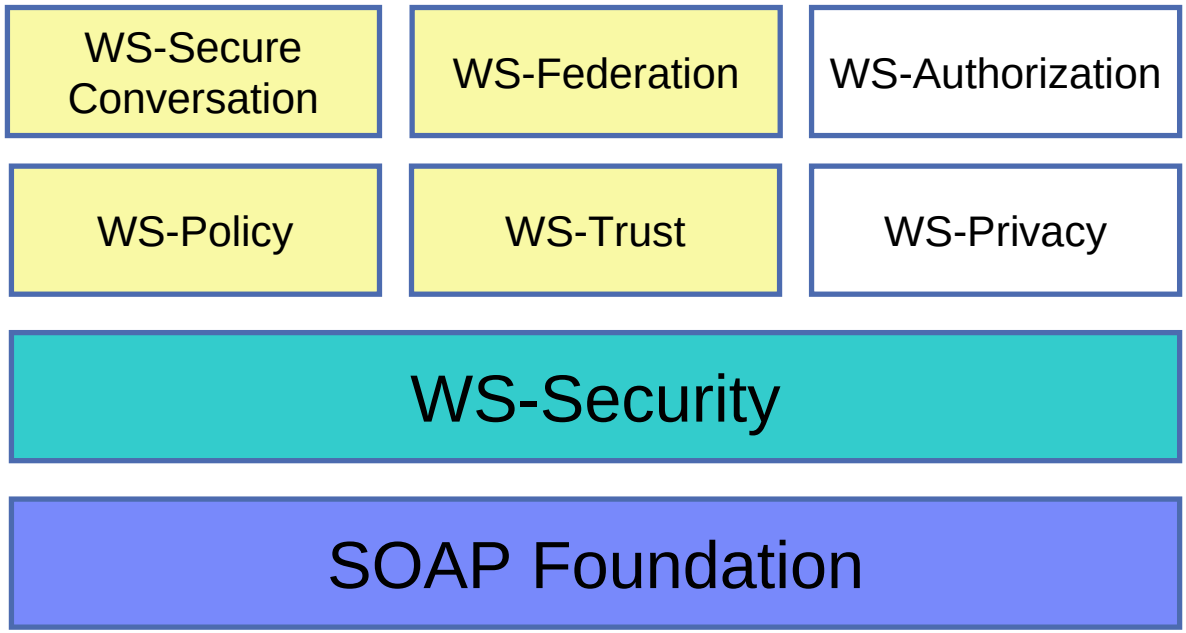
HTTP SSO with Liberty

SAML

Liberty

WS-Federation
WS-Security

Web Services Security Roadmap



Web services zone page:
http://www-106.ibm.com/developerworks/webservices/