Kurumsal Kimlik Ve Erişim Yönetimi(KEY)

Salih Abamor
IBM Tivoli Software

Eylül 2010

Kimlik Yönetimi Nedir ?

Kimlik Yönetimi, dijital kimliklerin tanımlanması, bakımı ve kullanımını destekleyen süreçler ve altyapıların bütünüdür

Dijital Kimlik bir kullanıcı, uygulama, cihaz olabilir

Dijital Kimlik kurum içi veya dışı olabilir

Neden KEY?

- Güvenlik
  - –Mevcut durum analizi
  - –Süreç yönetimi ve iyileştirilmesi

- Operasyonel Verimlilik
  - –Otomasyon
  - –Self Servis
  - –Kullanıcı/Şifre senkronizasyonu

KEY'le gelen Fırsatlar

Kimliklere Güven

Customers or criminals?

Partners or competitors?

Employees or hackers?

Erişimin Yönetilmesi

Servislerin Korunması

Payroll

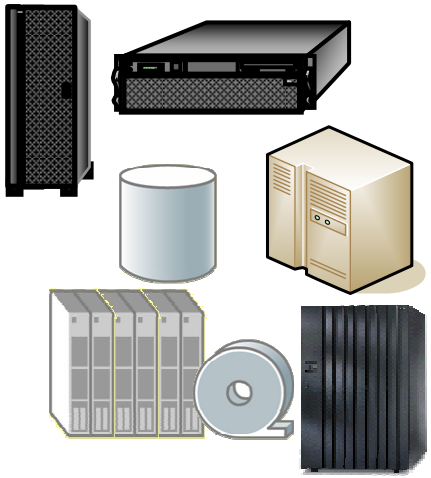
Online banking

Loan applications

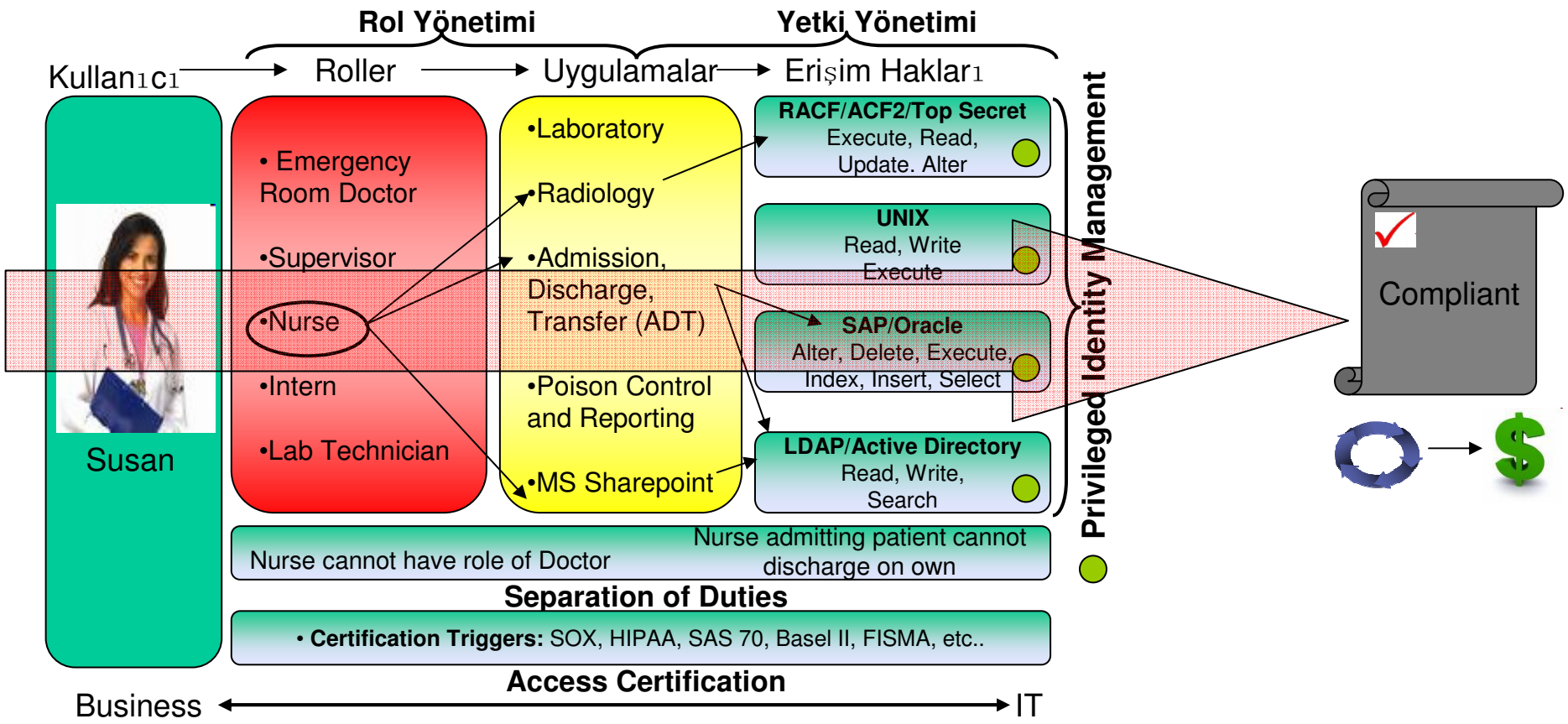
Retail sales

Inventory

Verilerin ve mahremiyetin korunması



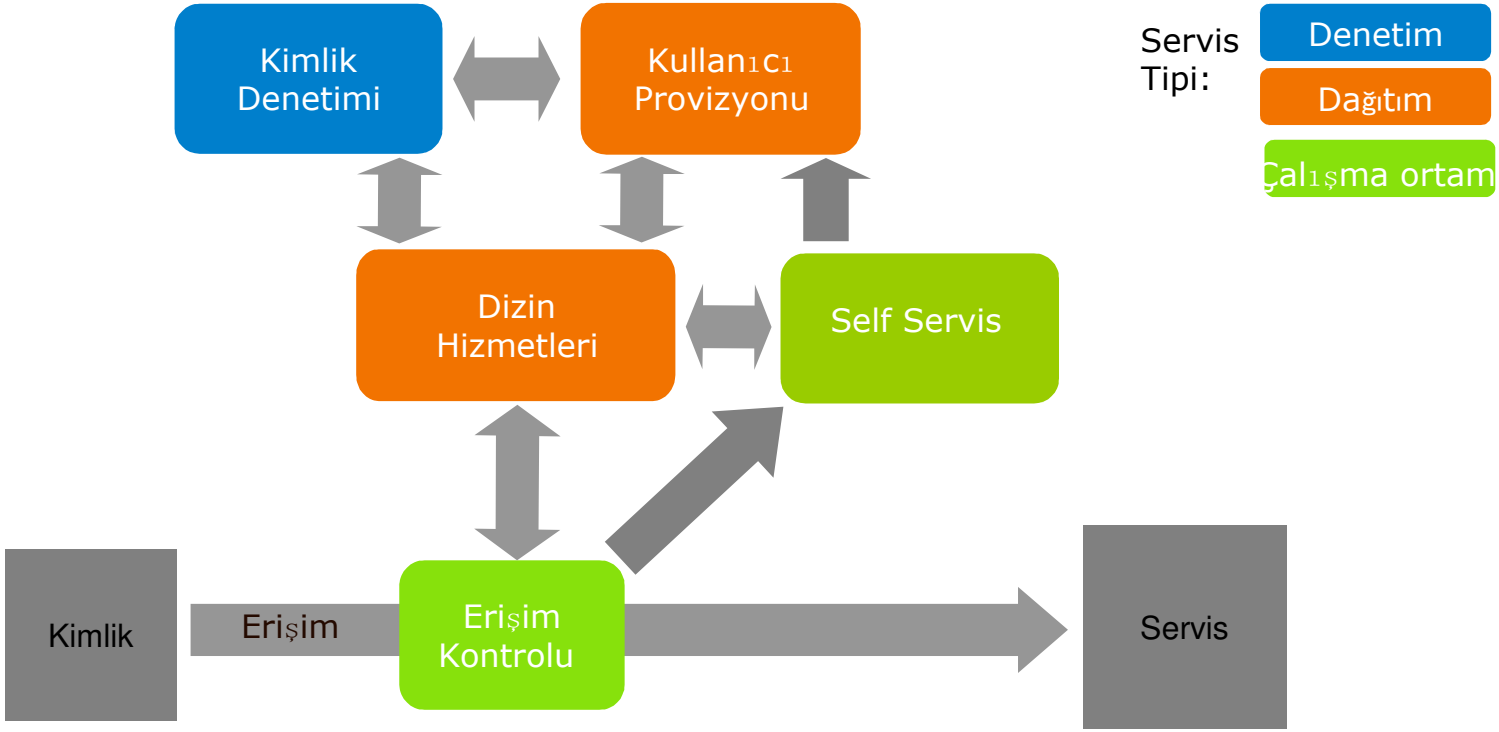
Basit, Güvenilir, ve Verimli



Source: Gartner & IBM

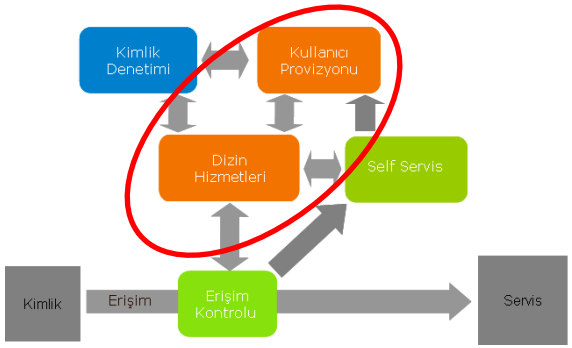
KEY'in İki Parçası

- Kimlik Yönetimi, KEY'in denetim ve otomasyon bileşenidir
- Erişim Yönetimi, KEY'in çalışma ortamı bileşenidir



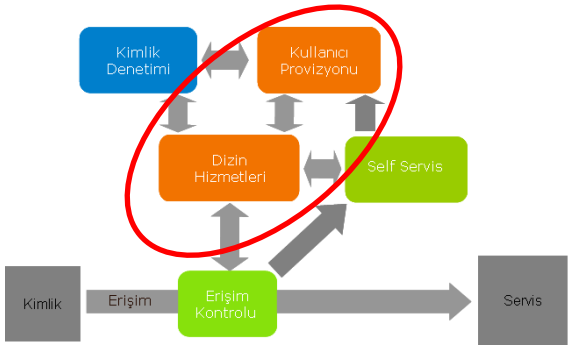
Synchronising Identities with Authoritative Sources

- An organisation will have an existing authoritative list of identities
  - E.g. HR data, list of customers, current registered users
- There may be multiple authoritative sources and an authoritative source may also be updated by other authoritative sources
- Synchronisation requires:
  - Defined rules that determine which entries are used
  - Source attributes mapped to the identity attributes
  - Identity attributes mapped back to the authoritative source attributes
- You should only have ONE authoritative source for each identity type



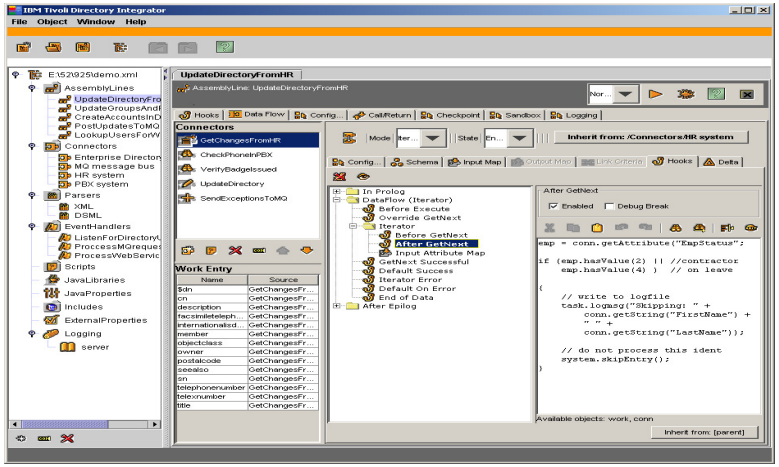
Data Cleansing

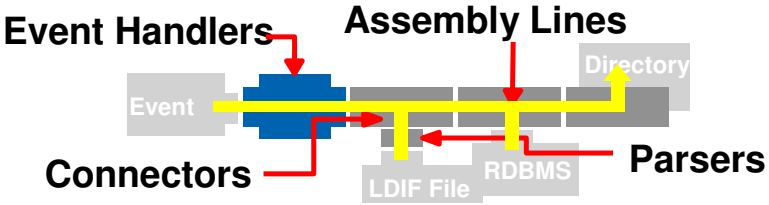
- The data needs to be inspected to determine quality
  - All required attributes have values
  - Is the unique key unique
  - Are coded values correct
- Cleaning of data to ensure quality is not a one time action, but ongoing
- Manually entered data fields have low data quality
- Never assume HR has valid data
  - Usually the only data that is correct is surname and given name as that goes on your group certificate
  - HR data is not always maintained



IBM Tivoli Directory Integrator

IBM Tivoli Directory Integrator provides real-time synchronization between identity data sources so that enterprises can establish an authoritative, up-to-date, identity data infrastructure.





Key features

- **On Demand Data Infrastructure for Security**
  - Support both Meta- & Virtual Directory function & migrate easily between the two - with one tool and one skill set to manage
  - Applications can run TDI synchronizations remotely & asynchronously
  - Excellent Web services support, including WS-provisioning and rich XML parsing
- **Authoritative Infrastructure for Identity Management**
  - A wide array of available connectors, including using TIM Agents as TDI connectors
  - Synchronizations based on business rules and flexible logic: e.g. Assembly Lines can call other Assembly Lines
- **Highly Manageable Metadirectory Connections**
  - Reusable integration solutions
  - Enhanced failover capabilities for high-availability and Assembly Line Pooling for bandwidth management

TDI 6.1.1 Server

Axis Easy Web Service Server Connector
Axis Easy Web Service Invoke
Axis Java-to-Soap
Invoke Soap Web Service
Axis Soap-to-Java
Complex Types Generator
Wrap Soap

LDAP Connector
LDAP Server Connector
Tivoli Access Manager Connector
Windows Users and Groups Connector

Active Directory Changelog Connector v2
IBM Directory Server Changelog Connector
Netscape/iPlanet Changelog Connector
zOS LDAP Changelog Connector

BTree Connector
JDBC Connector
Properties Connector
SystemStore Connector
RDBMS Changelog Connector

AssemblyLine Connector
Server Notifications Connector
AssemblyLine Function Component

Domino Change Detection Connector
Domino Users Connector
Lotus Notes Connector

Exchange Changelog Connector
Mailbox Connector
SendEMail Function Component

TIM DSMLv2 Connector
DSMLv2 SOAP Connector
DSML v2 SOAP Server Connector
Generic JNDI Connector
ITIM Agent Connector

EMF SDOToXML Function Component
EMF XMLToSDO Function Component

Timer Connector

AssemblyLine

Active Correlation Technology Connector
Generic Log Adapter Connector
RAC Connector
Entry to CommonBaseEvent Function

JMX Connector
SNMP Connector
SNMP Server Connector
TCP Connector
TCP Server Connector

Remedy/Peregrine /CCMDB tickets

Many Custom Components downloadable from OPAL or tdi-users.org or on request

CCMDB
Netcool
RSS
Google

PeopleSoft Connector
Siebel Connector
SAP ALE IDoc Connector
SAP R/3 Business Object Repository
SAP R/3 User Registry
SAP R/3 RFC Functional Component

Script Connector
Generic Java Method
Parser FC
Scripted Function Component

Remote Command Line Function Component
z/OS TSO/E Command Line Function Component
Command Line Connector

Memory Queue FC
MemQ Connector
Memory Stream Connector

File System Connector
FTP Client Connector
URL Connector
HTTP Client
HTTP Server Connector

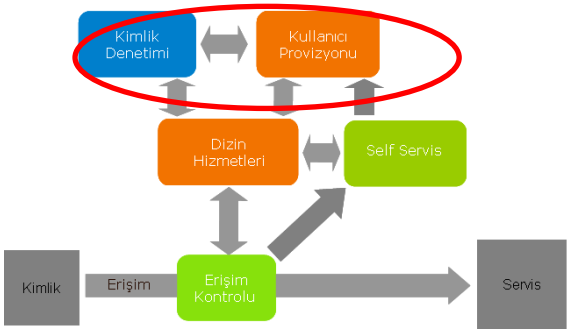
IBM MQ Series Connector
JMS Pub/Sub Connector
MQe Password Store Connector
System Queue Connector

CSV Parser
DSML v1 Parser
DSML v2 Parser
Fixed Record Parser
HTTP Parser
LDIF Parser
Line Reader/Writer
SOAP Parser
Script Parser
Simple Parser
XML Parser
XML Sax Parser
XSL based XML Parser

JVM on Windows, Linux, AIX, iSeries, zOS, Sun, HP

Identity Administration & Identity Provisioning

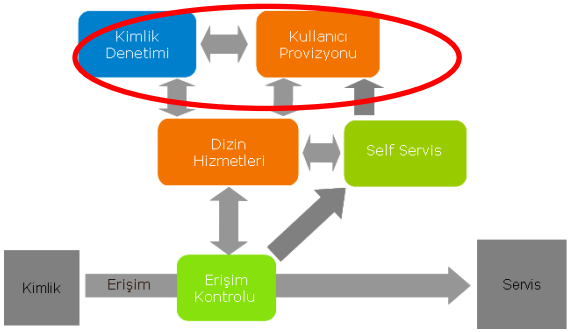
- Enables an administrator to perform life cycle management upon identities
- Applies policies that determines which end points the identity is provisioned to
- Policies may be based upon a identity type or the roles that an identity may be assigned to



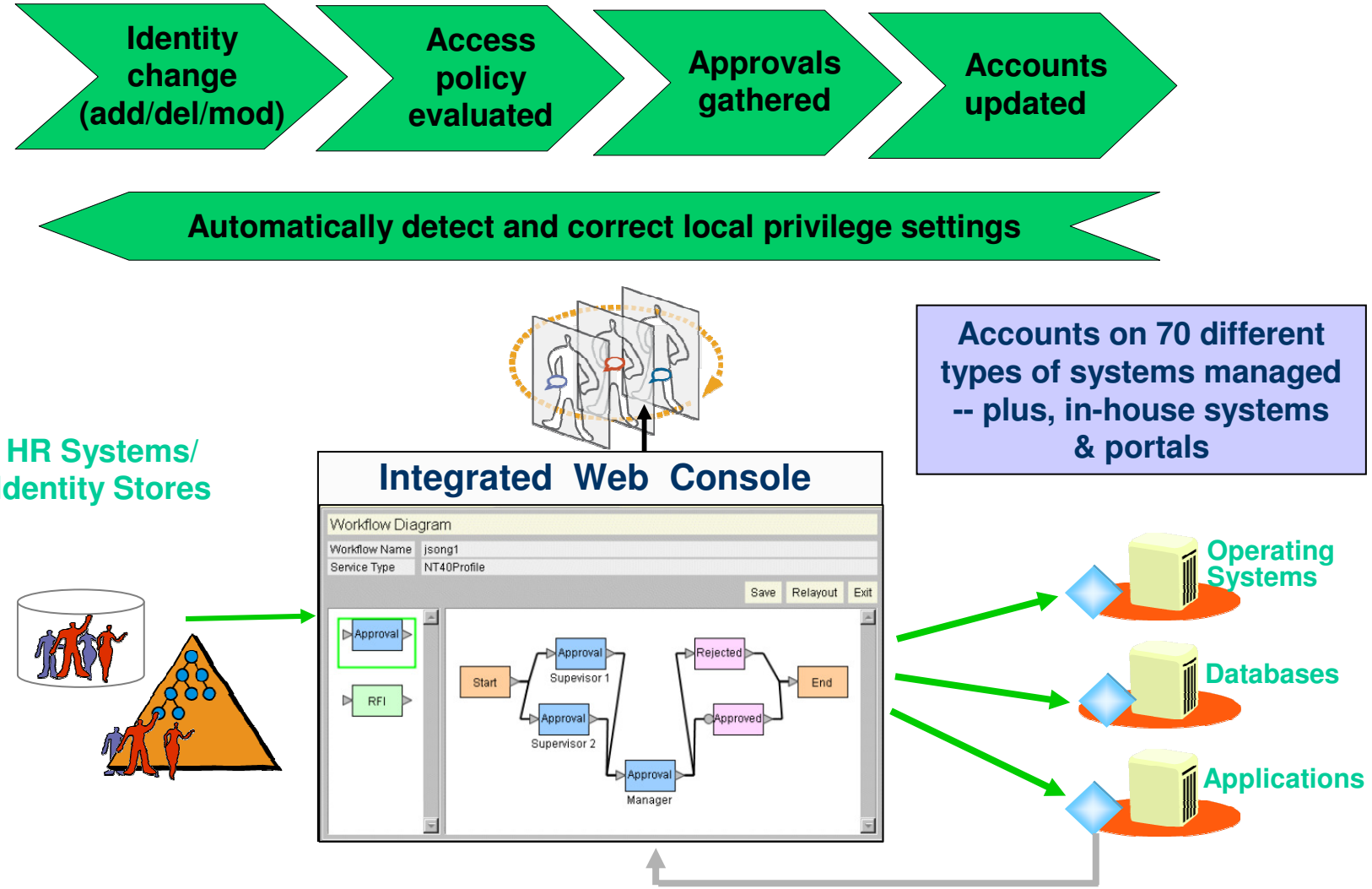
Self Service

- Enables a user to perform a limited set of Identity Administration tasks upon their identity credentials

- Typical Self Service functions are:
  - Password reset
  - Provisioning of a particular application
  - Creation of a digital identity
  - Updating identity credentials

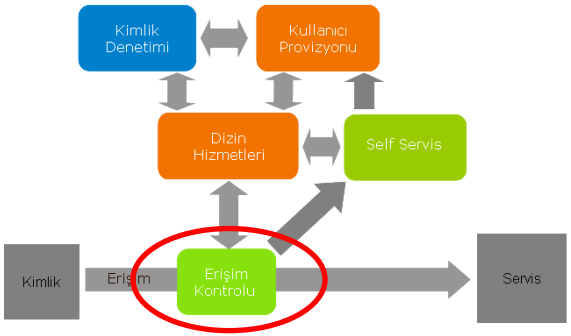


IBM Tivoli Identity Manager: Automating the Identity Lifecycle

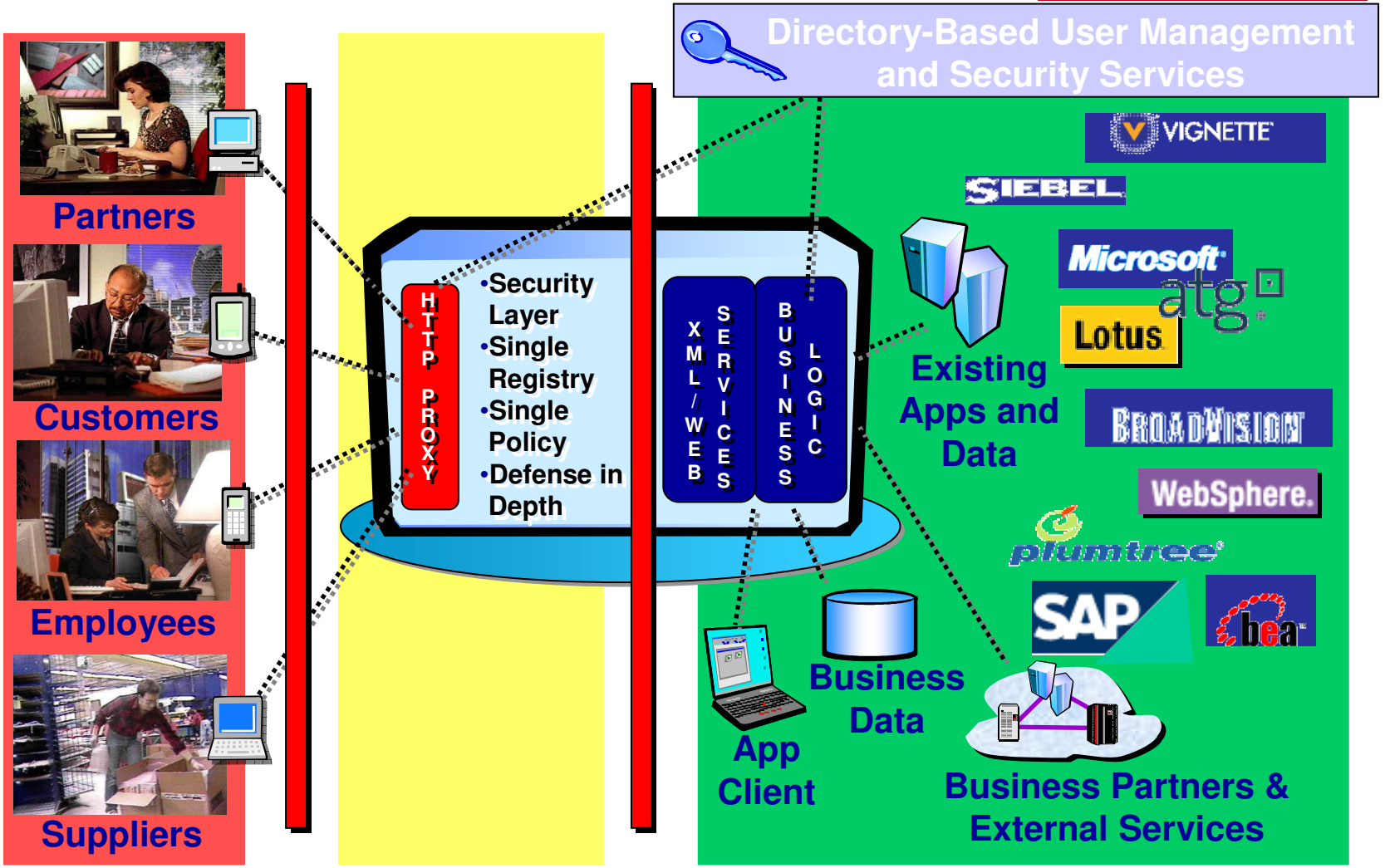


Access Control

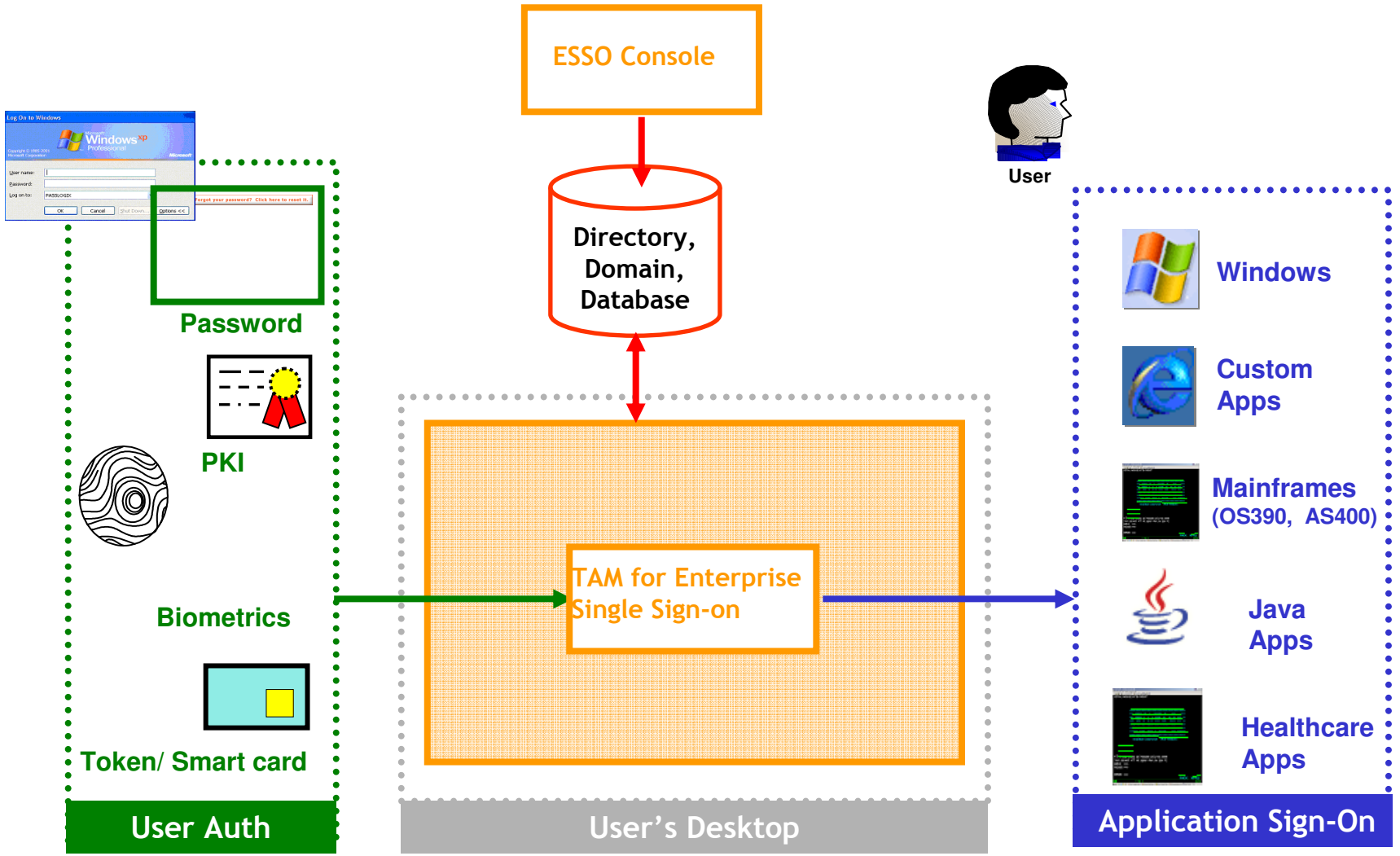
- Controls an identity's access to services
- Requests the identity to authenticate if the services be accessed may only be accessed by authenticated identities
- May accept different credentials from a users that may be:
  - UserID / Password
  - Digital certificate
  - Token



IBM Tivoli Access Manager for e-business



IBM Tivoli Access Manager for ESSO Architecture

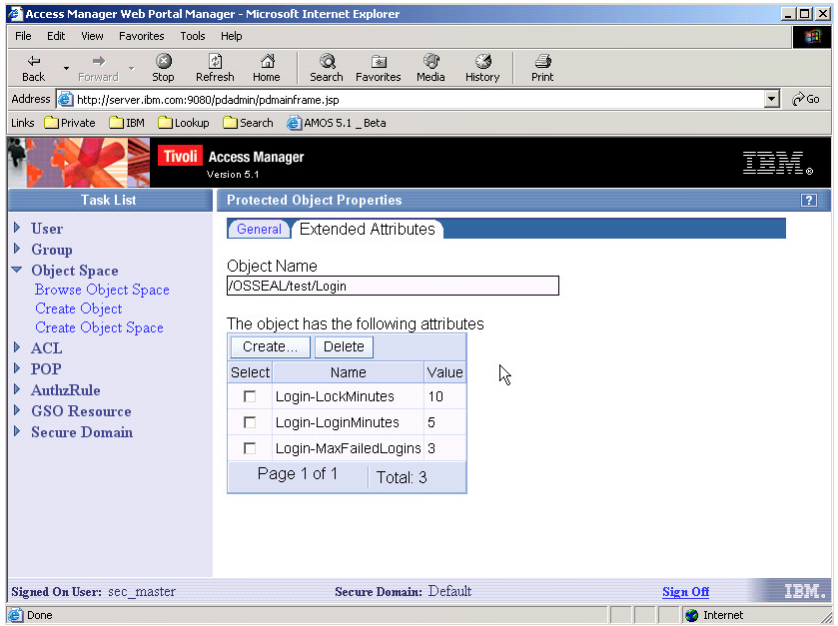


IBM Tivoli Access Manager for Operating Systems

Tivoli Access Manager for Operating Systems protects individual application and operating system resources by addressing system vulnerabilities surrounding privileged user access (e.g. super user or root accounts)

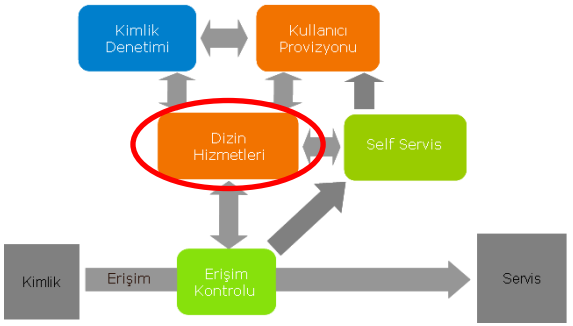
Key Features

- **Defends against the top security threat that enterprises face: misuse by internal users and employees**
- **Centralized, policy-based user access management, tracking and control in a heterogeneous OS environment**
- **Delivers mainframe-class security and auditing in a lightweight, easy-to-use product**
- **Provides Persistent Universal Auditing to document compliance with government regulations, corporate policy and other security mandates**
- **Common Criteria certified**



Dizin Hizmetleri- Tivoli Directory Server

- A persistent store that contains the known identities and their associated credentials.
  - An example of the list of credentials is defined by inetOrgPerson
- Specific credentials such as UID and Password may be used by access control to identify who the identity is
- Access control also uses group membership to determine which resources the identity may access
- Identity details are maintained by Identity Administration and Identity Provisioning

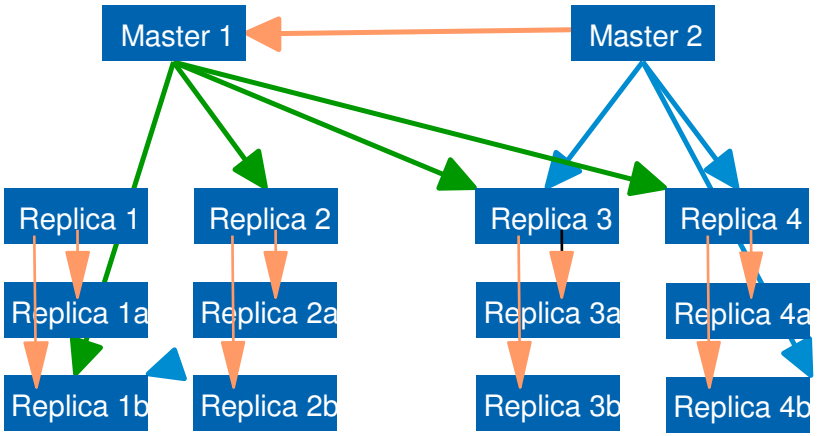


IBM Tivoli Directory Server

IBM Tivoli Directory Server provides an identity data foundation for rapid development and deployment of Web applications, security and identity management on System z and distributed platforms

Key features

- **LDAP support ensures compatibility with industry standard LDAP based applications**
- **Reliable IBM DB2® Universal Database engine provides *scalability to hundreds of millions of entries*, as well as groups of hundreds of thousands of members**
- **Robust replication capability for both master/subordinate replication, gateway, cascaded and peer-to-peer replication with up to dozens of master servers**
- **Eases management and usability with Web Administration GUI and features such as Dynamic and Nested Groups, along with Sorted and Paged Search Results**
- **Broad range of platform support: AIX, Solaris, Linux (RedHat and SuSE), HP-UX, Windows, OS/400, z/OS**



Özetle