„Evolution, Direction, and Dynamics ”

Version 1.0

Dr. Horst Walther, SiG Software Integration GmbH,

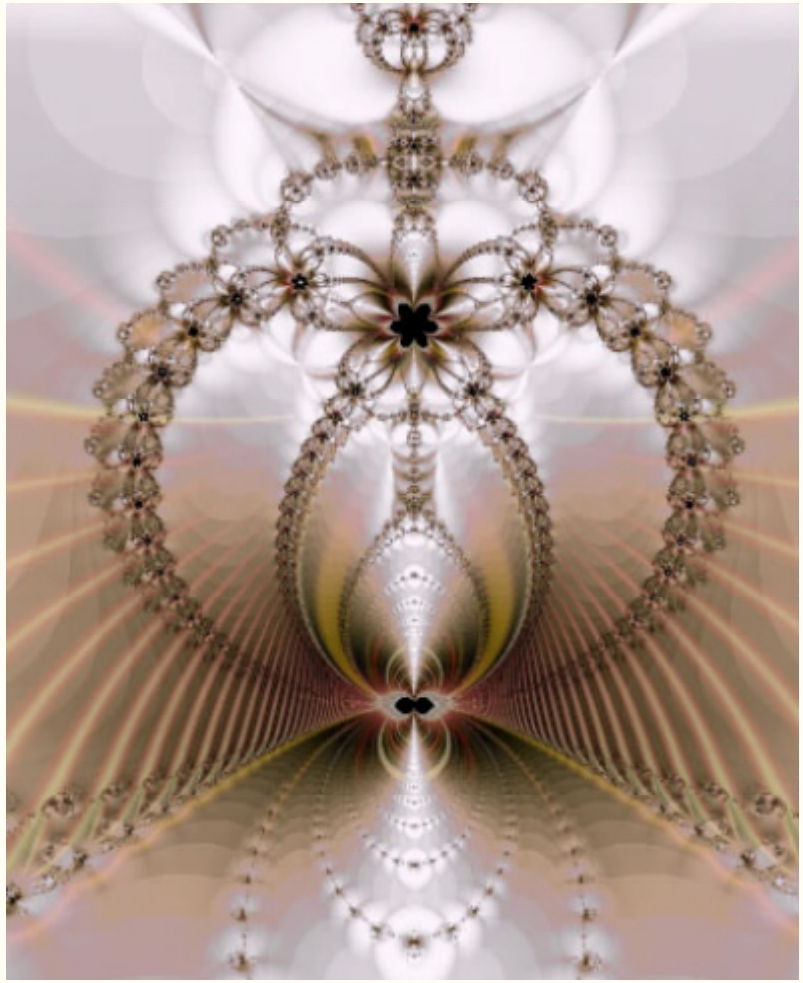
2004-10-20 Lefkosia / Cyprus

Content

- Introduction
  - Definition of Identity Management
- Technology
  - Evolution, Drivers, Components
- Assessment
  - Applicability, Industry Maturity (Gartner, Lifecycle), Appropriateness
- Crystal Ball
  - What comes next

- *Aim*:
  To get people comfortable with topic – a common understanding.
- *Approach*:
  Lecture based.

Introduction



- Barings Bank – an Example
- Motivation - True stories
- Identity Management Questions
- Related terms
- What is the digital Identity?
- A multi domain view to Identity
- What is Identity Management?
- Lifecycle of a digital Identity
- Identity Management Processes
- Identity Administration
- Community Management
- Identity Integration

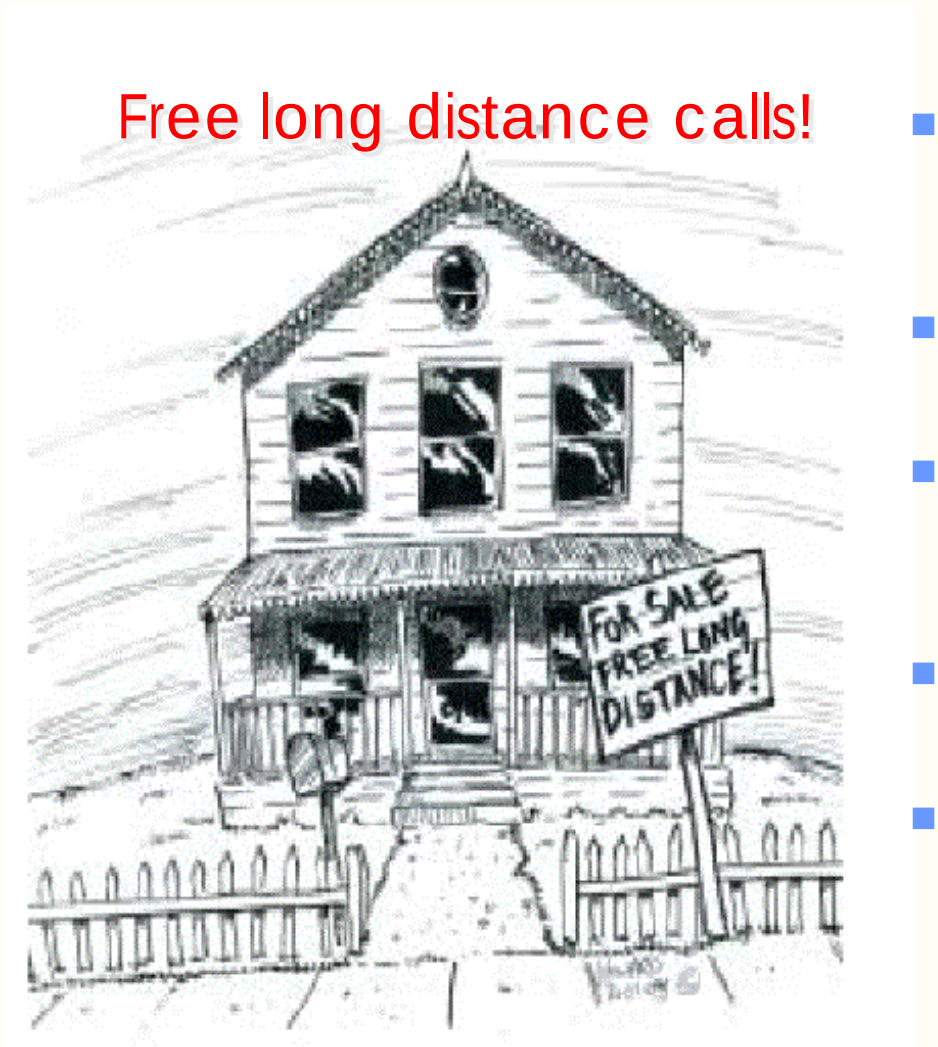
Barings Bank – an Example

- 1995 the Barings-Bank was acquired by the Dutch ING-Group for **one pound.**
- The **Bank of the British kings** has been one of the noblest in London since 1762 .
- Until 1992 Nick Leeson in Singapore started **exploiting price differences** between Japanese Derivates.
- The resulting loss mounted up to **1,4 Billion** Dollars.
- Leeson was convicted of fraud and sentenced to **6 ½ years** in Singapore's Changi prison.
- Leeson was responsible for trading derivates in Singapore **and** for the Back-Office where the Trades were settled.

  - A **catastrophic mix!**

➔ A role based separation of duties would have cost less.

Motivation - True stories (1)...



- A Top-Manager working for a Telecom-Provider moved to a new house.
- Phone costs were neither charged nor determined.
- When he left the company, (consequentially) no one thought of switching off the line.
- The house was sold several times meanwhile.
- Finally it's advantage of allowing free long distance calls was openly advertised.

Motivation - True Stories (2)...

The extra line

- One of my former employees, a Novell Administrator, had left the company 2 years ago to set-up his own operations.
- About 6 months later I discovered a line which I couldn't account for.
- I could track it to a neighbouring lawyers office.
- His secretary logged on to our Server and drew from our resources.
- My former colleague invoiced her monthly for this service.
- Except my wife no other person ever came to know about that.

Identity Management Questions

What is Identity Management?

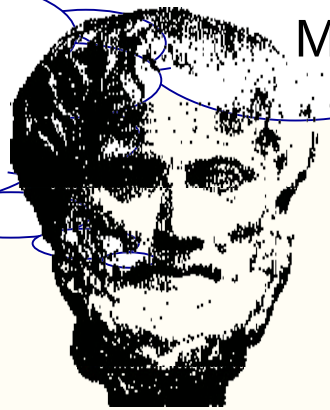
What is Management good for?

Which business process are touched by Identity Management?

How is Identity Management differentiated from other practices?

Which roles and responsibilities are engaged Identity Management?

Why Identity Management now?



Identity Management related terms

MS Passport – Liberty Alliance

Identity – role - persona

Role Based Access Control

WS-Federation

Directory Service

Meta-Directory Service

User Management

Identity Management

Public Key Infrastructure

Authentication

Single Sign On

Digital Identity

SAML / DSML / PSML / XCAML

Virtual Directory Service

User Provisioning

Role Engineering

Trust Management

Privilege-Management

Authorisation

Extranet Access Management

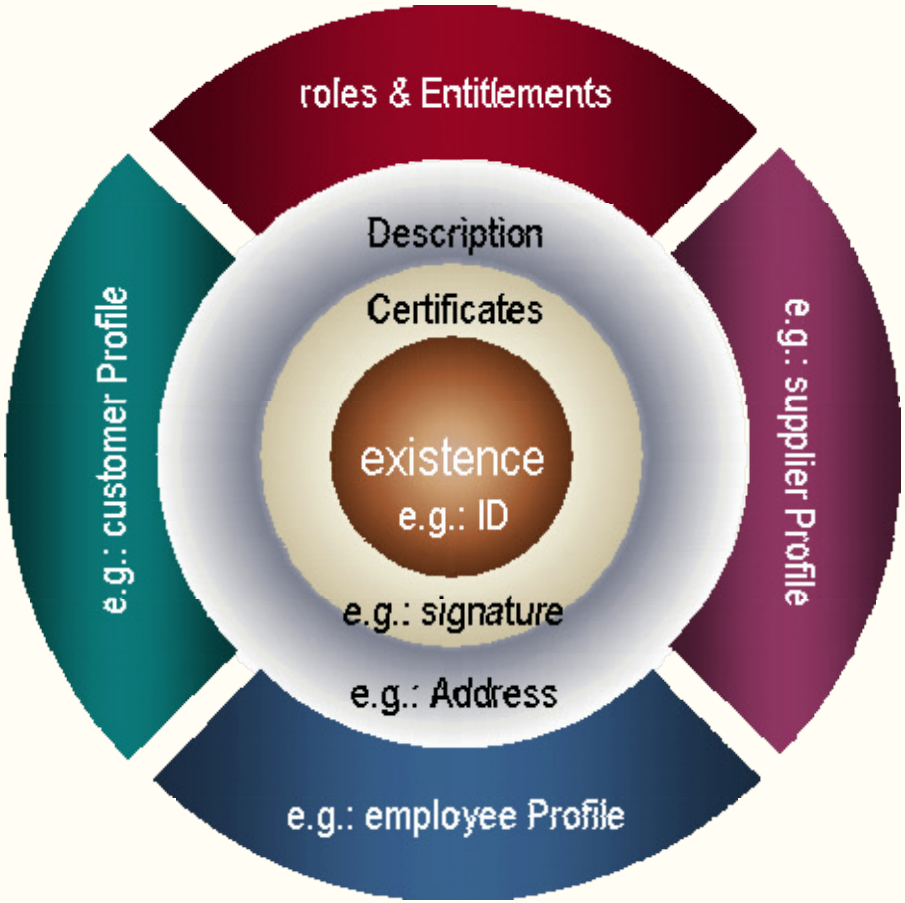
Privileges / entitlements / access rights

Federated Identity Management

X.500 / X.509 / LDAP / LDIFF / LDUP

What is the digital Identity?

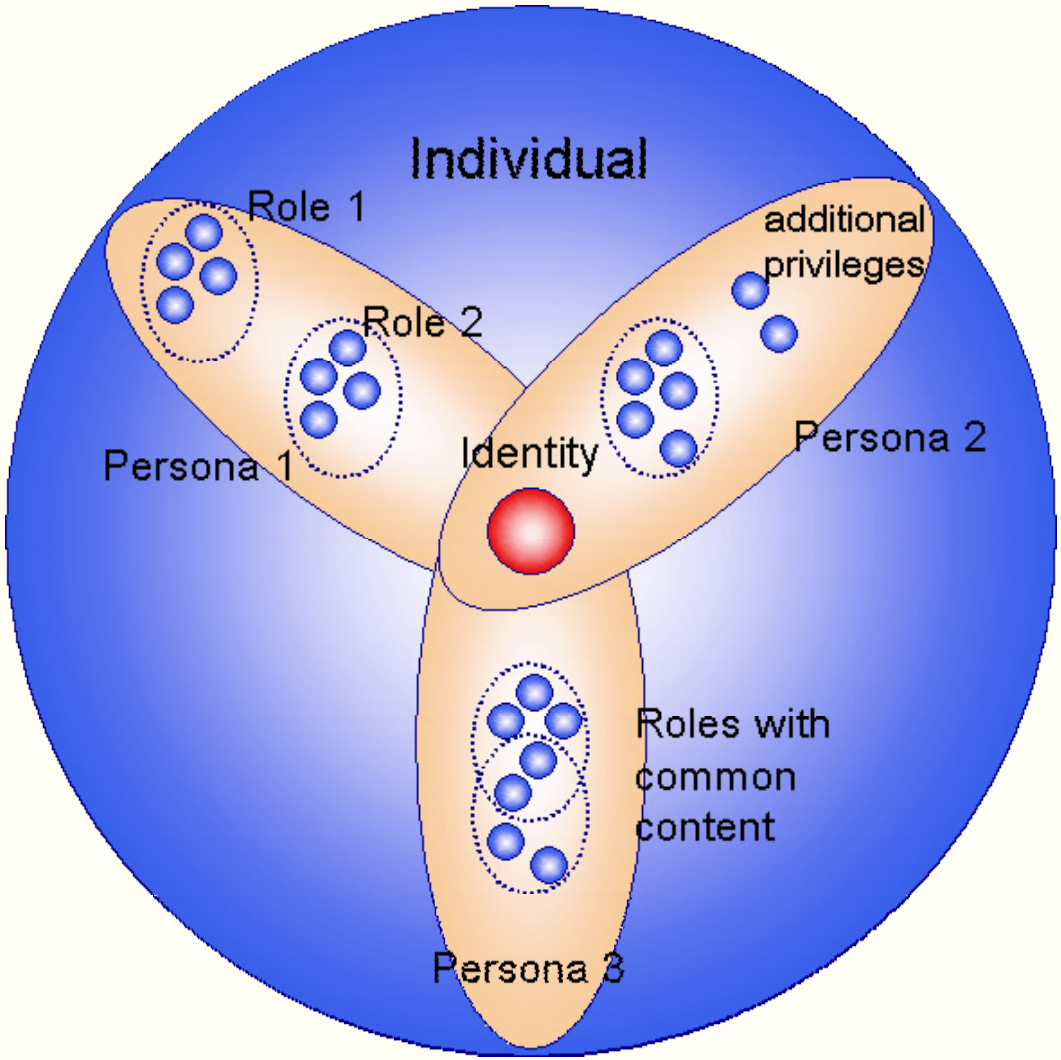
Digital Identity may be expressed as a layered model.



- Core - **Existence**:
  - A unique identifier (the real & true identity)
  - "ID", Name, Number
  - Natural person, corporation, application or Hardware.
  - Same lifetime like the object
- 1st Layer - Certificate:
  - Certificate (various strengths)
  - From Password to digital Signature
- 2nd Layer - **Description**:
  - Role independent common Attributes
  - Address information
  - characteristic characteristics.
- The 3rd Layer - **Context**:
  - Role
  - Privileges

➔ Comparable to a passport in the tangible world.

A multi domain view to Identity



- Privilege
- Role
- Persona
- Individual
- Identity

The individual …

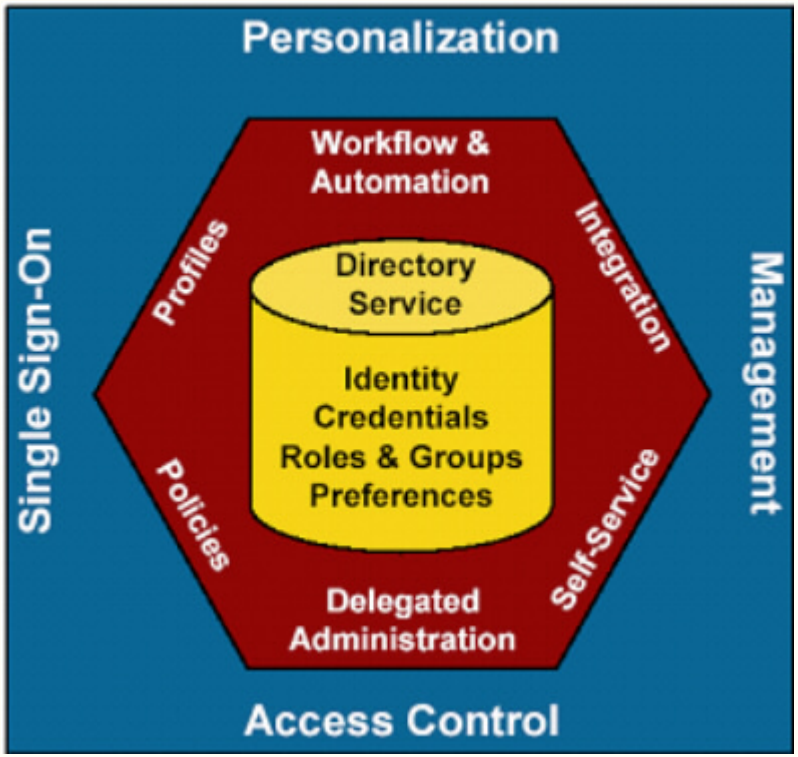
➔ Is determined by it's identity,

➔ Is made out of several personas,

➔ which each of them incarnates several roles,

➔ each supplied with a rich set of entitlements and other resources

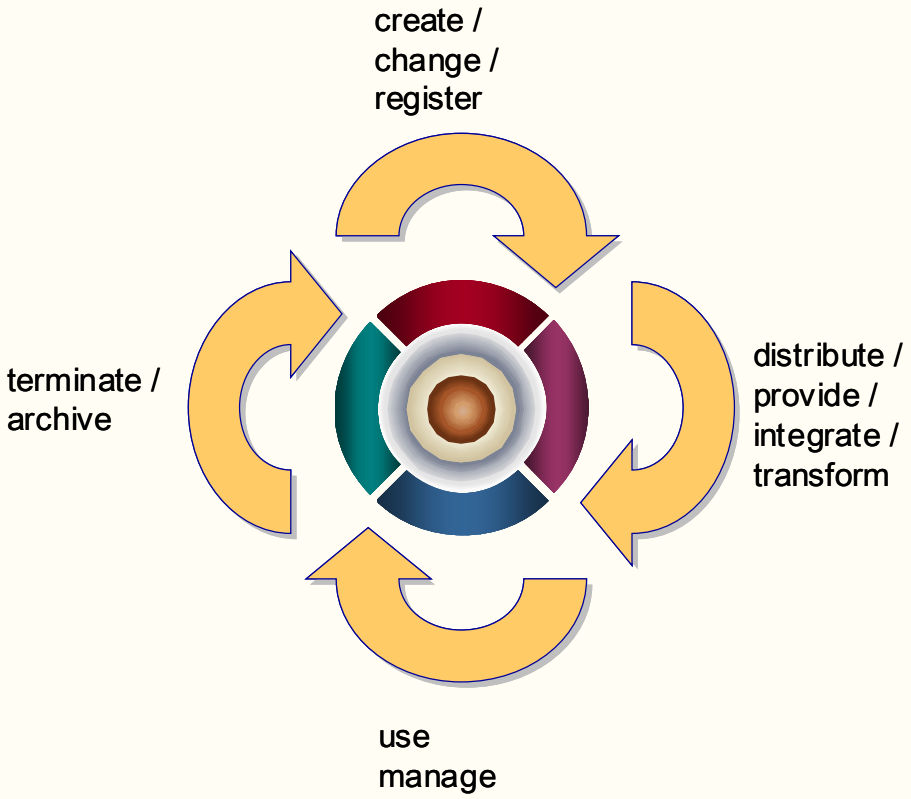
What is Identity Management?



- There is **no common understanding** about the term Identity management
- Analysts and vendors also use the terms ...
  - "**Identity Management**," (Microsoft, Forrester Group)
  - "**Identity and Access Management**," (Gartner Group , Burton Group)
  - „**Secure Identity Management**" (Novell, Entrust, SUN)
  - And more …

➔ Our definition: Identity Management is the holistic **Management** of digital Identity.

Lifecycle of a digital Identity

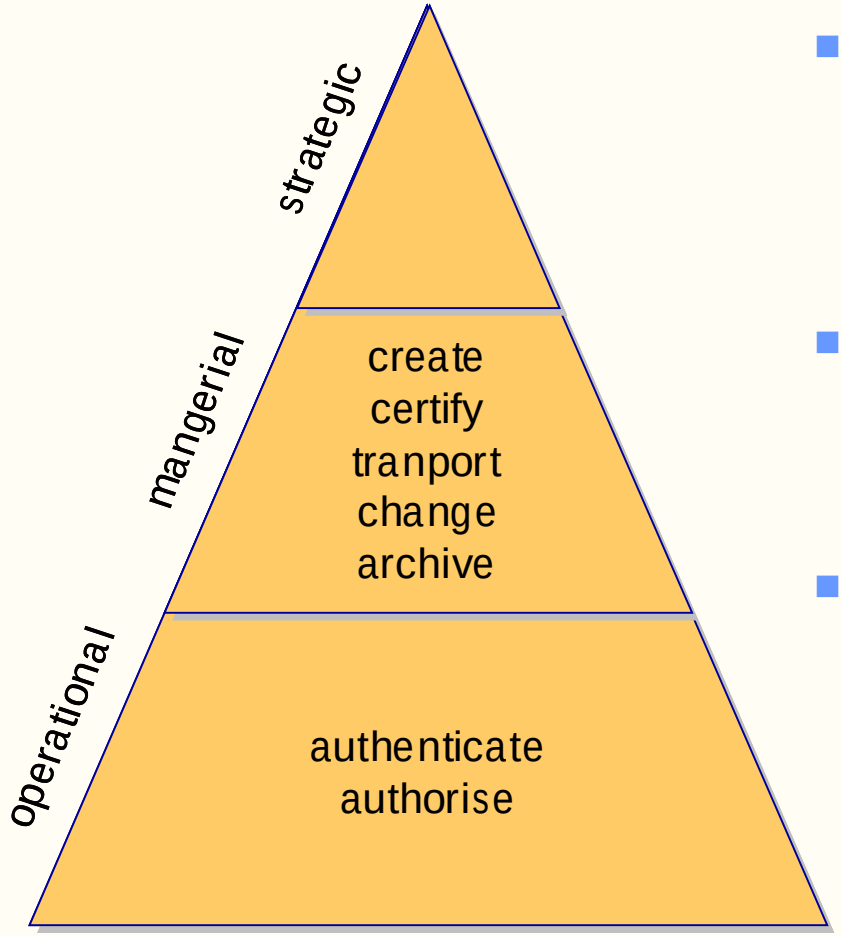


Identity Management deals with ...

- creation
  change
  registration,
- Distribution
  provision
  integration
  transformation,
- Usage
- Termination
  archiving

➔ Identity Management covers all Processes to maintain a digital Identity during it's entire life.

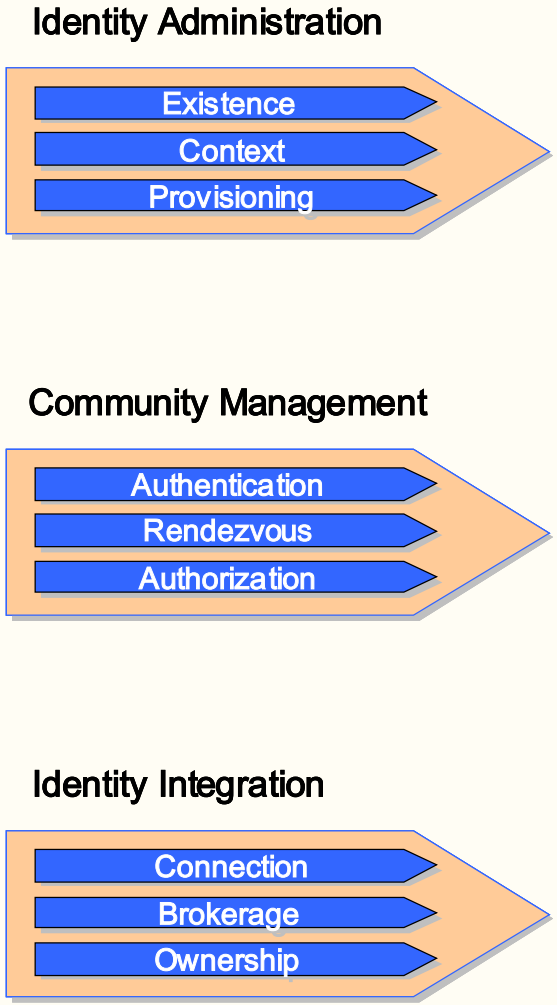
Processes of Identity Management



- By operational or managerial
  - operational: authenticate and authorise
  - managerial: administer digital Identities
- By business or technical
  - business: administer and use
  - technical: integrate, transport, transform and publish
- By existence, certificate and context
  - create, change, delete
  - certify, revoke
  - assign, change, removal of roles and privileges

➔ The processes of Identity Management may be grouped in different ways.

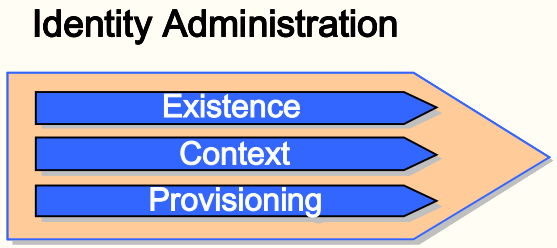
Processes of Identity Management

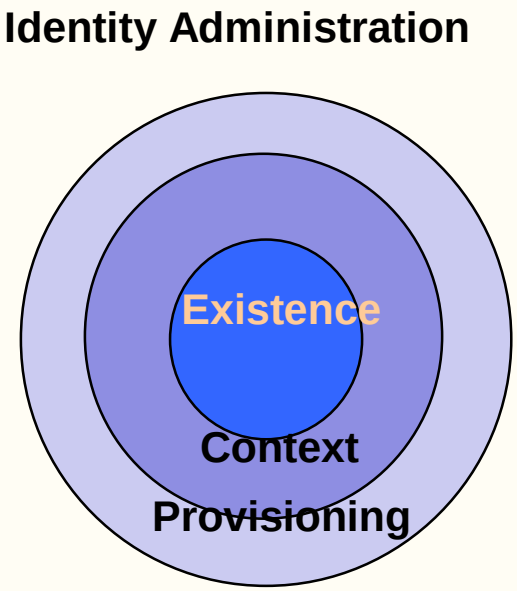


- Identity Administration
  - Management of digital identities, their relation to Organisational units and the assignment of resources.
- Community Management
  - Authentication, publishing and authorisation of persons according to their digital identities.
- Identity Integration
  - Mechanisms to attain synchronisation and actualisation of digital identities, that are distributed across the organisation and and contain partially redundant information.

➔ The most comprehensive definition of Identity Management originates form Microsoft.

Identity Administration

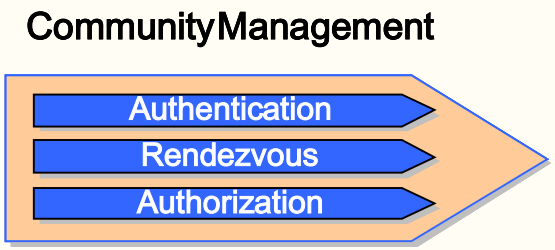




Management of digital identities, their relation to Organisational units and the assignment of resources.

- **Existence**
  - Create, manage, synchronise digital identities.
- **Context**
  - Administer the relations of persons to organisational units (Roles) and their Resources (privileges).
- **Provisioning**
  - Dynamically providing people with the tools they need to do their jobs. Based on a person's digital context, the system delivers the resources necessary for that person based on business rules.

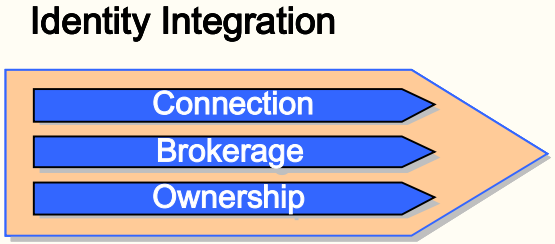
Community Management



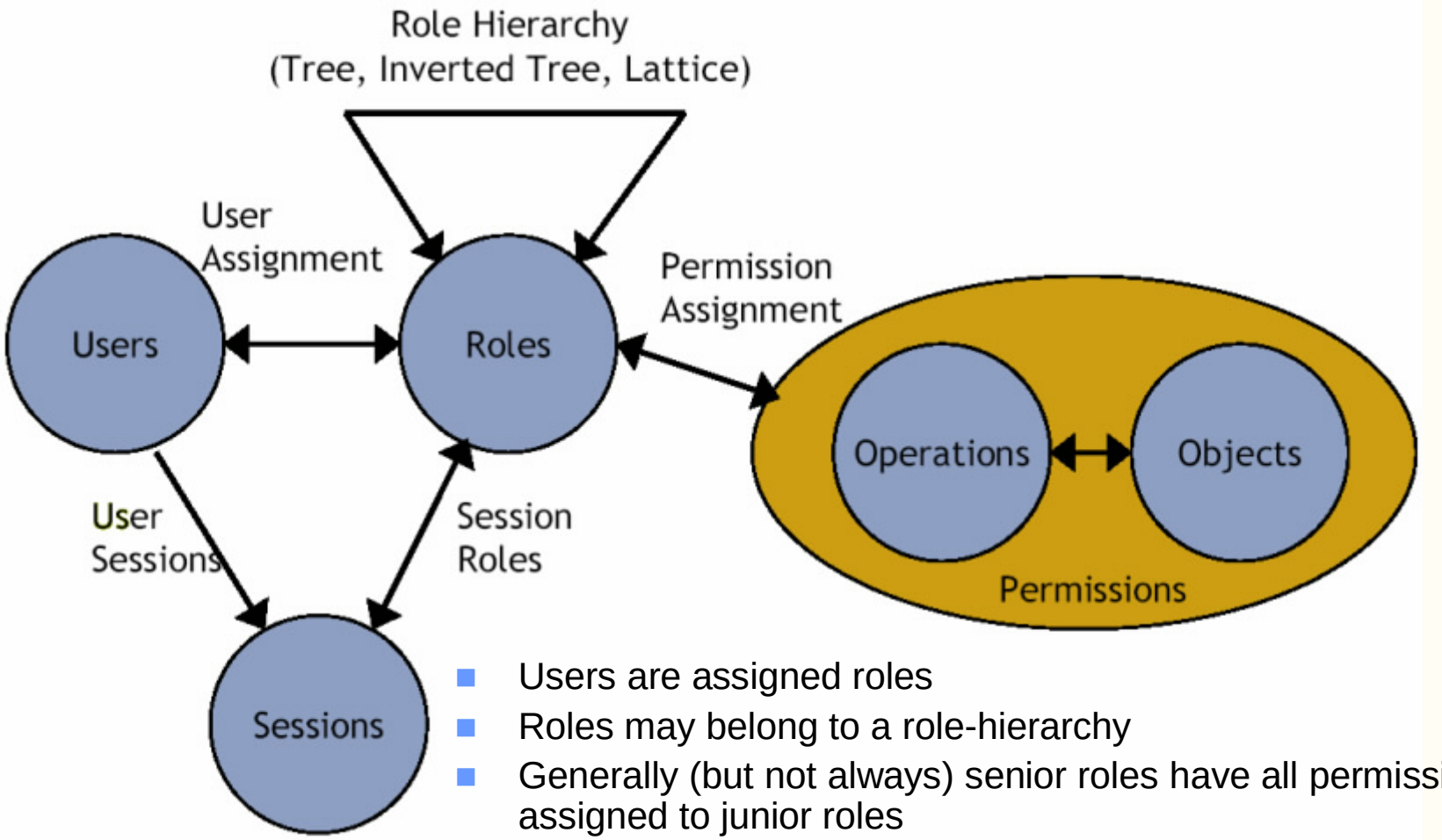
- ***Authentication***
  - verifying the identity of a person using an organization's computing infrastructure.
- ***Rendezvous***
  - connecting employees, partners, customers, and resources with each other. Easily locate and use the network resources to collaborate with each other.
- ***Authorization***
  - granting access to resources based on the credentials of a person's identity and context.

Identity Integration

- ***Connection***
  - linking heterogeneous systems together such that identities can be maintained and used across an entire network infrastructure.
- ***Brokerage***
  - the interchange of identity-related data and operations between heterogeneous systems based on rules that map to a company's business processes.
- ***Ownership***
  - recognizing that while identity information can be duplicated in many systems throughout an organization, some identity attributes can only be authoritatively managed in one place.



Role based access control



- Users are assigned roles
- Roles may belong to a role-hierarchy
- Generally (but not always) senior roles have all permissions assigned to junior roles
- Permissions are operations on objects.
- Permissions can be assigned + (additional) or - (subtractive)
- Roles can be assigned temporarily per session

Source: Ferraiolo, Sandhu, Gavrila: A Proposed Standard for Role-Based Access Control, 2000.

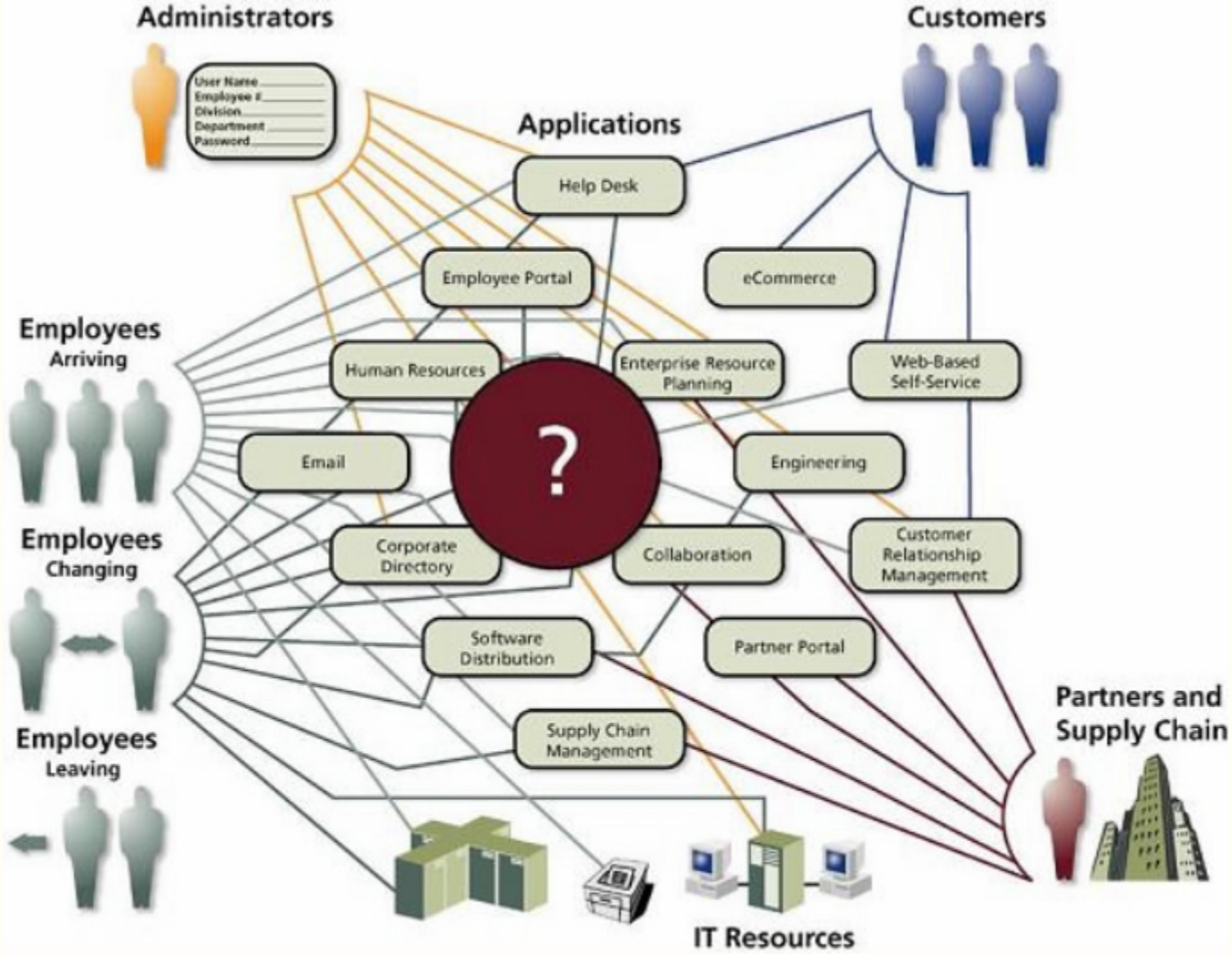
The Identity Network Constituents

- **The Identity Principal** – This is the individual to which the identity profile or attribute information corresponds.
- **The Primary Authenticator** – This is any entity which authenticates an Identity Principal and subsequently shares (asserts) that authentication with another party -- the recipient or relying party.
  Normally, the Primary Authenticator is the party that *introduces* the identity principal into the network.
- **The Identity Provider** (*asserting party*) – This is any party which hosts identity profile and attribute data concerning an Identity Principal.
  This party, in turn, provides that information to other parties upon request and with the permission of the Identity Principal.
- **The Service Provider** (*relying party*) – This is any party which provides services to end-users and relies upon the authentication of a Primary Authenticator or upon the profile information of an Identity Provider.
- **The Identity Network Operator** – This is any third party which provides a standardized legal and business framework within which each of the above constituent are able to engage one another in secure, quality assured identity interchange.
  The Identity Network Operator pools the interests of each constituent and focuses on identifying the redundant processes and eliminating them, providing services which boost confidence and quality, while reducing risk and liability for all.

Assessment

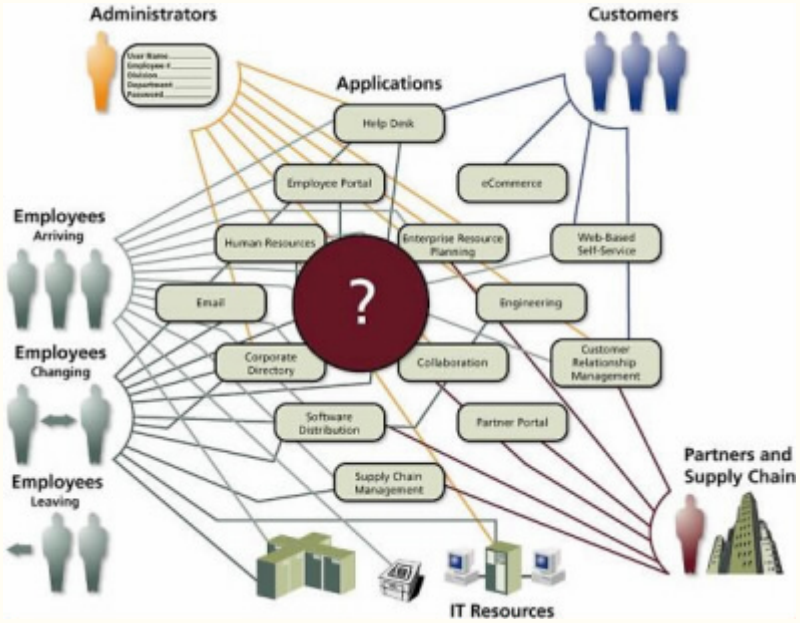
- The identity (well known) problem
- Business Consequences
- Drivers - Why Identity Management?
- Drivers - Why Identity Management?
- New requirements to the Security architecture
- The e-Business Challenge
- The answer – Virtual Enterprise Network
- The fortress approach is no longer enough

The identity (well known) problem



➔User information fragmented, duplicated and obsolete; Redundant processes; No visibility or auditability

Business Consequences



- Flawed security
- High administration and support costs
- Lost business
- Unrealized business opportunities
- Inefficient supply chains
- Audit and regulatory exposure
- Cash outflow

Drivers - Why Identity Management?

- Thinking in business processes ...
  - Demands for a unified Infrastructure.
  - Isolated identities, defined per application and privileges hamper the Implementation.
- Blurring limits ...
  - Reduction of the enterprises vertical range of manufacture
  - towards a virtual enterprise
  - The logical networking is followed by its electronic incarnation.
  - Doing e-Business request the enterprises turning their inside out.
  - External Partners become connected to internal business processes.
- Automated cross company collaboration ...
  - Cannot be supported by enterprise focused technical solutions.
  - Standardised Formats, Protocols and Processes become essential
  - Privileges must be passes through the enterprise perimeter in a reliable way.
- Resource-virtualisation (Grid-Computing, Web-Services)...
  - Need unique digital Identities
  - automated access control.

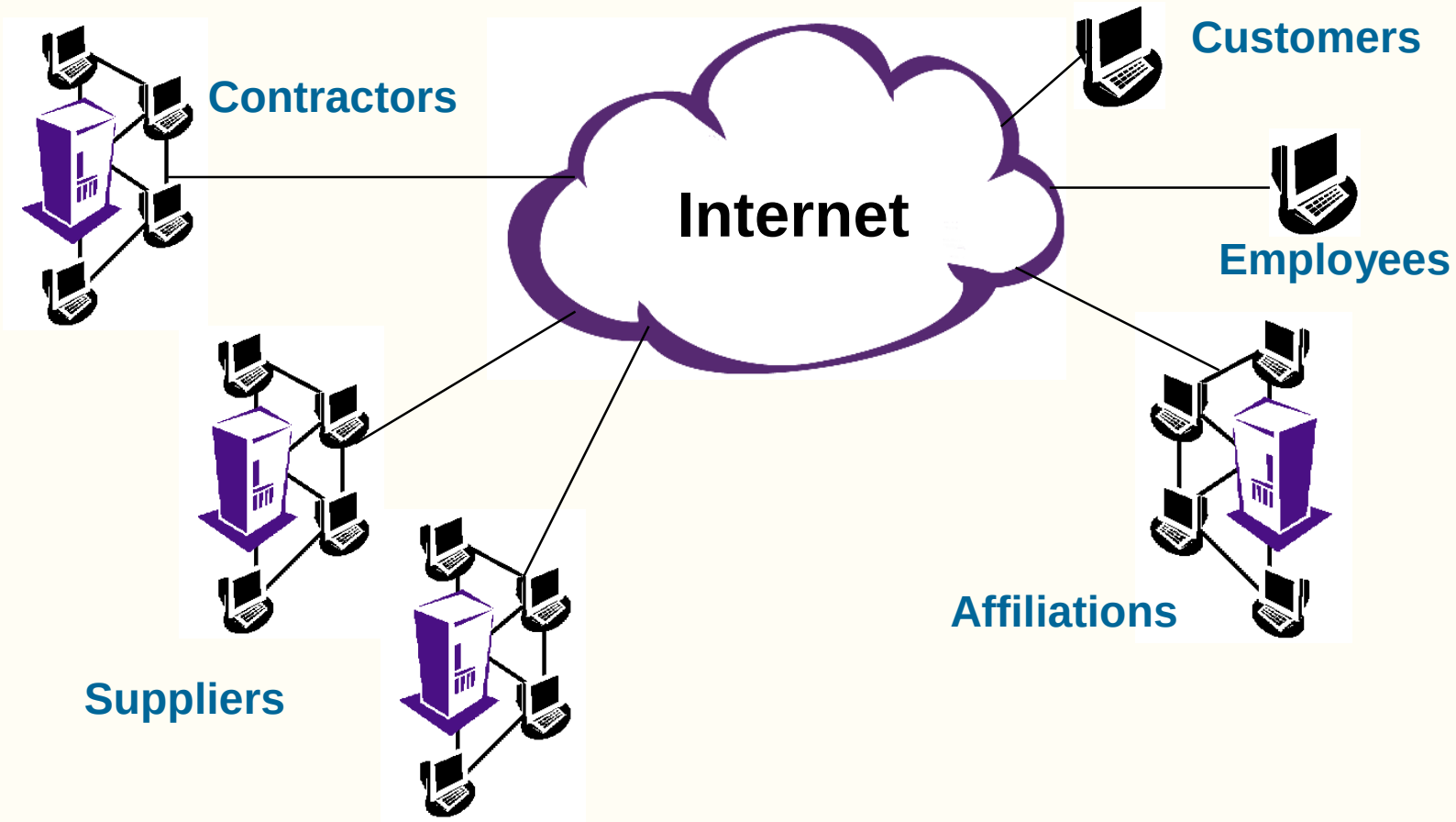
Drivers - Why Identity Management?

(continuation ..)

- Increasing Dynamic
  - Change becomes the normal situation.
  - Users are change their business roles more frequently
  - They change departments,
  - They collaborate in projects.
  - They work in an affiliation for some weeks
  - Temporary external staff needs to access internal resources.
- Raised Security awareness
  - Daily experienced threats of the public Internet,
  - An overall high IT-dependency
  - The actual worldwide political situation
  - A “Could you lend me your Password!" is no longer acceptable.
- Compliance issues
  - Die electronic interlinking of business processes carries risks.
  - Public regulations define corresponding compliance issues.
  - Banks according to Basel Accord II need to set up accruals for their operational risks.
  - Only in case they can prove lower risks costs can be reduced.

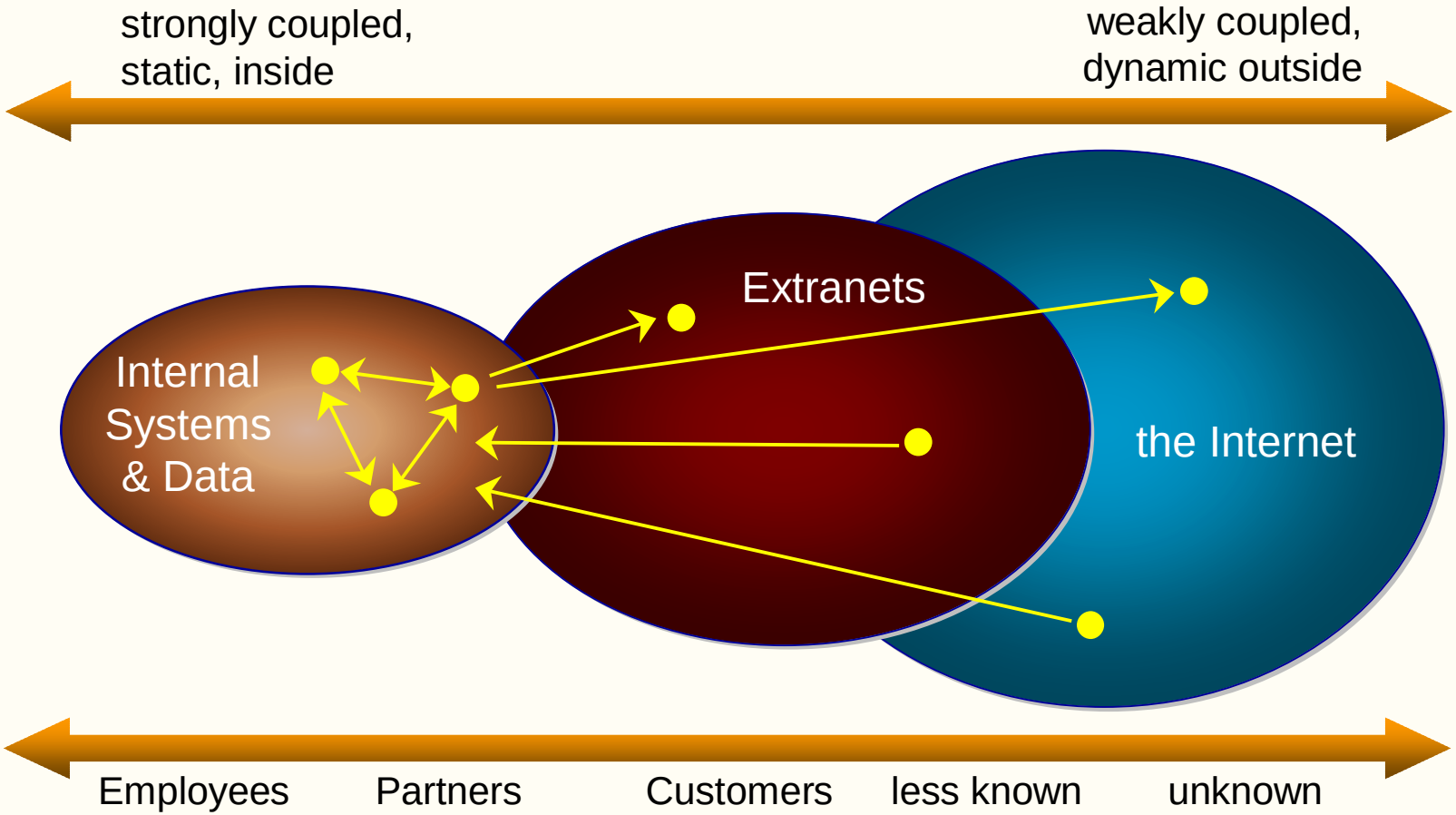
New requirements to the Security architecture

- The means of Communication change …



The e-Business – challenge

- Interoperability *and* Portability: While doing e-Business companies have to turn their inside out



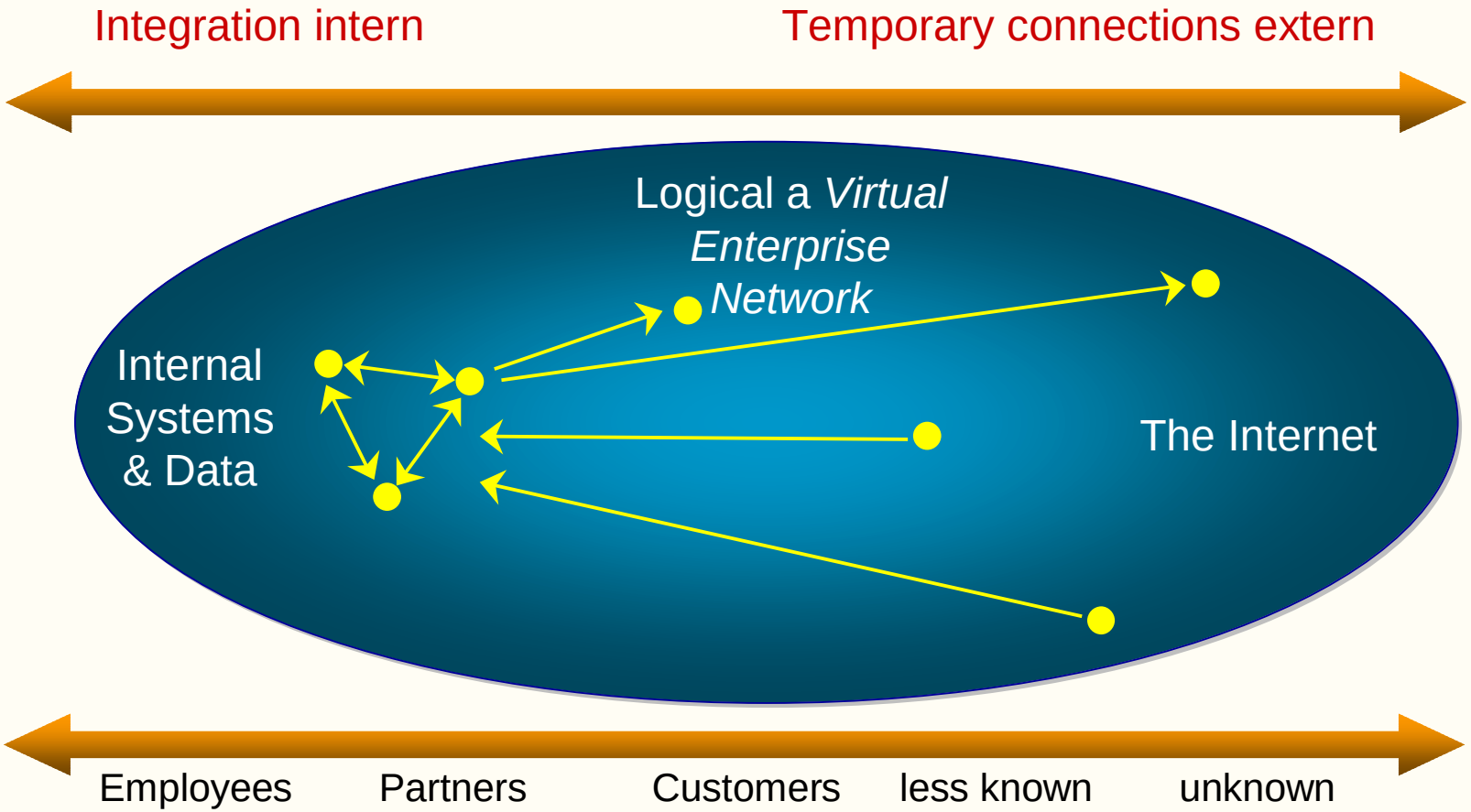
The e-Business Challenge (2)

The blurring Perimeter turns the companies inside out …

- the Requirement to open up the Net leads to two contradictory movements **more flexible access** and **stricter security**
- Security measure **across** logical and physical **border.**
- Applications, databases and operating systems lack a **scalable** and **holistic Mechanism**, to administer identities, certificates and policies across all borders.
- **Wireless**- and other terminals increase the Complexity
- "**SSO**" done wrong poses threats.
- The unavoidable overlap of **public** and **private** Identity Structures makes the situation even more complex.

The answer – Virtual Enterprise Network

- The answer: a flexible Infrastructure



The fortress approach is no longer enough

The fortress approach is not appropriate for e-Business

- It fails to the degree, as applications have to be opened to partners and customers.
- Firewalls alone are no longer sufficient.
- Assignment (and removal) of keys to access the Hotel room.
- Secured Safes with limited access “behind the counter”
- Security personal patrols.

yesterday

Fortress-Model

today

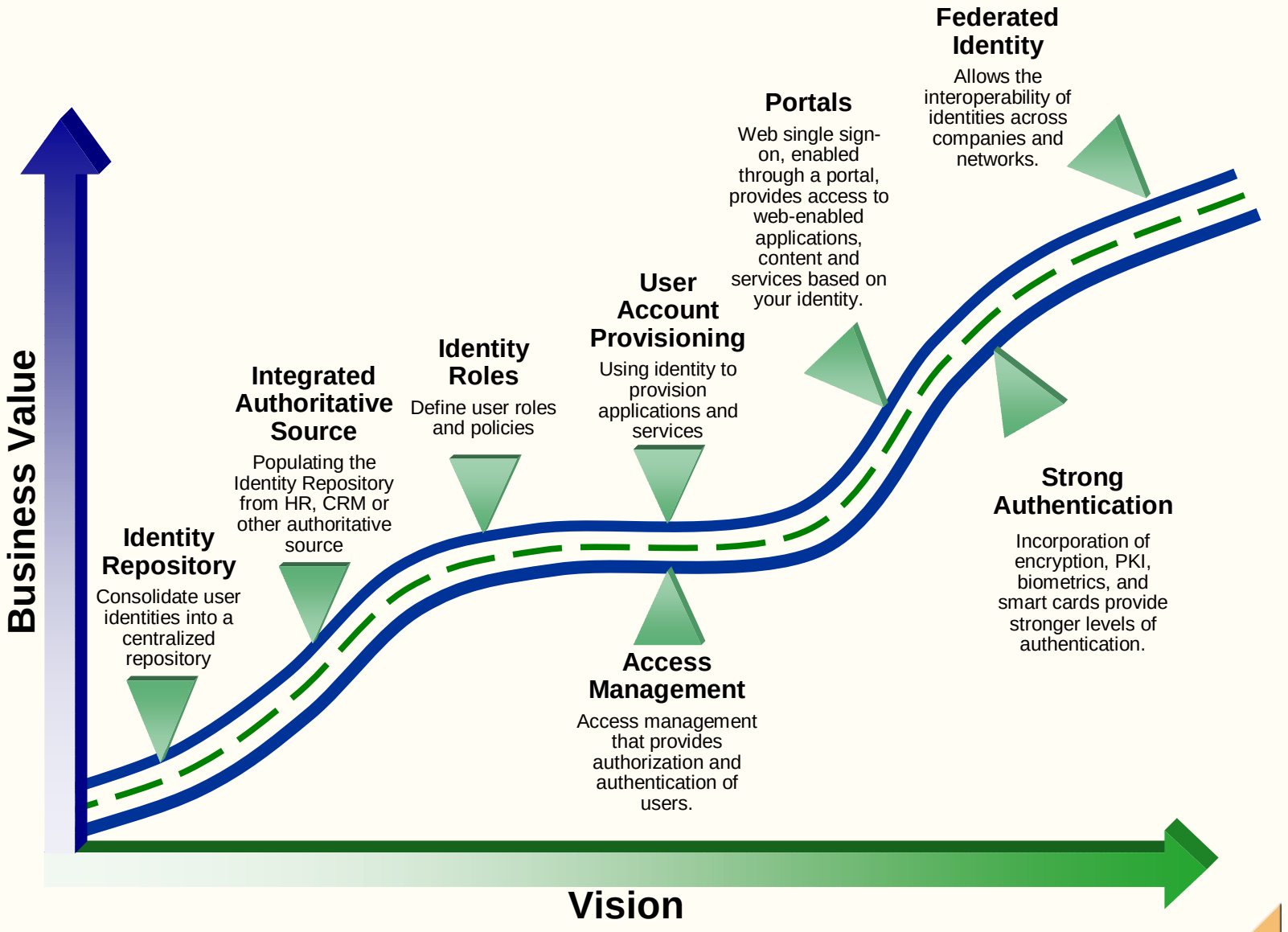
Hotel-Model

Crystal Ball

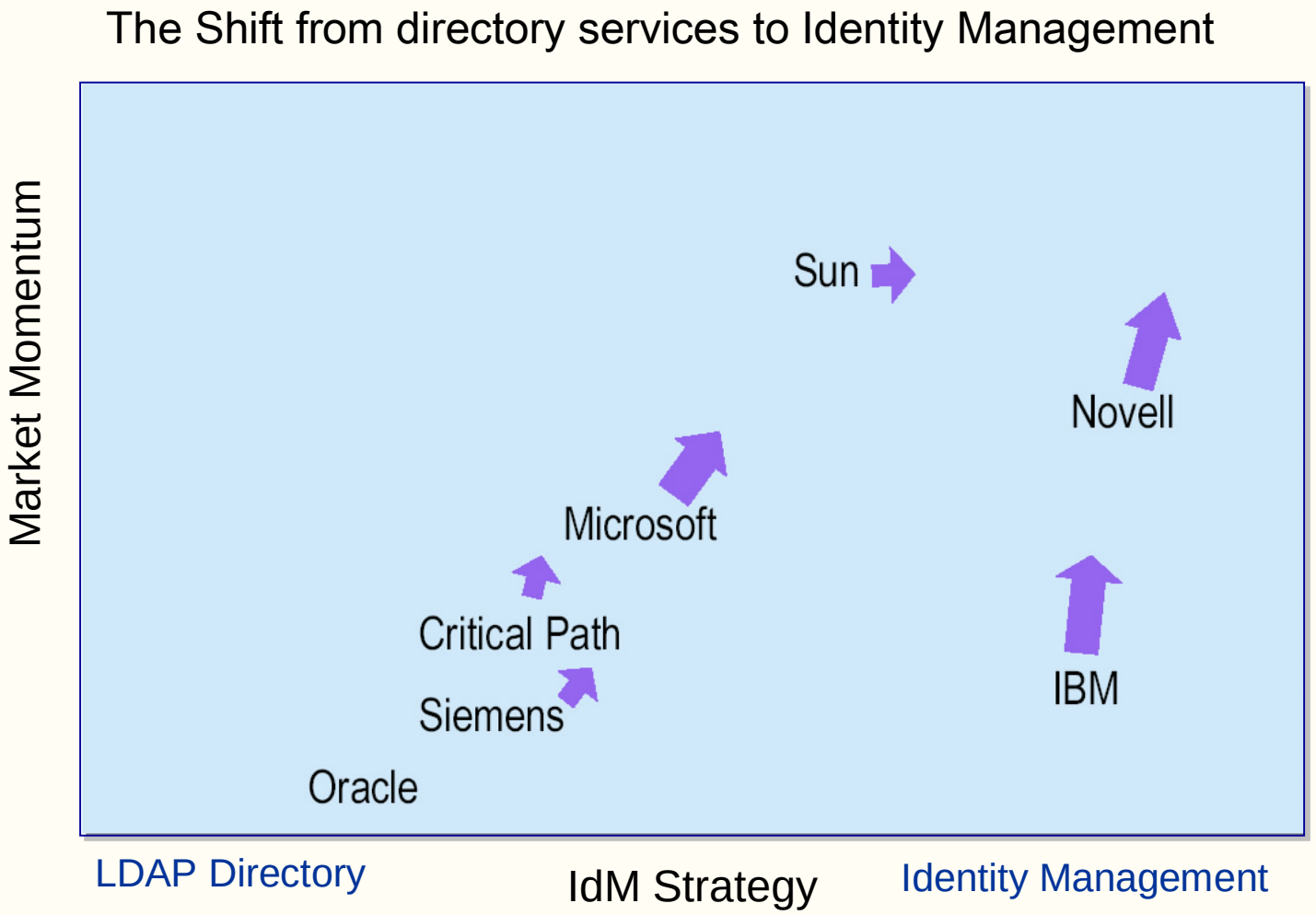
What comes next?

- What have we achieved so far?
- Market trends
- The Shift to Identity Management
- The Future of Identity Management
- Expectation – The hype is about to end soon

What have we achieved so far?



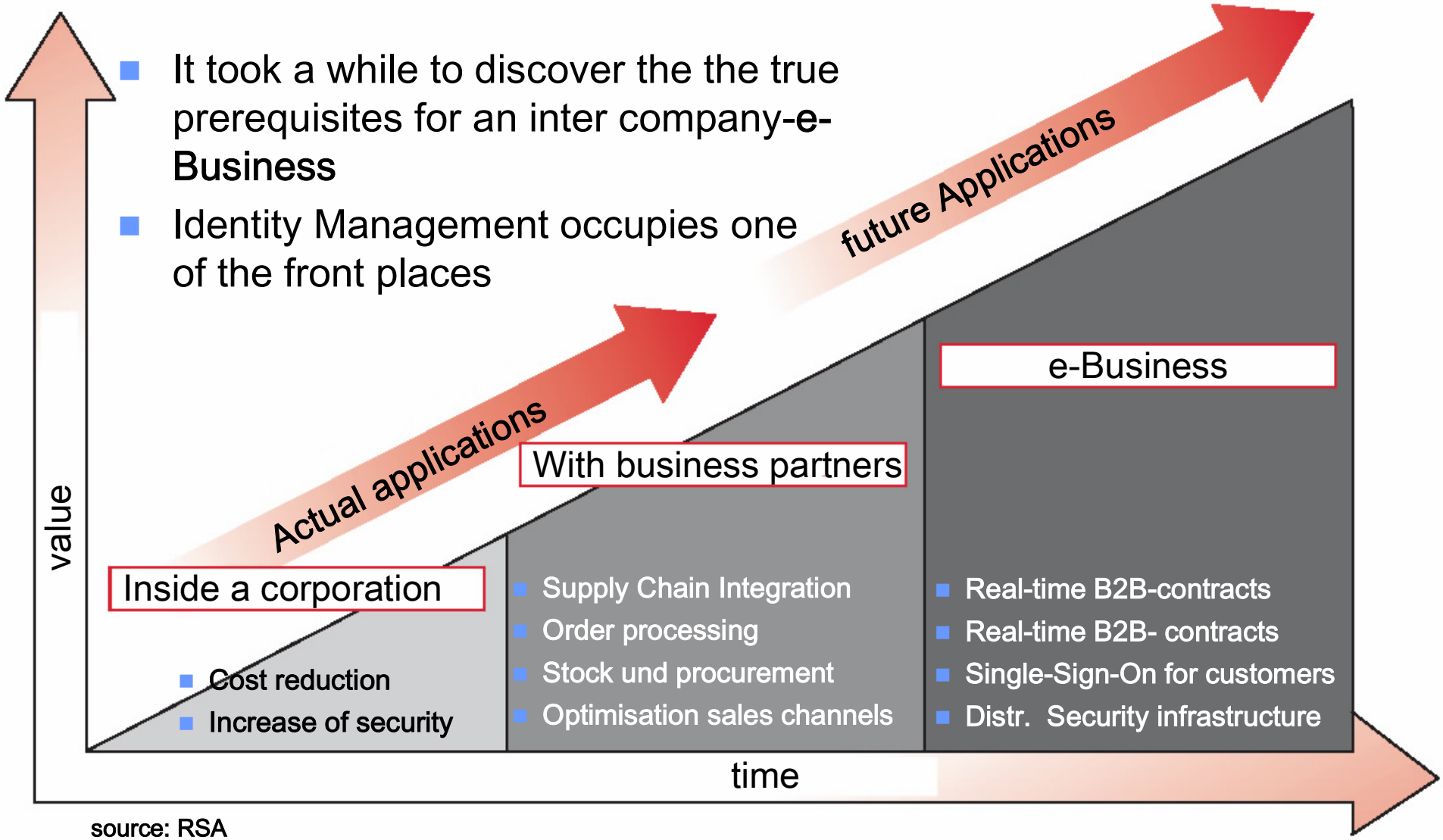
Market trends:



➔Identity Management strategies generate momentum (Burton Group)

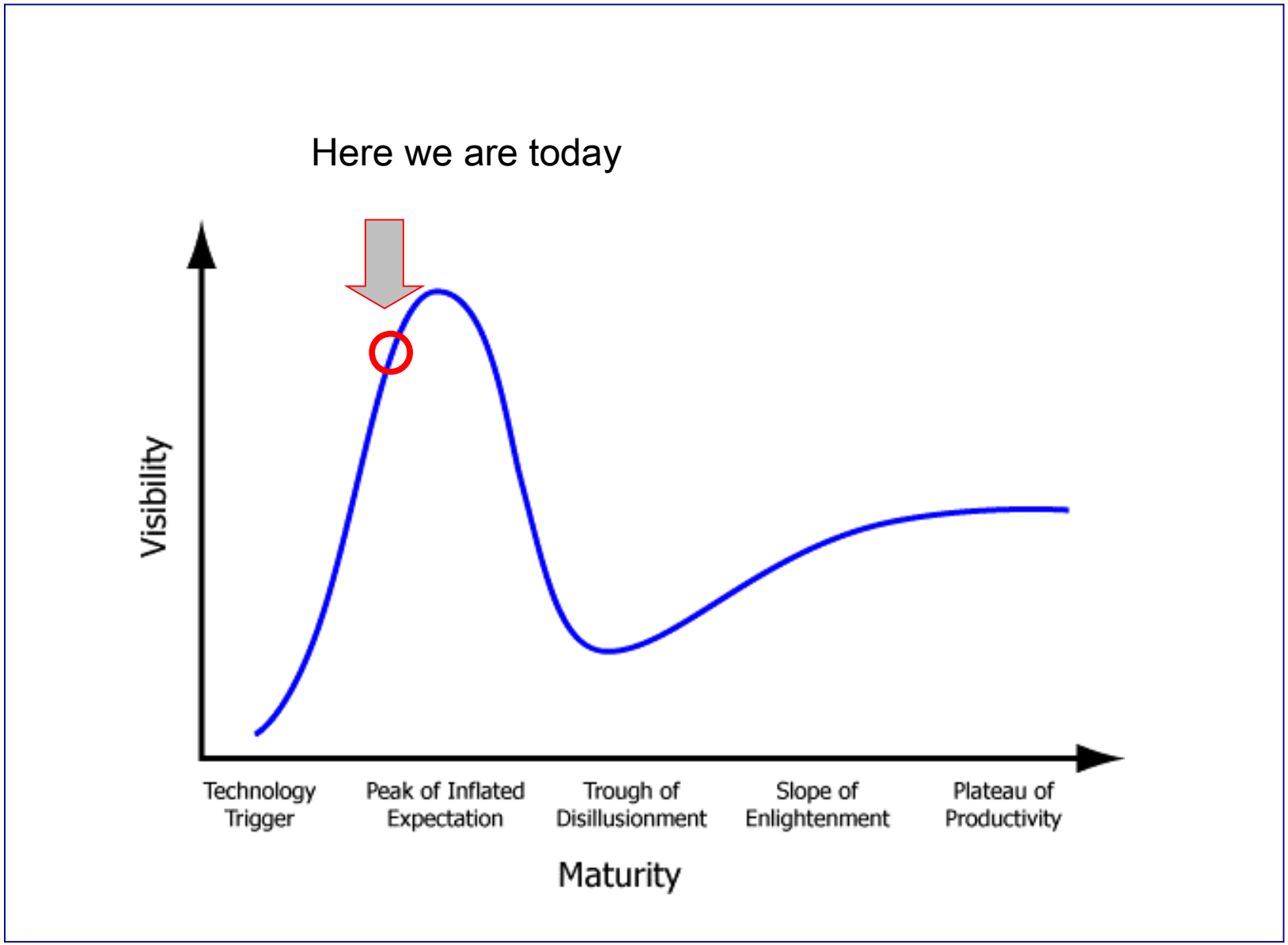
The Future of Identity Management

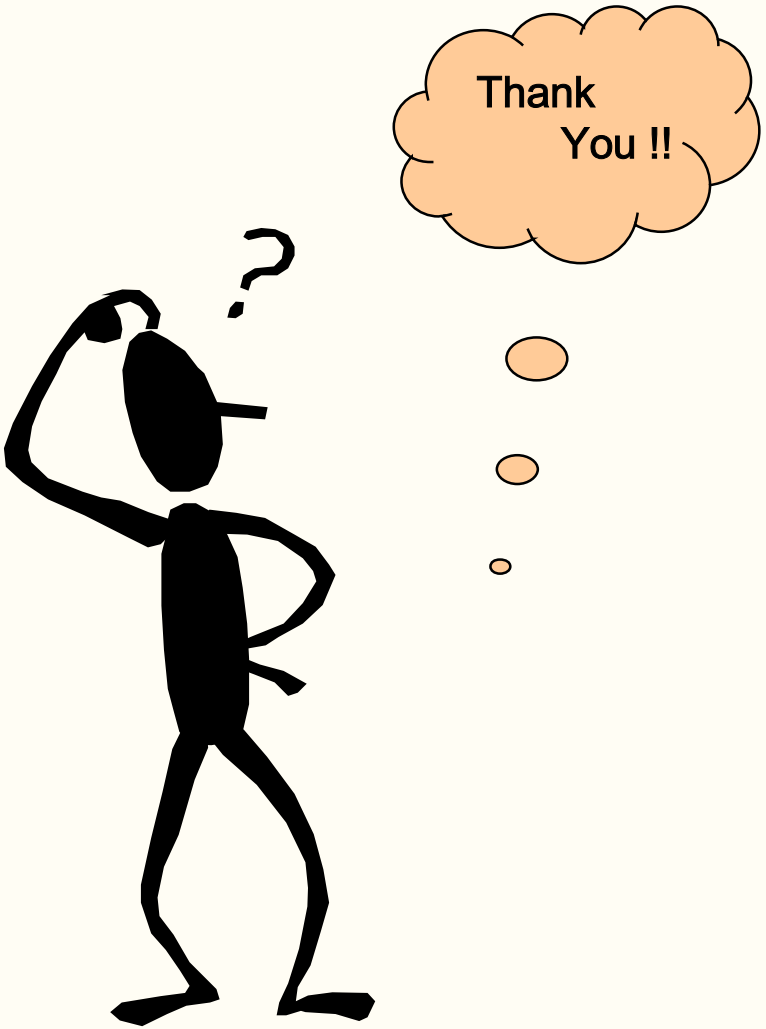
- It took a while to discover the the true prerequisites for an inter company-**e-Business**
- Identity Management occupies one of the front places



source: RSA

Expectation – the hype is about to end soon

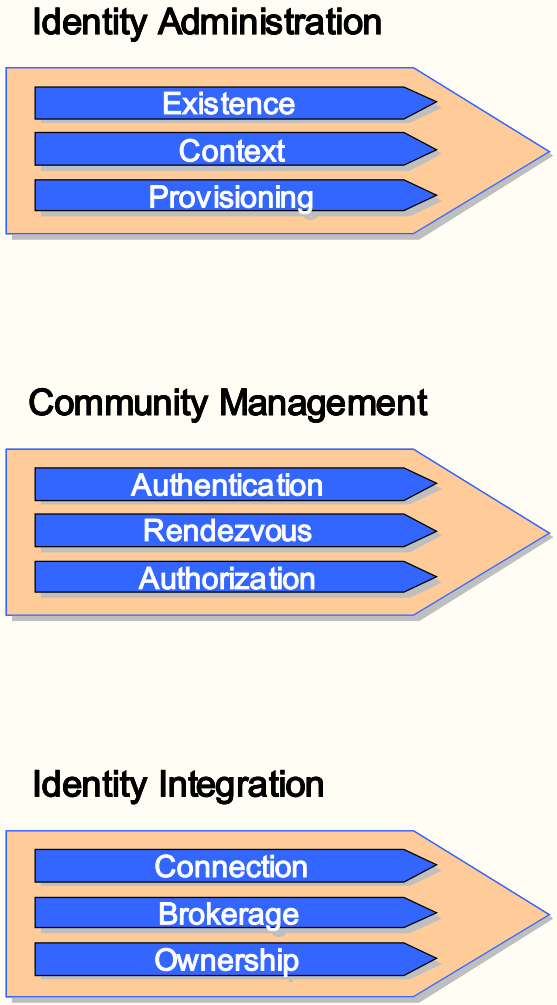



Thank
You !!

Stop, Appendix

From here on the back-up-slides follow ...

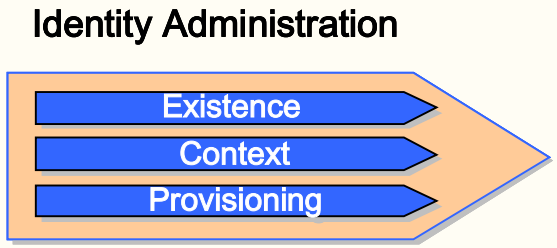
Processes of Identity Management



- Identity Administration
  - Management of digital identities, their relation to Organisational units and the assignment of resources.
- Community Management
  - Authentication, publishing and authorisation of persons according to their digital identities.
- Identity Integration
  - Mechanisms to attain synchronisation and actualisation of digital identities, that are distributed across the organisation and and contain partially redundant information.

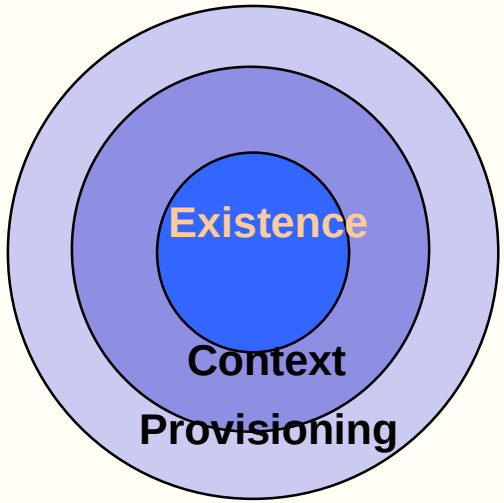
➔ The most comprehensive definition of Identity Management originates form Microsoft.

Identity Administration

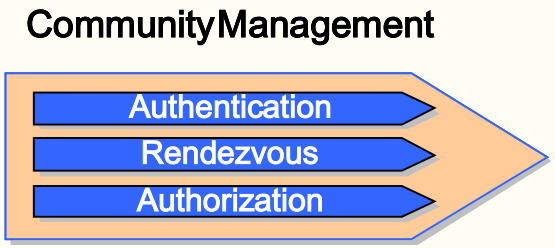


Management of digital identities, their relation to Organisational units and the assignment of resources.

- **Existence**
  - Create, manage, synchronise digital identities.
- **Context**
  - Administer the relations of persons to organisational units (Roles) and their Resources (privileges).
- **Provisioning**
  - Dynamically providing people with the tools they need to do their jobs. Based on a person's digital context, the system delivers the resources necessary for that person based on business rules.



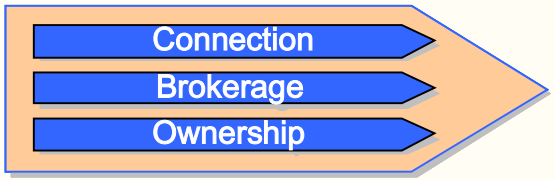
Community Management



- ***Authentication***
  - verifying the identity of a person using an organization's computing infrastructure.
- ***Rendezvous***
  - connecting employees, partners, customers, and resources with each other. Easily locate and use the network resources to collaborate with each other.
- ***Authorization***
  - granting access to resources based on the credentials of a person's identity and context.

Identity Integration

Identity Integration



- ***Connection***
  - linking heterogeneous systems together such that identities can be maintained and used across an entire network infrastructure.
- ***Brokerage***
  - the interchange of identity-related data and operations between heterogeneous systems based on rules that map to a company's business processes.
- ***Ownership***
  - recognizing that while identity information can be duplicated in many systems throughout an organization, some identity attributes can only be authoritatively managed in one place.