The Future of Identity in the Cloud: Requirements, Risks & Opportunities

Marco Casassa Mont

marco.casassa-mont@hp.com

HP Labs
Systems Security Lab
Bristol, UK

Presentation Outline

- Setting the Context: Cloud Computing
- Identity in the Cloud, Risks and Requirements
- Current Approaches and Initiatives
- Towards the Future of Identity in the Cloud
- Conclusions

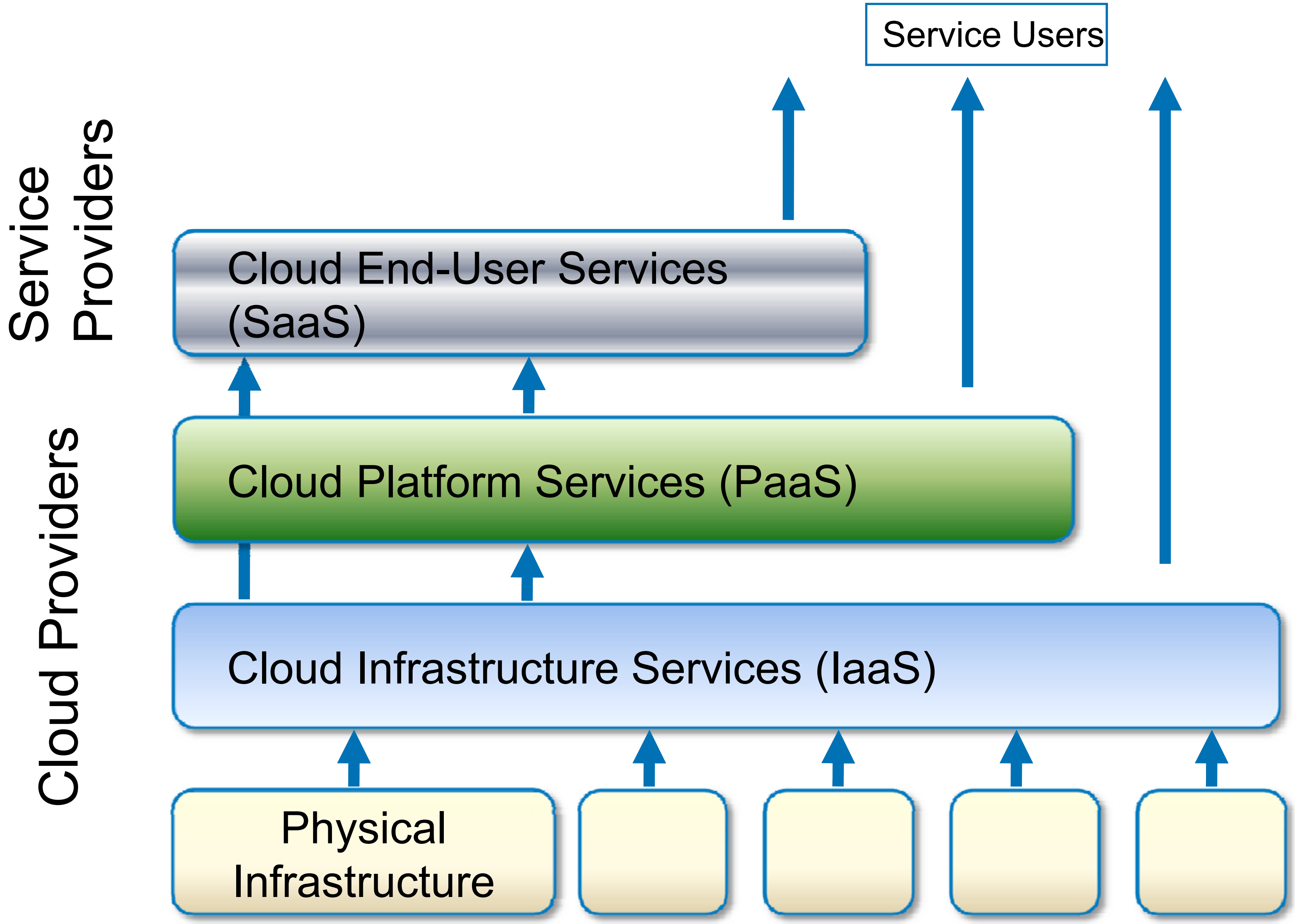
Cloud Computing: Definition

- No Unique Definition or General Consensus about what Cloud Computing is …
- Different Perspectives & Focuses (Platform, SW, Service Levels…)

- Flavours:
  - Computing and IT Resources Accessible Online
  - Dynamically Scalable Computing Power
  - Virtualization of Resources
  - Access to (potentially) Composable & Interchangeable Services
  - Abstraction of IT Infrastructure

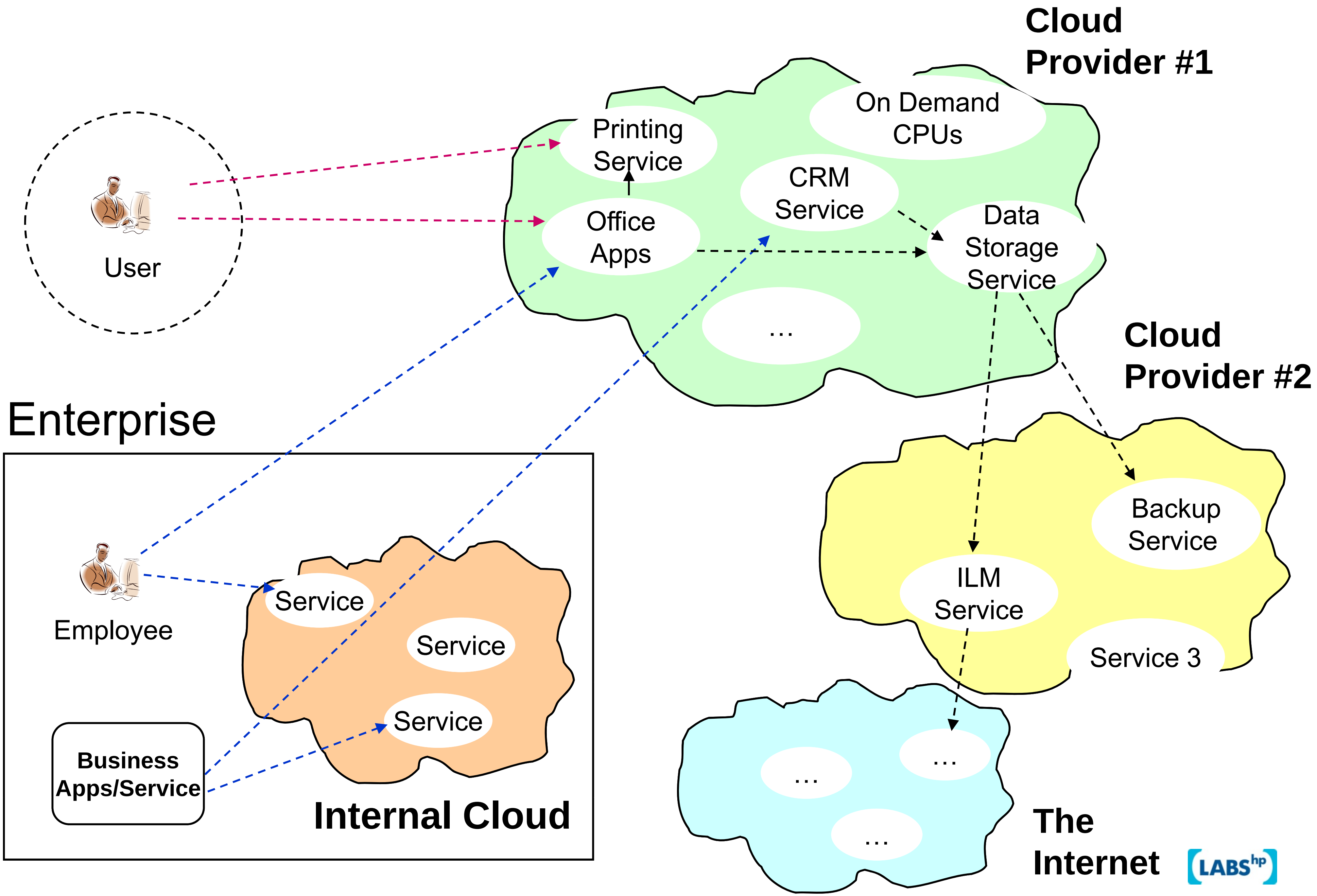
    → No need to understand its implementation: use Services & their APIs
  - Related "Buzzwords": Iaas, PaaS, SaaS, EaaS, …
  - Some current players, at the Infrastructure & Service Level: Salesfoce.com, Google Apps, Amazon, Yahoo, Microsoft, IBM, HP, etc.

Cloud Service Layers


Service Users
Service Providers
Cloud Providers
Cloud End-User Services (SaaS)
Cloud Platform Services (PaaS)
Cloud Infrastructure Services (IaaS)
Physical Infrastructure

Source: HP Labs, Automated Infrastructure Lab (AIL), Bristol, UK - Peter Toft

Cloud Computing: Models



Cloud Computing: Key Aspects

- **Internal, External and Hybrid Clouds**
  - Cloud Providers and/or The Internet
    - Infrastructure Providers
    - Service Providers
- **Composition of Services**
  - Within a Cloud Provider
  - Across Cloud Providers
- **Entities consuming Services in the Clouds**
  - Organisations:
    - Business Applications, Services, etc.
    - Employees
  - Private Users

Cloud Computing: Implications

- **Enterprise:**

  Paradigm Shift from “Close & Controlled” IT Infrastructures and Services to Externally Provided Services and IT Infrastructures

- **Private User:**

  Paradigm Shift from Accessing Static Set of Services to Dynamic & Composable Services

- **General Issues:**
  - Potential Loss of Control (on Data, Infrastructure, Processes, etc.)
  - Data & Confidential Information Stored in The Clouds
  - Management of Identities and Access (IAM) in the Cloud
  - Compliance to Security Practice and Legislation
  - Privacy Management (Control, Consent, Revocation, etc.)
  - New Threat Environments
  - Reliability and Longevity of Cloud & Service Providers

Cloud Computing: Initiatives

Recent General Initiatives aiming at Shaping Cloud Computing:

- **Open Cloud Manifesto**
  - Making the case for an Open Cloud

dedicated to the belief that the cloud should be open

- **Cloud Security Alliance**
  - Promoting Best Security Practices for the Cloud
- **Jericho Forum**
  - Cloud Cube Model:
    Recommendations & (Security) Evaluation
    Framework
- …

Presentation Outline

- Setting the Context: Cloud Computing
- Identity in the Cloud, Risks and Requirements
- Current Approaches and Initiatives
- Towards the Future of Identity in the Cloud
- Conclusions

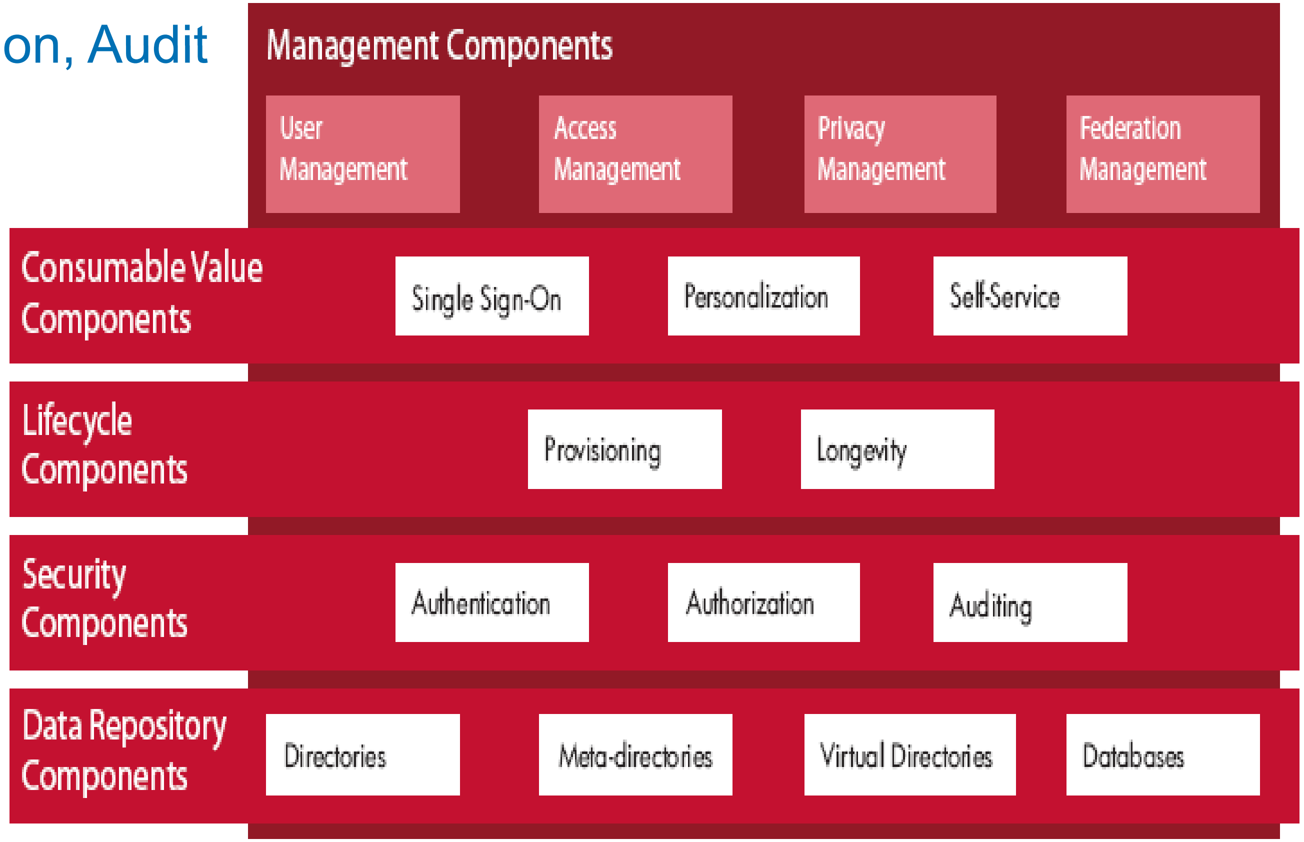
Identity and Access Management (IAM)

- Enterprise IAM

  - Network Access Control (NAC)
  - Directory Services
  - Authentication, Authorization, Audit
  - Provisioning
  - Single-Sign-On, Federation
  - …

- IAM is part of IT Security Strategy

  - Risk Management
  - Policy Definitions
  - Compliance & Governance Practices
  - Legislation



Management Components

User Management

Access Management

Privacy Management

Federation Management

Consumable Value Components

Single Sign-On

Personalization

Self-Service

Lifecycle Components

Provisioning

Longevity

Security Components

Authentication

Authorization

Auditing

Data Repository Components

Directories

Meta-directories

Virtual Directories

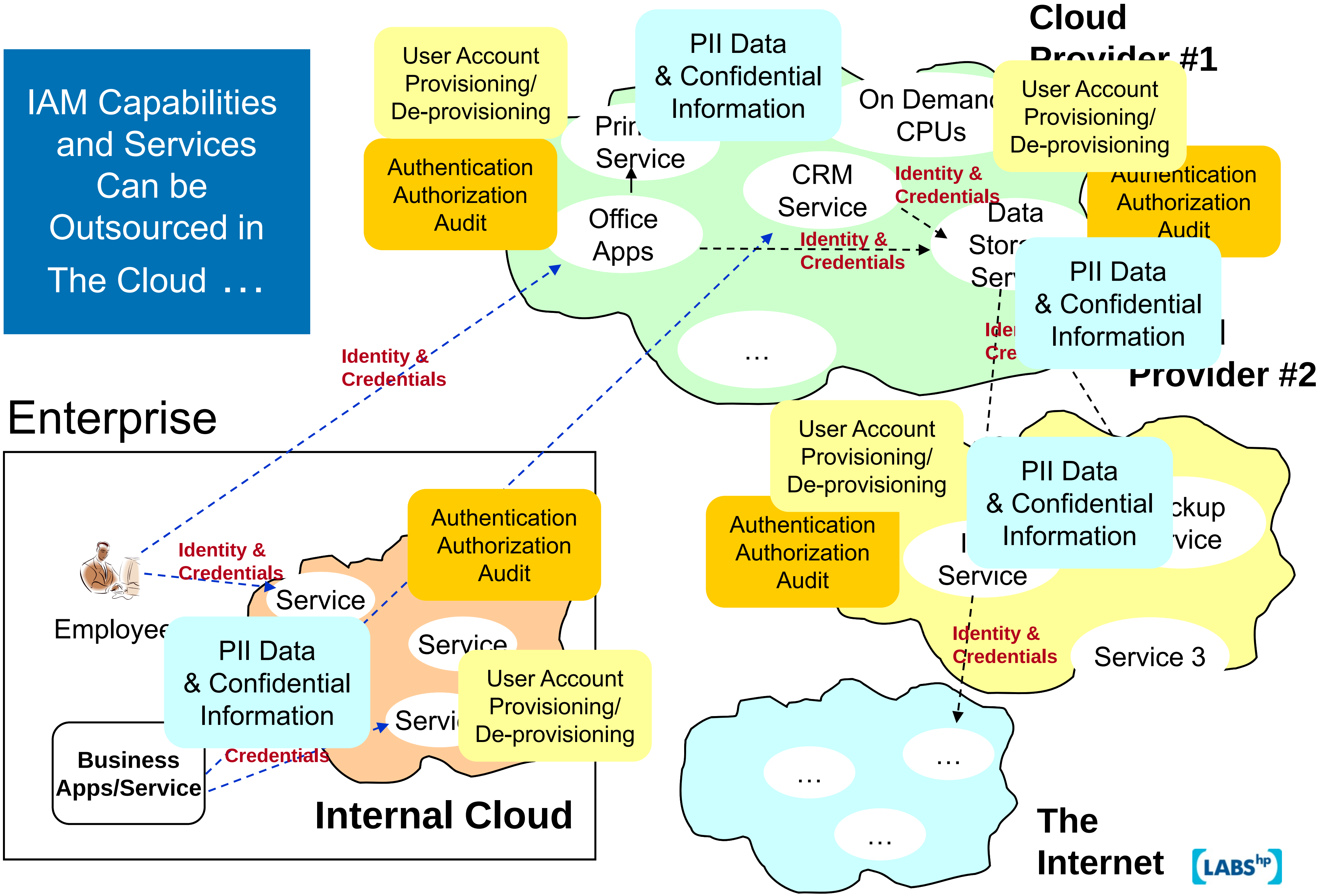
Databases

→ Based on Enterprise Contexts

→ Need to Think about IAM in the Cloud Paradigm

Identity in the Cloud: Enterprise Case

IAM Capabilities and Services Can be Outsourced in The Cloud …



Identity in the Cloud: Enterprise Case

Issues and Risks [1/2]

- Potential Proliferation of Required Identities & Credentials to Access Services
  → Misbehaviours when handling credentials (writing down, reusing, sharing, etc.)

- Complexity in correctly "enabling" Information Flows across boundaries
  → Security Threats
  (Enterprise → Cloud & Service Providers, Service Provider → Service Provider, …_

- Propagation of Identity and PII Information across Multiple Clouds/Services
  → Privacy issues (e.g. compliance to multiple Legislations, Importance of Location, etc.)
  → Exposure of business sensitive information
  (employees' identities, roles, organisational structures, enterprise apps/services, etc.)
  → How to effectively Control this Data?

- Delegation of IAM and Data Management Processes to Cloud and Service Providers
  → How to get Assurance that these Processes and Security Practice are Consistent with Enterprise Policies?
  - Recurrent problem for all Stakeholders: Enterprise, Cloud and Service Providers …
  → Consistency and Integrity of User Accounts & Information across various Clouds/Services
  → How to deal with overall Compliance and Governance issues?

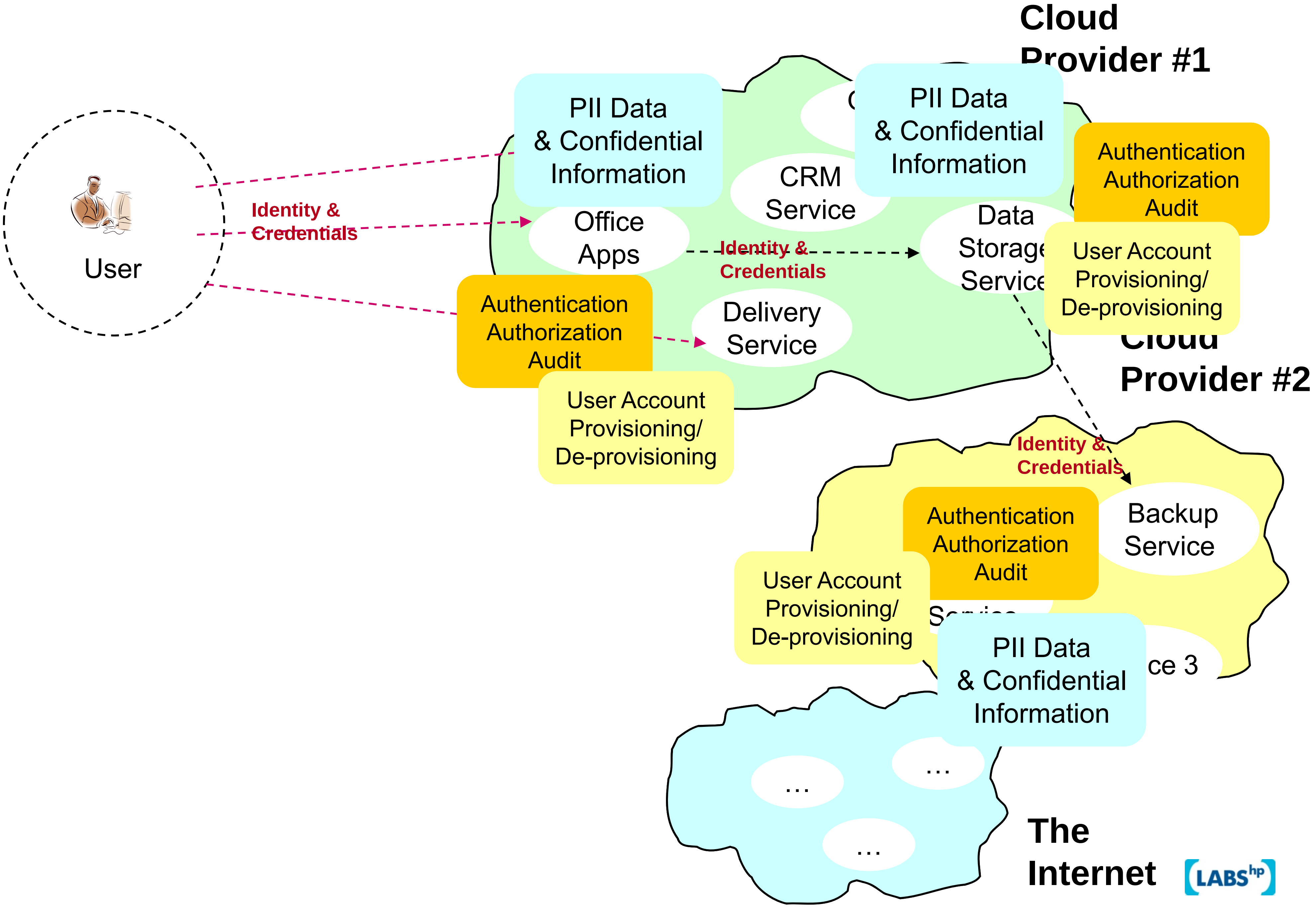
Identity in the Cloud: Enterprise Case

Issues and Risks [2/2]

- Migration of Services between Cloud and Service Providers
  → Management of Data Lifecycle

- Threats and Attacks in the Clouds and Cloud Services
  → Cloud and Service Providers can be the "weakest links" wrt Security & Privacy
  → Reliance on good security practice of Third Parties

Identity in the Cloud: Consumenr Case



Cloud Provider #1
User
Identity & Credentials
PII Data & Confidential Information
Office Apps
CRM Service
PII Data & Confidential Information
Authentication Authorization Audit
Data Storage Service
Identity & Credentials
User Account Provisioning/ De-provisioning
Authentication Authorization Audit
Delivery Service
User Account Provisioning/ De-provisioning
Cloud Provider #2
Identity & Credentials
Authentication Authorization Audit
Backup Service
User Account Provisioning/ De-provisioning
Service
PII Data & Confidential Information
ce 3
…
…
…
The Internet

Identity in the Cloud: User Case

Issues and Risks

- Potential Proliferations of Identities & Credentials to Access Services
  → Misbehaviours when handling credentials (writing down, reusing, sharing ,etc.)

- Potential Complexity in Configuring & Handling Interactions between various Services
  → Introducing vulnerabilities

- Propagation of Identity and PII Information across Multiple Clouds/Sites
  → Privacy issues (e.g. compliance to multiple Legislations, Importance of Location, etc.)
  → How to handle Consent and Revocation?
  → How to effectively Control this data?

- Trust Issue
  → How to get Assurance that Personal Data and Confidential Information is going to be Handled as Expected, based on Users' (privacy) Preferences and Expectations?
  → Migration and Deletion of Data

- New Threats
  → Bogus Cloud and Service Providers
  → Identity Thefts
  → Configuration & Management Mistakes

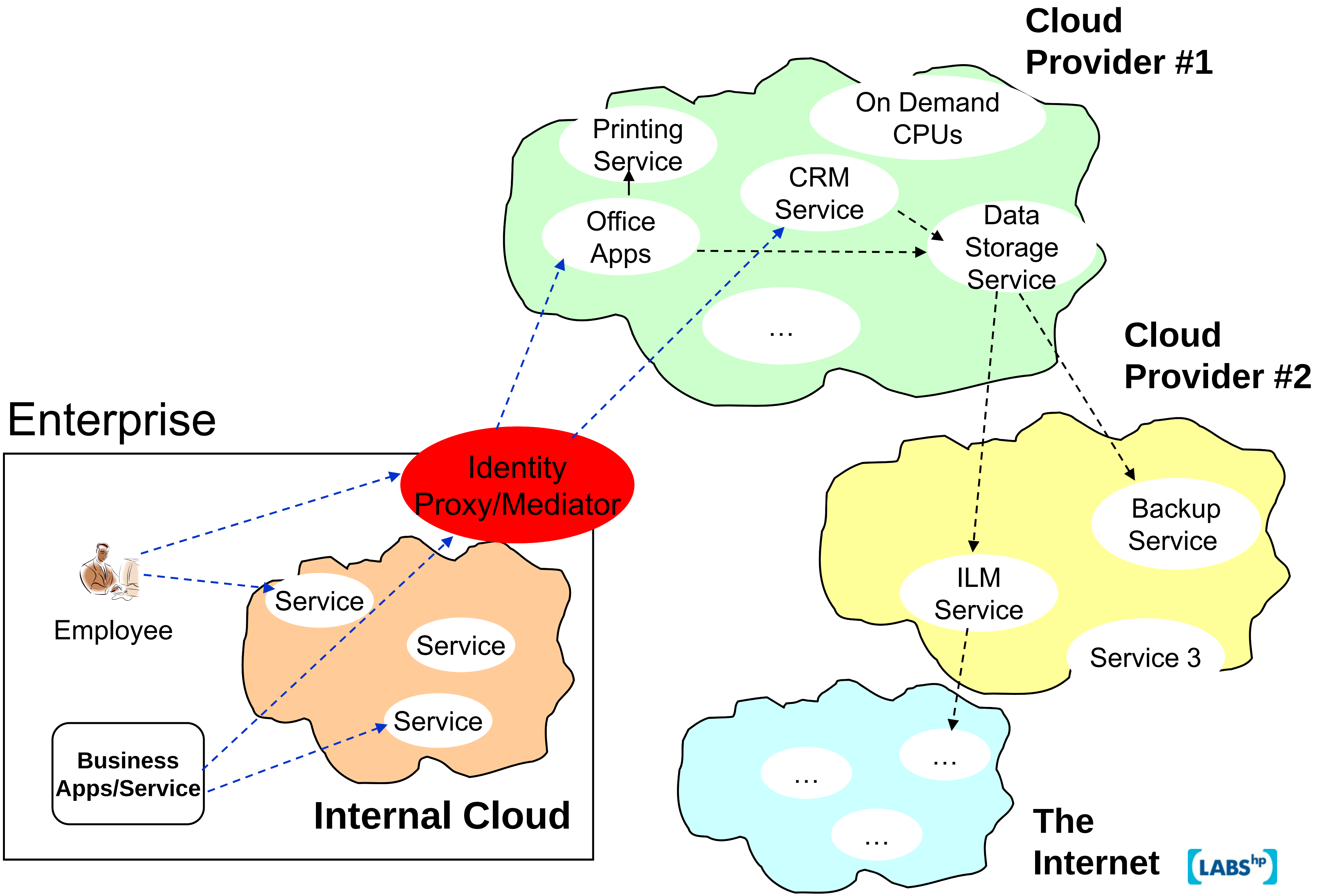
Identity in the Cloud Requirements

- Simplified Management of Identities and Credentials
- Need for Assurance and Transparency about:
  - IAM (Outsourced) Processes
  - Security & Privacy Practices
  - Data Lifecycle Management
- Compliance to Regulation, Policies and Best Practice
  - Need to redefine what Compliance means in The Cloud
- Accountability
- Privacy Management: Control on Data Usage & Flows
- Reputation Management

Presentation Outline

- Setting the Context: Cloud Computing
- Identity in the Cloud, Risks and Requirements
- Current Approaches and Initiatives
- Towards the Future of Identity in the Cloud
- Conclusions

Identity in the Cloud:Identity Proxy Approach



Identity Proxy/Mediator Approach

- Enterprise-focused
- Centralised Management of Credentials and User Accounts
- Interception by Identity Proxy and mapping to “External Identities/Accounts”

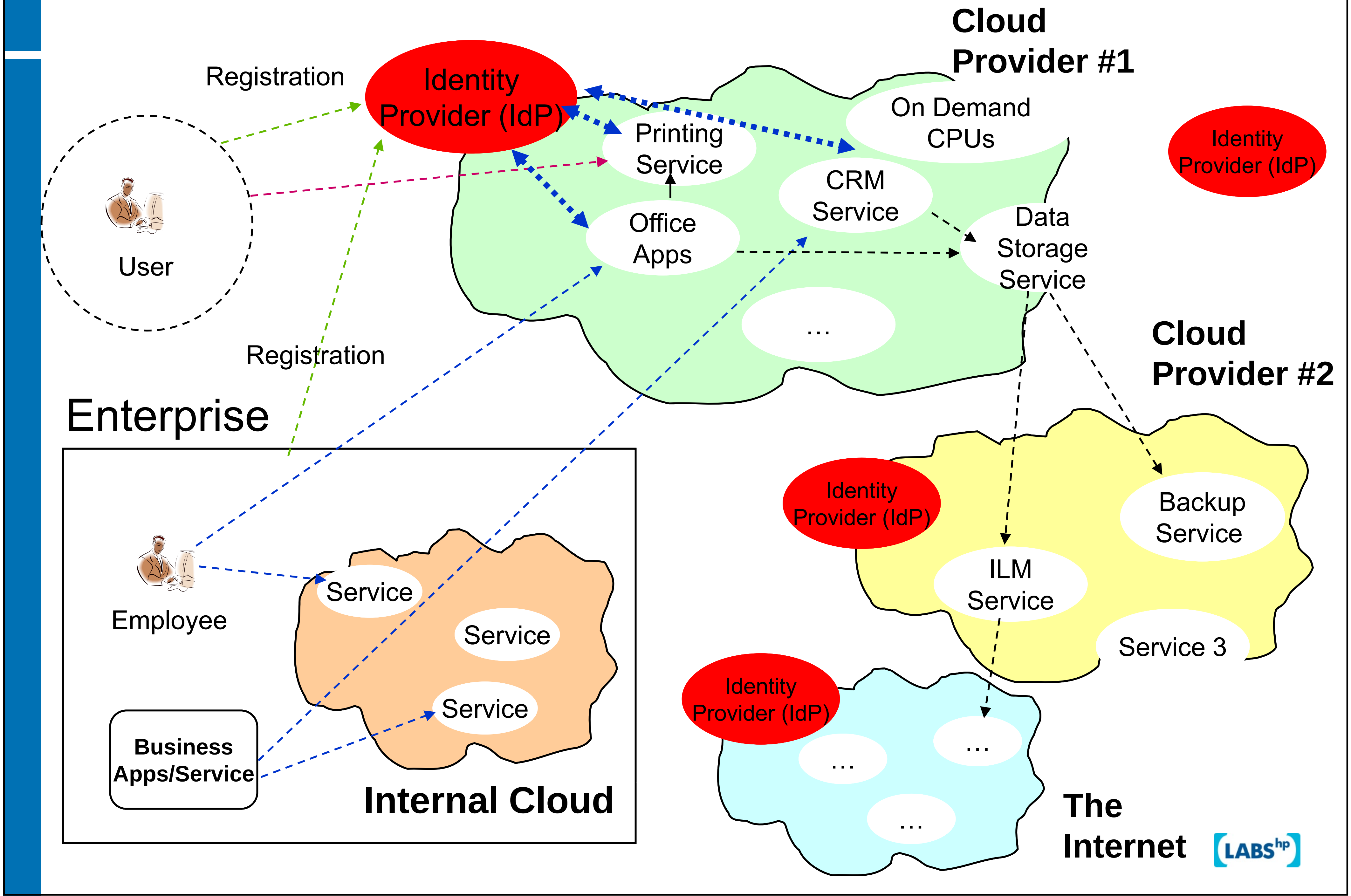
Pros

- Enterprise Control on Identities and mappings
- Centralisation & Local Compliance

Cons

- Scalability Issues. What about the management of Identities exposed between Composed Services (Service1→Service2)?
- Lack of Control beyond first point of contact
- Accountability and Global Compliance Issues

Identity in the Cloud: Federated Approach



Identity in the Cloud: Federated Approach

- Federated Identity Management: Identity & Service Providers
- Cloud Provider could be the "Identity Provider" for the Services/Service Providers in its Cloud
- Approach suitable for Enterprises and private Users

Pros

- "Cloud Provider-wide" Control and Management of Identities
- Potential setting of Security and Privacy constraints at the Identity Provider site
- Circle of Trusts → Auditing, Compliance Checking, etc.
- Handled with Contracts and SLAs

Cons

- IdPs become a bottleneck/central point of control → privacy issues
- Scalability across multiple Cloud Providers. Federated IdPs?
- Reliance on IdPs for Assurance and Compliance (Matter of Trust …)

Presentation Outline

- Setting the Context: Cloud Computing
- Identity in the Cloud, Risks and Requirements
- Current Approaches and Initiatives
- Towards the Future of Identity in the Cloud
- Conclusions

Future of Identity in the Cloud: Drivers

- It is Not just a Matter of Technologies and Operational Solutions
- Need for effective Compliance to Laws and Legislation (SOX, HIPAA, EU data Directives, etc.), Business Agreements and Policies
- Need for more Assurance:
  - Enterprises: Assurance that IAM, Security, Privacy and Data Management processes are run as expected by Cloud Providers and Service Providers
  - Service Providers: Assurance from other Service Providers and Cloud Providers
  - End-Users: Assurance about Privacy, Control on Data, etc.
- Need for Transparency and Trust about IAM processes and Data Management in the Clouds
- Privacy Management

Future of Identity in the Cloud: Opportunities

- New Ways to provide Services, Compose them and get the best deals, both for Users and Organisations

  → Identity and Identity Management is going to Play a key Role

- Unique Chance to re-think what Identity and Identity Management means in the Cloud and how to Handle it

  → vs. simply trying to adapt and use the old IAM model

- New Technological, Personal and Social Challenges

  → Opportunity for Research and Development of new Solutions

Future of Identity in the Cloud

Overview of some HP Labs Research Areas

1. Trusted Infrastructure and Cloud Computing
2. Identity Assurance
3. Identity Analytics
4. EnCoRe Project – Ensuring Consent and Revocation

HP Labs, Systems Security Lab (SSL), Bristol, UK
http://www.hpl.hp.com/research/systems_security/

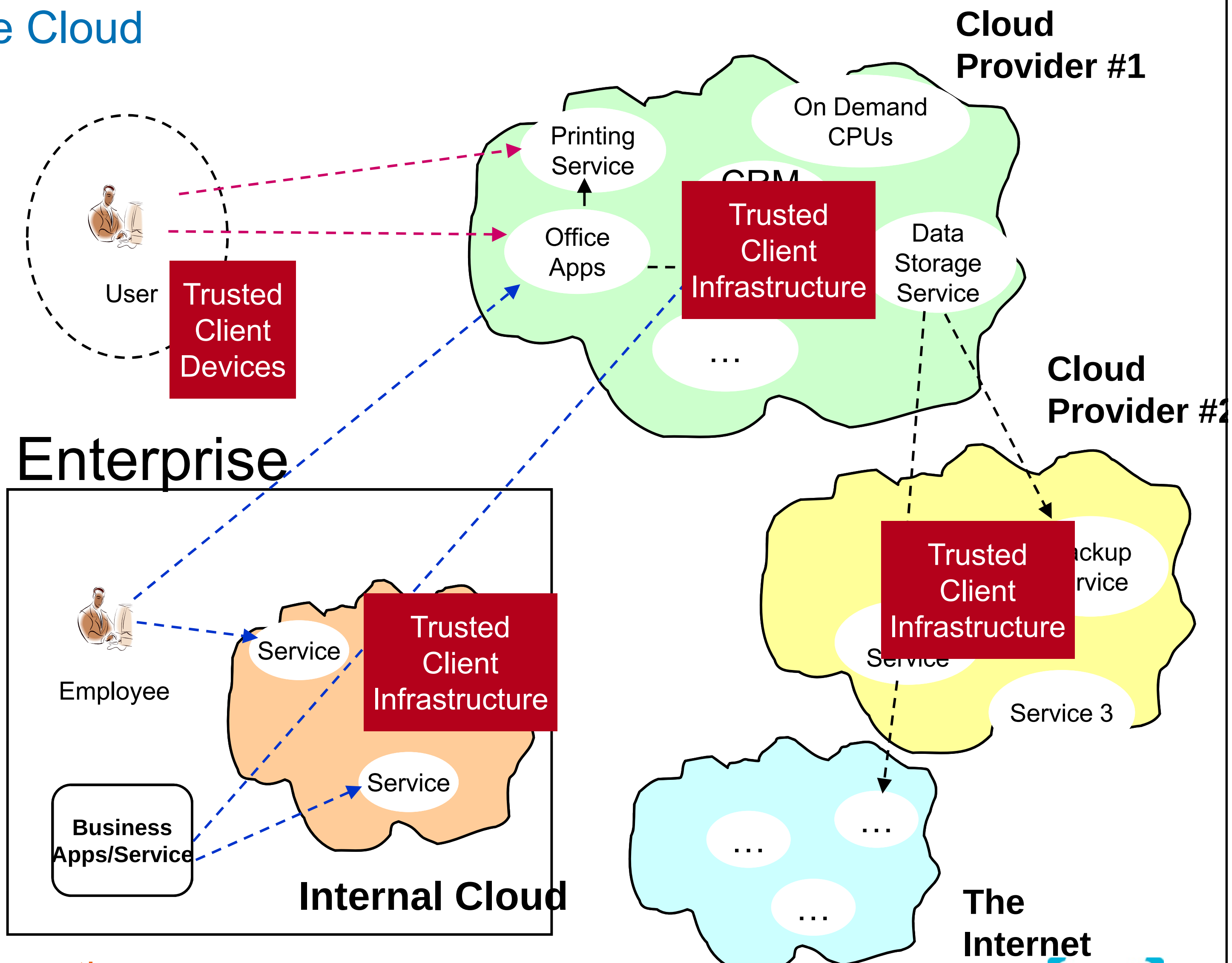
1. Trusted Infrastructure

- Ensuring that the Infrastructural IT building blocks of the Cloud are secure, trustworthy and compliant with security best practice

- Role of Trusted Computing Group (TCG)

/

- Impact and Role of Virtualization



Cloud Provider #1

Printing Service

On Demand CPUs

CRM

Office Apps

Trusted Client Infrastructure

Data Storage Service

…

User

Trusted Client Devices

Enterprise

Employee

Service

Trusted Client Infrastructure

Service

Business Apps/Service

Internal Cloud

Cloud Provider #2

Trusted Client Infrastructure

ackup rvice

Service

Service 3

…

…

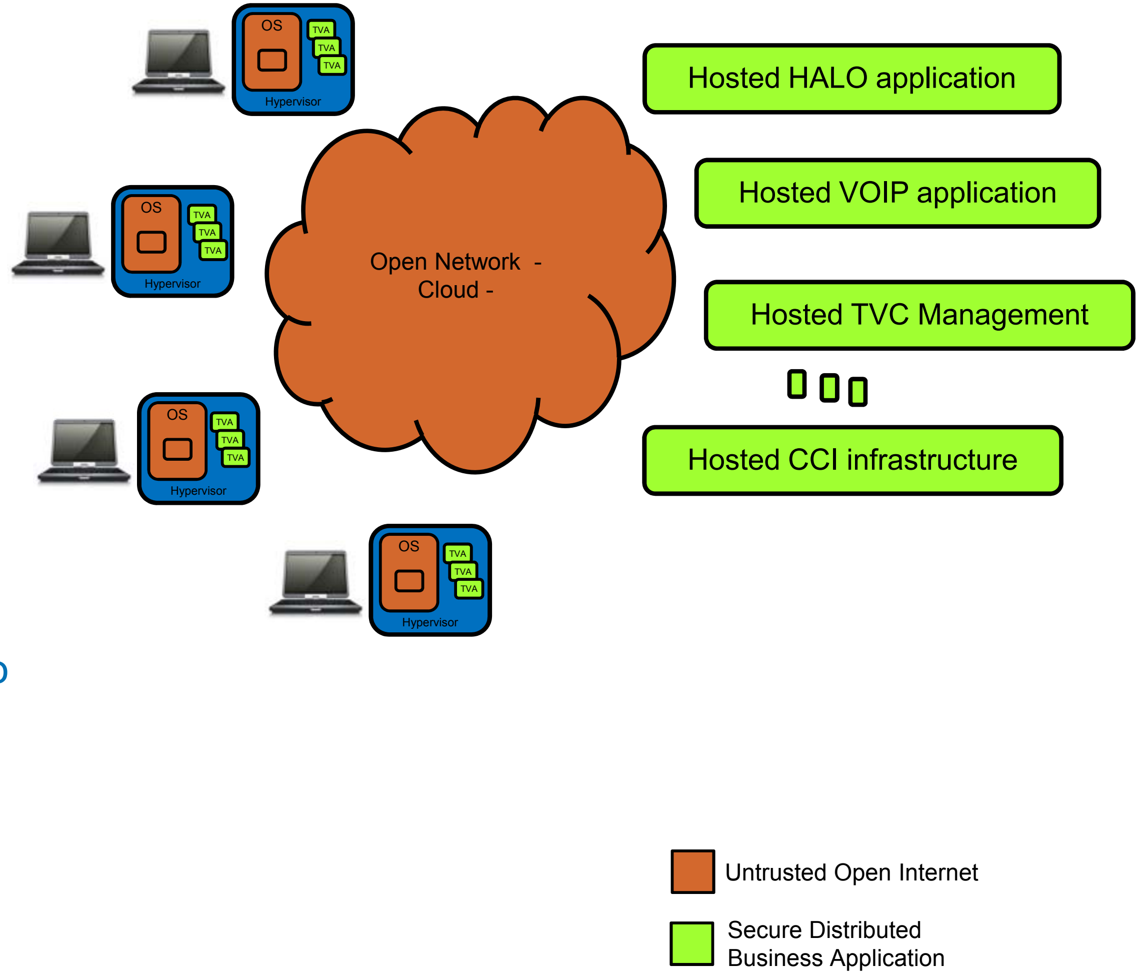
…

The Internet

TCG: http://www.trustedcomputinggroup.org

Trusted Infrastructure
Evolution Towards Services in The Cloud

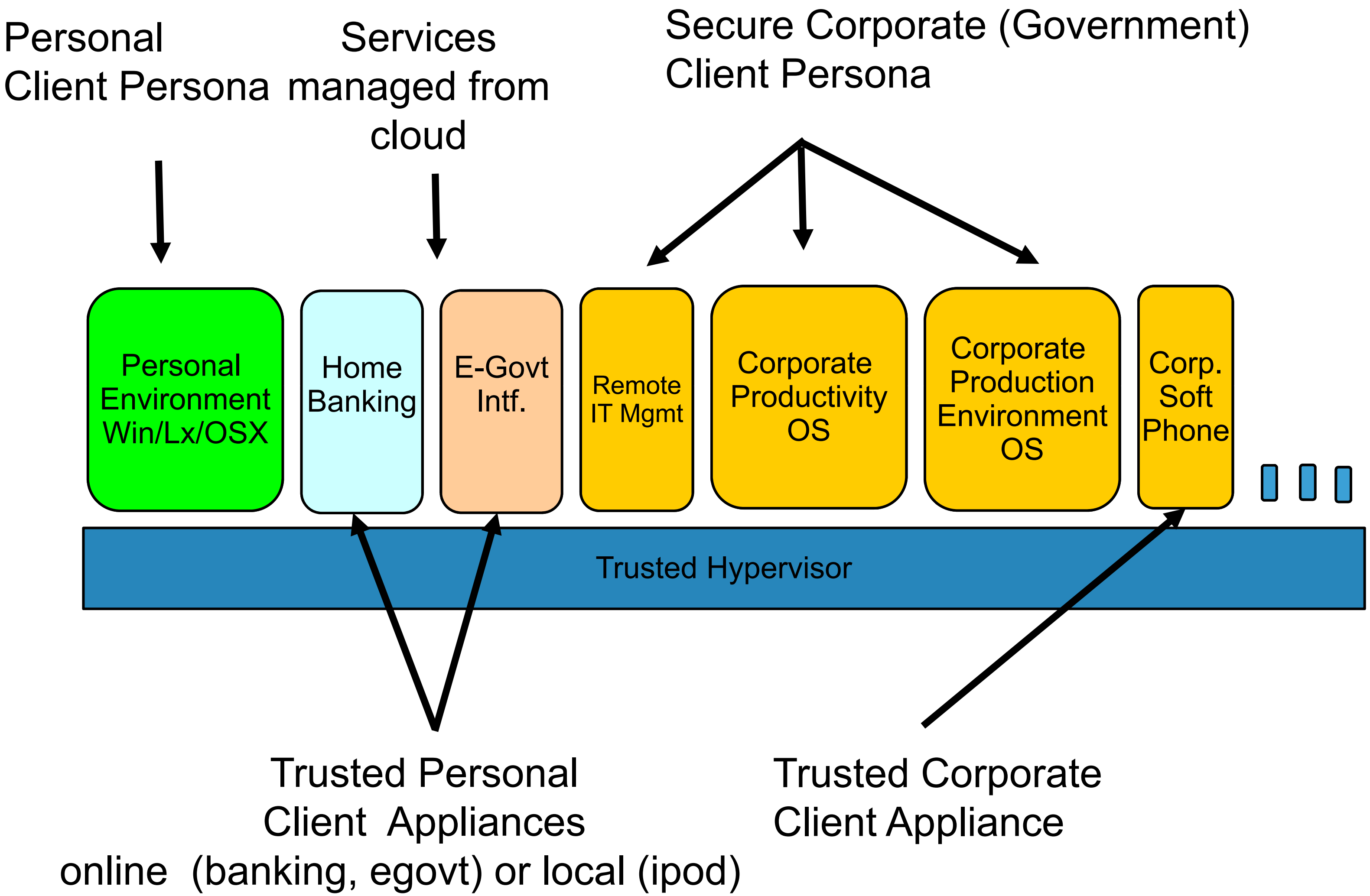
- More and more applications and services will be delivered on remote infrastructures we don’t own
- However, we need to maintain the user experience whether or not there is good network connectivity
- A new business need is emerging that will benefit from a mix of thin and thick client capabilities
- Hence we need:
  - a new generation of client devices that provide ***safe*** and ***adaptive*** access to cloud services…
  - …and ***more than ever*** we need to be able to manage them ***at reduced cost***
  - A new generation of **servers** that are trusted and whose security capabilities can be tested and proved



Source: HP Labs, Systems Security Lab, Richard Brown

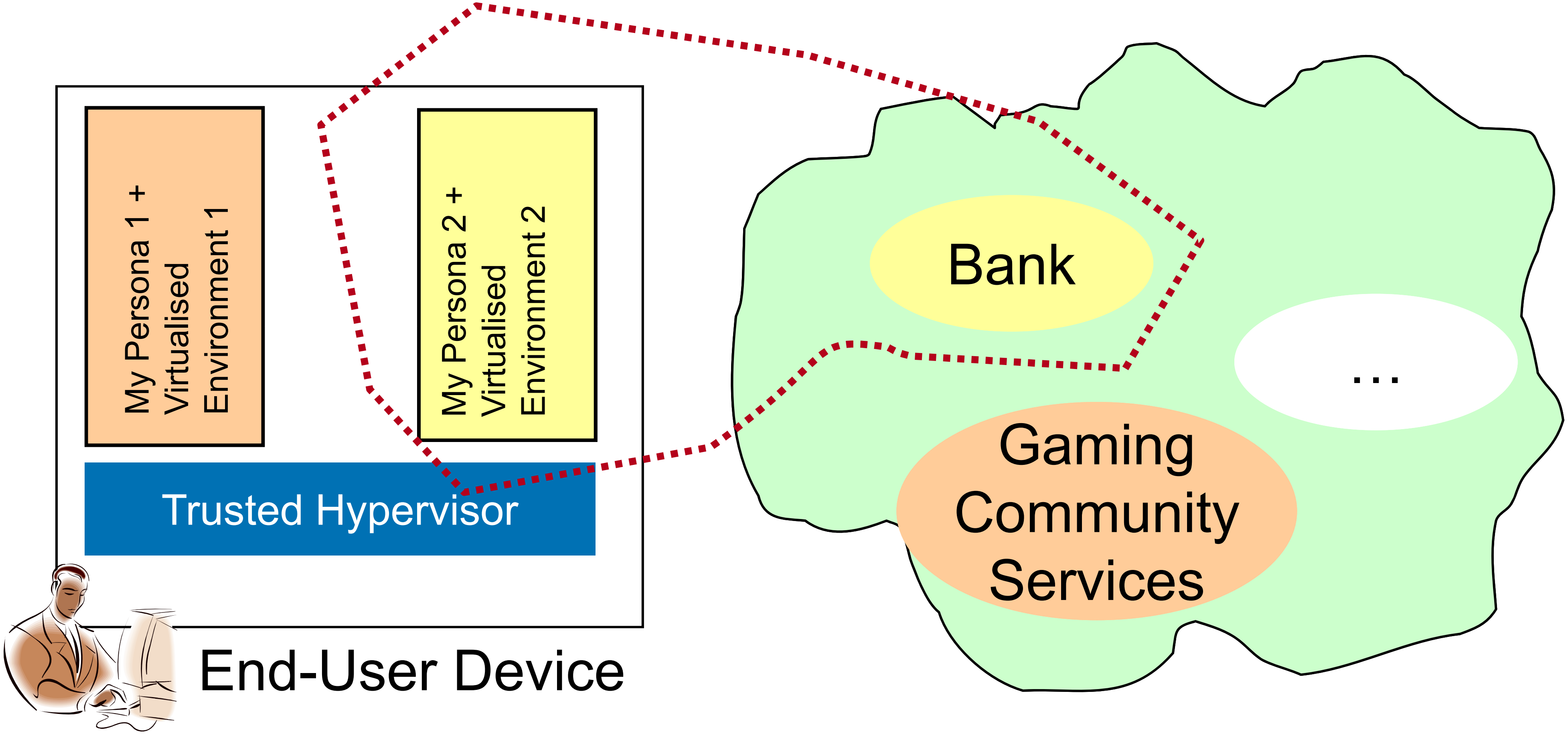
Trusted Infrastructure: Trusted Virtualized Platform

HP Labs: Applying Trusted Computing to Virtualization



Source: HP Labs, Systems Security Lab, Richard Brown

Paradigm Shift: Identities/Personae as “Virtualised Environment” in the Cloud


My Persona 1 + Virtualised Environment 1
My Persona 2 + Virtualised Environment 2
Trusted Hypervisor
End-User Device
Bank
…
Gaming Community Services

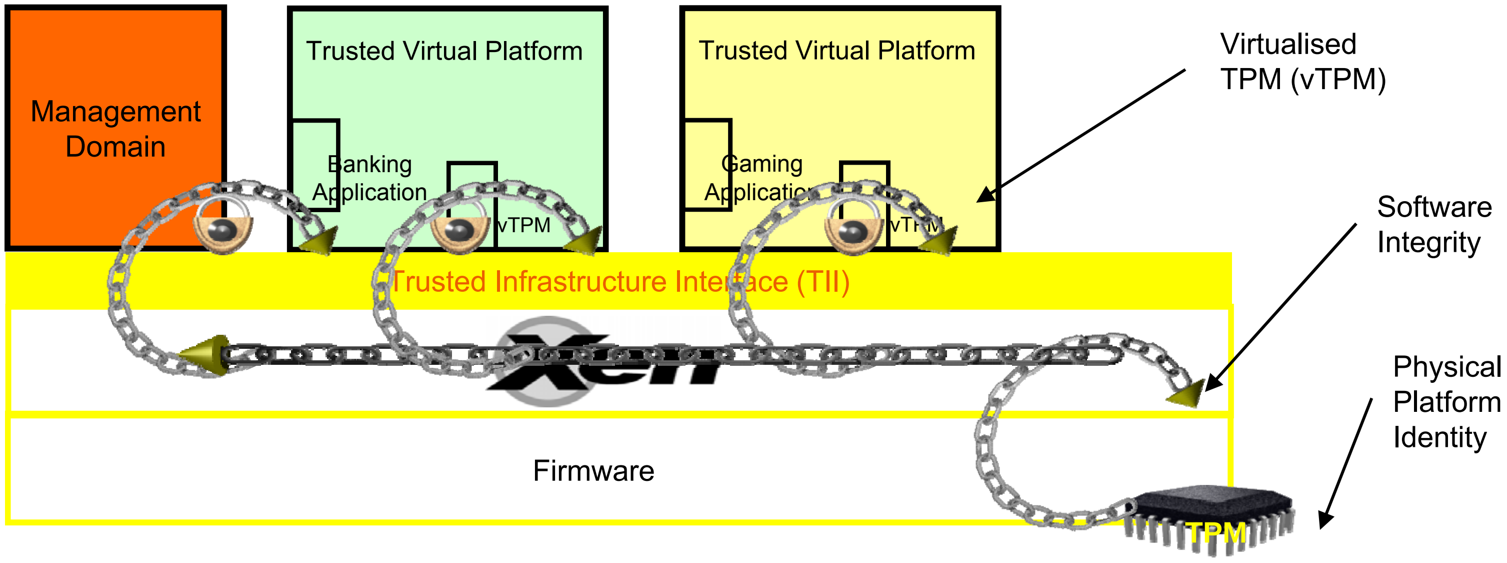
Using Virtualization to push Control from the Cloud/Service back to the Client Platform

- User’s Persona is defined by the Service Interaction Context
- User’s Persona & Identity are “tight” to the Virtualised Environment
- Persona defined by User or by Service Provider
- Potential Mutual attestation of Platforms and Integrity

Specifiable, Manageable and Attestable Virtualization Layer

Leverage Trusted Computing technology for Increased Assurance

→ Enabling remote attestation of Invariant Security Properties implemented in the Trusted Virtualization Layer



Source: HP Labs, Systems Security Lab, Richard Brown

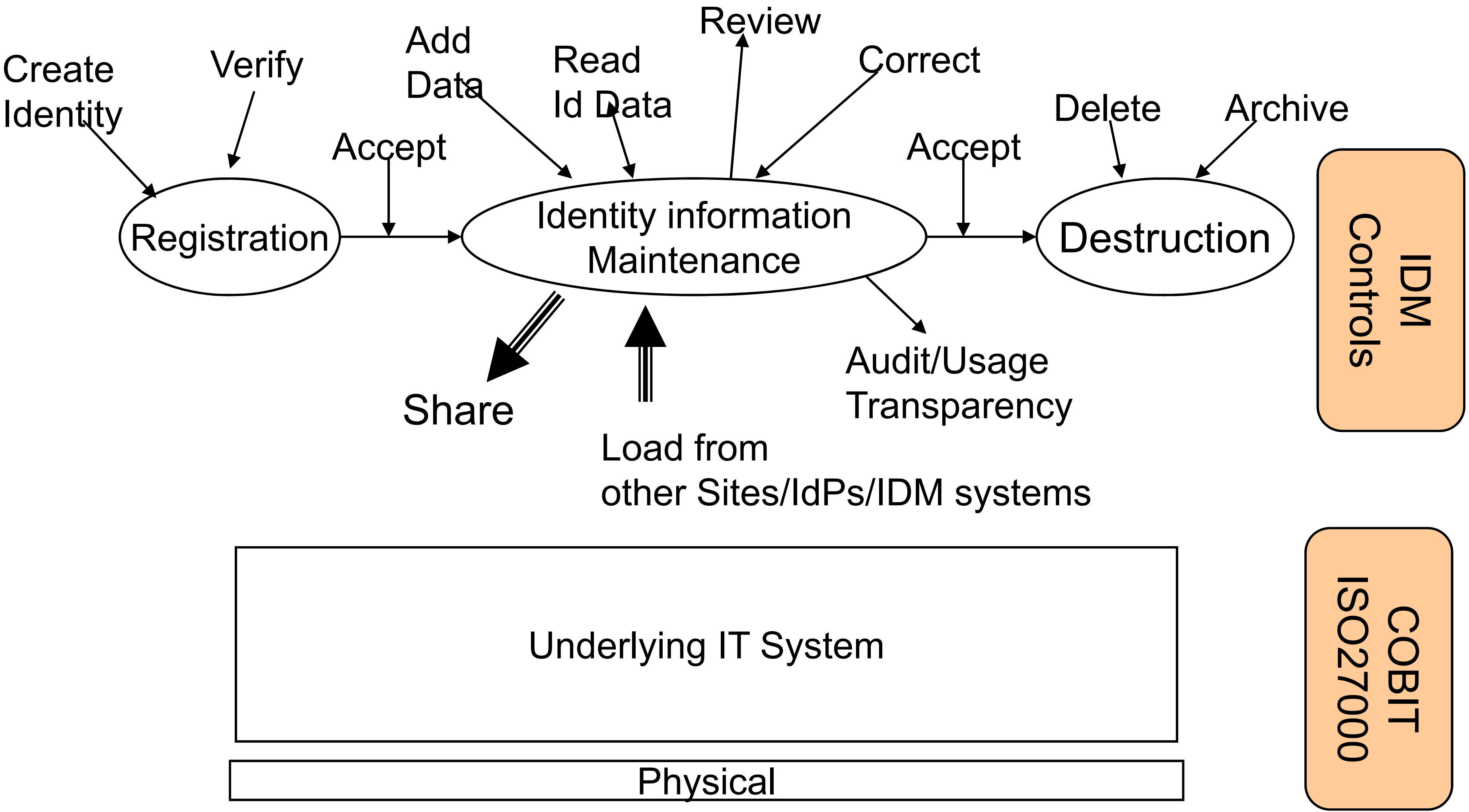
2. Identity Assurance

- Identity Assurance is concerned with “Providing Visibility into how Risks Associated with Identity Information are being Managed”
- How Does a Third Party, in the Cloud (Cloud Provider, Service Provider, etc.) deal with Security and IAM Aspects, Compliance to Laws and Legislation?
- How to provide Identity Assurance in the Cloud?
- HP Labs (Systems Security Lab) are exploring Mechanisms and Approaches in this space

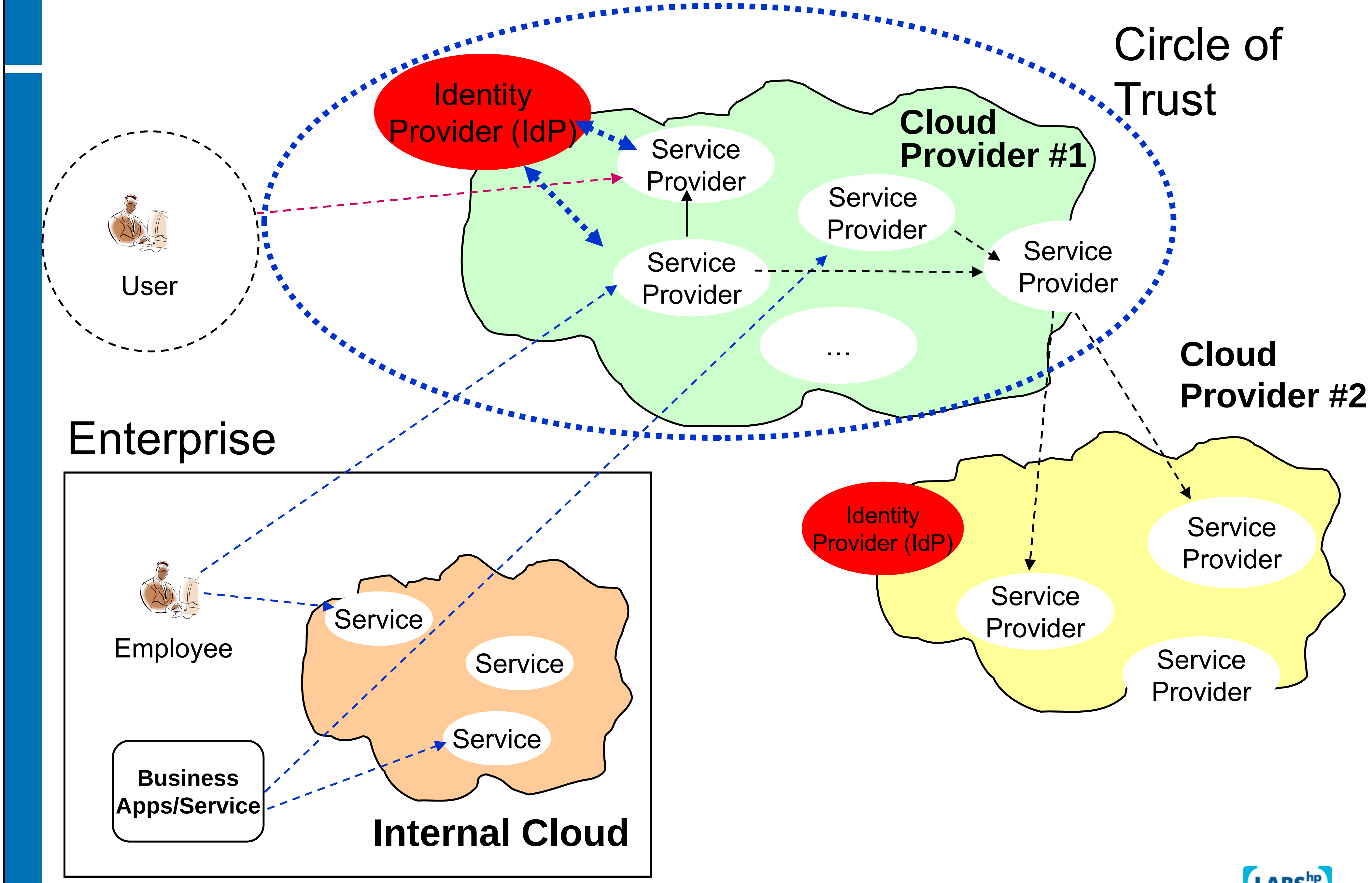
Reference: http://www.hpl.hp.com/techreports/2008/HPL-2008-25.html

Identity Assurance

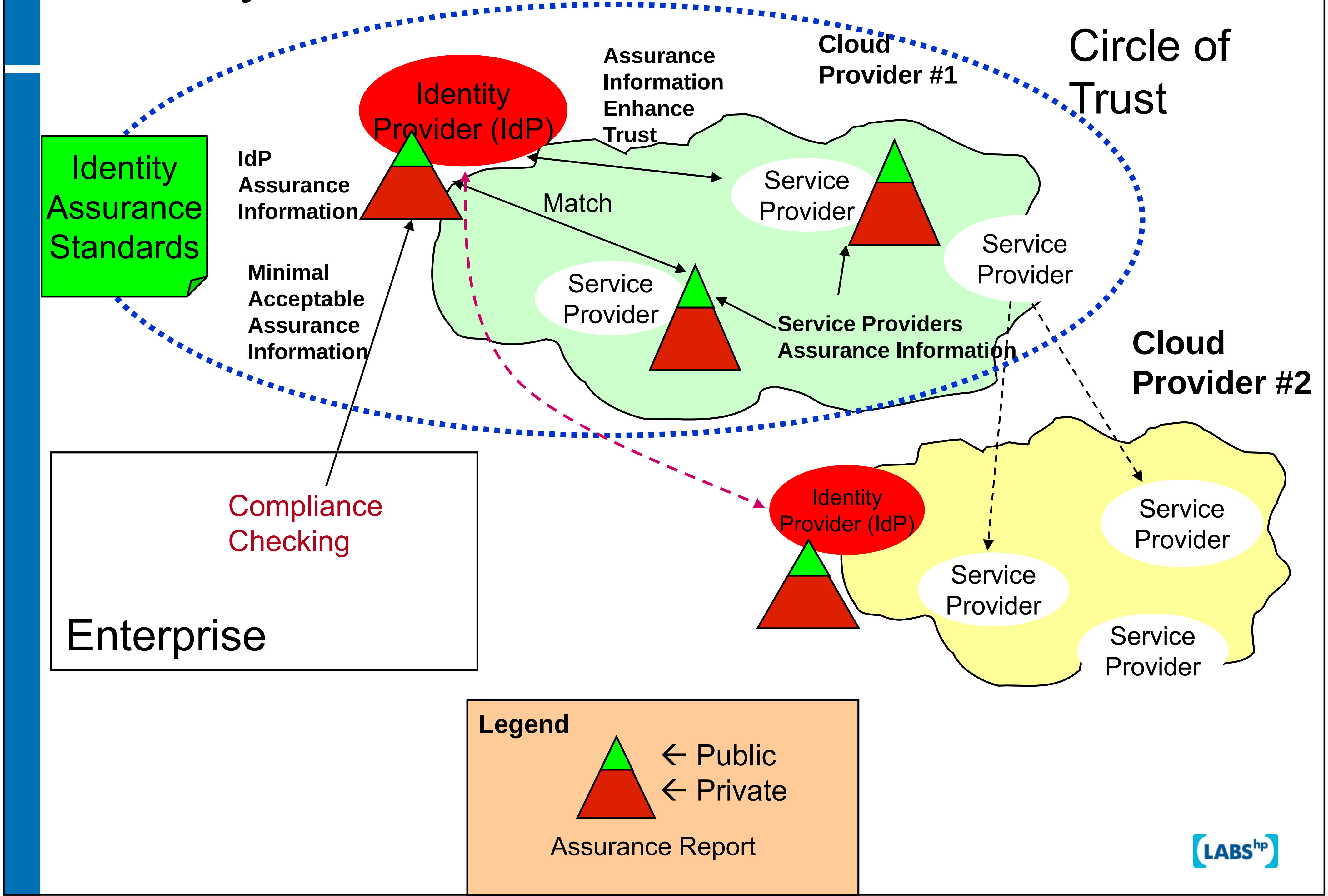
Information Management Process, Operations and Controls



Identity Assurance: Stakeholders in the Cloud



Identity Assurance in the Cloud



Circle of Trust

Identity Assurance Standards

IdP Assurance Information

Minimal Acceptable Assurance Information

Identity Provider (IdP)

Assurance Information Enhance Trust

Cloud Provider #1

Match

Service Provider

Service Provider

Service Provider

Service Providers Assurance Information

Cloud Provider #2

Identity Provider (IdP)

Service Provider

Service Provider

Service Provider

Compliance Checking

Enterprise

Legend

← Public

← Private

Assurance Report

HP Labs Model-based Assurance Approach

Explicit and Automated Monitoring of IAM Processes and Controls based on Audits & Logs

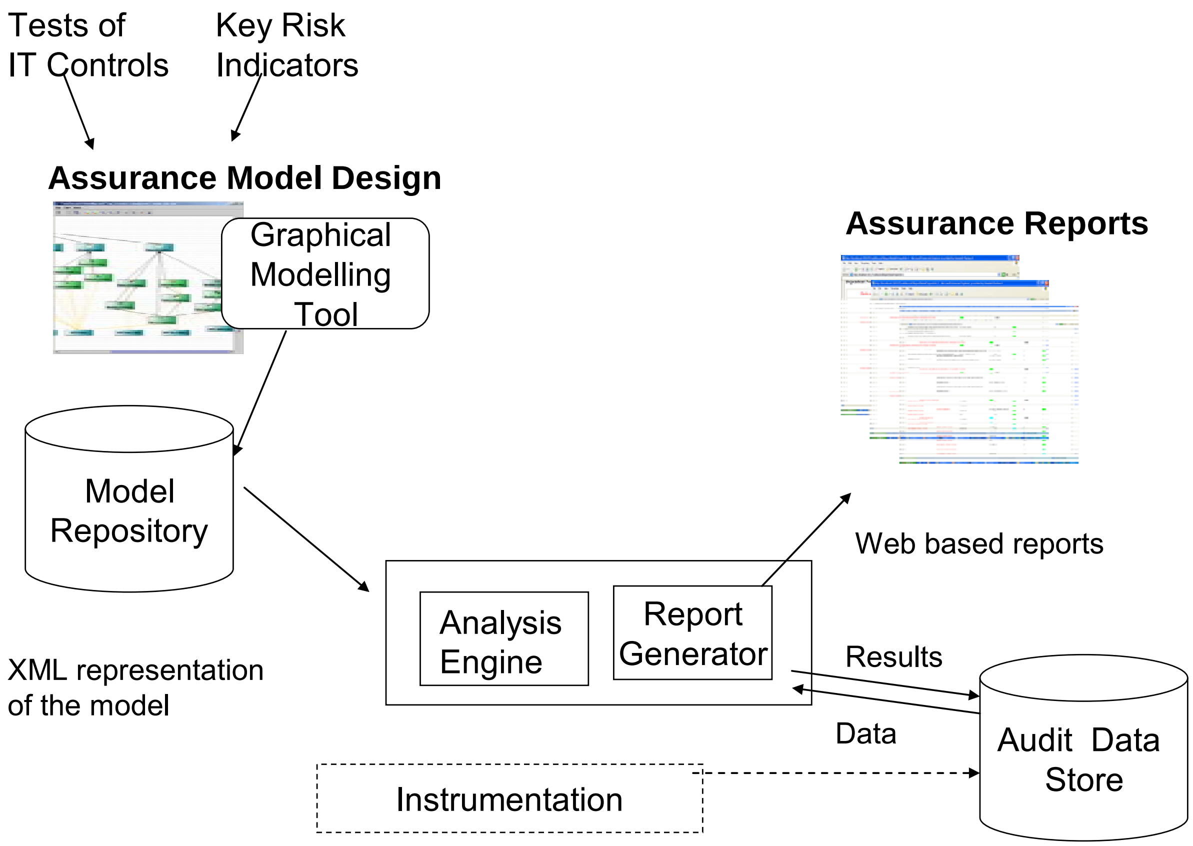
The model design process proceeds in four steps:

1. Categorize IT Controls/ Processes/Mechanisms needed for Assurance

2. Identify Measurable Aspects of these Controls
   - Performance Indicators
   - Correctness Tests

3. Build the Control Analysis Model

4. Use the model to monitor for changing conditions and to provide assurance reports



Tests of IT Controls

Key Risk Indicators

Assurance Model Design

Graphical Modelling Tool

Model Repository

XML representation of the model

Analysis Engine

Report Generator

Assurance Reports

Web based reports

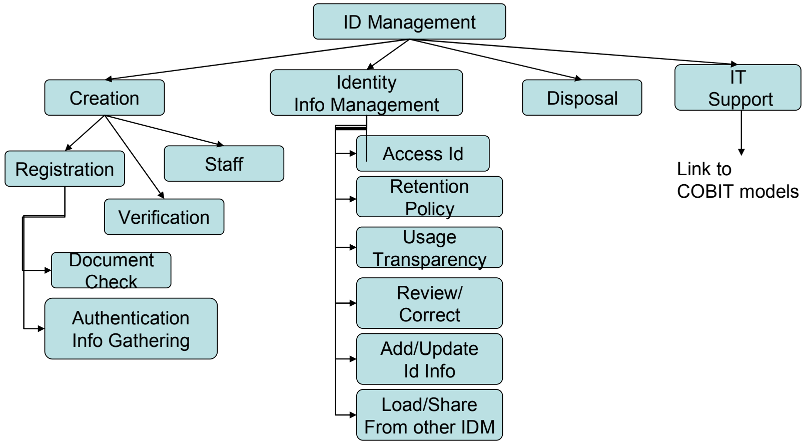
Results

Data

Audit Data Store

Instrumentation

Identity Assurance Model



ID Management

Creation

Registration

Staff

Verification

Document Check

Authentication Info Gathering

Identity Info Management

Access Id

Retention Policy

Usage Transparency

Review/ Correct

Add/Update Id Info

Load/Share From other IDM

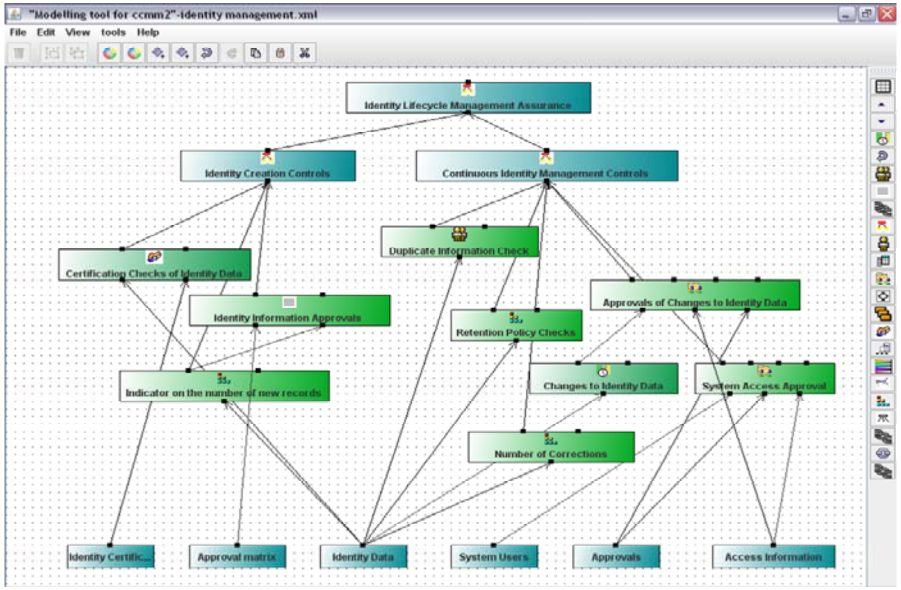
Disposal

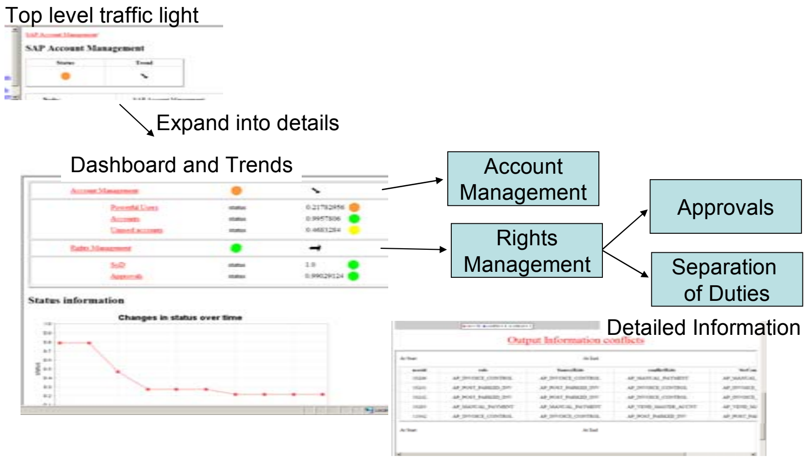
IT Support

Link to COBIT models

Identity Assurance Conceptual Model

Representation of Model in Our Tool


"Modelling tool for ccmm2"-identity management.xml
File
Edit
View
tools
Help
Identity Lifecycle Management Assurance
Identity Creation Controls
Continuous Identity Management Controls
Duplicate Information Check
Certification Checks of Identity Data
Identity Information Approvals
Retention Policy Checks
Approvals of Changes to Identity Data
Indicator on the number of new records
Changes to Identity Data
System Access Approval
Number of Corrections
Identity Certific...
Approval matrix
Identity Data
System Users
Approvals
Access Information



Top level traffic light

Expand into details

Dashboard and Trends

Account Management

Rights Management

Approvals

Separation of Duties

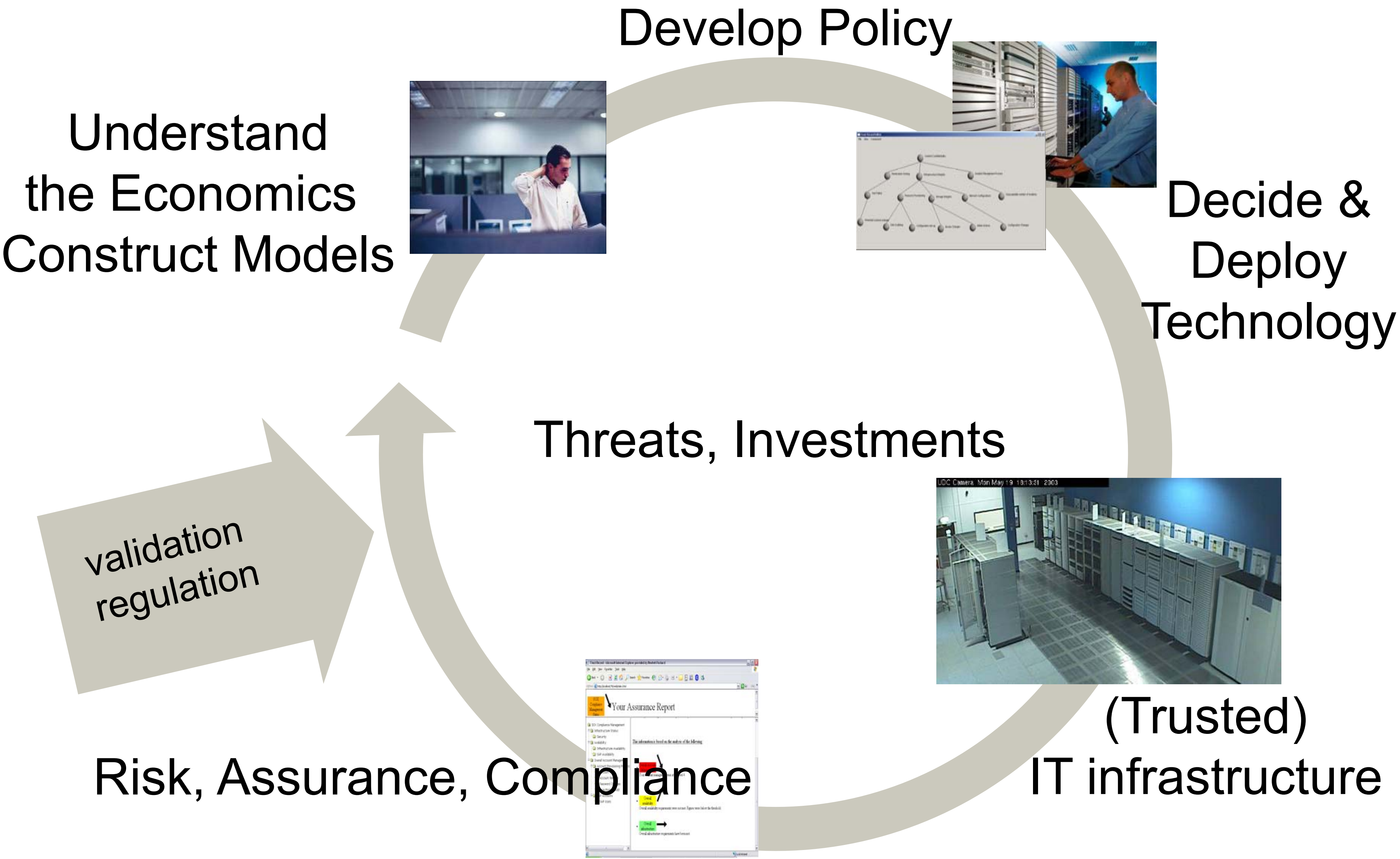
Detailed Information

Evaluation of Model Against Audit Data and Logs → Assurance Reports

3. Security and Identity Analytics Providing Strategic Decision Support

- Focus on Organisation IT (Security) Decision Makers (CIOs/CISOs)
- The growing complexity of IT and the increasing Threat Environment will make related Security Investment Decisions Harder
- The Decision to use The Cloud and its Services is Strategic
- Where to Make Investments (e.g. either IdM or Network Security, how to make business & security aligned …)? Which Choices need to be made? Which Strategy?
- The HP Labs "Security Analytics" Project is exploring how to apply Scientific Modelling and Simulation methodology for Strategic Decision Support
- Identity Analytics Project is focusing on the IAM vertical

Organisations' IT Security Challenges



Develop Policy

Decide & Deploy Technology

(Trusted) IT infrastructure

Risk, Assurance, Compliance

Understand the Economics Construct Models

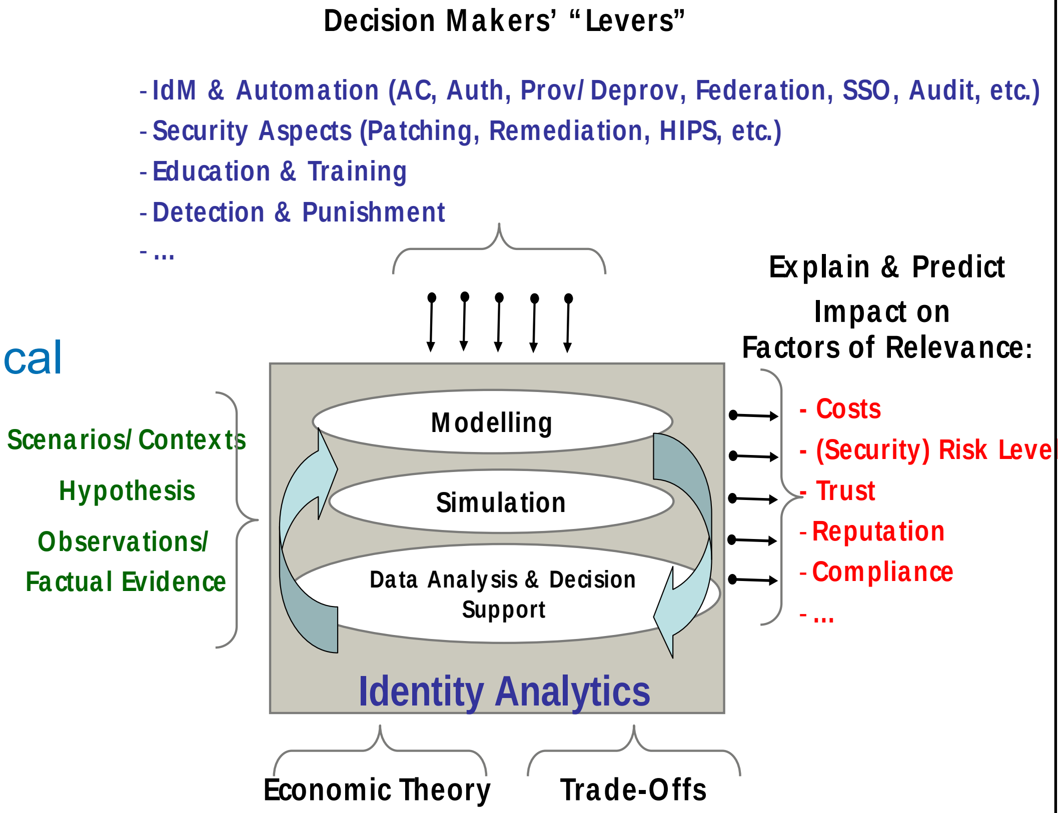
Threats, Investments

validation regulation

UDC Camera Mon May 19 18:13:31 2003
Your Assurance Report
This information is based on the analysis of the following
Overall availability
Overall infrastructure
SOX Compliance Management
Infrastructure Status
Security
Availability
Infrastructure Availability
SAP Availability

Identity Analytics - Overview

- **Problem: How to derive and justify the IAM strategy?**
  - How much should we spend on IAM? Where to invest? Multiple choices: Provisioning vs. Biometrics vs. Privacy Mgmt …
  - What is the impact of new IT technological choices from security, privacy, usability and cost perspectives?

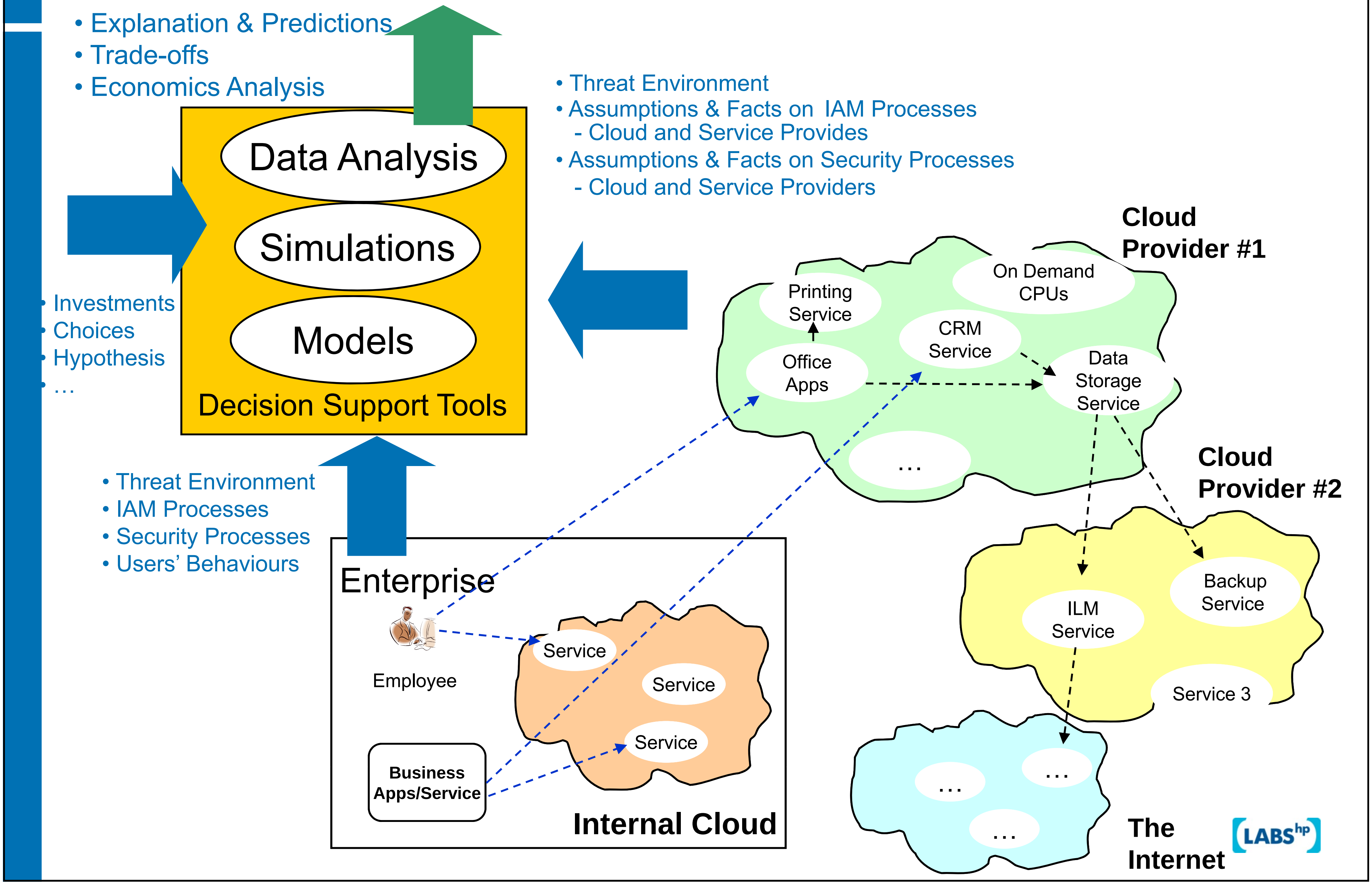


Decision Makers' "Levers"
- IdM & Automation (AC, Auth, Prov/Deprov, Federation, SSO, Audit, etc.)
- Security Aspects (Patching, Remediation, HIPS, etc.)
- Education & Training
- Detection & Punishment
- …
Explain & Predict Impact on Factors of Relevance:
- Costs
- (Security) Risk Level
- Trust
- Reputation
- Compliance
- …
Scenarios/Contexts
Hypothesis
Observations/ Factual Evidence
Modelling
Simulation
Data Analysis & Decision Support
Identity Analytics
Economic Theory
Trade-Offs

- **Identity Analytics Approach:**
  - System Modelling involving Processes, IT Systems & Technologies, People, Behaviours, etc. along with cause-effect relationships
  - Using Models & Simulations to explore impact of choices and predict outcomes
  - Exploring the Economics angle (losses, costs, etc.) by means of Utility Functions

HPL Project Material: http://www.hpl.hp.com/personal/Marco_Casassa_Mont/Projects/IdentityAnalytics/IdentityAnalytics.htm

Identity Analytics Applied to The Cloud



- Explanation & Predictions
- Trade-offs
- Economics Analysis

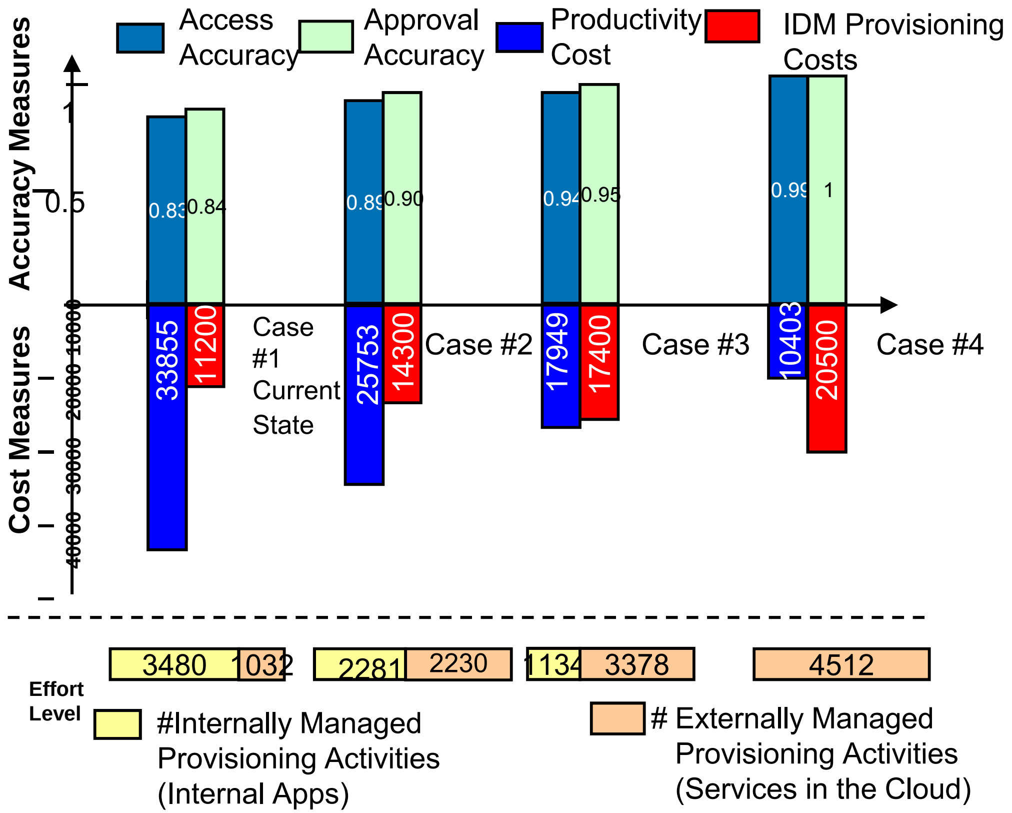
- Threat Environment
- Assumptions & Facts on IAM Processes
  - Cloud and Service Provides
- Assumptions & Facts on Security Processes
  - Cloud and Service Providers

- Investments
- Choices
- Hypothesis
- …

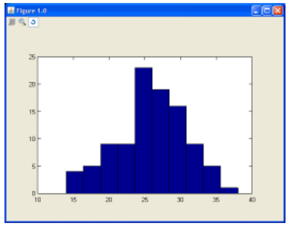
- Threat Environment
- IAM Processes
- Security Processes
- Users' Behaviours

Identity Analytics Applied to The Cloud

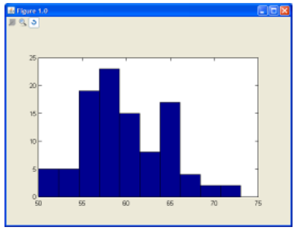
Example: Predictions of Outsourcing of IAM Services to the Cloud



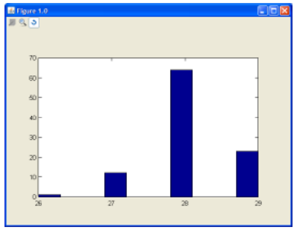
High-Level Metrics
Tailored to Target CIOs/CISOs & Strategic decision makers



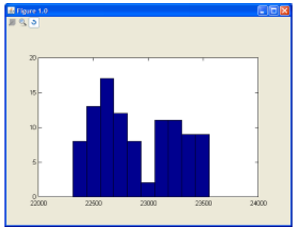
# Hanging Accounts



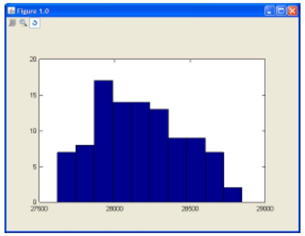
Denied Good Accounts



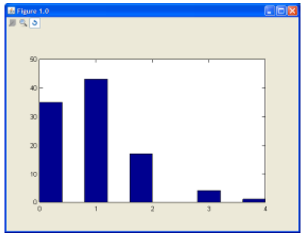
Misconfigured Account



Overall Approval Time



Overall Deployment Time

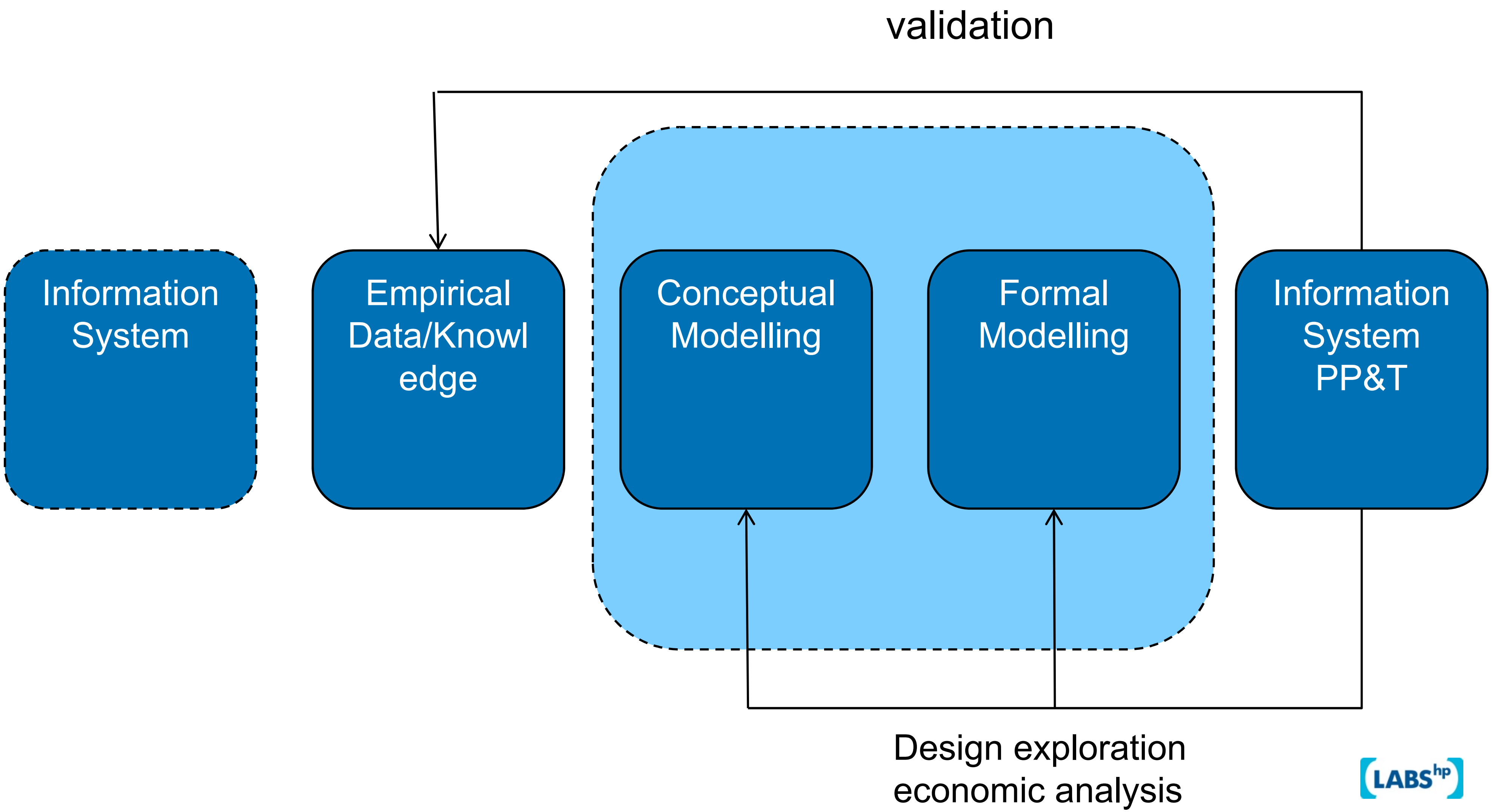


Bypassed Approval Ste

Low-Level Measures
Tailored to Target Domain Experts

Security & Identity Analytics Methodology

Scientific Approach based on Modelling & Simulation



4. TSB EnCoRe Project Consent and Revocation Management

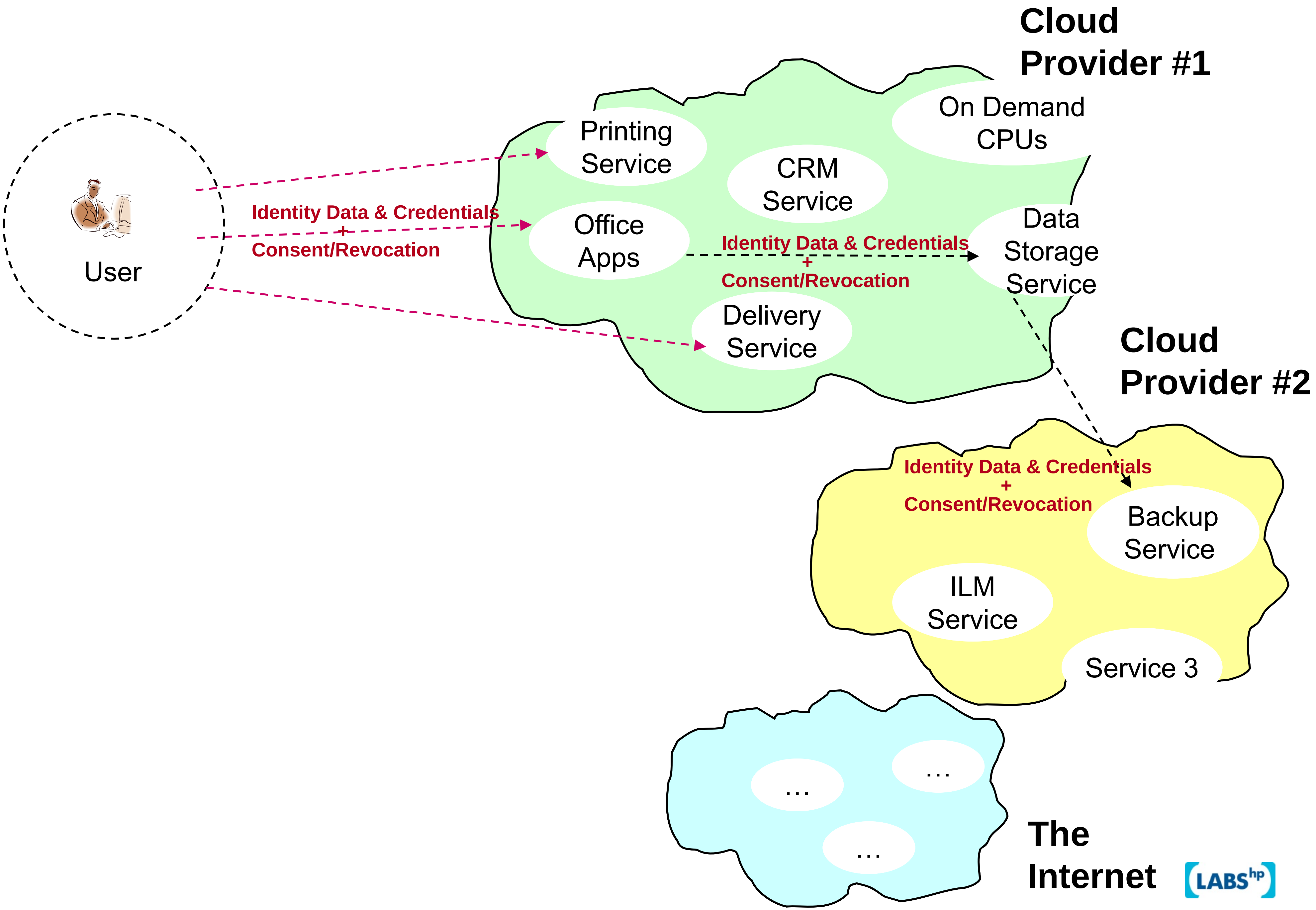
- EnCoRe: Ensuring Consent and Revocation
  UK TSB Project – http://www.encore-project.info/

"EnCoRe is a multi-disciplinary research project, spanning across a number of IT and social science specialisms, that is researching how to improve the rigour and ease with which individuals can grant and, more importantly, revoke their consent to the use, storage and sharing of their personal data by others"

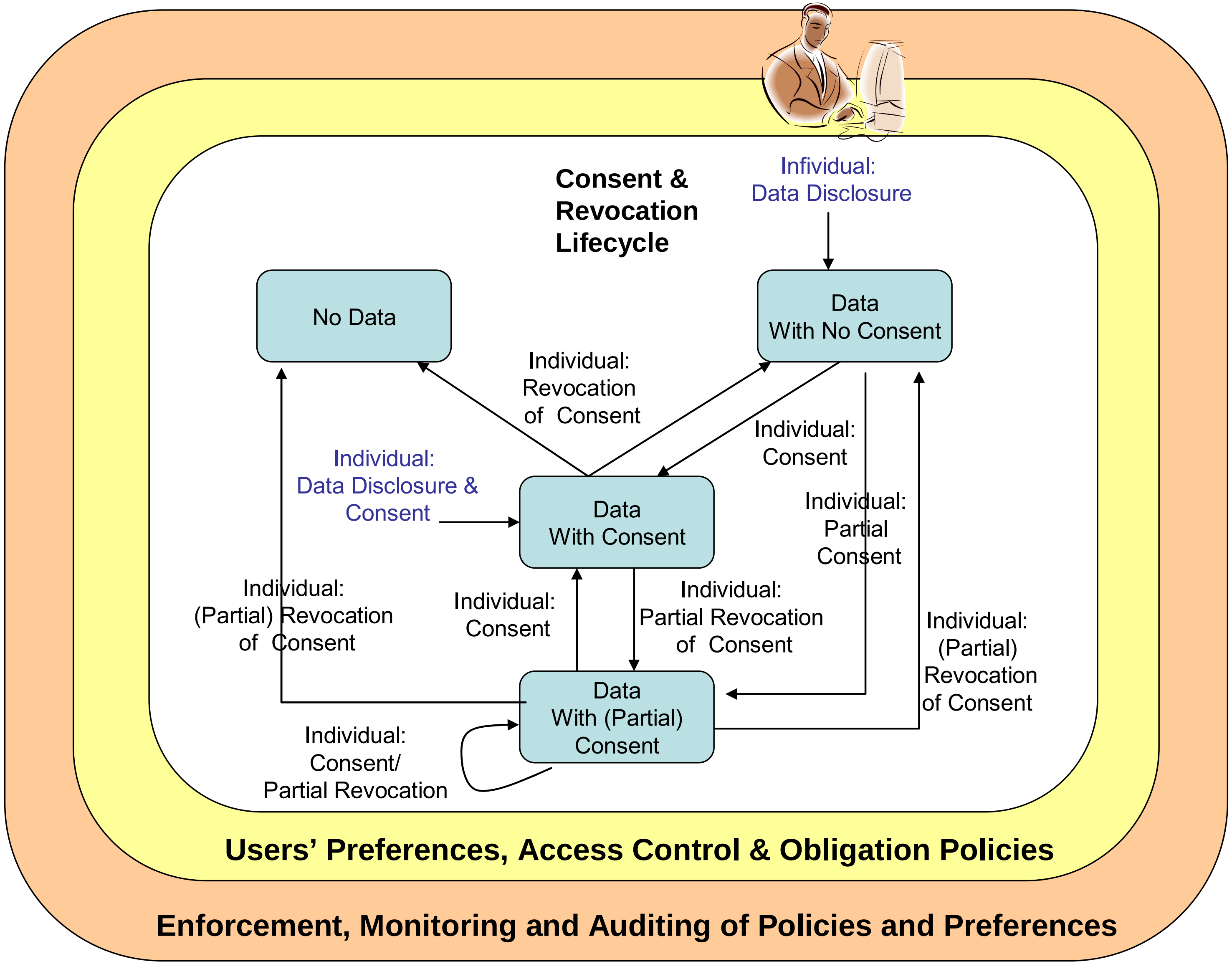
- Recognise the Importance of Cloud Computing and its Impact on Identities and Privacy

→ Problem: Management of Personal Data (PII) and Confidential Information along driven by Consent & Revocation

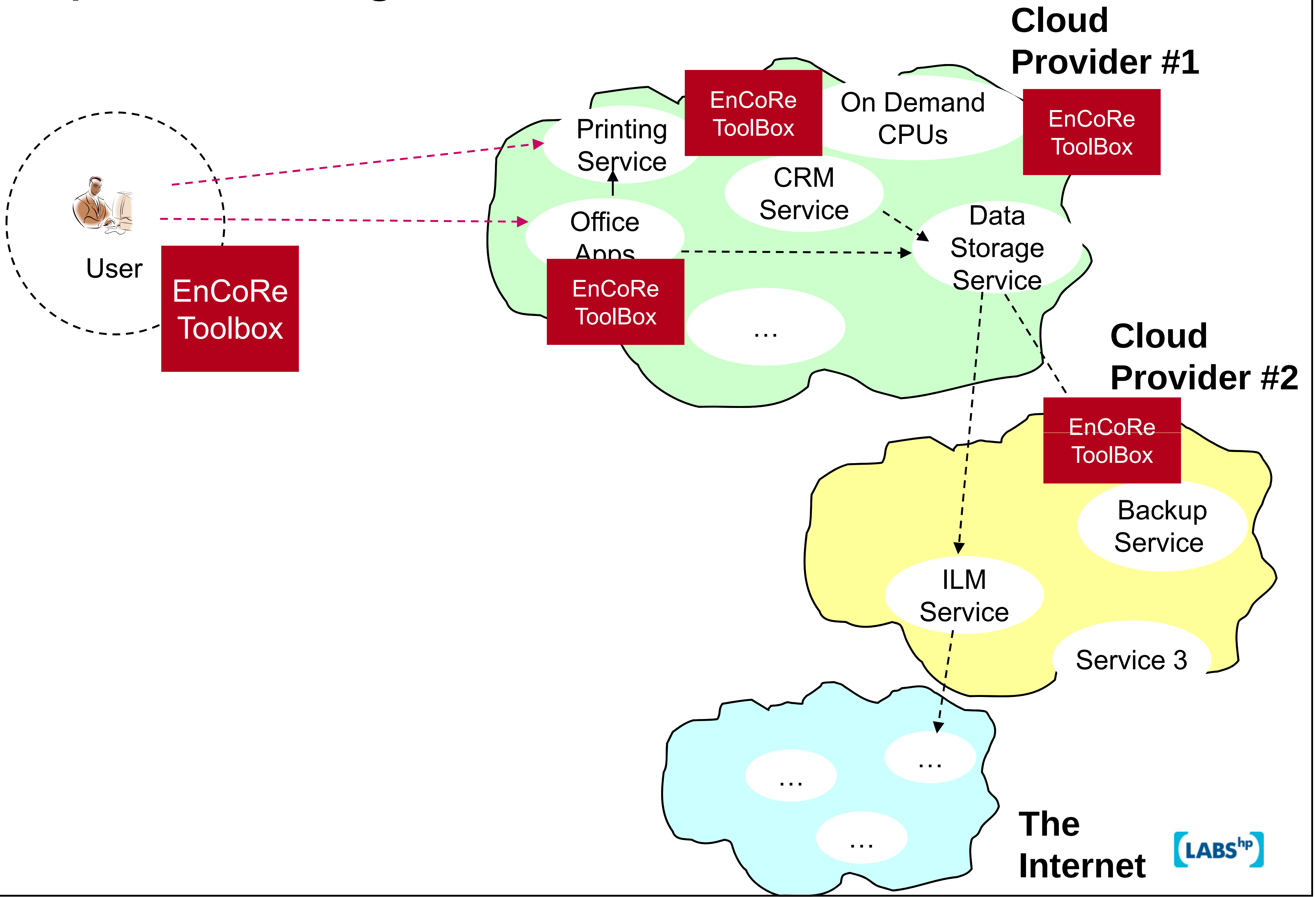
Identity Data + Consent/Revocation



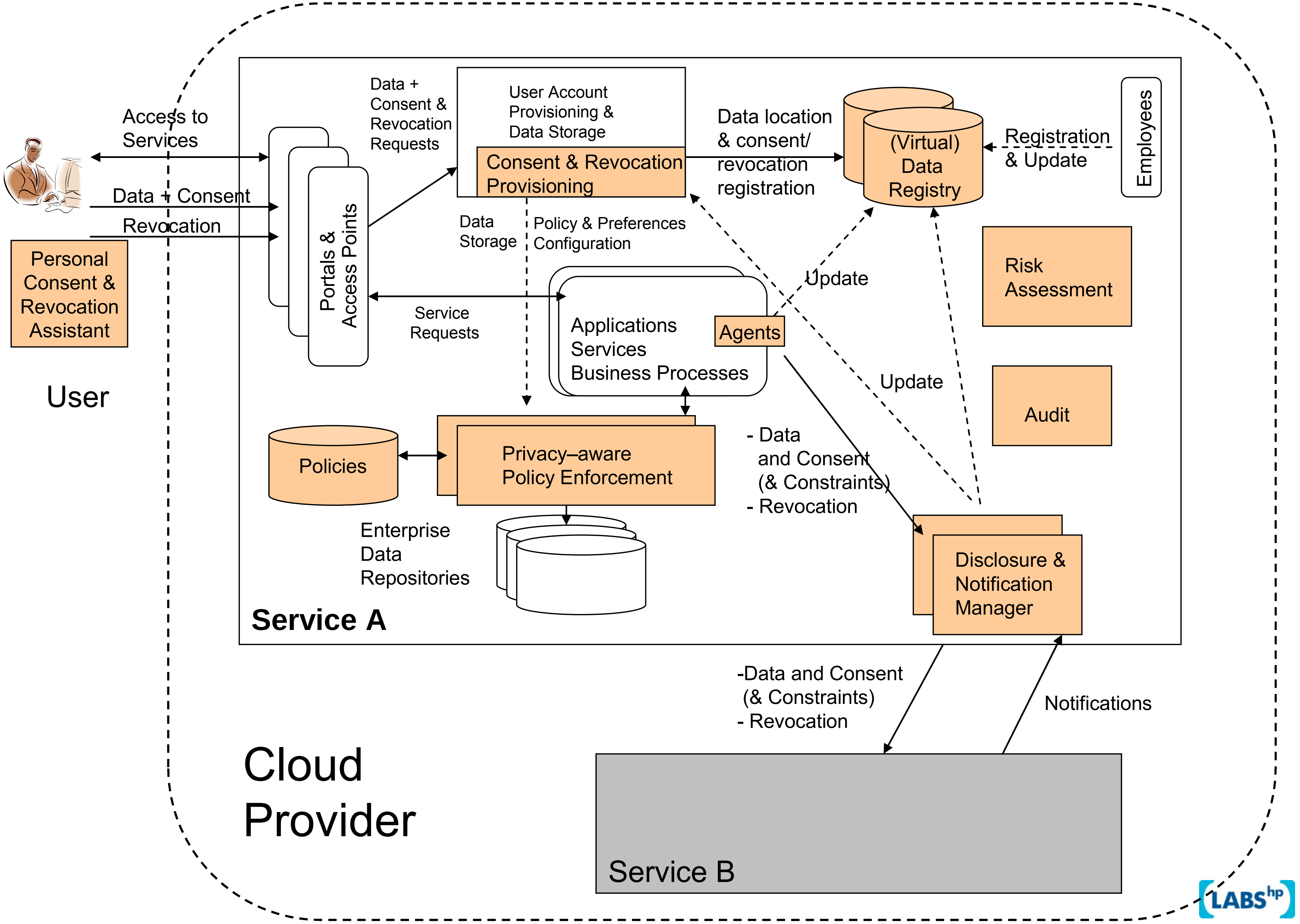
Consent and Revocation Lifecycle



EnCoRe:
Explicit Management of Consent and Revocatior



EnCoRe: Explicit Management of Consent and Revocation



Access to Services
Data + Consent
Revocation
Personal Consent & Revocation Assistant
User
Portals & Access Points
Data + Consent & Revocation Requests
User Account Provisioning & Data Storage
Consent & Revocation Provisioning
Data location & consent/ revocation registration
(Virtual) Data Registry
Registration & Update
Employees
Data Storage
Policy & Preferences Configuration
Update
Service Requests
Applications Services Business Processes
Agents
Risk Assessment
Update
Audit
Policies
Privacy–aware Policy Enforcement
- Data and Consent (& Constraints)
- Revocation
Enterprise Data Repositories
Disclosure & Notification Manager
Service A
-Data and Consent (& Constraints)
- Revocation
Notifications
Cloud Provider
Service B

Presentation Outline

- Setting the Context: Cloud Computing
- Identity in the Cloud, Risks and Requirements
- Current Approaches and Initiatives
- Towards the Future of Identity in the Cloud
- Conclusions

Conclusions

- The Cloud and Cloud Computing are Real, Happening Now!
- Identity & Identity Management have a key role in the Cloud
- Need to be aware of Involved Issues and Risks:

  - Lack of Control on Data
  - Trust on Infrastructure
  - Privacy Issues
  - Assurance and Accountability
  - New Threat Environments
  - Complexity in handling Identities
  - Complexity of making informed decisions

- Need to re-think to the Identity Paradigm in the Cloud rather thar just Adapting Current Solutions
- New Opportunities for Research and Development of Innovative Solutions for various Stakeholders

Thanks and Q&A

Contact: Marco Casassa Mont,
HP Labs, marco.casassa-mont@hp.com

LABS hp