IBM Software Group

Federated Identity Management Overview

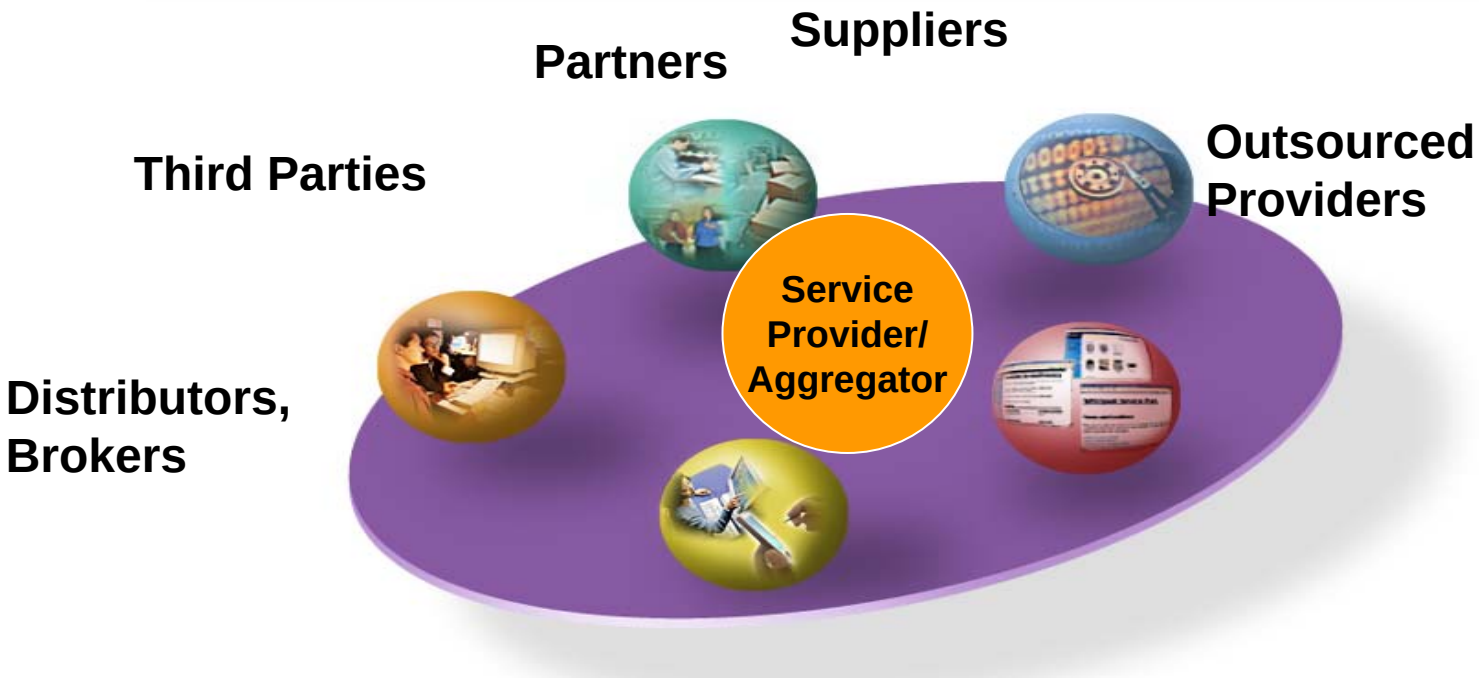
Tivoli software

Oleg Bascurov
Tivoli Technical Sales
bascurov@de.ibm.com

e business software

© 2005 IBM Corporation

Problem: Ineffective Identity Management



1. No standard mechanism to “trust” identities from M&A, Partners & Third Parties
2. Lack of trust means replication of creating “identity accounts”
3. Costly/Inefficient Account Management
4. Security Exposure, compliance and privacy

© 2005 IBM Corporation

Federation and Federated Identity Management

A **federation** is a state comprised of a number of *self-governing* regions… A federation is also an organisation, such as a trade union or *business*, with a structure analogous to that of a federal state.

[Source: Wikipedia]

A **federation** is a group of two or more trusted business partners with **business** and **technical agreements** which allow a user from one federation partner (participating company) to seamlessly access resources from another partner in a **secure** and **trustworthy** manner.

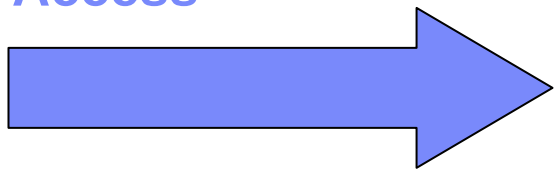
Evolution….NOT a Revolution - concept is nothing new

CREDIT CARD
STATE DRIVER LICENSE
PASSPORT

© 2005 IBM Corporation

Governments as Identity Federation Partners

TRUST provides Access



US Citizen =

User

USA =

Identity Provider

Germany =

Service Provider

When a US citizen travels to Germany, Germany verifies the identity of the US citizen by checking its passport. In the online world, we don't have federation. We refer to Germany as a **Service Provider**. A "service provider" is one that **"TRUSTS"** an identification from an **Identity Provider** (USA), as proof of Identity.

© 2005 IBM Corporation

Federated Identity Management

… from a business point of view:

- Federated Identity Management is the set of business agreements, technical agreements and policies that enable companies to partner to lower their overall identity management costs and improve user experience.

… **from a technology point of view:**

- User session lifecycle management
  - Single-sign-on, access control, single-sign-off
  - Identity mapping across partners
  - User information exchange
- Identity lifecycle management
  - Provisioning of users and linking of user identities
- Requires a Trust Infrastructure
  - Enables the on-line equivalent of real-world business relationships
- Enables secure application interaction
  - Users/applications are able to securely access business partner resources in a trustworthy manner

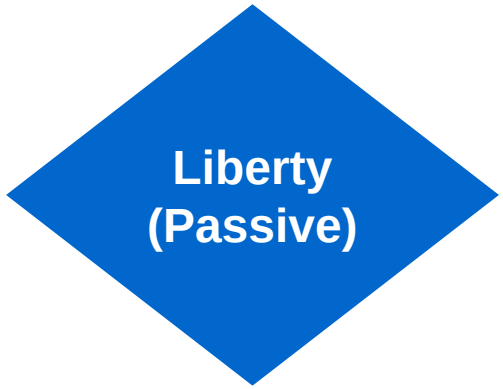
© 2005 IBM Corporation

Technology, Standards and Specifications

HTTP SSO
(SAML protocol)

Identity Federation Mgt
(SAML protocol)

ID Management for
Federated Web Services
(HTTP and SOAP-based SSO)



Support for various
Web Services protocols

© 2005 IBM Corporation

IBM Approach – Tivoli Federated Identity Manager

- Federated Identity Management is User Lifecycle Management
  - Simplifies the administration of user management between companies
- Recognition that the foundation of a federated model is TRUST
  - Key Management, Security Token Service and WS-Trust
- Standards & Technology support
  - Liberty, SAML, WS-Federation and WS-Security Family
  - Interoperability and conformance testing
- Integration of Federated Identity across IBM middleware
  - Tivoli Access Manager, Tivoli Identity Manager, WebSphere Application Server, WebSphere Portal

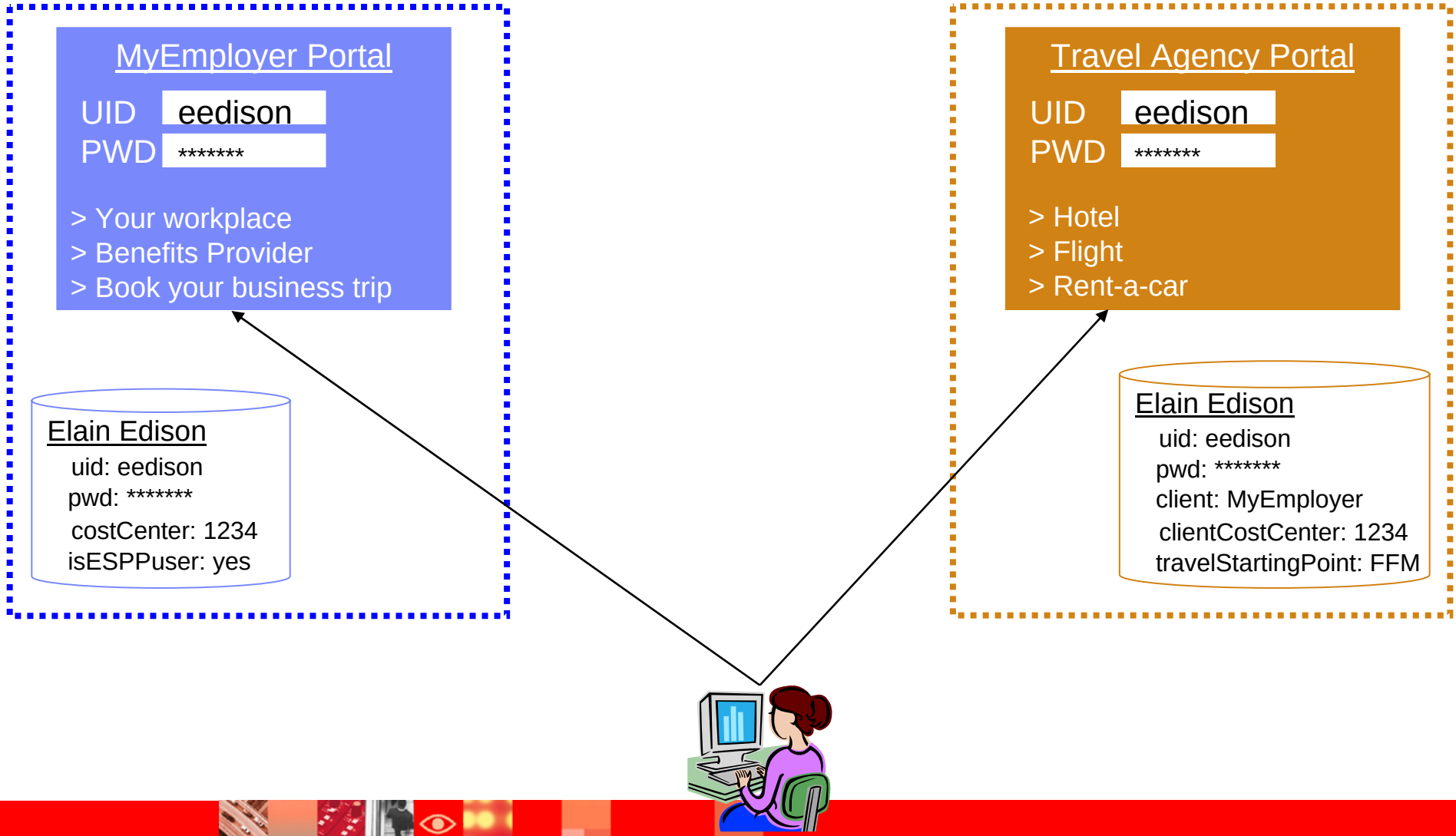
© 2005 IBM Corporation

A FIM Example

Oleg Bascurov
Tivoli Technical Sales
bascurov@de.ibm.com

© 2005 IBM Corporation

Current Situation



© 2005 IBM Corporation

Establishing a Federation (1)

MyEmployer Portal

UID
PWD

> Your workplace
> Benefits Provider
> Book your business trip

Elain Edison
uid: eedison
pwd: *******
costCenter: 1234
isESPPuser: yes

Identity Provider

Federation

Business Agreements:
- MyEmployer provides **up-to-date** data necessary for booking **on-demand**
- Travel Agency **relies** on the on-demand provided data and considers any valid user coming from MyEmployer's sites being **authorized** to book travels
- …

--- examples ---

Travel Agency Portal

UID
PWD

> Hotel
> Flight
> Rent-a-car

Elain Edison
uid: eedison
pwd: *******
client: MyEmployer
clientCostCenter: 1234
travelStartingPoint: FFM

Service Provider

© 2005 IBM Corporation

Establishing a Federation (2)

MyEmployer Portal

UID
PWD

> Your workplace
> Benefits Provider
> Book your business trip

Elain Edison
uid: eedison
pwd: *******
costCenter: 1234
isESPPuser: yes

Identity Provider

WS-Federation

Technical Agreements:

- The federation is established on the basis of **Web-Services Federation** and other related Web-Services Security Standards
- MyEmployer provides user's **ID, first name, last name and cost center information**
- …

--- examples ---

Travel Agency Portal

UID
PWD

> Hotel
> Flight
> Rent-a-car

Elain Edison
uid: eedison
pwd: *******
client: MyEmployer
clientCostCenter: 1234
travelStartingPoint: FFM

Service Provider

© 2005 IBM Corporation

Establishing a Federation (3)

MyEmployer Portal

UID
PWD

> Your workplace
> Benefits Provider
> Book your business trip

Elain Edison
uid: eedison
pwd: *******
costCenter: 1234
isESPPuser: yes

Identity Provider

WS-Federation

Policies:
- Travel Agency is **not allowed** to persistantly store personal user information provided by MyEmployer, with exception of a user id
- Travel Agency has to obtain an **user consent** to persistantly store personal user information a user provides for a booking
- …

--- examples ---

Travel Agency Portal

UID
PWD

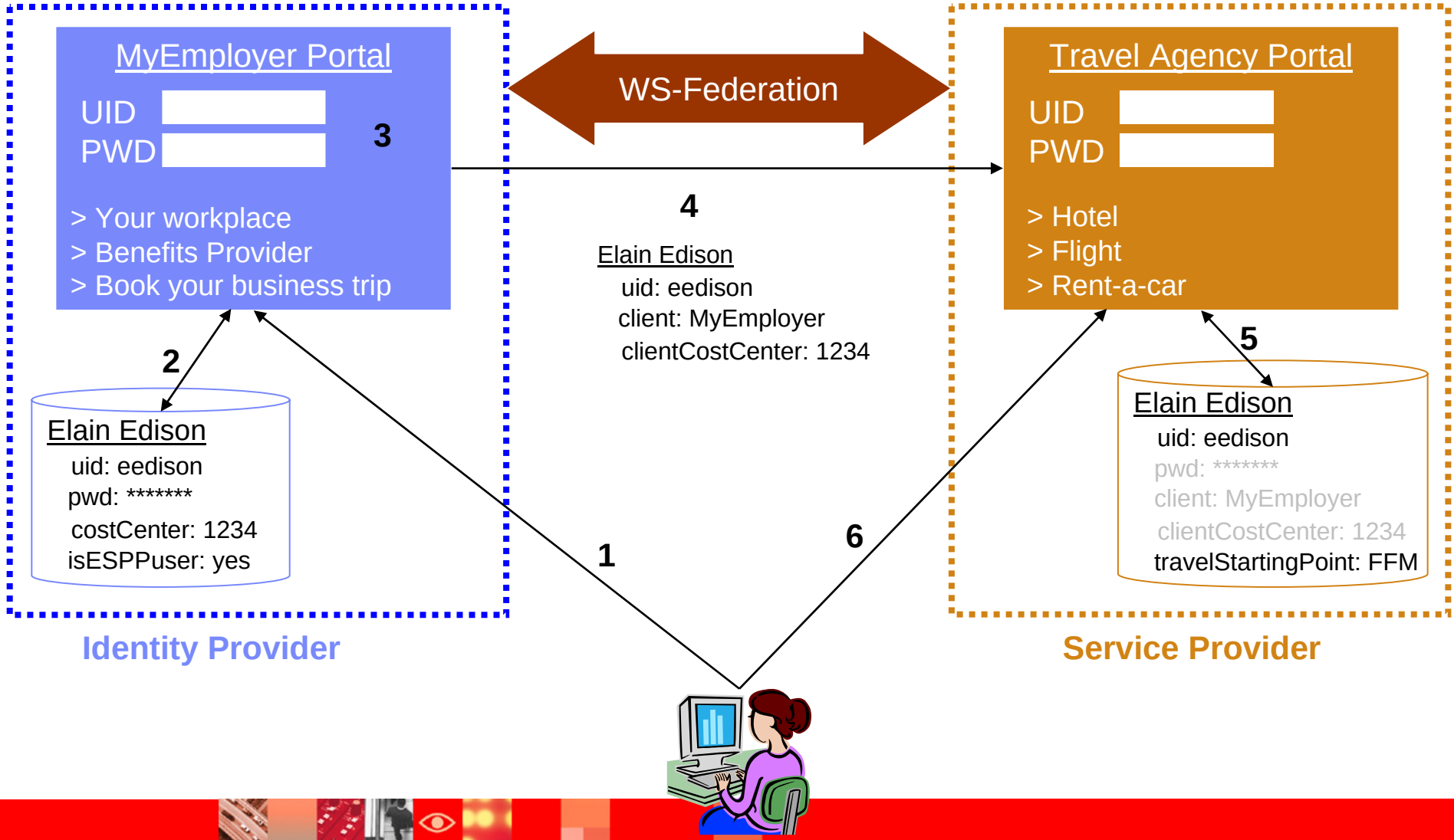
> Hotel
> Flight
> Rent-a-car

Elain Edison
uid: eedison
pwd: *******
client: MyEmployer
clientCostCenter: 1234
travelStartingPoint: FFM

Service Provider

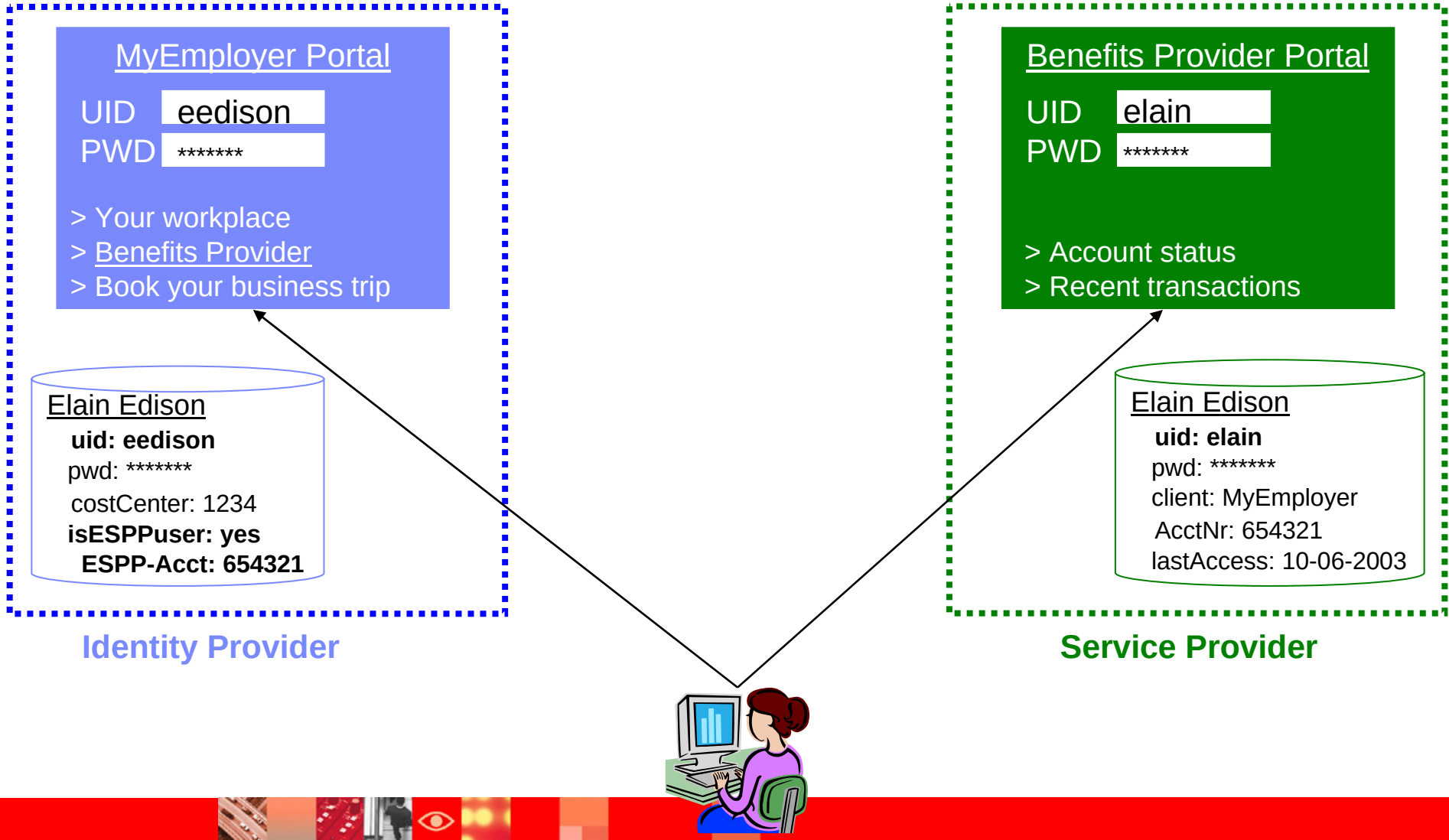
© 2005 IBM Corporation

Target



© 2005 IBM Corporation

Scenario 2 – Current Situation



© 2005 IBM Corporation

Establishing Federation

MyEmployer Portal

UID
PWD

> Your workplace
> Benefits Provider
> Book your business trip

Elain Edison
uid: eedison
pwd: *******
costCenter: 1234
isESPPuser: yes
ESPP-Acct: 654321

Identity Provider

Liberty Federation

Business Agreements
…
Technical Agreements
…
Policies:
…

Benefits Provider Portal

UID
PWD

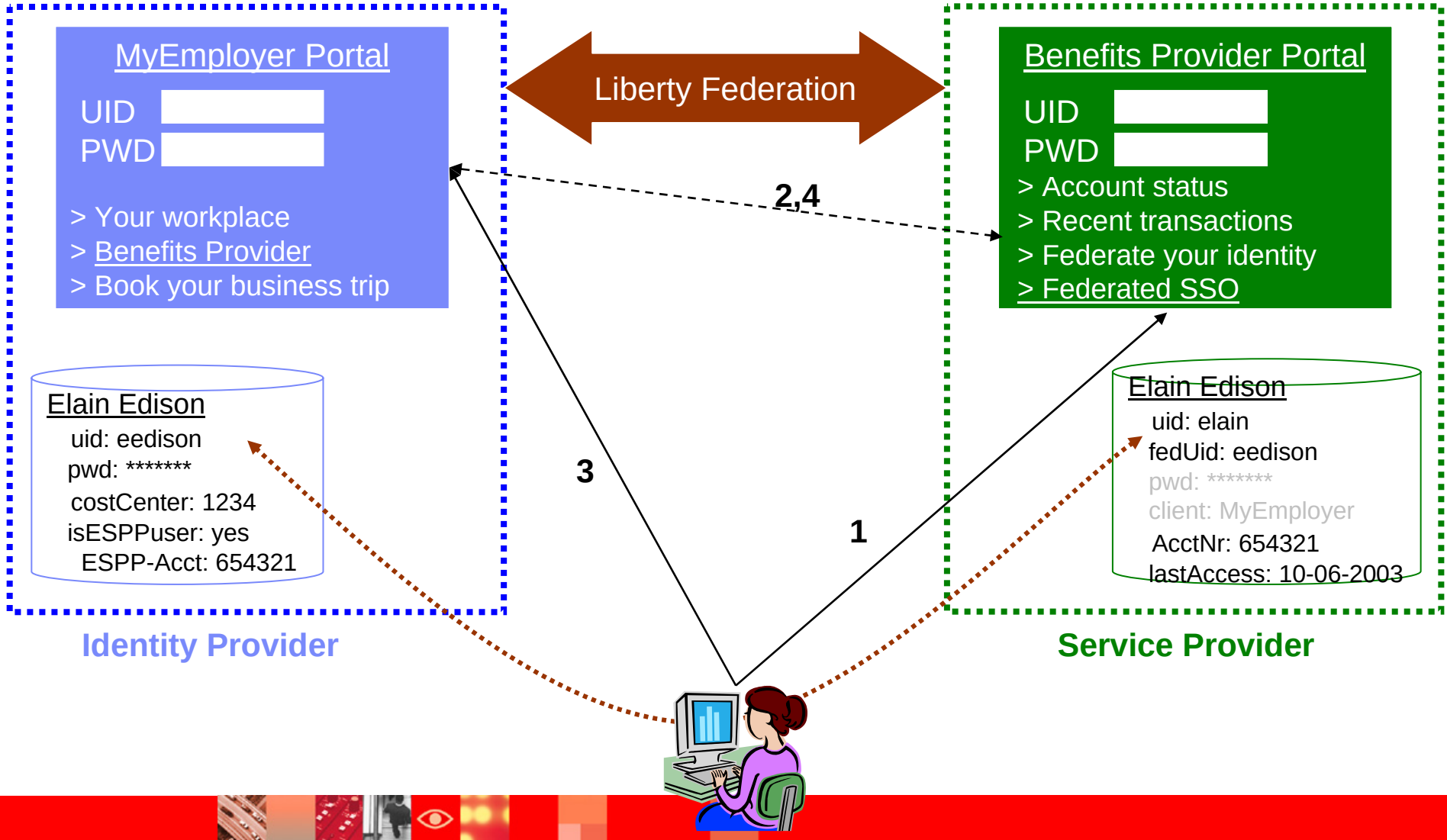
> Account status
> Recent transactions
> Federate your identity

Elain Edison
uid: elain
pwd: *******
client: MyEmployer
AcctNr: 654321
lastAccess: 10-06-2003

Service Provider

© 2005 IBM Corporation

Scenario 2 – Demo: Login Using Federated Single Sign-on



© 2005 IBM Corporation

Danke für Ihre Aufmerksamkeit!
Für weitere Informationen besuchen Sie
http://www.ibm.com/software/de/tivoli/security

Tivoli software

Oleg Bascurov
Tivoli Technical Sales
bascurov@de.ibm.com

e business software

© 2005 IBM Corporation