IBM Security Forum

Soluções para um ambiente seguro

Federação de Identidades e Segurança em SOA – Conceitos e Casos

Felipe Peñaranda Silva,
CISSP, PCI-QSA, ITIL Service Manager
Security Specialist
felpenar@br.ibm.com

Agenda

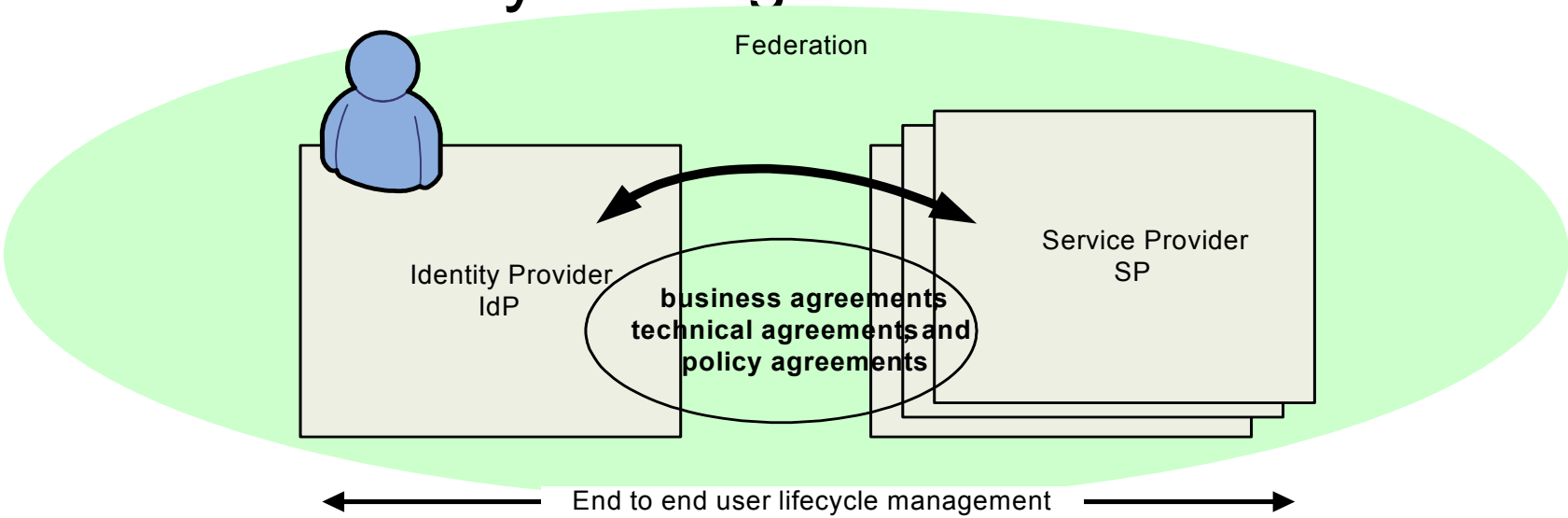
- Federação de Identidades
- Segurança em SOA
- Casos

Federated Identity Management - Conceito

- “ Federação é um grupo de dois ou mais parceiros de negócios com acordos legais e de negócio, incluindo restrições de responsabilidade legal entre os mesmos. A participação em uma federação permite que um usuário ou aplicação de um parceiro de negócio acesse, de forma transparente, os recursos de outro parceiro, de uma forma segura e confiável”

Fonte: IBM-Red Books – Enterprise Security Architecture vol. 2

Federated Identity Management



- Objetivos
  - **Reduzir os custos de Gestão de Identidades**
  - **Melhorar a experiência do usuário**
  - **Prover segurança e confiança “end-to-end” na integração de aplicações inter-organizacionais**

Contexto de Negócio para Federação de Identidades

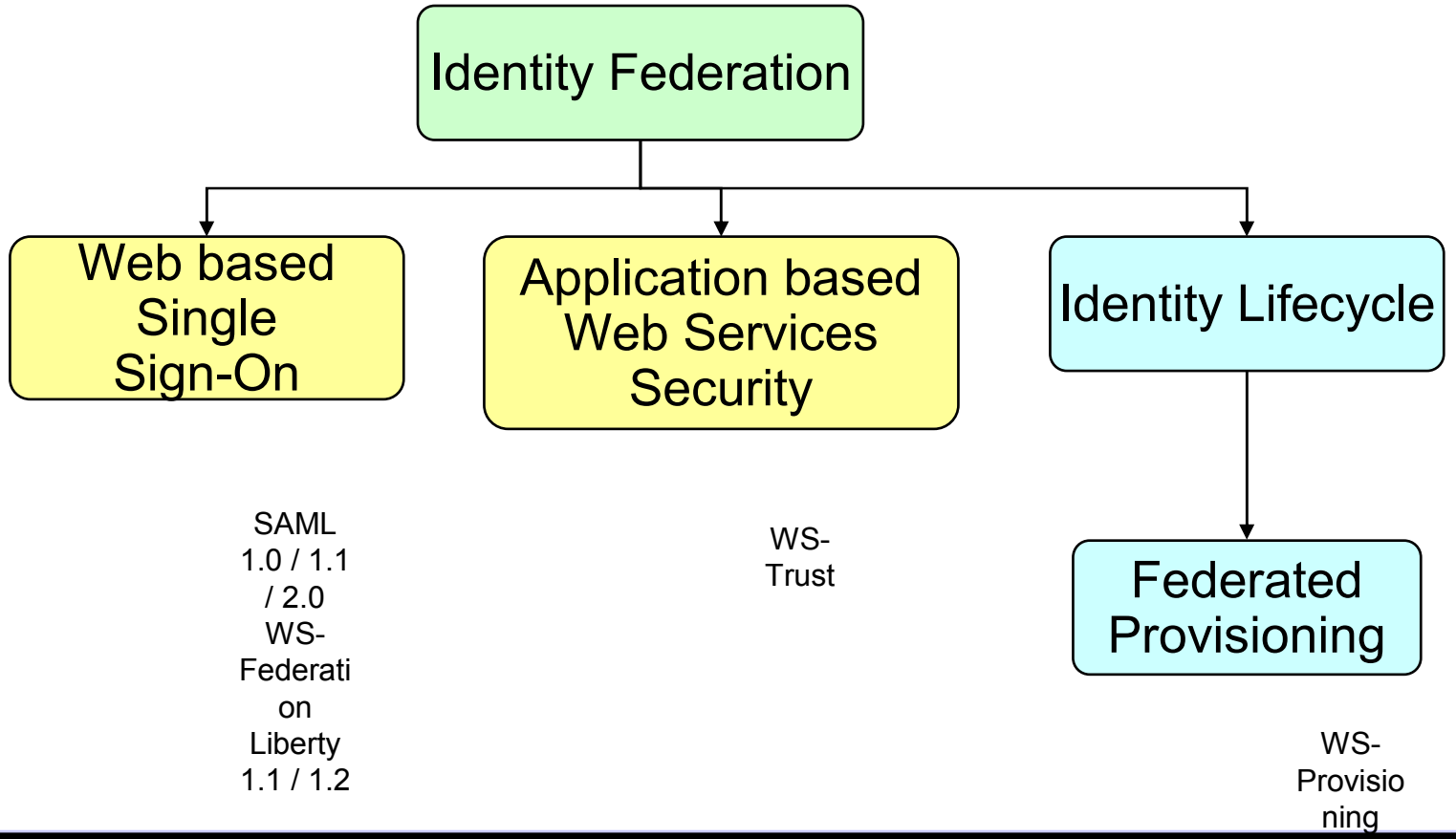
- **Fusões e Aquisições:** “Quão rápido uma empresa terá acesso ao mercado (clientes) da outra empresa ?”
- **Colaboração entre unidades de negócio autônomas:** Mantem a autonomia, porém proporciona flexibilidade de acesso *cross-unit*
- **Desenvolvimento colaborativo de novos produtos entre parceiros**
- **Aquisição de novos clientes através de parcerias**
- **Acesso de funcionários a provedores de serviços**
  - **Automação de clientes B2B**
- **SaaS (Software-as-Services)**
- **Colaboração no Governo**
- **Governança Corporativa**

Analise dos modelos de negócio de federação por setor

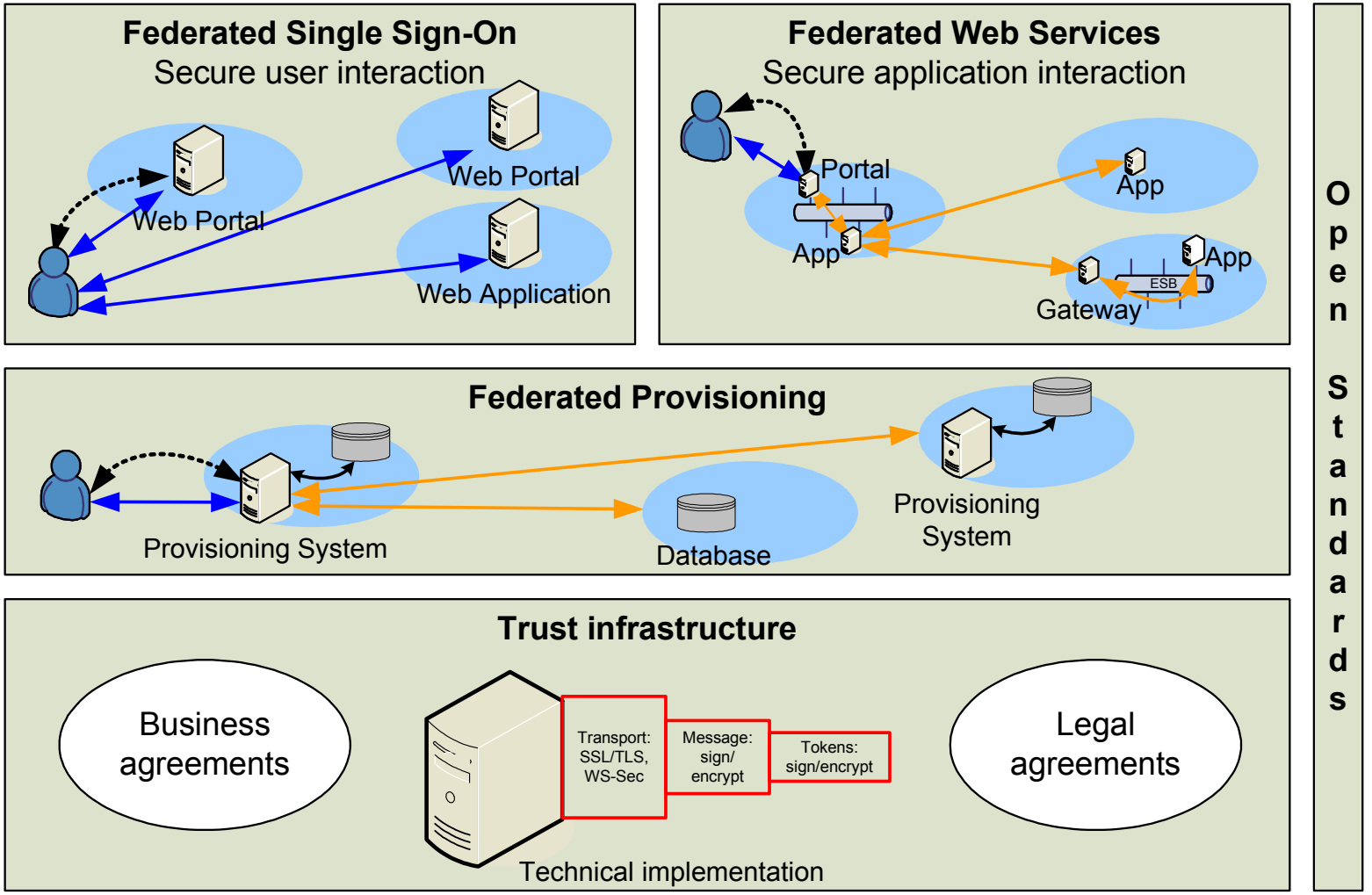
1. Fusões e Aquisições
2. Colaboração entre unidades de negócio
3. Desenvolvimento colaborativo entre parceiros
4. Acesso de funcionários a provedores de serviços
5. Automação de provedores de serviços
6. Governança Corporativa
7. Colaboração no Governo

Setor / Exemplo	1	2	3	4	5	6	7
Comunicação / Telco	x	x	x	x	x	x	
Distribuição	x	x		x		x	
Financeiro	x	x	x	x	x	x	
Indústria	x	x		x		x	
Governo		x					x

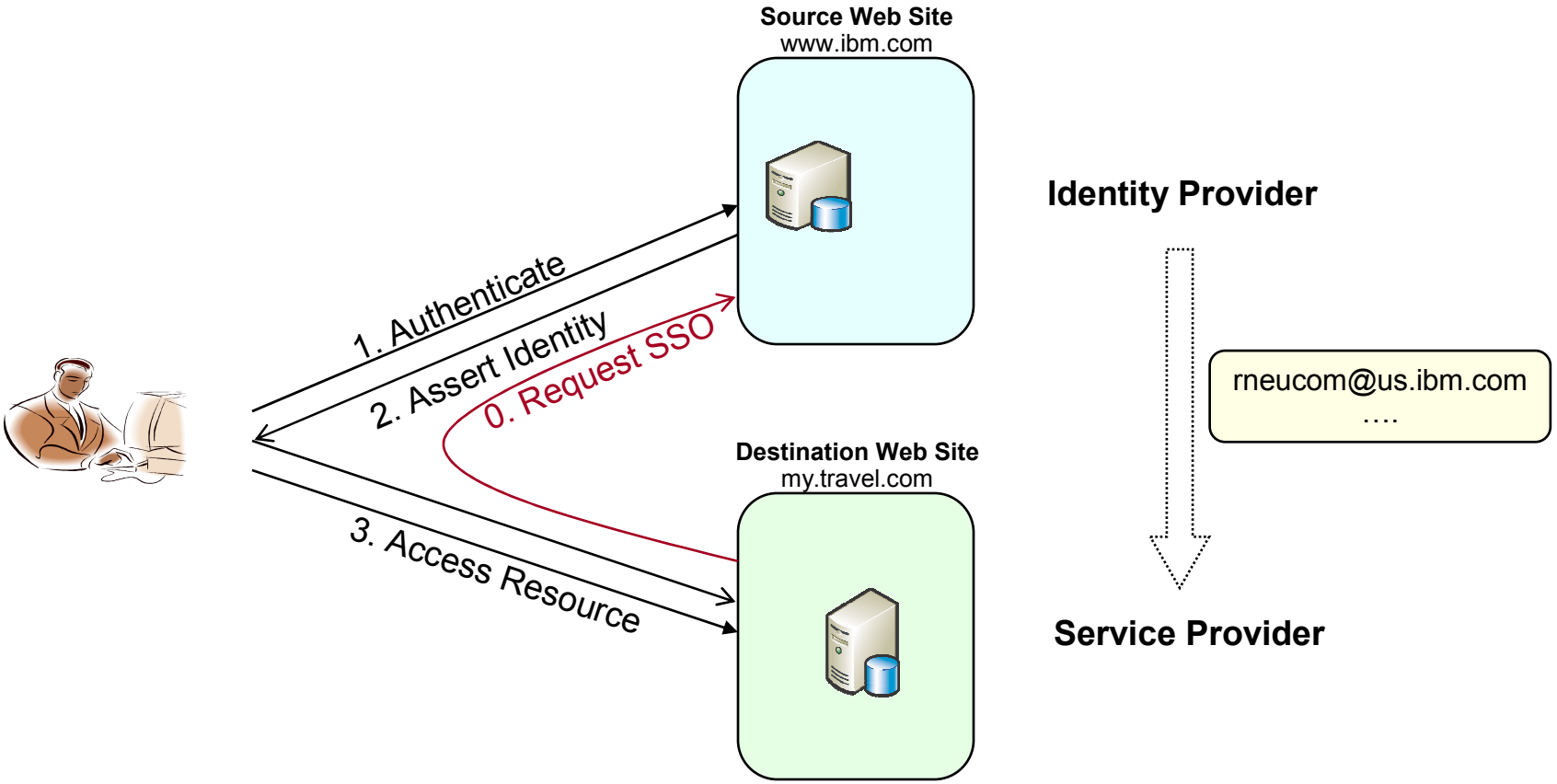
Componentes do Federated Identity Management



Componentes do Federated Identity Management



Federated Single Sign-On

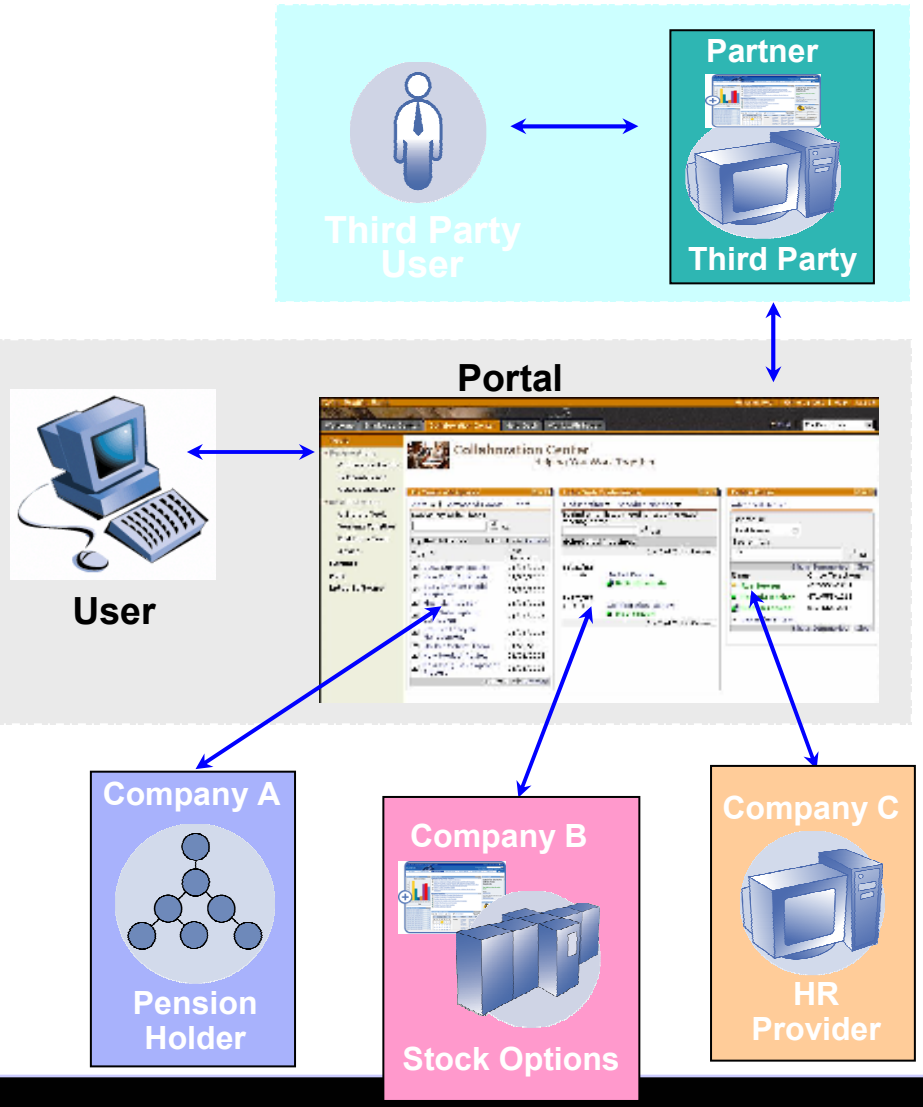


Cenário Típico:

- Múltiplas corporações ou unidades de negócio distintas dentro da mesma corporação
- Objetivo: compartilhar informações de identidades em transações entre parceiros que estabeleceram relação de confiança.

Valor:

- Promover novos negócios, com baixo custo
- Baixo custo de gerenciamento de identidades e help-desk
- Logs e auditoria



Federação de Identidades

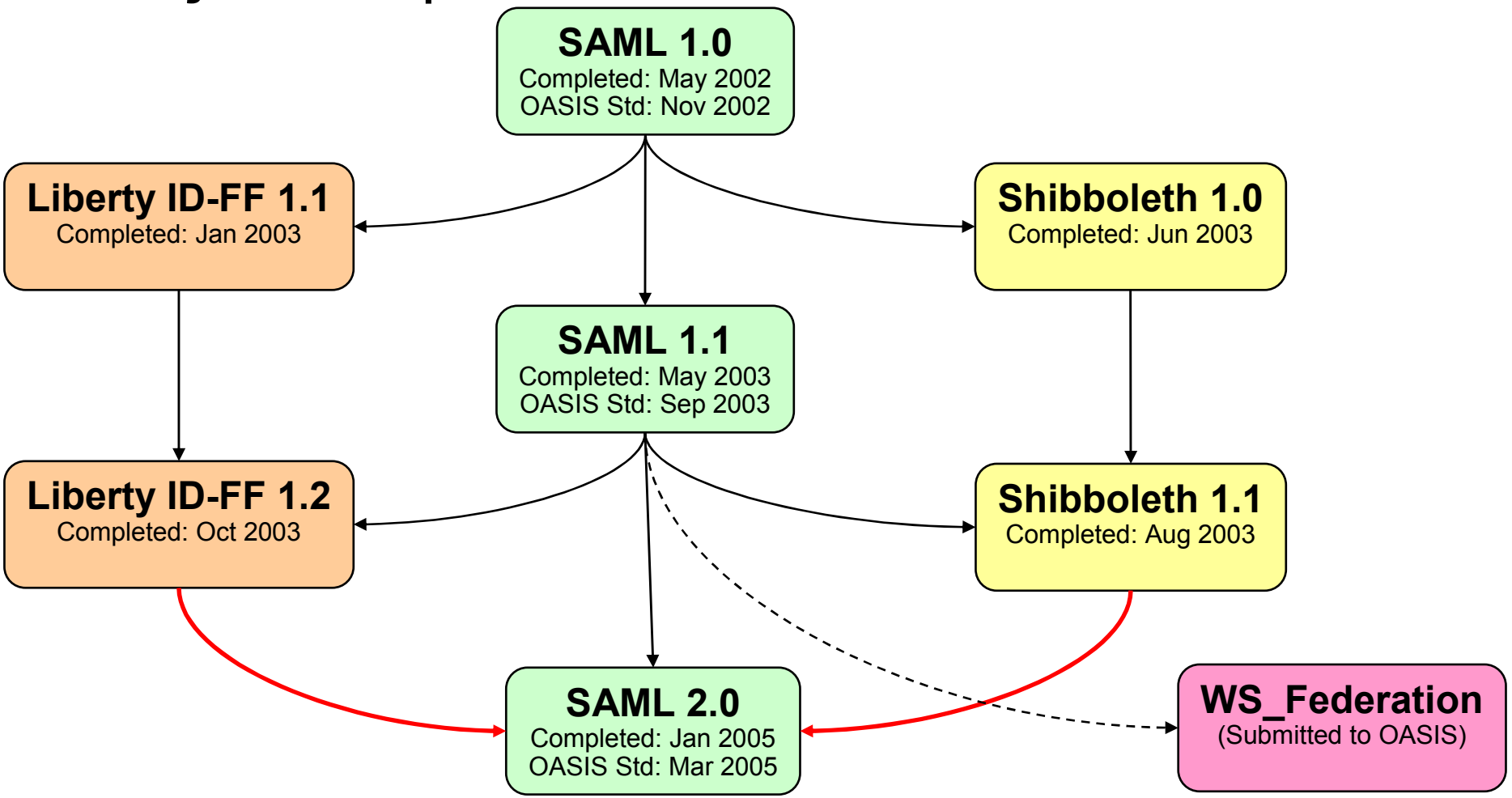
- A identidade de um usuário se diz "**federada"** entre um conjunto de *providers* quando existe um acordo entre eles de um conjunto de identificadores e/ou atributos para se referenciar ao usuário.

- Formas de federação de identidades:
  - ***Single Sign-On com Account Linking***
    - Userids may differ between sites (out-of-band resolution)
  - ***Attribute Federation***
    - Atributos do usuário (in the assertion) são usados para fazer o "link" da conta
  - ***Persistent Federation***
    - A persistent "*name identifier*" is used to identify each user
  - ***Transient Federation***
    - Supports role-based and anonymous identity mapping

Famílias de padrões - Federated SSO

- SAML
  - Defined by an OASIS TC
  - Provides a standard format for asserting identity information
  - Also defines a number of SSO protocols (SAML 1.0, 1.1, 2.0)
- WS-Federation
  - Part of the overall “Web Services Security Roadmap”
  - Describes how to manage trust across trust domains
  - Defines protocols to simplify single-sign-on and session management in Passive and Active client environments
- Liberty Alliance
  - Defined by Liberty Alliance
  - Defines a set of specifications for identity federation
  - Define SSO protocol and protocols for management of aliases and account linking
  - Liberty ID-FF 1.1 & 1.2 are based on SAML 1.x

Evolução dos padrões - Federated SSO



Federação de Identidades (FIM): Hipóteses e Questões

- Hipótese 1: **As atividades de Federação de Identidade (FIM) são percebidas com potencial de trazer vantagem competitiva para as empresas participantes.**

- **Questões:**
  - As atividades de FIM podem ser utilizadas para aumentar barreiras de entrada nos mercados ?
  - As atividades de FIM podem ser utilizadas para aumentar os custos de mudança, mantendo o usuário mais “leal” ao produto/serviço da empresa ?
  - As atividades de FIM podem ser utilizadas para tornar a empresa única ?
  - As atividades de FIM podem ser utilizadas para redução de custos ?
  - As atividades de FIM podem ser utilizadas para criar parcerias e aumentar a oferta de produtos complementares ?
  - As atividades de FIM podem ser utilizadas para dificultar a ameaça de produtos substitutos ?
  - As atividades de FIM podem ser utilizadas para transformar a cadeia de valor ?

Fonte: Competitividade e Qualidade Percebida: Estudo sobre as atividades de Federação de Identidade: José Marcelo de Freitas Vilela

Federação de Identidades (FIM): Hipóteses e Questões

- Hipótese 2: **As atividades de Federação de Identidade (FIM) contribuem para as empresas na estratégia de customização em massa.**
- **Questões:**
  - As atividades de FIM auxiliam as empresas a obter menor custo dos processos para oferecer produtos/serviços diferenciados em novos mercados ?
  - As atividades de FIM auxiliam as empresas na integração de constantes mudanças nos requisitos de comunicação e processamento das informações ?
  - As atividades de FIM podem ser usadas para personalizar a oferta de produtos e serviços ?

Fonte: Competitividade e Qualidade Percebida: Estudo sobre as atividades de Federação de Identidade: José Marcelo de Freitas Vilela

Valor para o negócio

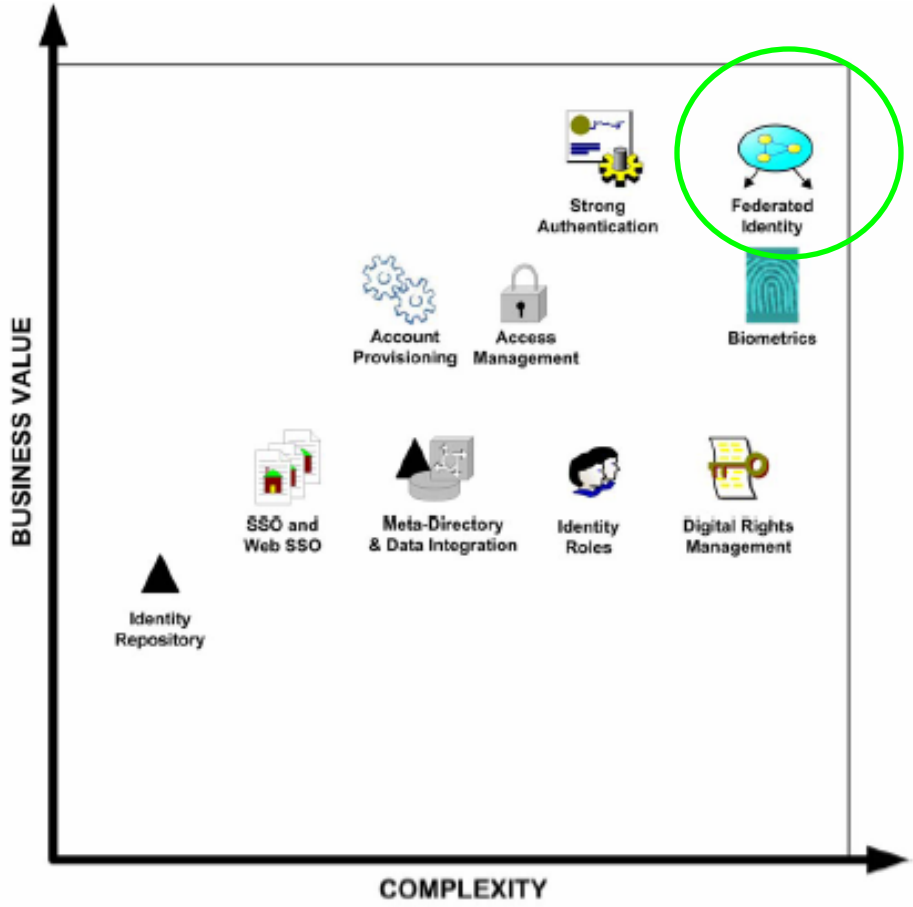


Figure 6.1: The incremental value components of an Identity Management initiative.

Segurança em SOA

O que é …..?

… um serviço ?

Uma tarefa repetitiva – ex: checar o crédito de um cliente; abrir uma conta nova

… orientação a serviço ?

Uma maneira de integrar o **negócio como serviços relacionados**

… arquitetura orientada a serviço (SOA)?

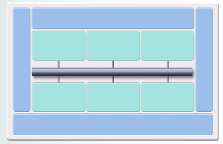
Uma arquitetura de TI que suporta orientação a serviço

… uma aplicação composta ?

Um conjunto de serviços **relacionados & integrados** que suportam um processo de negócio construido em cima de SOA

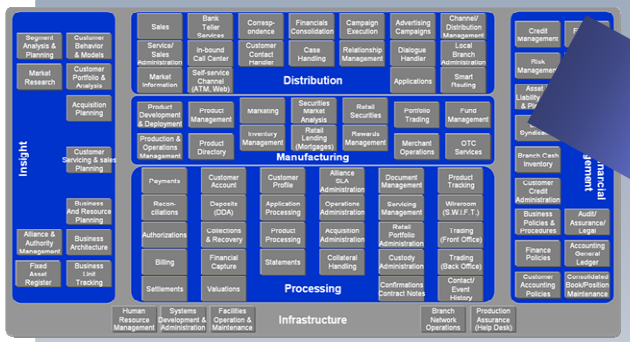
Service Oriented Architecture (SOA)

Diferentes conceitos para grupos diferentes

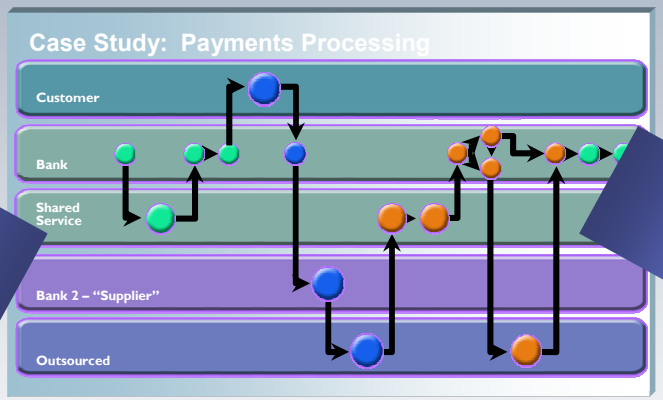
	Perfis
Possibilidade que o negócio tem para se expor como ***um conjunto de serviços*** para clientes e parceiros	**Business** 
Um ***estilo de arquitetura*** que requer um provedor, um consumidor e uma descrição do serviço. Endereça características como baixo acoplamento, reuso e implementações simples e compostas	**Architecture** 
Um ***modelo de programação*** completo com padrões, ferramentas, métodos e tecnologias como Web services	**Implementation** 
Um ***conjunto de acordos*** entre consumidores e provedores de serviços que especificam a qualidade do serviço e identificam métricas de negócio e TI	**Operations** 

Negócios flexíveis necessitam de TI flexível…

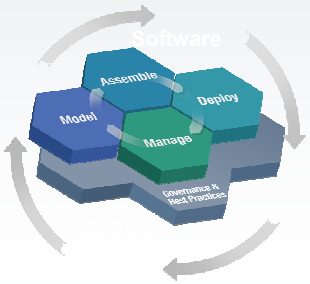
Visão completa de negócio



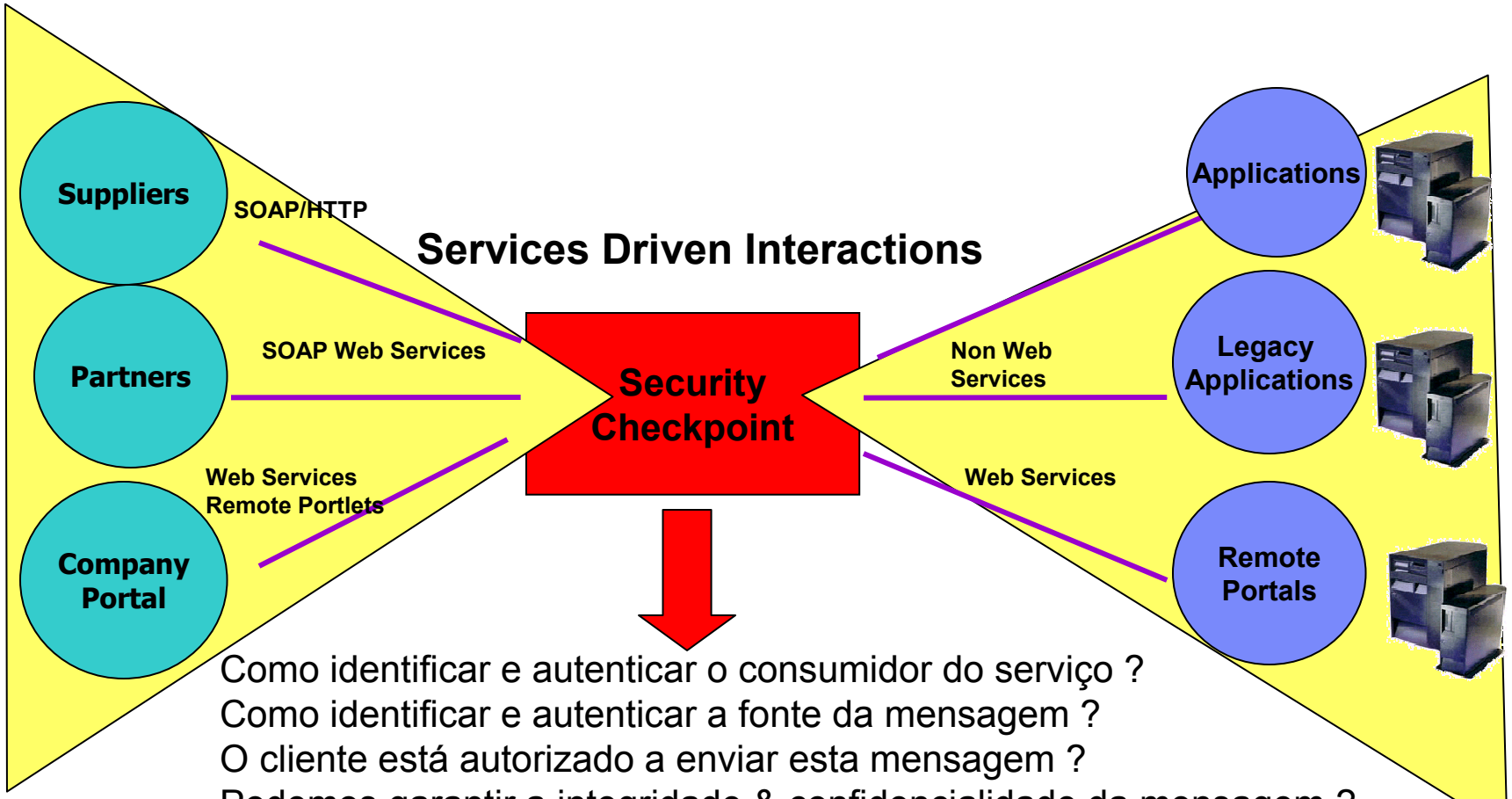
Processo a otimizar



Criando TI flexível

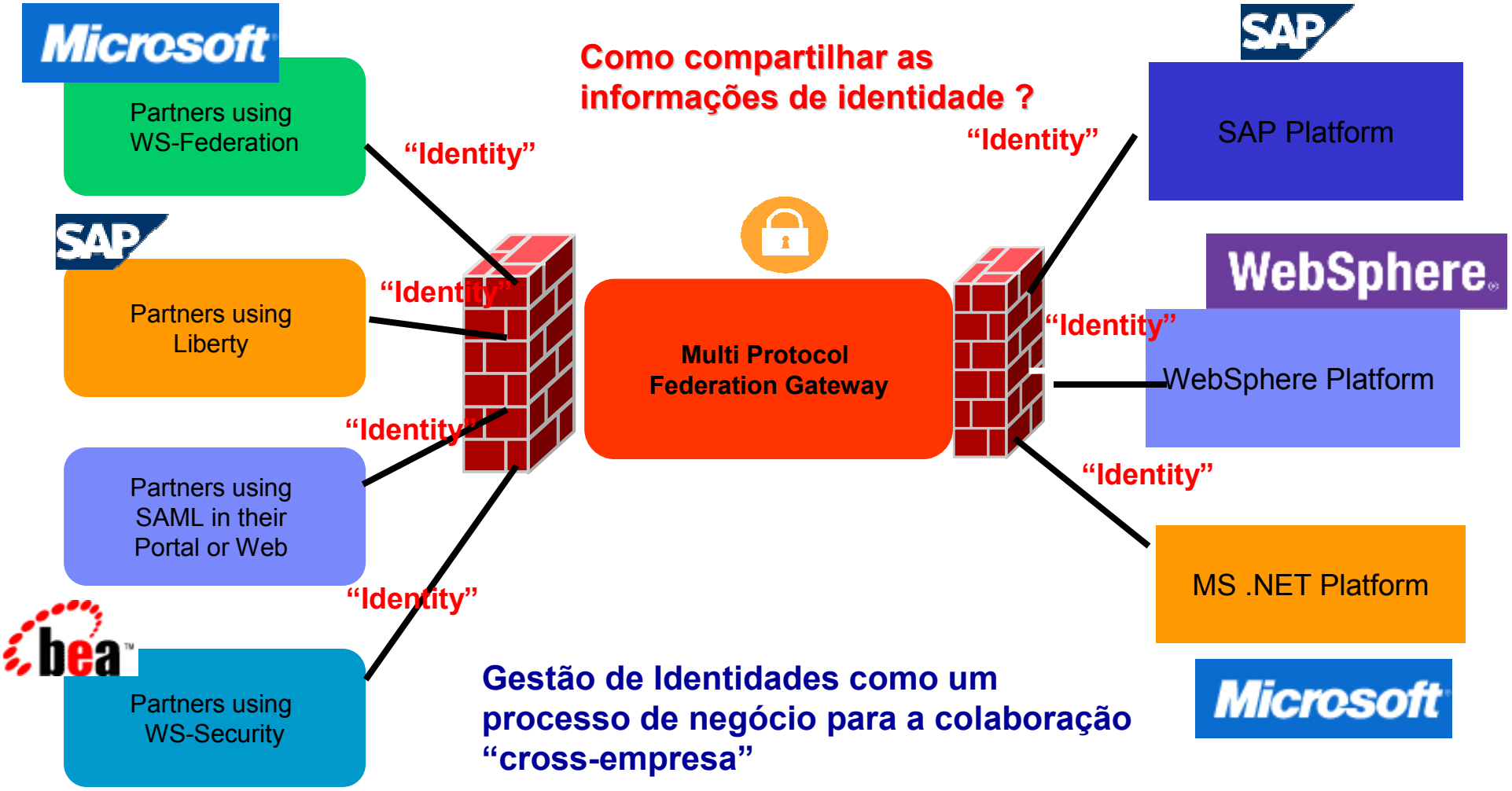


Segurança em SOA

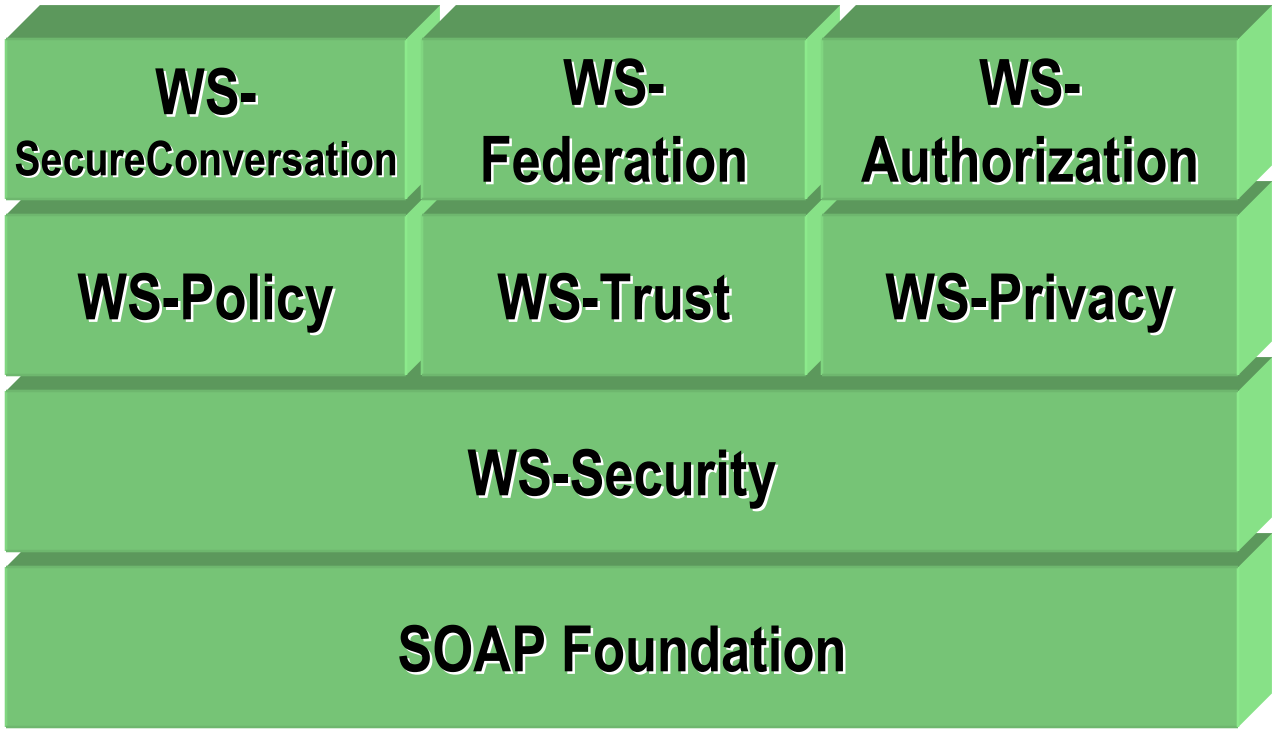


Como identificar e autenticar o consumidor do serviço ?
Como identificar e autenticar a fonte da mensagem ?
O cliente está autorizado a enviar esta mensagem ?
Podemos garantir a integridade & confidencialidade da mensagem ?
Como posso auditar o acesso a Web Services?

Problema de integração de identidades



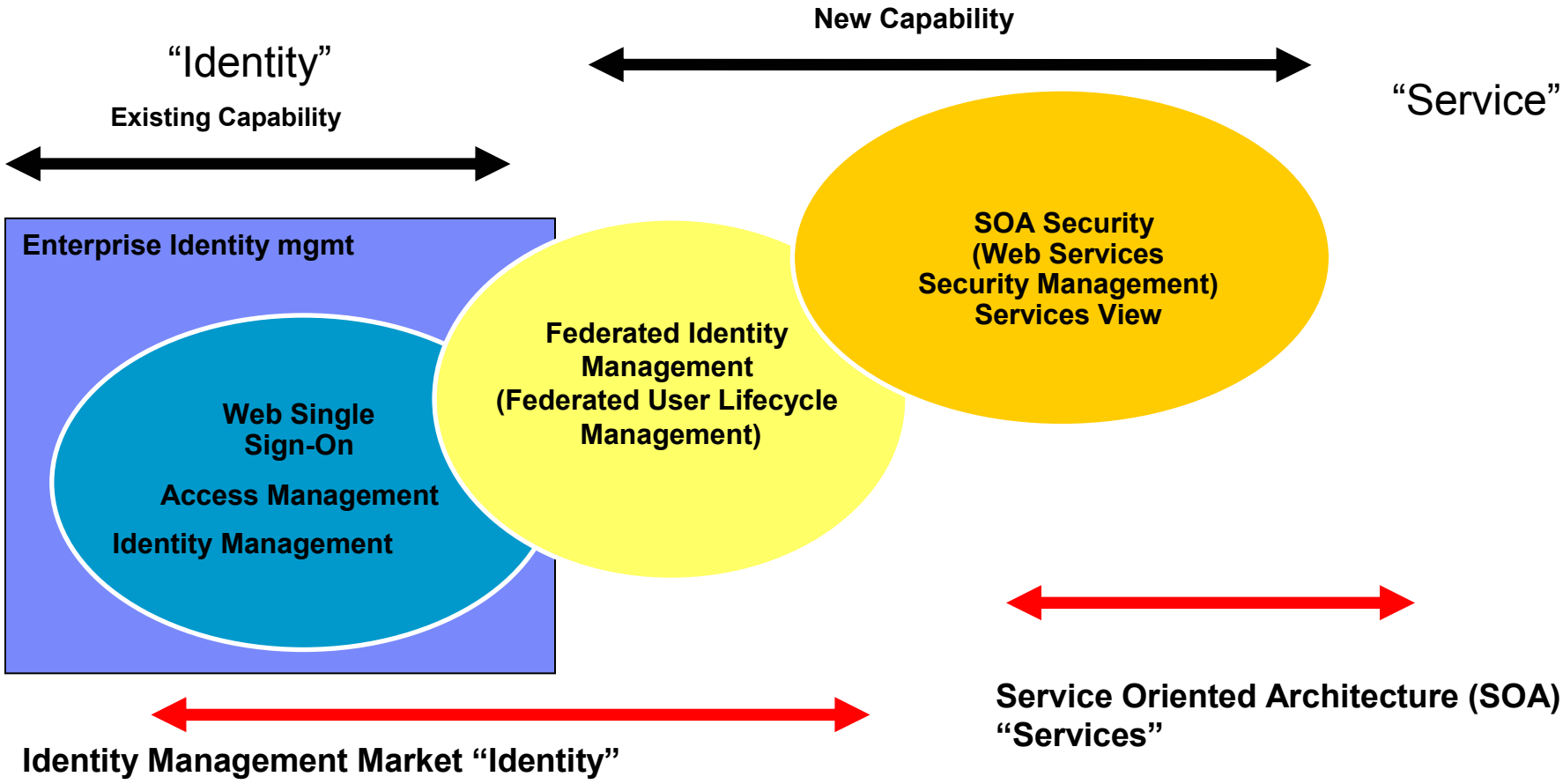
Web Services Security Specifications*



[illegible]

* www.ibm.com/developerworks/library/ws-secmap/

Gestão de identidades & SOA



Identity transformation from a product-centric view to a service-centric view – move to adoption of service-oriented architectures with federation characteristics for simplifying identity management and strengthening corporate compliance

Casos

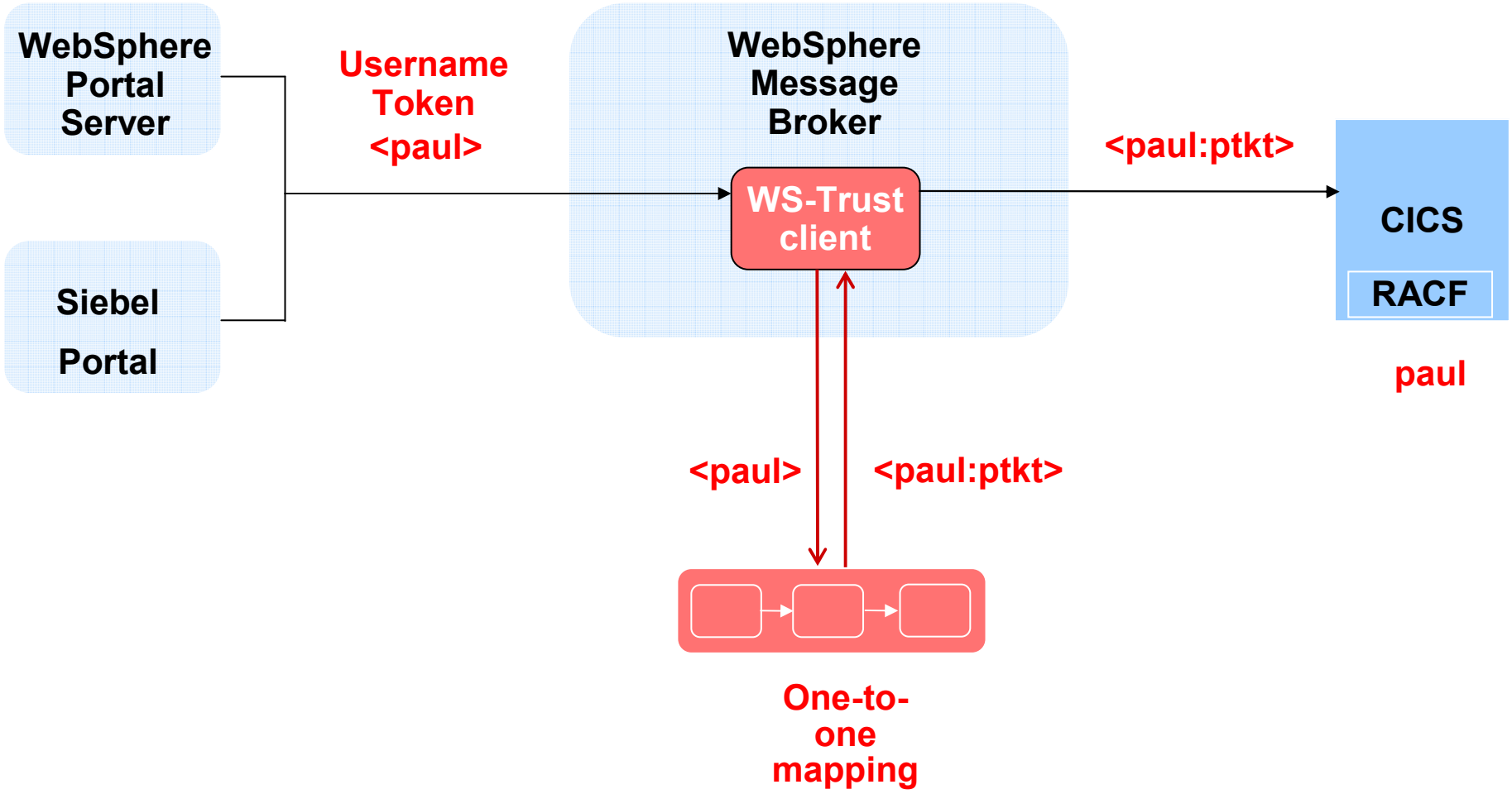
Dados do Cliente

- Client: An Immigration Agency
- Country: in Asia Pacific IOT
- Industry: Government
- Use case: SOA Security

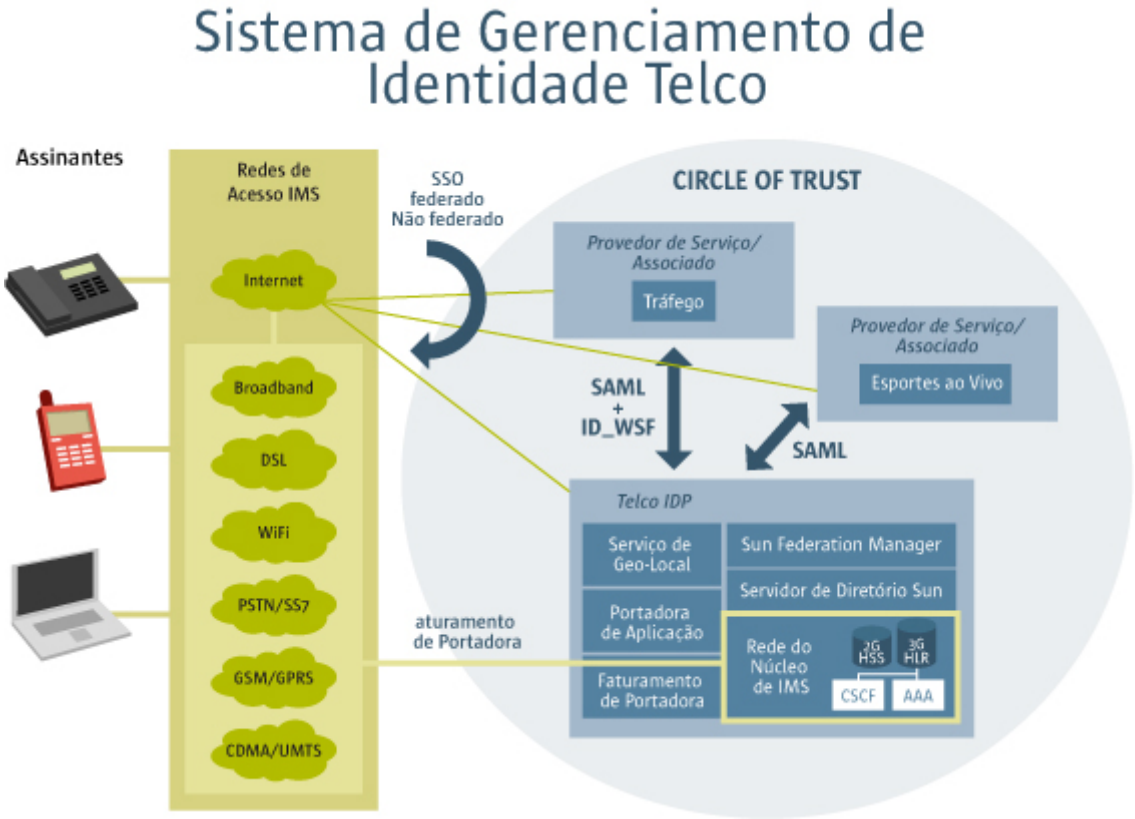
Necessidade de negócio

- Criar um novo front-end para o seu staff interno
- Em vez de acessar várias aplicações usando interface mainframe, tudo seria consolidade em uma interface de portal
- No curto prazo, seria para 6.000 usuários. Mais tarde, milhões de usuários (internet) seriam adicionados.
- A utilização de *web services* para acessar os sistemas legados (mainframe), exigiu uma nova abordagem para a propagação de identidades

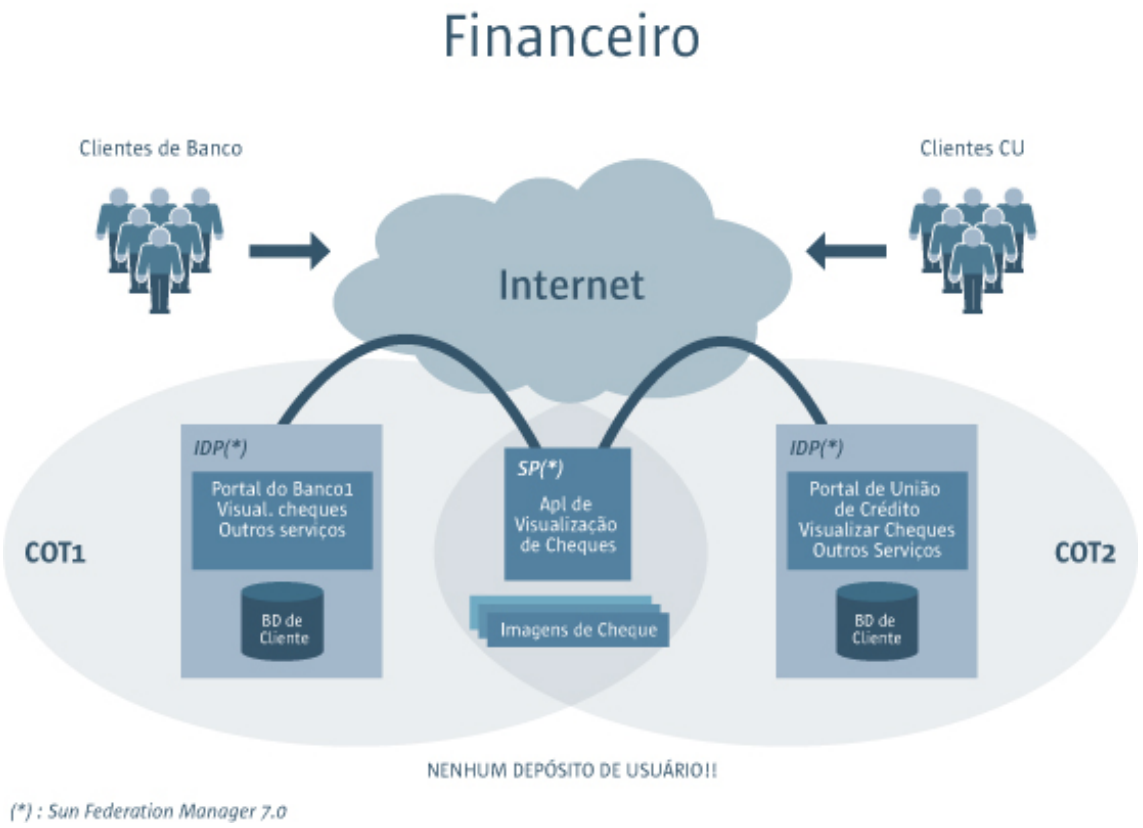
Architecture (brief description + picture)



Telco – Disponibilização de conteúdo de parceiros



Finanças – Visualização de imagens de cheques



IBM Tivoli Federated Identity Manager

- Federated Single Sign-On
  - Integration with IBM Tivoli Access Manager
  - Supported Protocols:
    - SAML 1.0 / 1.1 / 2.0
    - WS-Federation
    - Liberty 1.1 / 1.2
- Federated Web Services
  - WS-Trust based integration with Enterprise Service Buses, XML Gateways
  - Integration with WebSphere Application Server
    - SOAP, JCA and JDBC integration
    - SAML modules to allow WAS to generate/consume SAML assertions in WS-Security headers of SOAP message
  - Evolving into Identity Propagation in SOA
- Federated Provisioning
  - Provides linking of local provisioning systems
  - Supported Protocol:
    - WS-Provisioning

IBM Tivoli Federated Identity Manager - Vídeo

IBM Security Forum

Soluções para um ambiente seguro

Federação de Identidades e Segurança em SOA – Conceitos e Casos

Felipe Peñaranda Silva,
CISSP, PCI-QSA, ITIL Service Manager
Security Specialist
felpenar@br.ibm.com