

GT Middleware RNP

WRNP

GT Middleware: Contexto, produtos e perspectivas

Coordenação

Oswaldo Carvalho

Luiz Eduardo Buzato

UFMG

UNICAMP

Plano da Apresentação

- Middleware, por que?
 - Ganhos institucionais
 - Ganhos de interoperabilidade
 - Ganhos em cooperação multi-institucional
- O GT-Middleware
- Conclusões

O que é “middleware”?

- Camada de software que gerencia segurança, acesso e troca de informações com o propósito de tornar mais fácil e confiável a comunicação e a colaboração por meio de tecnologias da informação.
- Diretórios são a parte mais importante de qualquer estrutura de middleware

Diretório Corporativo

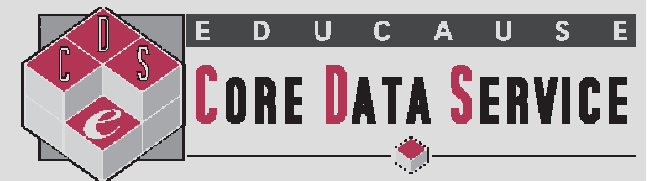
- Conjunto de bases de dados sobre pessoas e vínculos com uma organização
- Comumente oferece informações usando LDAP
- Integrado com processos de negócio e bases corporativas

Situação das universidades americanas com relação a diretórios

	DR
Deployed	76.1%
Piloting	3.7%
In progress	14.7%
Considering	4.3%
Not planned	1.2%

Carnegie classification

Por que?



2003 Summary Report

Por que?

- No âmbito institucional, ganhos na segurança, administração e usabilidade de TI
- No âmbito nacional, maior interoperabilidade, com aproveitamento de uma aplicação por muitas instituições
- No internacional (e também nacional), cooperação multi-institucional mais eficaz, segura e confortável

Ganhos Institucionais com Diretórios

TI Institucional: Situação Típica

- Sistemas isolados de autenticação
 - Sistemas acadêmicos
 - Sistemas de pessoal
 - Ensino à distância
 - Instalações Linux, Windows
 - Correios
 - Lattes, SIAPE, CAPES, IBICT,...

Cada aplicação ou sistema

- Seu diretório de usuários
- Seu administrador de contas
- Um login e uma senha para lembrar...

Problemas com sistemas isolados de autenticação

- Segurança definida por cada administrador
- Matrículas, contratações, demissões envolvem ações de diversos administradores
- Dificuldade de apresentação racional do conjunto de aplicações a que um usuário tem acesso

Problemas com nichos de informações sobre pessoas e vínculos

- Redundância e por vezes inconsistência de dados como endereços ou telefones.
- O desenvolvedor de cada aplicação deve construir seu próprio sistema de autenticação e sua base de usuários, aumentando seus custos
- A gerência de sistemas que dependem de informações de bases sob outra gerência institucional é complicada (Como exigir que certos computadores só sejam usados pelos alunos de Computação?)

Sistemas com Diretórios

- O diretório é a referência central
- Gerência de usuários eficiente
- Login e senha únicos
- Segurança e controle de acesso mais fortes ,
com concessões e cancelamentos de privilégios
em um único ponto

Sistemas com Diretórios

- Administração Unix e Windows simplificada, com admissão automática de calouros, restrições de uso,...
- A implantação de serviços e aplicações com características dependentes de credenciais do usuário é facilitada

Sistemas com Diretórios

- Catálogos de telefones e emails são facilmente mantidos
- Podem ser consultados por qualquer cliente de email como Thunderbird, Eudora ou Outlook.

Sistemas com Diretórios

- Novas aplicações são desenvolvidas com autenticação LDAP, padronizada, segura e barata
 - Existem bibliotecas LDAP para Java, C, C++, PHP, Delphi e qualquer linguagem que se preze
- Diversos produtos em software livre (Moodle, DSpace, PostFix...) têm autenticação LDAP

Sistemas com Diretórios

- O diretório é a base para a implantação de um portal corporativo (uPortal, p. ex.)
- Voz em IP é melhor implantada usando diretórios LDAP

Ganhos de Interoperabilidade

Exemplo: Diário de Classe

- Especificação simplificada:
 - Aplicação Web
 - Um aluno pode ver seus resultados e só estes
 - O professor pode ver e alterar todos

Exemplo: Diário de Classe

- Cada universidade tem dados sobre alunos e professores em um formato
- Como fazer um diário de classe para *todas* as universidades federais brasileiras, o que multiplicaria pelo menos por 50 o mercado?

Diretórios e Interoperabilidade

- Diretórios podem armazenar qualquer tipo de informação
- Interoperabilidade exige um “*esquema*” comum
 - Clientes de correio (Outlook, Eudora, Netscape, Notes, OpenOffice) usam qq LDAP com o esquema *inetOrgPerson* (ou coisa parecida) para localizar pessoas
- Universidades americanas adotam esquemas como *eduPerson*, *eduOrg*, *eduCourse*
- Com um esquema IFES para alunos, professores e matrículas, é fácil fazer um diário de classe para todas as IFES (e outras IES)

Ganhos na Cooperação Multi- Institucional com Diretórios



COLUMBIA UNIVERSITY
IN THE CITY OF NEW YORK

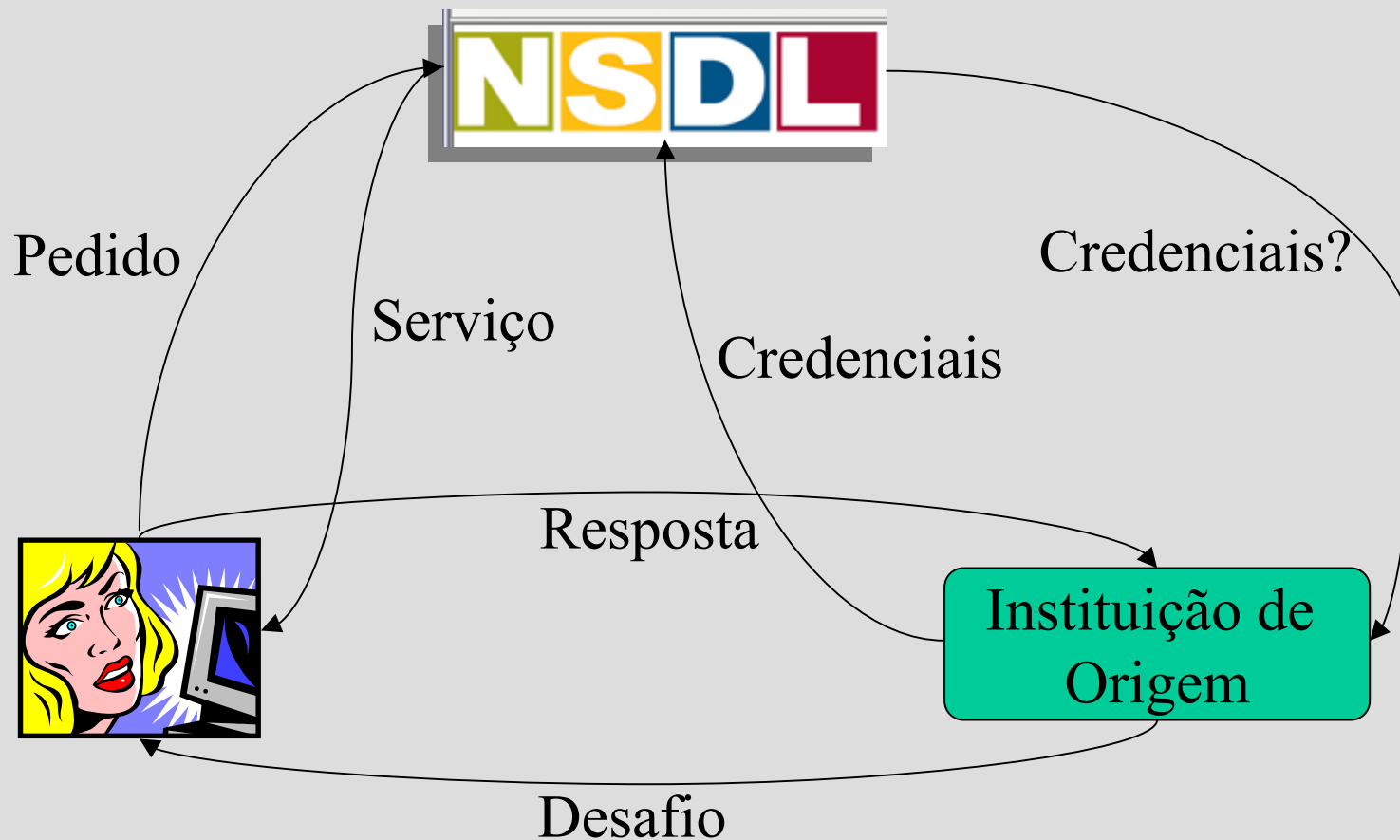
Explore
More

Call For

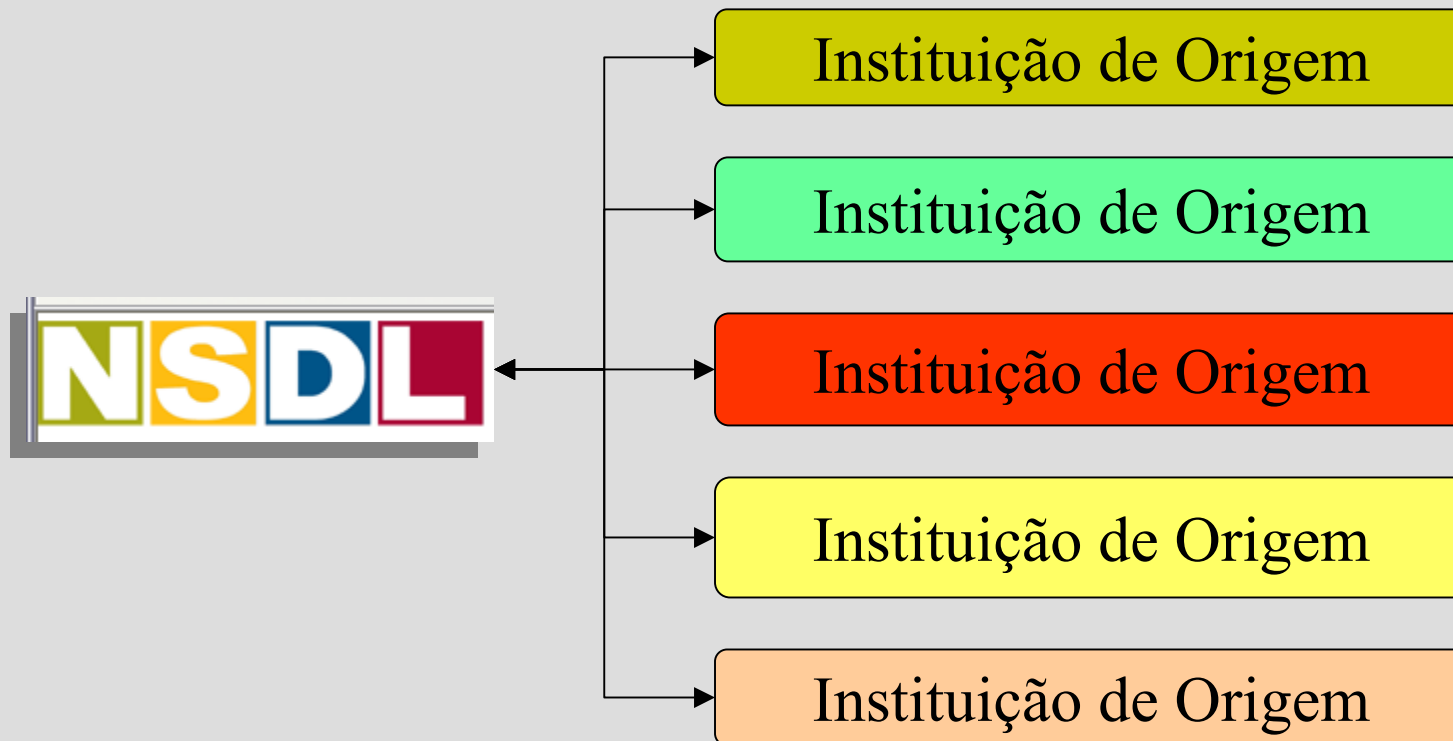
Welcome to the **National Science Digital Library's Enhanced Access Pilot Project Website for Middle Schools**, presented by Columbia University.

- Biblioteca Digital para Ensino Médio
- Alunos \neq Professores
 - Autenticação e autorização para milhões
 - Credenciais confiáveis e atualizadas
- Como?

Shibboleth: Uso de Provedores de Identidade

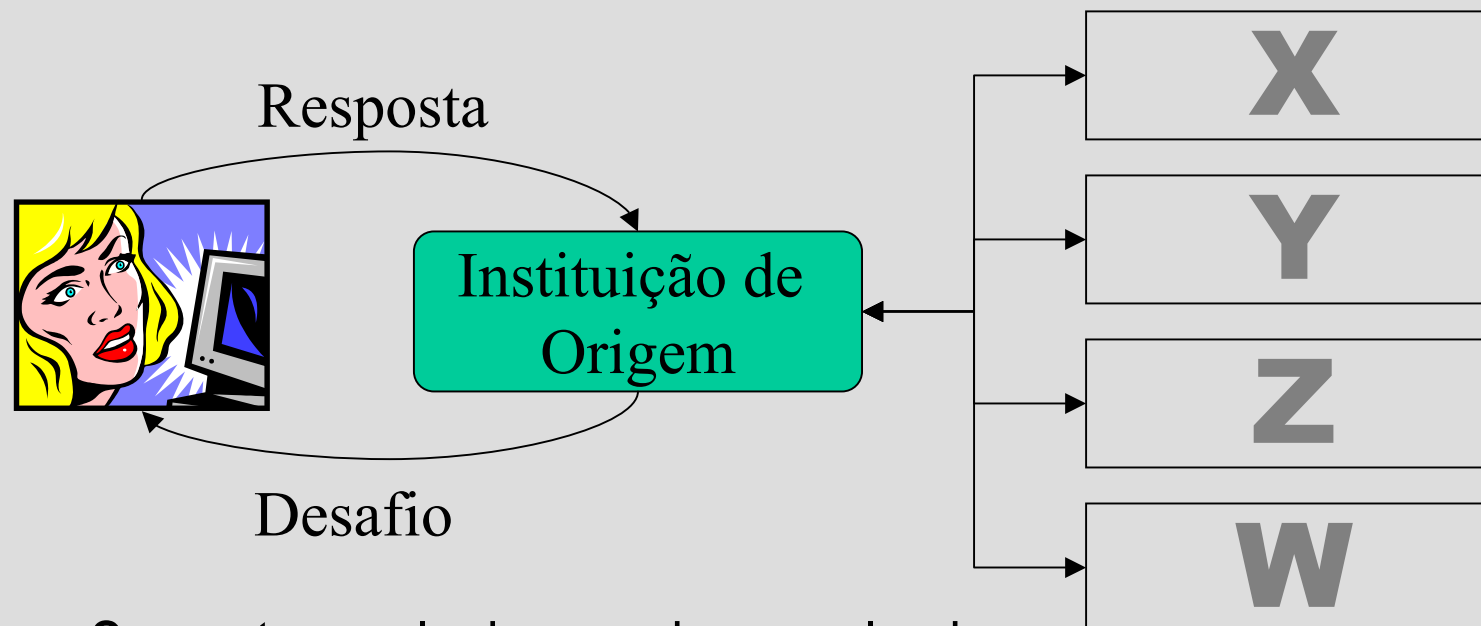


Um serviço, múltiplos provedores de identidade

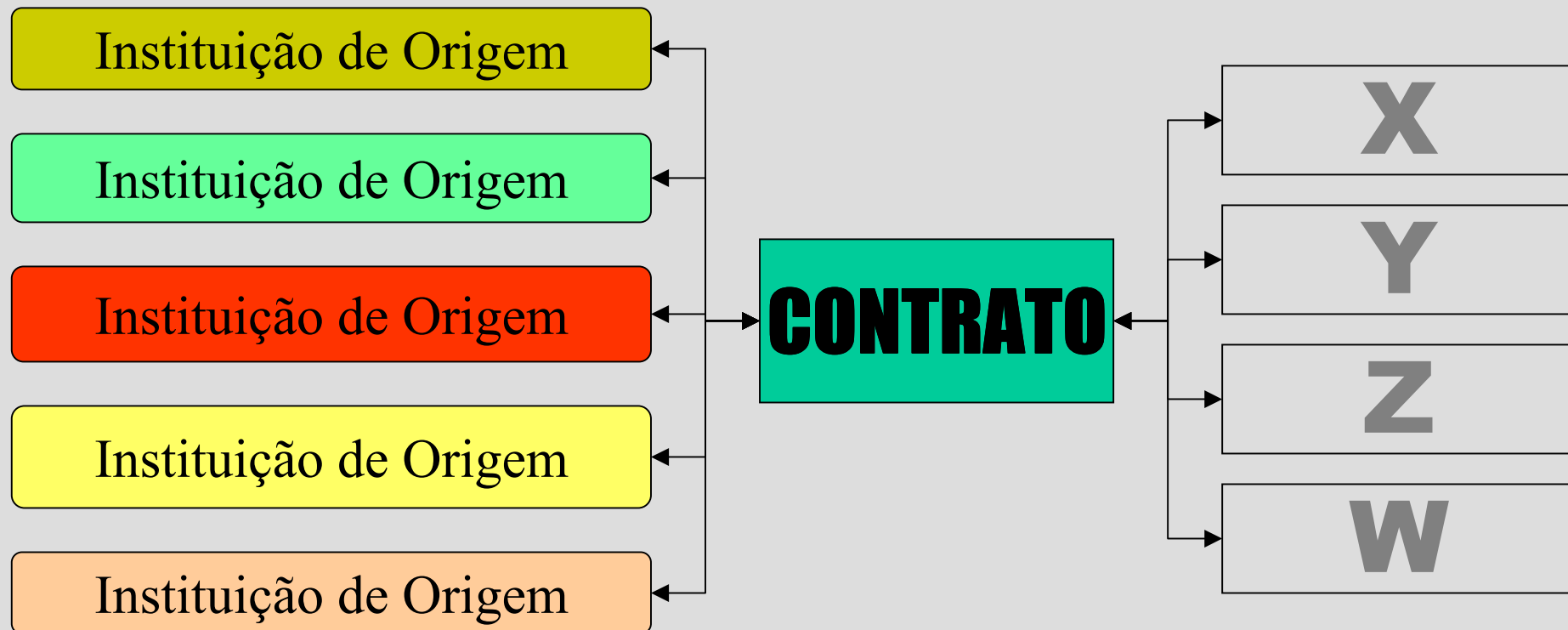


- A NSDL confia nas instituições
- A NSDL não tem uma base de usuários, delegando este serviço às instituições

Um usuário, múltiplos serviços



- Somente um login e senha para lembrar
- Só a instituição de origem vê a senha
- A instituição confia nos provedores de serviços



- Contrato entre a federação e provedores de identidades e de serviços

A Federação InQueue

- Experimental, só para teste de tecnologia
- A UFMG faz parte
- Exemplo de serviço:
 - <https://authdev.it.ohio-state.edu/twiki/bin/view>

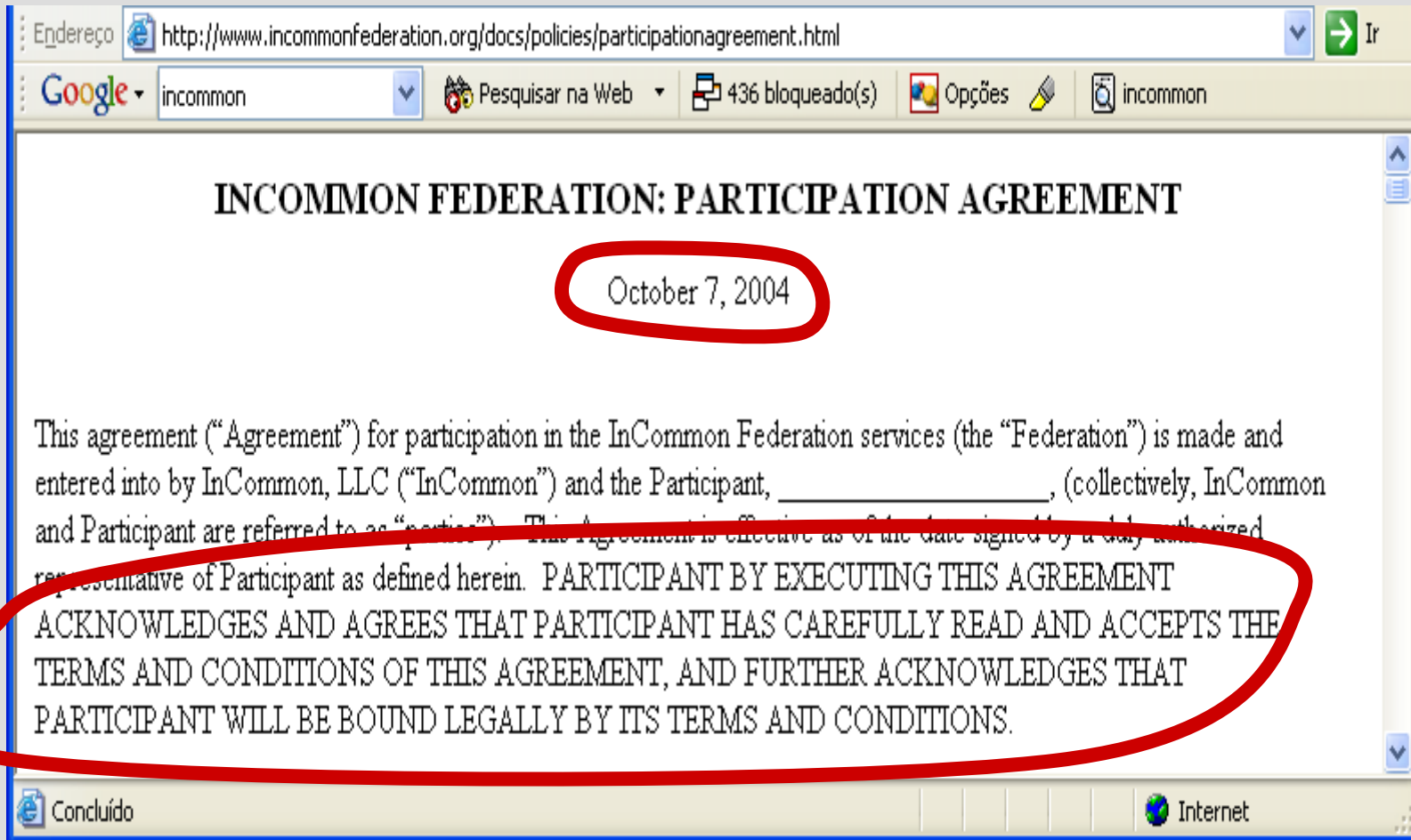
Outros Beneficiários

- MEC
- CNPq, Lattes
- IBICT
- SIAPE
- RNP
- CAPES
- FINEP
- FAPs
- **GT Medições!**

O Contexto Internacional: Federações

- Inqueue
 - Internet2, experimental
- InCommon
 - Internet2, exclusiva para universidades norte-americanas, recentemente em operação
- FEIDE, SWITCH, SDSS
 - Federações de universidades da Noruega, Suíça, Reino Unido

InCommon Agreement



Endereço <http://www.incommonfederation.org/docs/policies/participationagreement.html> Ir

Google incommon Pesquisar na Web 436 bloqueado(s) Opções incommon

INCOMMON FEDERATION: PARTICIPATION AGREEMENT

October 7, 2004

This agreement ("Agreement") for participation in the InCommon Federation services (the "Federation") is made and entered into by InCommon, LLC ("InCommon") and the Participant, _____, (collectively, InCommon and Participant are referred to as "parties"). This Agreement is effective as of the date signed by a duly authorized representative of Participant as defined herein. PARTICIPANT BY EXECUTING THIS AGREEMENT ACKNOWLEDGES AND AGREES THAT PARTICIPANT HAS CAREFULLY READ AND ACCEPTS THE TERMS AND CONDITIONS OF THIS AGREEMENT, AND FURTHER ACKNOWLEDGES THAT PARTICIPANT WILL BE BOUND LEGALLY BY ITS TERMS AND CONDITIONS.

Concluído Internet

InCommon Insurance

12. Insurance. Participant covenants and agrees to obtain and maintain in force, at its own expense, throughout the term of this Agreement, general commercial liability insurance coverage with a combined single limit of not less than \$3,000,000.00 each occurrence or its equivalent, whether such insurance is maintained through self-insurance or through third party insurance, against claims, regardless of when asserted, that may arise out of, or result from, Participant's participation in the Federation.

O Contexto Nacional

- Não temos um levantamento sistemático de TI como o Core Data Service: o que se segue é percepção pessoal
- Diretórios
 - UFMG, UFRGS e UFSM têm diretórios operacionais
 - A UNICAMP terá em meados de 2005
- E é só, tanto quanto eu saiba...

Conclusão da 1a Parte

- Diretórios propiciam muitos ganhos
- No primeiro mundo, todos estão adotando
- Para participar das redes de confiança mundiais, é preciso se habilitar como provedor de identidades e credenciais
- No Brasil, o movimento é incipiente
- **E então, como fazer um diretório?**

O GT-Middleware

Objetivos do *GT-Middleware*

- Estímulo à adoção por universidades brasileiras de uma estrutura de middleware
 - correta institucionalmente
 - coerente nacionalmente
 - obedecendo a padrões internacionais
- Aumentar ganhos com diretórios, facilitando a implantação de serviços habilitados para diretórios

Metodologia

- Implantação de pilotos na UNICAMP e UFMG
- Desenvolvimento de produtos que podem ser usados por outras universidades com grandes reduções de custos
- Oferta de informação e capacitação
 - Documentação dos produtos e implantações piloto
 - Site informativo
 - Cursos e treinamentos

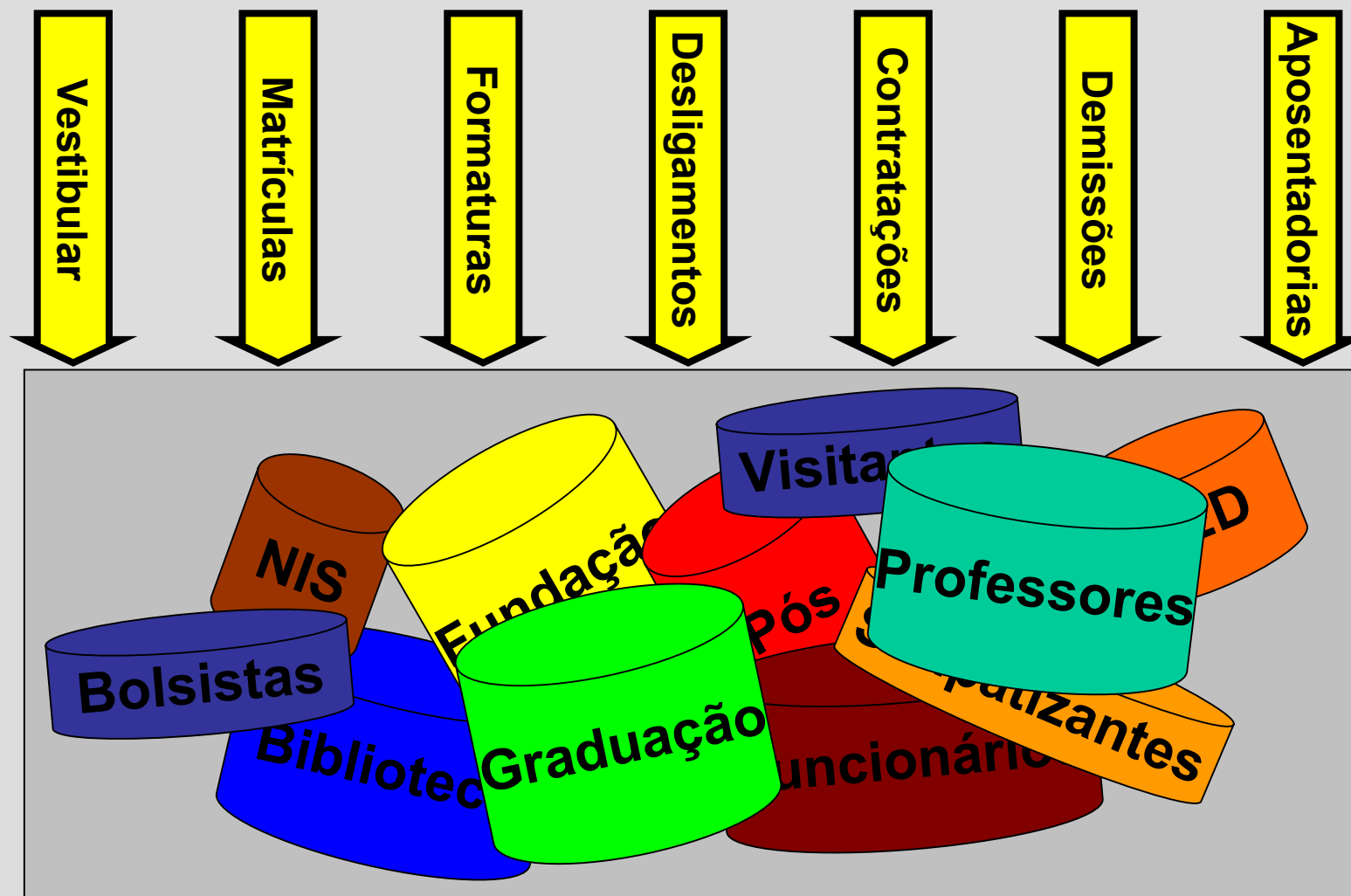
Opções Tecnológicas do GT

- Aproveitamento máximo dos resultados produzidos no exterior (vamos no vácuo)
- Padrões e sistemas abertos: Java, XML, LDAP, OpenLDAP, ...
- Concentração nos aspectos de autenticação e autorização
- Coexistência com sistemas legados

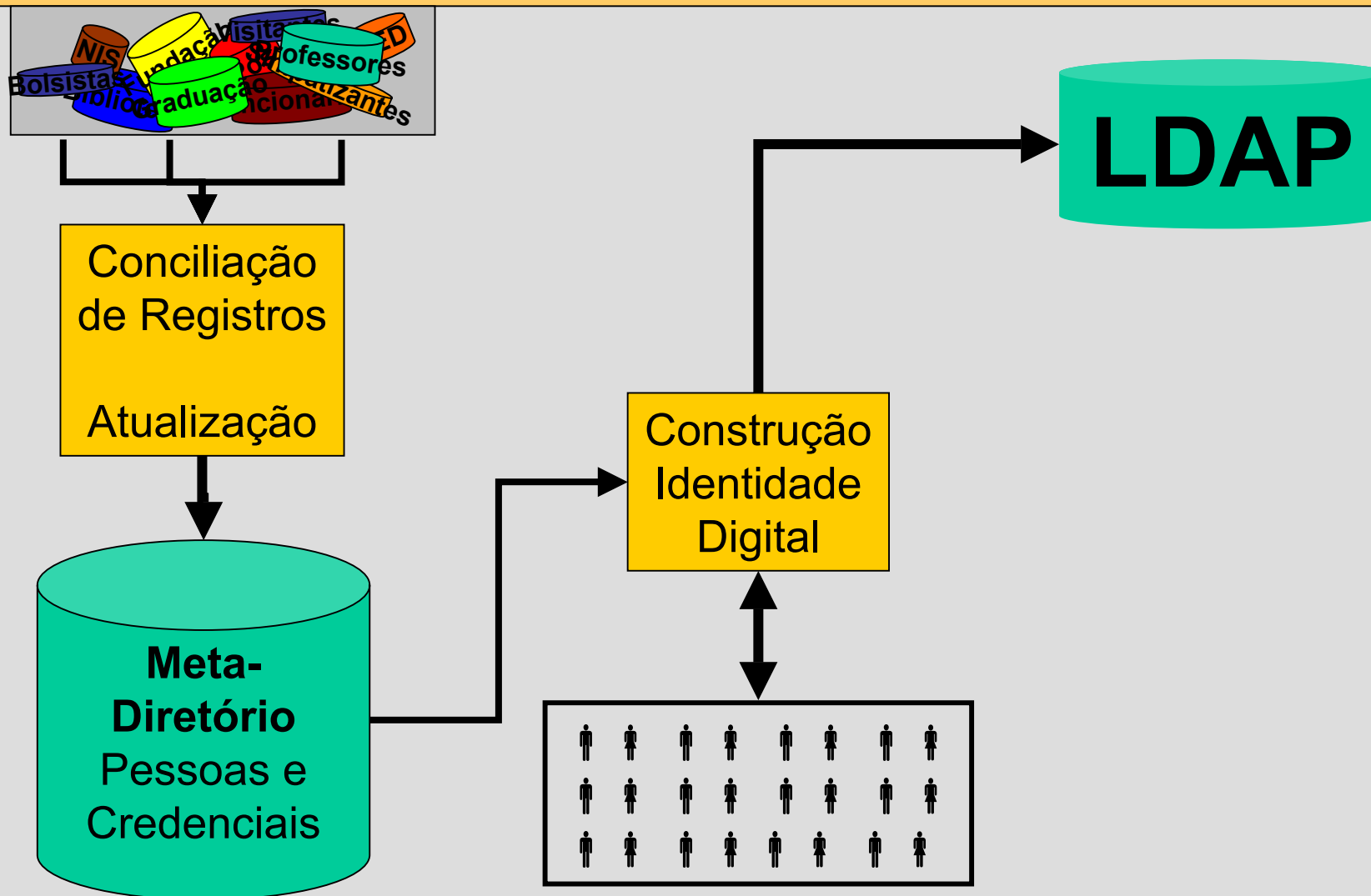
Premissas

- A instituição possui bases corporativas em funcionamento, com possíveis redundâncias e mesmo discrepâncias de dados
- Não se exige nenhuma alteração nos processos de negócio que alimentam as bases corporativas já existentes
- A equipe de implantação deve ter acesso por programas às bases corporativas

Legado típico: dados sobre pessoas e vínculos



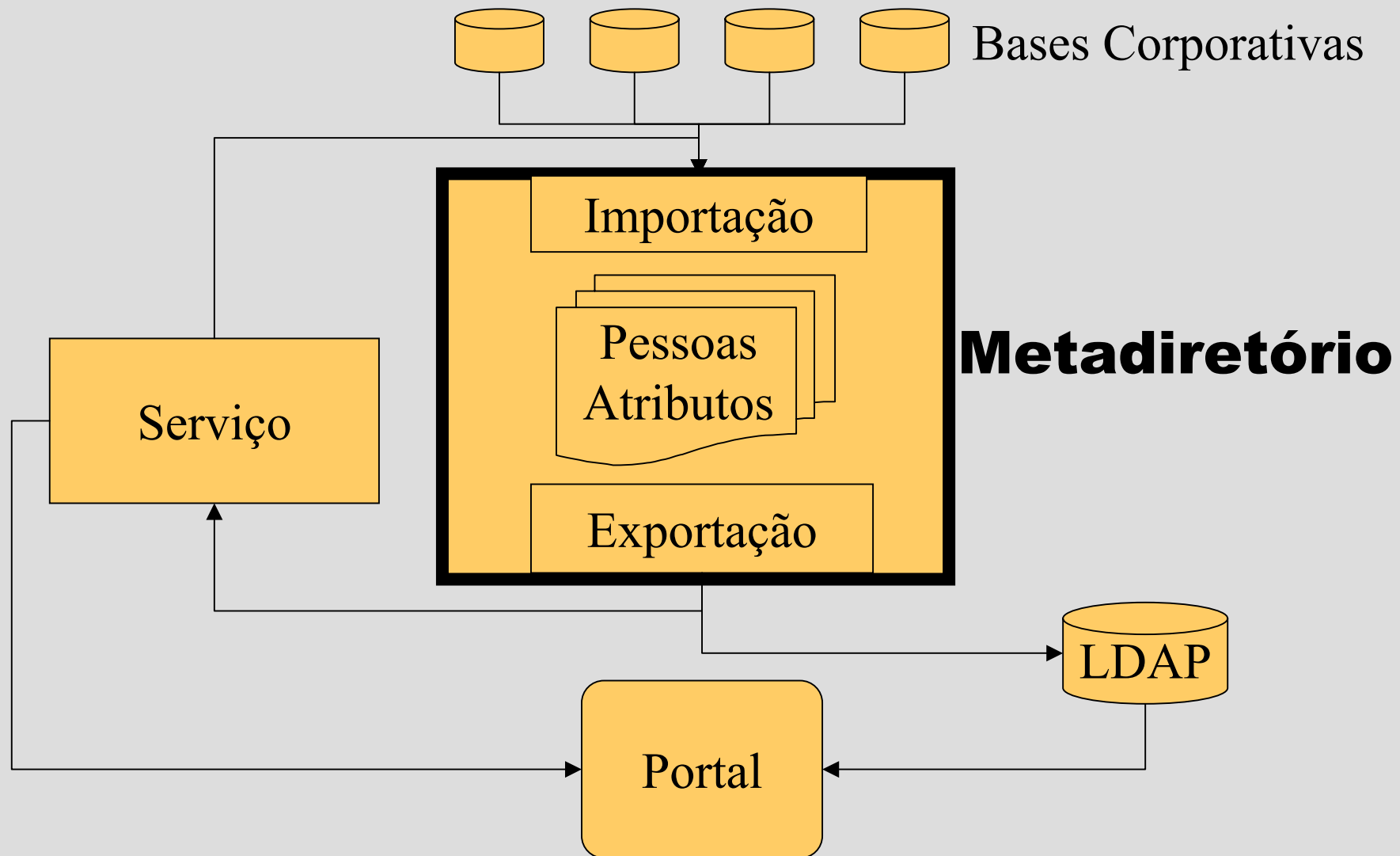
Construção de um Diretório



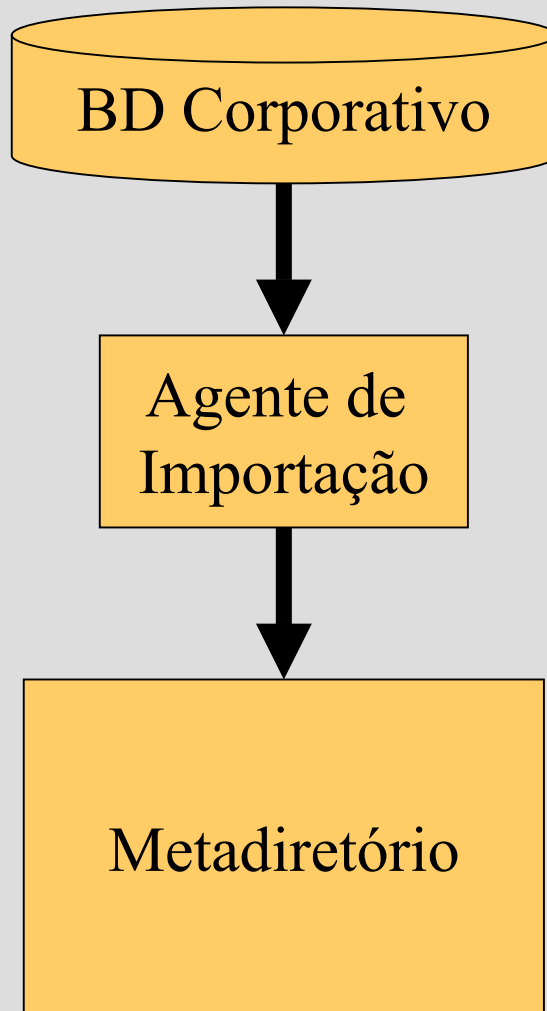
Construção de um Diretório

- Requisitos
 - Algumas competências técnicas
 - Fácil
 - Acesso a bases corporativas
 - Apoio institucional no mais alto nível
 - Integração com gerência de identidades institucional
 - Harmonização com processos de negócio básicos como o registro de calouros, a contratação de funcionários, etc.
 - Interação com *toda* a população!

Arquitetura de Referência



Agente de Importação

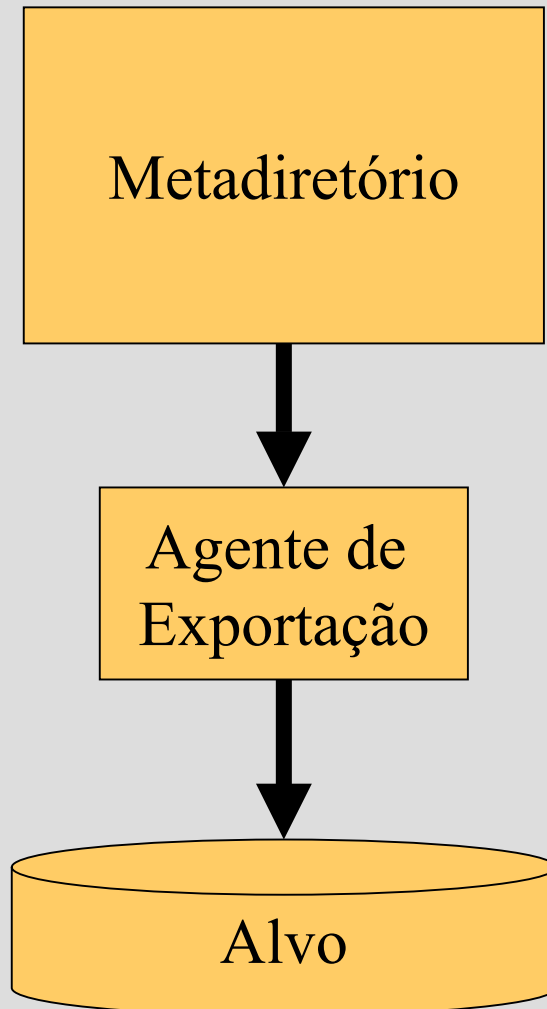


- Um agente de importação
 - Acessa as bases corporativas
 - Formata dados usando o esquema XML do metadiretório
 - Deposita objetos na caixa de entrada do metadiretório
- A instituição deve desenvolver um agente de importação para cada base corporativa que alimenta o metadiretório
- O metadiretório guarda a chave primária do objeto no BD corporativo

Importação: Atualização X Conciliação

- Para todo objeto depositado na caixa de entrada, o metadiretório verifica se algum objeto já foi absorvido com a mesma chave primária da fonte
- Se isto ocorrer, o objeto é tratado como uma Atualização de Atributos
- Senão, é executado um procedimento de Conciliação e Inserção

Agentes de Exportação

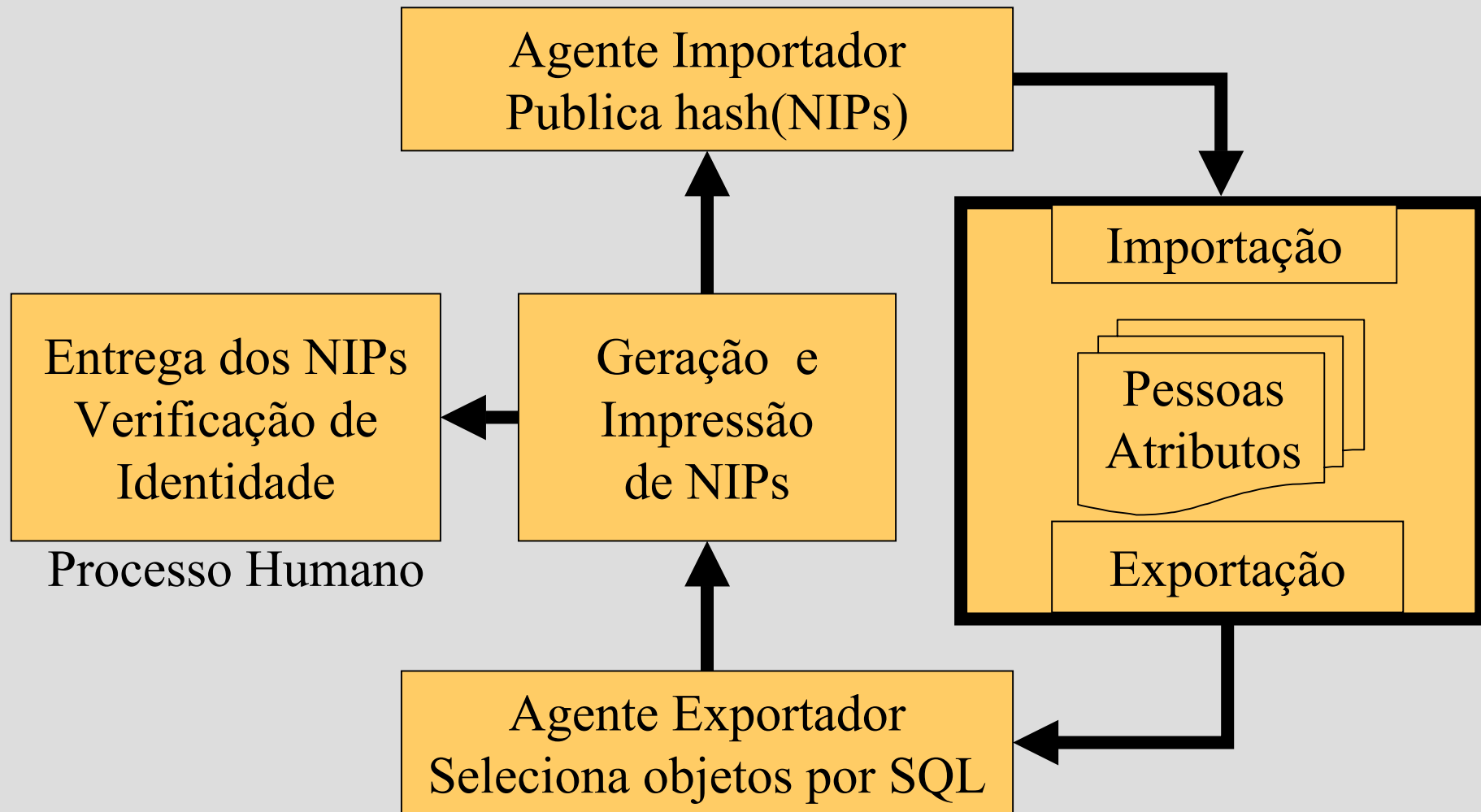


- Objetos do metadiretório são selecionados (SQL) por um agente de exportação
- O agente de exportação transforma o formato XML do metadiretório em um formato adequado para o alvo da exportação
- O alvo pode ser um LDAP, uma base legada, ou qq coisa

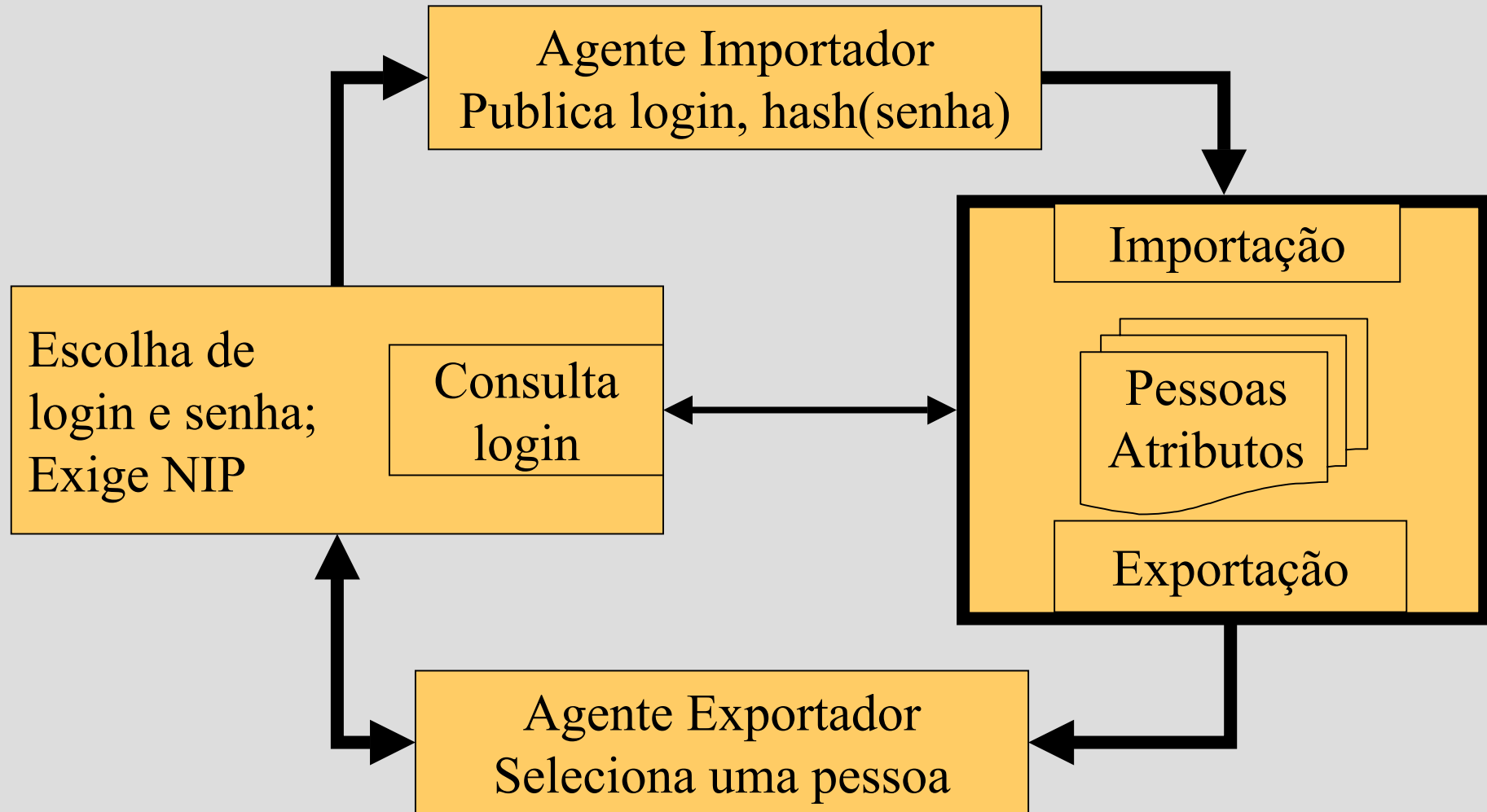
Exportação LDAP

- Importantíssima
- Serviços de autenticação e consulta padronizados, adotados pela indústria
- Mecanismos de replicação embutidos, proporcionando desempenho e disponibilidade

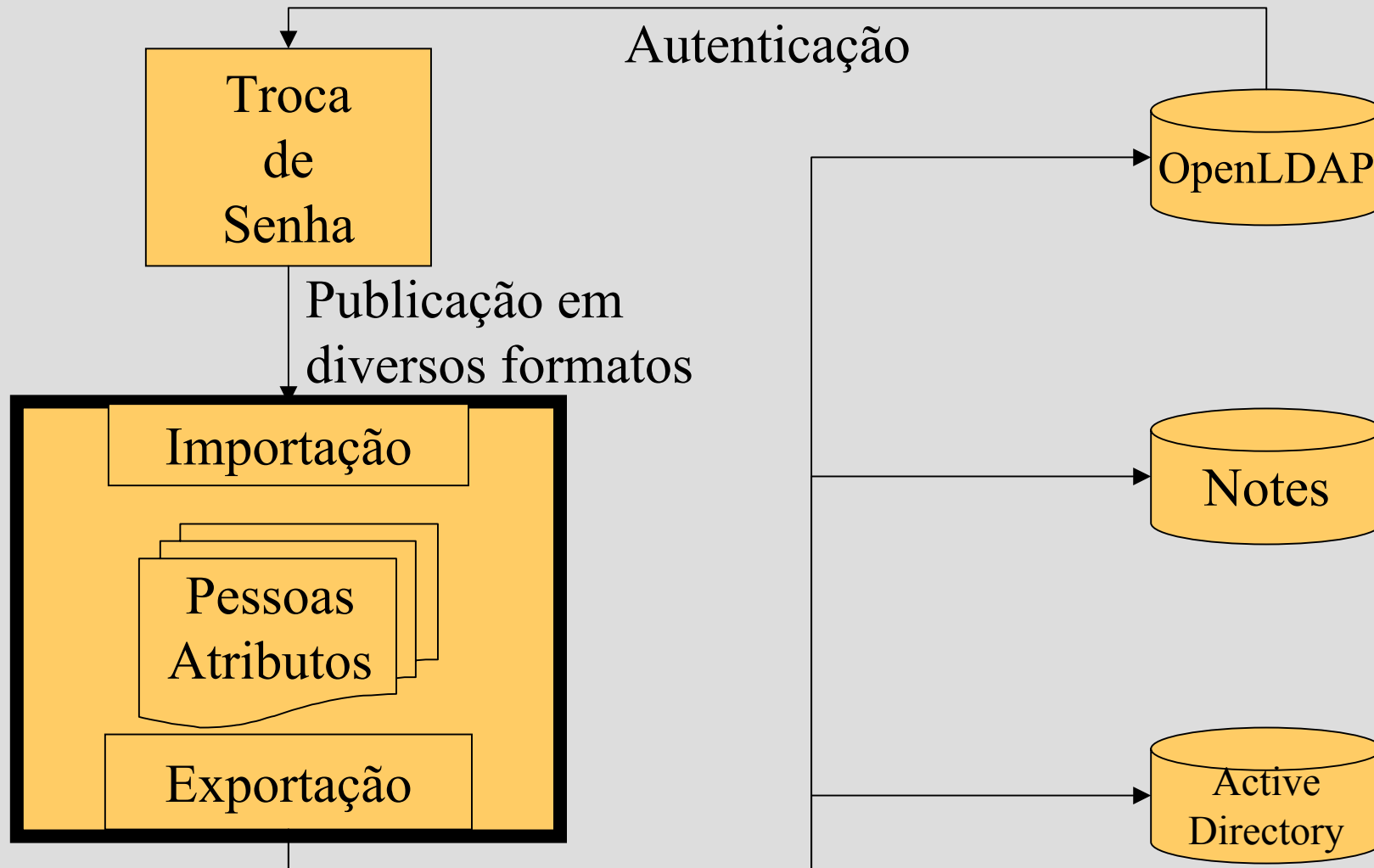
Identidade Digital: NIPs



Identidade Digital: login e senha



Sincronização de Senhas



Grupos

- Grupos são introduzidos por entradas em uma tabela (nomeDoGrupo, SQL)
- A expressão SQL versa sobre atributos já presentes no MD
- nomeDoGrupo transforma-se em um atributo para os objetos que satisfazem a expressão SQL
- Novos grupos podem utilizar em sua SQL atributos introduzidos por outros grupos já existentes

Perfis de um serviço

- Um serviço é normalmente oferecido em diversas modalidades para seus usuários
- Correio é um exemplo: domínio para endereço, tamanho máximo da caixa postal, servidor principal são parâmetros que tipicamente dependem dos vínculos do usuário com a instituição

Tabela de perfis

- Uma tabela de perfis tem
 - Um nome (perfisCorreio, p. ex.)
 - Os campos *nomeDoPerfil* e *grupo*
 - Uma definição dos atributos associados ao nome do perfil
- Uma pessoa pode atender a nenhum, a um ou mais perfis de uma tabela de perfis

Criação de contas PostFix

- Passo 1: criação da tabela de perfis contaPostFix
- Passo 2: registrar um serviço criaçãoDeContasPostFix associado a esta tabela
- Passo 3: instalação de uma aplicação de criação de contas, que
 - Usa o diretório LDAP como mecanismo de autenticação
 - Consulta o metadiretório (ou mesmo o LDAP) para obter os perfis permitidos para aquele usuário
 - Consulta o metadiretório para detetar possíveis conflitos com endereços escolhidos pelo usuário
 - Cria efetivamente a conta PostFix
 - Publica no metadiretório o(s) parâmetros de e-mail escolhidos

Portais Institucionais

- UNICAMP e UFMG vão adotar o uPortal
- Já temos um protótipo em demonstração

Padrão brEduPerson

- O padrão brEduPerson, inicialmente uma interseção das demandas por atributos da UNICAMP e da UFMG, é um subproduto do GT Mid

Conclusões

- Podemos ganhar muito com diretórios
- A construção de um diretório não é difícil
- O GT Middleware pode ajudar
- Próximos passos
 - Aferição de interesse e diagnóstico
 - Planejamento
 - Execução

Referências

- Tudo sobre diretórios pode ser encontrado no Enterprise Directory Implementation Roadmap da Internet2 e NMI
 - <http://www.nmi-edit.org/roadmap/directories.html>
- Educause Core Data Service

Obrigado

Questões?

osvaldo@lcc.ufmg.br buzato@ic.unicamp.br