Capítulo 1

Gerenciamento de Identidades Federadas[1]

Michelle S. Wangham[◇], Emerson Ribeiro de Mello[†], Davi da Silva Böger[⋆], Marlon Guerios[‡], Joni da Silva Fraga[⋆]

[⋆] Universidade Federal de Santa Catarina

[◇] Universidade do Vale do Itajaí

[†] Instituto Federal de Santa Catarina

[‡] Inohaus

email:wangham@univali.br, mello@ifsc.edu.br, dsboger@das.ufsc.br, marlonguerios@inohaus.com.br, fraga@das.ufsc.br

Abstract

Identity management is an integrated system of policies, business processes and technologies that enables organizations to provide resources safely, only to their users. This also involves issues related to definition, certification and life cycle management of digital identities. The federated identity model is an approach to optimize the exchange of identities information through federations that share trust relantionships. This chapter analyzes the challenges and proposed solutions to provide federated identity management to collaborative networks.

Resumo

O gerenciamento de identidades consiste de um sistema integrado de políticas, processos de negócios e tecnologias que permite às organizações proverem recursos de forma segura, somente aos seus usuários. Este também envolve aspectos relacionados com a definição, certificação e gerenciamento do ciclo de vida das identidades digitais. O modelo de identidades federadas é uma abordagem para otimizar a troca de informações relacionadas às identidades, através de relações de confiança construídas nas federações. Neste capítulo, são analisados os desafios e as soluções para prover gerenciamento de identidades federadas às redes colaborativas.

[1]Desenvolvido dentro do escopo do projeto "Serviços para Transposição de Credenciais de Autenticação Federadas", GT-STCFed da RNP.

1.1. Introdução

Segundo [Camarinha-Matos et al. 2008], um novo ambiente competitivo para as diversas organizações governamentais e privadas vem se desenvolvendo nos últimos anos e a tendência para negócios colaborativos está forçando uma mudança na forma na qual estas organizações são gerenciadas. Segundo os autores, a participação em redes colaborativas tem sido muito importante para as organizações que anseiam encontrar uma vantagem competitiva diferenciada. Uma rede colaborativa consiste de várias entidades autônomas, heterogêneas e geograficamente distribuídas, que colaboram para encontrar um objetivo comum e compatível e cujas interações são suportadas pelas redes de computadores [Camarinha-Matos et al. 2008]. Três tipos de redes colaborativas serão abordados neste capítulo: as redes colaborativas de organizações (*Collaborative Networks of Organizations* - CNO), as redes nacionais de pesquisa e educação (*National Research and Education Network* - NREN) e as redes colaborativas governamentais (*Collaborative Digital Government* ou *Collaborative E-Government*).

As redes colaborativas possuem uma série de requisitos de interoperabilidade e de segurança. A interoperabilidade é necessária para tratar vários aspectos de heterogeneidade entre os membros da rede, que incluem as diversas plataformas computacionais utilizadas, as várias políticas (administrativas, de segurança, de negócios) às quais esses membros estão sujeitos e as diferentes tecnologias de segurança adotadas. Um suporte a essa heterogeneidade é essencial para garantir que a rede possa atender o maior número possível de participantes. A segurança, por sua vez, é fundamental para que os membros de uma rede colaborativa possam depositar confiança nas interações com outros membros.

Os modelos usuais de autorização se apoiam em uma autoridade de autenticação para mediar a confiança entre partes desconhecidas (terceira parte confiável). Desta forma, as interações entre essas partes são alcançadas pela apresentação de credenciais emitidas por uma autoridade de autenticação confiável. Em ambientes complexos como as redes colaborativas, este modelo de simples intermediação se apresenta como limitado, já que cada domínio possui suas próprias políticas, infraestruturas de segurança e ainda uma forma particular de gerenciar as identidades dos principais [Jøsang e Pope 2005].

O *gerenciamento de identidades* consiste de um sistema integrado de políticas, processos de negócios e tecnologias que permite às organizações o tratamento e manipulação de identidades (atributos de identidade) de seus usuários [Jøsang e Pope 2005, Chadwick 2009]. O gerenciamento de identidades também envolve aspectos relacionados com a definição, certificação e gerenciamento do ciclo de vida das identidades digitais, infraestruturas para troca e validação dessas informações, juntamente com os aspectos legais [Jøsang e Pope 2005].

Nas redes colaborativas, o aumento de provedores de serviços e a crescente necessidade de compartilhar recursos para usuários de diferentes organizações que possuam algum tipo de afinidade são fatores que motivam a constituição de federações. Uma federação é uma forma de associação de parceiros de uma rede colaborativa que usa um conjunto comum de atributos, práticas e políticas para trocar informações e compartilhar serviços, possibilitando a cooperação e transações entre os membros da federação [Carmody et al. 2005]. O gerenciamento de identidades federadas, baseado nestes acordos comerciais, técnicos e políticos, permite que as organizações de uma federação inte-

rajam com base na gestão da identidade compartilhada [IBM 2005]. Como exemplo de soluções que proveem o gerenciamento de identidades federadas, tem-se o *Shibboleth*, os *frameworks* do *Liberty Alliance*, *OpenID* e o *Microsoft CardSpace*.

Uma das funções básicas oferecidas por essas soluções de federação de identidades é a autenticação única (*Single Sign-On* - SSO) [Maler e Reed 2008]. Esta autenticação traz facilidades para os usuários, pois permite que esses passem pelo processo de autenticação uma única vez e usufruam das credenciais obtidas por todos os serviços que desejarem acessar. Garantir tal conceito dentro de um único domínio administrativo e de segurança não é algo complexo, porém garantir o SSO em uma federação com diferentes tecnologias de segurança é algo desafiador [de Mello et al. 2009].

Um problema a ser tratado no gerenciamento de identidades é a privacidade das informações [Hansen et al. 2008]. Em um cenário ideal, os usuários devem exercer o direito de determinar como suas informações serão manipuladas, informando quais informações poderão ser compartilhadas com terceiros, como esse compartilhamento deve ser feito e também indicando o período de tempo o qual essas informações poderão ficar disponíveis nos sistemas.

O objetivo deste capítulo é analisar os desafios e as propostas de soluções para prover gerenciamento de identidades federadas às redes colaborativas, em especial, para as organizações virtuais, para as redes nacionais de pesquisa e educação e para redes colaborativas governamentais. Os conceitos, problemas e soluções propostas para o gerenciamento de identidades apresentados neste capítulo são complementados com a apresentação de cenários de uso em redes colaborativas que demonstram a aplicabilidade das soluções de gerenciamento de identidades apresentadas.

Este capítulo está dividido em sete seções. Nesta primeira seção, foi apresentado o contexto geral em que o trabalho está inserido, destacando os objetivos e a motivação para a escolha do tema. Na Seção 1.2, os conceitos básicos sobre gerenciamento de identidades são introduzidos e os modelos de gerenciamento de identidades presentes na literatura são descritos e comparados. Ainda nesta seção, os requisitos necessários que um sistema de gerenciamento de identidades deve atender, tais como, privacidade, anonimato, interoperabilidade das identidades e gerenciamento de confiança, são apresentados. A Seção 1.3 apresenta os benefícios e funcionalidades oferecidos pelo gerenciamento de identidades federadas e como este modelo tem sido empregado em diferentes redes colaborativas. A Seção 1.4 tem por objetivo apresentar as principais soluções de gerenciamento de identidades federadas e compará-las. Os problemas relacionados à privacidade das identidades federadas e as soluções existentes na literatura para tratar deste importante requisito de segurança são apresentados na Seção 1.5. Na Seção 1.6 são descritas as principais bibliotecas e ferramentas disponíveis para implantar o gerenciamento de identidades em redes colaborativas. Por fim, a Seção 1.7 traz uma síntese dos principais aspectos do gerenciamento de identidades analisados e as tendências de pesquisa nesta área.

1.2. Conceitos e Modelos de Gerenciamento de Identidades

A Internet propiciou uma maior agilidade nas interações entre provedores de serviços e seus usuários. Um provedor de serviços pode ser caracterizado como uma loja virtual, um sistema acadêmico para realizar matrículas, um portal do governo e os usuários destes

sistemas podem ser caracterizados como clientes, alunos e contribuintes. Mecanismos de autorização garantem que somente usuários autorizados poderão obter acesso aos recursos providos, o que imediatamente sugere a necessidade de uma forma para a identificação digital desses usuários e uma forma para gerenciar tais identidades.

A identidade de uma pessoa é composta por uma grande quantidade de informações pessoais que caracteriza essa pessoa em diferentes contextos dos quais essa faz parte [Clauß e Köhntopp 2001]. A identidade é composta pela combinação de subconjuntos, chamados de *identidades parciais*, cujo alguns identificam unicamente uma pessoa (p.ex. cpf) e outros não (p.ex. sexo). Dependendo do contexto e da situação uma pessoa pode ser representada por uma identidade parcial diferente. A identidade parcial de uma pessoa no contexto de uma universidade pode conter informações como seu nome, data de nascimento e as disciplinas que cursa. No contexto de uma empresa, a identidade pode estar associada com funções, privilégios, direitos e responsabilidades. Cabe salientar que uma mesma informação pessoal pode estar presente em diferentes identidades parciais.

Um **sistema de gerenciamento de identidades** provê ferramentas para o gerenciamento dessas identidades parciais em um mundo digital. Segundo [Chadwick 2009], o gerenciamento de identidades consiste em um conjunto de funções e habilidades, como administração, descoberta e troca de informações, usadas para garantir a identidade de uma entidade e as informações contidas nessa identidade, permitindo assim que relações comerciais possam ocorrer de forma segura. Enquanto no mundo real uma pessoa escolhe quais informações revelar de si a outras pessoas, levando em consideração o contexto e a sensibilidade da informação, no mundo digital essa tarefa é desempenhada pelo *sistema de gerenciamento de identidades*.

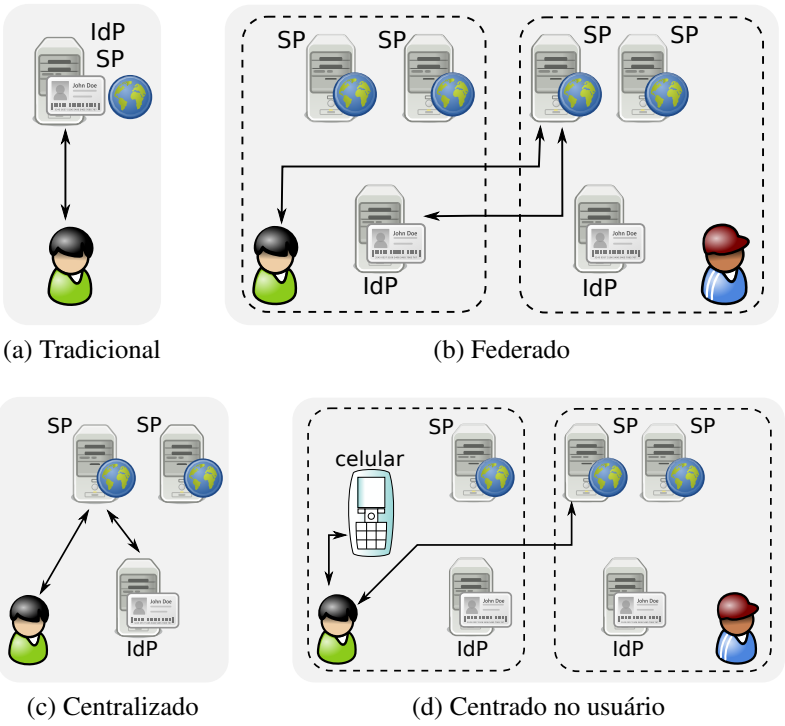
Assim, um *sistema de gerenciamento de identidades* consiste na integração de políticas e processos de negócios, resultando em um sistema de autenticação de usuários aliado a um sistema de gerenciamento de atributos. Em [Bhargav-Spantzel et al. 2007], o *sistema de gerenciamento de identidades* é caracterizado pelos seguintes elementos:

- **Usuário** – aquele que deseja acessar algum serviço;
- **Identidade** – conjunto de atributos de um usuário. Pode ser seu nome, endereço, filiação, data de nascimento, etc;
- **Provedor de Identidades (Identity Provider – IdP)** – responsável por emitir a identidade de um usuário. Após o usuário passar por um processo de autenticação, este recebe uma credencial, dita identidade, que é reconhecida como válida pelos provedores de serviço;
- **Provedor de Serviços (Service Provider – SP)** – oferece recursos a usuários autorizados, após verificar a autenticidade de sua identidade e após comprovar que a mesma carrega todos os atributos necessários para o acesso.

[Chadwick 2009] apresenta a definição de outros elementos presentes em um *sistema de gerenciamento de identidades*. O **identificador** consiste em um conjunto de caracteres e dígitos que são usados para identificar de forma única uma entidade em um

determinado domínio ou sistema. Uma **asserção de atributos** consiste em uma declaração, emitida por um terceiro confiável, indicando que uma determinada entidade possui os referidos atributos.

Em [Jøsang e Pope 2005, Jøsang et al. 2005, Bhargav-Spantzel et al. 2007], os *sistemas de gerenciamento de identidades* seguem modelos classificados como *tradicional*, *centralizado*, *federado* e *centrado no usuário*. Cada um desses modelos apresenta uma forma diferente de interação e disposição dos elementos citados acima. A Figura 1.1 ilustra cada modelo e estes serão descritos em detalhes a seguir.



(a) Tradicional (b) Federado

(c) Centralizado (d) Centrado no usuário

Figura 1.1: Classificação dos modelos de gerenciamento de identidade

O *modelo tradicional* é amplamente utilizado nos atuais sistemas computacionais presentes na Internet. Neste modelo, a identificação do usuário é tratada de forma isolada por cada provedor de serviços, o qual também atua como provedor de identidades (ver Figura 1.1a). Cabe ao usuário criar uma identidade digital para cada provedor de serviços que deseje interagir, não havendo assim o compartilhamento das identidades desses usuários entre diferentes provedores de serviço.

Apesar do *modelo tradicional* ser amplamente adotado, seu uso tende a ser custoso tanto para usuários quanto para provedores de serviços. Atualmente, é comum um usuário possuir múltiplas identidades para interagir com seu provedor de *e-mails*, sítio de notícias, livraria, etc. Cada provedor de serviços pode exigir um conjunto próprio de atributos para compor a identidade digital do usuário. Por outro lado, um conjunto comum de atributos pode ser exigido por diversos provedores de serviços, como nome da conta, senha, endereço, data de nascimento, etc [de Mello 2009].

Para os usuários, gerenciar inúmeras identidades é algo custoso. Primeiro por ter

que fornecer as mesmas informações diversas vezes. Segundo por ter que se preocupar em criar um nome de usuário e senha diferente para cada provedor de serviço, uma vez que usar a mesma senha por diversos provedores não é aconselhado. O custo gerado para os usuários também reflete de diversas formas nos provedores de serviço. A tarefa tediosa de sempre fornecer as mesmas informações no momento da criação de sua identidade, faz com que o usuário não seja tão fiel no preenchimento de atributos que não são cruciais para acessar o recurso oferecido pelo provedor.

O *modelo centralizado* surgiu como uma solução para a inflexibilidade do *modelo tradicional* e está fundamentado no compartilhamento das identidades dos usuários entre provedores de serviços e no conceito de autenticação única (*Single Sign-on* – SSO) [Bhargav-Spantzel et al. 2007]. O serviço *Microsoft Passport Network* foi um percursor deste modelo e visou evitar as inconsistências e redundâncias presentes no *modelo tradicional*, dando aos seus usuários a possibilidade de interagir com diversos provedores de serviços sem que necessitem realizar o processo de autenticação manual em cada um desses [Bhargav-Spantzel et al. 2007].

No *modelo centralizado*, só existe um único provedor de identidades o qual é responsável por autenticar os usuários, fornecer aos provedores de serviços informações sobre estes e todos os provedores de serviços devem confiar plenamente nas informações fornecidas pelo provedor de identidades (ver Figura 1.1c). O conceito de autenticação única (SSO) traz uma grande facilidade para os usuários, pois a estes só é necessário realizar o processo de autenticação uma única vez e usufruir das credenciais obtidas por todos os provedores de serviços que utilizar, até que estas credenciais expirem.

Segundo [Maliki e Seigneur 2007], o ponto fraco deste modelo é que o provedor de identidades possui controle absoluto sobre as informações de seus usuários, podendo assim usá-las da forma que bem entender, sendo este o principal motivo para o *Microsoft Passport Network* não ter tido sucesso.

Visando contornar as dificuldades apresentadas pelo modelo centralizado, o *modelo de identidade federada* está fundamentado sobre a distribuição da tarefa de autenticação dos usuários por múltiplos provedores de identidades, estando estes dispostos em diferentes domínios administrativos (ver Figura 1.1b). Um domínio administrativo pode representar uma empresa, uma universidade, etc e é composto por usuários, diversos provedores de serviços e um único provedor de identidades.

O gerenciamento de identidades federadas é uma abordagem para otimizar a troca de informações relacionadas a identidade através de relações de confiança construídas nas federações [Camenisch e Pfitzmann 2007]. Acordos estabelecidos entre provedores de identidades garantem que identidades emitidas em um domínio sejam reconhecidas por provedores de serviços de outros domínios e o conceito de autenticação única é garantido mesmo diante de diferentes domínios. Dessa forma, o *modelo de identidades federadas* consegue oferecer facilidades para os usuários, pois evita que estes tenham que lidar com diversas identidades e passar diversas vezes pelo processo de autenticação. Para os provedores de serviços, o benefício é que estes poderão lidar com um número menor de usuários temporários. O projeto *Liberty Alliance*, descrito na Seção 1.4.3, e o projeto *Shibboleth*, descrito na Seção 1.4.2, seguem o modelo de gerenciamento de identidades federadas (*Federated Identity Management* – FIM).

O aumento no número de provedores de serviços resultou em um número maior de identidades que o usuário deverá gerenciar. Modelos de gerenciamento como o centralizado e o federado trazem facilidades para esses usuários. A crítica sobre o modelo centralizado se faz principalmente sobre o provedor de identidades, que além de ser um ponto único de falhas possui total poder sobre os dados de seus usuários. [Jøsang e Pope 2005, Bhargav-Spantzel et al. 2007] consideram o gerenciamento de identidades federadas como um modelo centrado nos provedores de identidades. Apesar de haver a distribuição das identidades por diversos provedores, informações desses usuários, uma vez liberadas para esses provedores, podem ser disponibilizadas a terceiros.

O *modelo centrado no usuário* objetiva dar ao usuário o total controle sobre suas identidades digitais, contudo as principais propostas e implementações deste modelo fazem uso de um dos modelos apresentados anteriormente, sendo o modelo de identidade federado o mais usado. Na proposta de [Jøsang e Pope 2005] as identidades de um usuários, destinadas a diferentes provedores de serviços, são armazenadas em um dispositivo físico que fica em poder do usuário, como um *smartcard* ou mesmo um telefone celular (ver Figura 1.1d). O usuário se autentica neste dispositivo físico e cabe a este liberar as informações do usuário para cada provedor de serviços que o usuário acessar, respeitando totalmente as preferências de privacidade do usuário. As soluções OpenID (Seção 1.4.5), Microsoft CardSpace (Seção 1.4.6) e Higgins (Seção 1.4.7) seguem este modelo.

Duas abordagens de identificadores tem sido utilizadas para prover a infraestrutura necessárias para implantação do modelo centrado no usuário [Recordon e Reed 2006]:

- *Identidade Baseada no Endereço* – usa um único endereço digital para identificar o usuário, no contexto de uma relação particular. Este endereço digital é então referenciado para descobrir e invocar serviços de identidades associados. O OpenID segue esta abordagem;
- *Identidade Baseada no Cartão* – usa um *token* digital que contém ou faz referência a um conjunto de atributos que, individualmente ou coletivamente, identifica o usuário e fornece as informações necessárias para realizar uma transação baseada na identidade. Esta é a abordagem empregada por tecnologias que utilizam o protocolo WS-Trust, como *Cardspace* da Microsoft e o Projeto Higgins.

Os modelos apresentados basicamente diferem na forma como as identidades dos usuários são armazenadas e disponibilizadas, sendo que em alguns modelos o compartilhamento da identidade entre provedores de serviços, aliado ao conceito de autenticação única trazem facilidades para os usuários e são hoje essenciais, haja visto o grande número de serviços oferecidos através da Internet [Bhargav-Spantzel et al. 2007].

[Damiani et al. 2003] lista um conjunto de requisitos que um sistema de gerenciamento de identidades deve atender para garantir uma melhor experiência de uso para os usuários sem que isso afete a segurança de suas informações pessoais. Os requisitos listados por [Damiani et al. 2003] são:

- *Interoperabilidade* – As identidades dos usuários devem ser representadas em um formato comum de forma a permitir que a mesma possa ser compreendida e validada mesmo diante de múltiplos domínios administrativos e de segurança;

- *Mecanismo para revogação de identidades* – O sistema deverá prover uma forma para que seus usuários possam gerenciar as informações contidas em suas identidades bem como revogá-las;
- *Gerenciamento de confiança* – Relações de confiança entre provedores de serviços e provedores de identidades de diferentes domínios permitem que as identidades emitidas em um domínio sejam aceitas em outro. É necessário prover uma forma para indicar o nível de confiança associado a cada relação, o que irá influenciar no comportamento dos provedores de serviço;
- *Privacidade* – Usuários devem possuir meios para que possam expressar, e fazer valer, suas preferências de privacidade sobre as informações pessoais presentes em suas identidades;
- *Anonimato* – Aos usuários deve ser garantido o direito de permanecerem anônimos de forma que as informações fornecidas com sua identidade digital não possam ser usadas para descobrir dados de suas outras identidades. O uso de pseudônimos é uma forma para garantir o anonimato.

Segundo [Chadwick 2009], após a falta de sucesso do sistema de gerenciamento de identidades *Microsoft Passport*, Kim Cameron [Cameron 2005] elaborou uma lista com sete leis que ele julga necessárias para que um sistema de identidades obtenha sucesso, são estas:

1. **Consenso e controle do usuário** – Um sistema de identidade só deve revelar informações de um usuário após seus consentimento. A confiança do usuário em seu sistema de identidade é crucial para que o usuário continue a usá-lo;
2. **Revelação mínima para um uso restrito** – Deve-se obter a menor quantidade possível de informações relacionadas às identidades dos usuários. Todo sistema computacional possui falhas e está susceptível a ataques, o que poderia assim revelar informações confidenciais dos usuários a uma parte maliciosa. Dessa forma, deve-se manter a menor quantidade de informação possível e apagá-la assim que essa não for mais necessária [Chadwick 2009];
3. **Justificação das partes** – Sistemas de gerenciamento de identidades devem ser projetados para revelar informações sobre as identidades somente para partes que justifiquem tal necessidade. Somente as partes envolvidas diretamente na transação com o usuário deverão conhecer suas identidades;
4. **Identidades direcionadas** – Deve-se prover suporte a identificadores omnidirecionais, usados por entidades públicas e identificadores unidirecionais, usado por entidades privadas. Dessa forma, um usuário poderia escolher quais identificadores usar de acordo com cada provedor de serviços que for interagir, garantindo seu anonimato, mesmo que provedores de serviços entrem em conluio;
5. **Pluralismo de operadores e tecnologias** – Um sistema de identidades deve operar mesmo diante de diferentes tecnologias presentes em múltiplos provedores de

identidades. É necessário que exista um meta identificador aliado a um protocolo comum para o transporte das identidades;

6. **Integração com o usuário** – O usuário deve ser tratado como uma parte integrante do sistema de identidades para assim se proteger contra ataques de roubo de identidade. A interação humana com os sistemas é o elo mais fraco e a segurança nessa comunicação é algo essencial. Os usuários devem estar familiarizados com sistema de forma a identificar facilmente um ataque tão logo este ocorra;

7. **Experiência consistente através de contextos** – A unificação dos meta sistemas de identificação devem garantir aos usuários uma experiência de uso simples e consistente, mesmo atravessando contextos com diferentes operadores e tecnologias.

1.2.1. Níveis de garantia

Como visto na seção anterior, os sistemas de *gerenciamento de identidades federadas* apresentam facilidades para usuários e para provedores de serviços. Apesar das relações de confiança garantirem que as asserções de segurança emitidas pelos provedores de identidades serão consideradas válidas pelos provedores de serviços, essas não indicam a robustez do processo de autenticação pelo qual o usuário passou junto ao provedor de identidades.

O Instituto Nacional Americano de Padrões e Tecnologias (*National Institute of Standards and Technology* – NIST) lançou um guia sobre o processo de autenticação eletrônico [Burr et al. 2006] no qual foram definidos 4 níveis de garantia, do inglês *Level of Assurance* (LoA), sendo o nível 1 considerado o mais fraco e o nível 4 o mais robusto, indicando os requisitos técnicos para cada nível. Por exemplo, um processo de autenticação que faz uso de nomes de usuário e senha é considerado menos robusto que um processo que faça uso de certificados digitais com chaves públicas.

Provedores de serviços poderiam fazer uso desses níveis de garantia para oferecer diferentes níveis de permissão de acesso [Chadwick 2009]. No caso, usuários que se autenticarem com um nível 1, poderiam somente ter acesso de leitura a um recurso e usuários com um nível 4 poderiam ler e escrever. O SAML (ver Seção 1.4.1), usado na maioria das soluções de gerenciamento de identidades federadas, permite associar um nível de garantia em suas asserções de autenticação, provendo assim uma forma padronizada para troca dessa informação entre provedores de identidades e de serviços.

O documento do NIST também faz relação ao processo de registro dos usuários. Por exemplo, em um sistema que permite os próprios usuários efetuarem seu cadastro através de uma página *web* tem um nível 1, uma vez que não é possível garantir a real identidade deste usuário. Um processo de registro que exige a presença física da pessoa e esta deve fornecer documentos como RG, CPF e declaração de matrícula na instituição de ensino, terá um nível de garantia maior. A federação acadêmica CAFe [RNP 2010] (ver Seção 1.3.1), apresenta em seus procedimentos para ingresso de provedores de identidades, referências aos níveis de garantia, porém ainda não está muito claro como os provedores de serviços irão usufruir dessa informação.

1.3. Uso de Identidades Federadas

De acordo com [Camenisch e Pfitzmann 2007], em muitas áreas da sociedade, inúmeras transações (volumosas e de significativa importância) são realizadas digitalmente pela Internet. Trata-se de transações comerciais entre empresas (B2B), entre empresas e consumidores (B2C), bem como transações com a administração pública direta (G2B e G2C) e interações entre indivíduos (C2C). Na maioria das transações, os principais desafios são: como os parceiros reconhecem uns aos outros (autenticação)? E como estes obtêm as informações, sobre os parceiros de negócios, necessárias para realizar a transação desejada (troca de atributos)?

A colaboração entre diferentes parceiros em uma rede colaborativa passa pela ativação de uma série de funcionalidades dessas organizações. Como limites administrativos precisam ser transpostos, os processos de negócios estarão sob **diversos modelos administrativos** e podem também estar sob diversos mecanismos e tecnologias de segurança. Domínios administrativos distintos podem formar relações de confiança entre si, constituindo federações, permitindo que a autenticação em um possa ser transposta para os domínios associados (autenticação *Single Sign On* - SSO) [Camenisch e Pfitzmann 2007].

Dentre as formas de Redes Colaborativas (RCs), destacam-se as redes colaborativas de organizações (*Collaborative Networks of Organizations* - CNO), que são sistemas constituídos por componentes autônomos, geograficamente distribuídos, que colaboram através da rede para alcançar um objetivo comum [Camarinha-Matos et al. 2008], as redes nacionais de pesquisa e educação (*National Research and Education Network* - NRENs), provedores de serviço de Internet especializados que oferecem serviços de comunicação avançada para comunidade científica e canais dedicados para projetos de pesquisa [TERENA 2008] e as redes colaborativas governamentais (*Collaborative Digital Government* ou *Collaborative E-Government*), constituídas para apoiar as aplicações de Governo Eletrônico e para prover suporte ao trabalho colaborativo entre Instituições Governamentais [Dawes e Pardo 2008]. As seções a seguir descrevem como o gerenciamento de identidades federadas tem sido empregado nestas redes colaborativas.

1.3.1. Redes Nacionais de Pesquisa e Educação

Segundo a associação TERENA (*Trans-European Research and Education Networking Association*)[2] (2008), é crescente, não só na Europa, o número de países interessados em desenvolver e aprimorar suas redes nacionais (NRENs). No Brasil, tem-se a Rede Nacional de Ensino e Pesquisa (RNP), que oferece uma infraestrutura de rede Internet (rede Ipê), que conecta as principais universidades e institutos de pesquisa do país, cerca de 600 instituições, beneficiando-se de um canal de comunicação rápido e com suporte a serviços e aplicações avançadas.

Além do serviço de conectividade de rede com uso de tecnologias avançadas, as NREN oferecem uma diversidade de serviços para os parceiros que participam destas redes colaborativas, entre estes destacam-se: ferramentas avançadas para comunicação instantânea interativa, tais como videoconferência e Telefonia IP; centro de atendimentos a incidentes de segurança; serviços de vídeo digital; ferramentas de planejamento e ope-

[2] `http://www.terena.org`

ração de redes que monitoram o funcionamento de todos os enlaces da NREN; serviços de sincronização de relógios, *Grid Services* e serviços de comércio eletrônico. O portfólio de serviços oferecidos pelas NREN tem crescido a cada ano [TERENA 2008].

Nas atuais redes nacionais de pesquisa, a crescente necessidade de compartilhar recursos para usuários de diferentes instituições que possuam algum tipo de afinidade motivaram a constituição de **federações acadêmicas**. No contexto das NRENs, o *framework Shibboleth* (ver Seção 1.4.2) é a Infraestrutura de Autenticação e Autorização (*Authentication and Authorization Infrastructure* - AAI) mais empregada para constituição de federações acadêmicas. As federações *Incommon*, da rede norte-americana *Internet 2*, e a *CAFe*, da Rede Nacional de Pesquisa (RNP) do Brasil, são exemplos de federações construídas tendo como base este *framework*. Estas federações agrupam pessoas do meio acadêmico como alunos, técnicos administrativos e professores. Tal comunidade é o principal público alvo de muitas empresas, o que torna interessante a essas empresas o ingresso nas federações acadêmicas também como provedores de serviços.

Em operação piloto desde 2008, a Federação CAFe - Comunidade Acadêmica Federada[3] - reúne instituições de ensino e pesquisa brasileiras em uma rede de confiança, na qual cada instituição é responsável por autenticar e prover informações de seus usuários para provedores de serviços autorizados. A rede de confiança constituída pela federação permite a um usuário autenticado em sua instituição de origem acessar, através de um único login, serviços oferecidos via *web* tanto por sua própria instituição como pelos demais membros da federação.

Na CAFe, instituições de ensino e pesquisa podem integrar-se à Federação como provedores de identidades, provedores de serviços ou como ambos. Instituições de ensino podem, por exemplo, prover serviços de ensino a distância e de colaboração a qualquer usuário da federação. A federação está aberta a participação de empresas, podendo essas atuarem somente como provedores de serviços. Editoras, órgãos de fomento e empresas com esquemas de desconto para estudantes ou professores são exemplos de empresas que podem ter interesse no ingresso na federação CAFe [RNP 2010].

De acordo com [RNP 2010], a participação de uma instituição como um provedor de identidade na Federação CAFe envolve, dentre outros, os seguintes benefícios: (1) uso de um único sistema de controle de acesso para serviços internos e externos à instituição; (2) uma única conta (*login*) por usuário para acesso aos serviços e (3) a garantia de privacidade, pois só serão passadas a cada provedor de serviços as informações necessárias ao controle de acesso a esse serviço (configuradas individualmente por cada provedor de identidade). Já para os provedores de serviços, o principal benefício é a simplificação do procedimento de controle de acesso, pois a autenticação e disponibilização de informações sobre os usuários é realizada pelos provedores de identidades, eliminando a necessidade de manutenção dessas informações no provedor de serviços e a autorização para acesso a um recurso por um usuário pode ser realizada através de um mecanismo de controle de acesso baseado em atributos (*Attribute Based Access Control* - ABAC), como por exemplo, o nome da instituição de origem, tipo de vínculo, ou outro atributo disponibilizado pelo provedor de identidades.

[3] `http://www.cafe.rnp.br`

Na literatura, constata-se um forte interesse na formação de federação de federações, chamada de confederação, para prover um gerenciamento de identidades federadas ainda mais globalizado. Um bom exemplo é o *framework* eduGAIN [Lopez et al. 2006], desenvolvido dentro do projeto Europeu GÉANT, que tem a finalidade de ligar redes nacionais de educação e de pesquisa de países dentro da comunidade Europeia. Esta interligação de diferentes federações de identidades pode ser vista como uma confederação de provedores de identidades. No uso destes serviços, membros de instituições associadas a diferentes federações podem trocar informações de forma segura, como se fizessem parte de um mesmo provedor de identidade nacional. Por exemplo, um pesquisador visitante em um dos países da comunidade Europeia, com esta infraestrutura, poder acessar facilmente recursos em sua instituição de origem. Esta interconexão possibilita, portanto, que usuários acadêmicos europeus tenham a visão de que as múltiplas redes nacionais colaborativas formam uma única federação. O eduGAIN tem por finalidade a interoperabilidade entre as soluções existente de Infraestruturas de Autenticação e Autorização (AAI) usadas nas construções das federações de identidades.

1.3.2. Organizações Virtuais

Dentre a grande variedade de redes colaborativas de organizações, a cooperação na forma de organizações virtuais (OVs) é a estratégia que mais se destaca. Esta vem sendo adotada por empresas, profissionais liberais e laboratórios espalhados ao redor do mundo, os quais objetivam atender novas oportunidades de negócios (ONs), bem como ampliar sua participação em novos mercados ou alcançar excelência científica [Kürümlüoglu et al. 2005].

Uma OV corresponde a uma união temporária de organizações independentes que se agregam visando compartilhar recursos e funcionalidades para alcançar objetivos que estas não alcançariam sozinhas. A cooperação destas organizações é garantida pela automação e informatização de grande parte de suas infraestruturas, deixando-as acessíveis via Internet. Nas OVs, as alianças são voláteis e o fluxo de colaboração, algumas vezes, é gerado e conhecido dinamicamente, de acordo com o processo de negócio requerido. Diante deste cenário, as infraestruturas para negócios colaborativos necessitam ser mais flexíveis, transparentes e adaptativas, de acordo com as condições do ambiente de negócio e o nível de autonomia das organizações [Rabelo 2008]. O gerenciamento de identidades federadas facilitam uma abordagem integrada para negócios colaborativos [IBM 2005].

Apesar dos benefícios atraentes do gerenciamento de identidades federadas (ver Seção 1.2), este impõem novos riscos contra a privacidade e segurança devido as valiosas informações compartilhadas entre diferentes domínios administrativos utilizando protocolos de rede fracamente acoplados [Maler e Reed 2008]. Um requisito básico para este tipo de cooperação é a relação de confiança entre as organizações. A infraestrutura de confiança que deve ser construída fornece a representação e implementação técnica das relações de negócio e acordos jurídicos entre os parceiros de negócios [IBM 2005].

Como as OVs são sistemas abertos, os melhores padrões para propósito de autenticação devem ser de tecnologia neutra. Tecnologia neutra significa que regras e processos acomodam diferentes tecnologias desde que estas produzam os mesmos resultados. No setor privado, as principais iniciativas incluem *Liberty Alliance framework*, OpenID, Higgins, Cardspace e *Shibboleth* [Lewis 2008].

1.3.3. Redes Colaborativas Governamentais (E-GOV)

Esta seção descreve o uso de identidades federadas em um sistema específico das redes colaborativas governamentais, chamado de Governo Eletrônico (*e-Government - E-Gov*). Os programas de Governo Eletrônico[4] bem sucedidos dependem do uso adequado das tecnologias de informação e comunicação (TICs) empregadas nas organizações para promover os trabalhos colaborativos em prol de objetivos comuns [Dawes e Pardo 2008]. Nas redes governamentais, as colaborações podem ser de quatro formas: entre organizações públicas (G2G), entre organizações públicas e o terceiro setor, entre organizações públicas e privadas (G2B) e entre o governo e o cidadão (G2C).

Muitos países estão expandido os seus programas de e-Gov aprimorando as suas infraestruturas de colaboração, sendo que o grande desafio está em garantir a interoperabilidade entre estas infraestruturas devido a heterogeneidade dos procedimentos e dados existentes entre a administração pública central e as locais [Baldoni 2010]. Esta diversidade pode tornar difícil a implementação destes programas. O *gerenciamento de identidades federadas* é então um mecanismo necessário para implementar políticas interoperáveis em nível nacional [Gottschalk e Solli-Saether 2008].

A necessidade de autenticação digital está exigindo que os governos melhorem seus processos de emissão de certidões de nascimento, números de serviço social ou carteira de motorista. Os governos estão tendo que decidir como os processos de identificação existentes serão utilizados para a identidade digital e se deverão definir novas leis ou outras medidas para melhorar a emissão de documentos de identidade [Lewis 2008].

Nos programas de e-Gov, o gerenciamento de identidades pode levar a prestação de serviços *online* eficientes [Baldoni 2010]. Como consequência, nos últimos anos, vários governos têm aprovado diretrizes para melhorar os serviços de e-Gov e as medidas de identificação para acesso a informação individual do cidadão e de registros do governo disponíveis em sítios *web*.

A Nova Zelândia, em 2008, lançou um *framework* de interoperabilidade *e-Government Interoperability Framework* - **e-GIF** que define um conjunto de políticas, normas e orientações que abrangem as formas de assegurar a interoperabilidade dos dados do setor público, entre as tecnologias de informação e comunicação (TIC) e entre os processos de negócios eletrônicos. Este *framework* permite que qualquer agência possa juntar suas informações, TICs ou processos com as de outras agências tendo como base um padrão internacional aberto. O problema do gerenciamento de identidades é parte do e-GIF o qual possui sua própria versão da especificação SAML (NZ SAML). A primeira versão do *framework* foi centrada na autenticação e as versões subsequentes terão como foco atributos de identidade e autorização. Quando desejável, a federação de identidades pode incorporar a autenticação única através do serviço *Government Logon Service* (GLS) e utilizar o provedor de identidades e pseudônimos. A identificação é executada através de um *Identities Verification Service* (IVS) que monta uma asserção de identidade para os provedores de serviços da agência do governo e para o usuário de maneira controlada.

[4]O desenvolvimento de programas de Governo Eletrônico tem como princípio a utilização das modernas tecnologias de informação e comunicação (TICs) para democratizar o acesso à informação, ampliar discussões e dinamizar a prestação de serviços públicos com foco na eficiência e efetividade das funções governamentais.

Em 2005, o Reino Unido desenvolveu um sistema de gerenciamento de identidade e um *e-GIF*. O *e-GIF* define as políticas e especificações técnicas que regem os fluxos de informação entre o governo e o setor público. Este *framework* cobre interconectividade, integração de dados e gerenciamento de conteúdo e acesso a *e-services*. O sistema de gerenciamento de identidades oferece serviços através do sítio *web Government Gateway* ou através do *UK Central Government Portal Direct.gov*. Um cidadão, para utilizar qualquer serviço do *Gateway*, precisa primeiro se registrar. Isso geralmente requer que o cidadão forneça o nome completo, endereço de *e-mail* e escolha uma senha. Cada membro irá fornecer fatos conhecidos até mesmo para os serviços individuais que estão sendo inscritos, como por exemplo para o Número de Seguridade Nacional. Ao inscrever-se, este será obrigado a fornecer esses fatos conhecidos para cada serviço, a fim de verificá-los com os dados existentes. Este sistema é baseado em dados existentes nas bases de dados do governo. Cada cidadão registrado receberá em casa um PIN. O *framework* de registro e autenticação fornece diferentes níveis de autenticação, dependendo de cada serviço específico. Existem quatro níveis de autenticação, iniciando em "nenhuma autenticação necessária" e indo até "autenticação biométrica e certificado digitais requeridos".

Na Dinamarca, desde 1986, os cidadãos tem sido registrados digitalmente. O governo tem o objetivo de que até 2012 todas as comunicações escritas relevantes entre as empresas, os cidadãos e o setor público devam ser eletrônicas. Em 2006, o Parlamento decidiu que o uso de padrão aberto deve ser obrigatório em soluções para o setor público. No mesmo ano, foi estabelecido que um portal do cidadão deveria ser criado em substituição aos portais municipais. Um dos pontos principais desta mudança é que os indivíduos, que costumavam ter registros em várias agências e usar várias identidades digitais (ver Seção 1.2), passam a ter acesso a diversos serviços a partir do portal do cidadão, fazendo uso de uma única identidade digital. Para permitir este cenário, aumentou-se a necessidade de uma melhor integração entre os diferentes serviços, o que significa até mesmo uma melhor integração entre os setores público e privado.

Na Itália, em 2001, a reforma da constituição Italiana atribuiu novas possibilidades para ação das autoridades regionais, este processo de descentralização impactou também a infraestrutura de e-gov, devido a interoperabilidade necessária entre as infraestruturas regionais que passaram a ser criadas. Em 2003, foi criado o *National Centre for IT in Public Administration* para promover a integração e cooperação das aplicações em nível nacional. Diversos documentos foram elaborados oferecendo as diretrizes necessárias para prover a interoperabilidade e definindo o *Sistema Pubblico di Connetività - SPC*.

O modelo de cooperação italiana segue uma arquitetura orientada a serviços e o modelo de gerenciamento de identidades federadas é usado para autorização e controle de acesso dos serviços disponíveis no SPC. A federação é necessária para utilizar o sistema de gerenciamento de identidades já existente nas autoridades regionais. A integração é feita através da especificação SAML v2.0.

Visando atender ao requisito de interoperabilidade, o programa de e-Gov do Brasil [GOV.BR 2010] definiu a arquitetura e-PING (Padrões de Interoperabilidade de Governo Eletrônico). Com esta arquitetura busca-se um conjunto mínimo de premissas, políticas e especificações técnicas que regulamentem a utilização da Tecnologia de Informação e Comunicação (TIC) no governo federal, estabelecendo as condições de interação com os

demais Poderes e esferas de governo e com a sociedade em geral. O e-PING ainda está sendo definido e até o momento nenhuma premissa, política ou especificação técnica para o gerenciamento de identidades foi definida.

1.4. Soluções de Gerenciamento de Identidades Federadas

Como as principais soluções de gerenciamento de identidades federadas, são baseadas na especificação SAML, esta seção inicia com a descrição desta especificação. Em seguida, as soluções mais empregadas nas redes colaborativas são descritas e analisadas.

1.4.1. Especificações SAML

A OASIS, um órgão padronizador, lançou um conjunto de especificações para definir uma infraestrutura para troca dinâmica de informações de segurança entre parceiros de negócio. A Linguagem de Marcação para Asserções de Segurança (*Security Assertion Markup Language* – SAML) [OASIS 2005g] tem como núcleo uma gramática XML para representar informações de segurança na forma de asserções, bem como protocolos para requisição e envio dessas asserções [OASIS 2005a].

Nas versões iniciais (1.0 e 1.1), a SAML tinha o objetivo de facilitar a troca de informações de identidade e autorização de usuários para permitir autenticação única (*Single Sign-On* - SSO) na *web*. A versão atual (2.0), por outro lado, estende essa infraestrutura com conceitos e mecanismos derivados de projetos como *Liberty Alliance* (ver Seção 1.4.3) e *Shibboleth* (ver Seção 1.4.2) que têm objetivos mais amplos, como a formação de federações para compartilhamento de informações de segurança e gerenciamento de identidades federadas. A SAML é hoje um padrão de fato e é utilizada, em parte ou por completo, em muitos outros projetos de gerenciamento de identidades, em especial todos os que serão abordados nas seções posteriores deste texto (*Shibboleth*, *Liberty Alliance*, *WS-Federation*, *OpenID* e *CardSpace*).

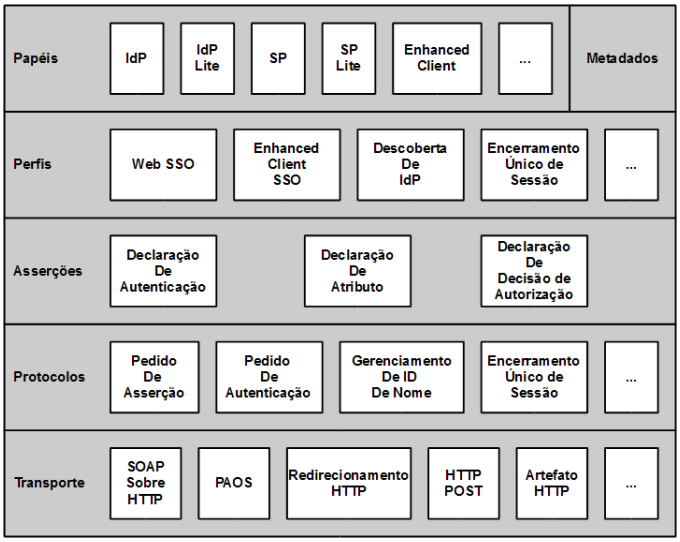


Figura 1.2: Arquitetura da SAML [Maler e Reed 2008]

As especificações SAML definem cinco componentes: papéis, perfis, asserções, protocolos e transporte, ilustrados pela Figura 1.2. No componente *papéis*, além dos

papéis que cada entidade pode desempenhar na infraestrutura SAML, são apresentados também os metadados que descrevem essas entidades. Os *perfis* agregam protocolos e asserções em fluxos de dados específicos para prover funcionalidades como gerenciamento de identidades e autenticação única. As *asserções* são essenciais para o gerenciamento de identidades e de contextos de segurança. Os *protocolos* são usados para requerer e transferir asserções entre as entidades. Esses protocolos podem ser mapeados em diferentes mecanismos de *transporte*. As próximas subseções apresentam estes componentes.

Asserções

As asserções SAML [OASIS 2005a], definidas por uma gramática XML, especificam o formato para representar informações de segurança acerca de um sujeito, que pode ser uma pessoa, organização, computador, etc. Essas informações são atestadas por uma entidade denominada de parte declarante (*asserting party*) ou autoridade SAML (*SAML authority*). A Figura 1.3 apresenta um exemplo de asserção SAML. Essa asserção contém as seguintes informações:

```
1  <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
2      Version="2.0" IssueInstant="2005-01-31T12:00:00Z">
3    <saml:Issuer
4       Format="urn:oasis:names:SAML:2.0:nameid-format:entity">
5      http://idp.example.org
6    </saml:Issuer>
7    <saml:Subject>
8      <saml:NameID
9         Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress">
10       j.doe@example.com
11     </saml:NameID>
12   </saml:Subject>
13   <saml:Conditions NotBefore="2005-01-31T12:00:00Z"
14      NotOnOrAfter="2005-01-31T12:10:00Z" />
15   <saml:AuthnStatement AuthnInstant="2005-01-31T12:00:00Z"
16      SessionIndex="67775277772">
17     <saml:AuthnContext>
18       <saml:AuthnContextClassRef>
19         urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
20       </saml:AuthnContextClassRef>
21     </saml:AuthnContext>
22   </saml:AuthnStatement>
23 </saml:Assertion>
```

Figura 1.3: Exemplo de asserção SAML

- O elemento raiz `saml:Assertion` (linhas 1 e 2) contém a declaração do espaço de nomes da SAML, a versão da SAML usada (atributo `Version`) e o momento em que a asserção foi emitida pela autoridade SAML (atributo `IssueInstant`);
- O elemento `saml:Issuer` (linhas 3 a 6) indica qual autoridade SAML emitiu a asserção, no caso `http://idp.example.org`;
- O elemento `saml:Subject` (linhas 7 a 12) indica o sujeito da asserção, no caso o detentor do e-mail `j.doe@example.com`;

- O elemento `saml:Conditions` (linhas 13 e 14) indica o prazo de validade da asserção, no caso entre 12:00h e 12:10h do dia 31 de janeiro de 2005;
- O elemento `saml:AuthnStatement` (linhas 15 a 22) representa uma declaração de autenticação. Essa declaração indica que o usuário em questão efetuou sua autenticação às 12:00h do dia 31 de janeiro de 2005 (atributo `AuthnInstant`) e que para tal foi usado um mecanismo de transporte protegido por senha (p.e. uma senha enviada sobre um canal SSL) (elemento `AuthnContext`, linhas 17 a 21).

No exemplo acima, a declaração de autenticação indica que o usuário fez uso de nome de usuário e senha como forma de autenticação. No entanto a SAML permite expressar informações de autenticação de diversos outros mecanismos, como certificados X.509 [Housley et al. 2002], *Kerberos* [Kohl e Neuman 1993] e *XML Signature* [Bartel et al. 2002]. Além disso, outros mecanismos podem ser definidos em extensões da especificação.

Apesar do exemplo anterior conter apenas uma declaração de autenticação, asserções podem conter diversas declarações da mesma autoridade sobre o mesmo sujeito. Os tipos de declaração definidos são os seguintes:

- Declaração de autenticação (*Authentication statement*) – criada pela entidade que realizou com sucesso a autenticação do usuário; a declaração indica quando a autenticação foi feita e qual o mecanismo utilizado (usuário/senha, assinatura digital, etc.);
- Declaração de atributo (*Attribute statement*) – contém atributos associados ao sujeito, como nome, filiação, certificado digital, etc. A SAML permite a utilização de gramáticas de atributos quaisquer, no entanto, provê perfis [OASIS 2005f] para a utilização de esquemas importantes como UUID [Leach et al. 2005], X.500/LDAP [ITU-T 2001, Hodges e Morgan 2002] e XACML [OASIS 2005c];
- Declaração de decisão de autorização (*Authorization decision statement*) – indica ações que o sujeito possui o direito de executar sobre determinados recursos.

Protocolos

Além da gramática de asserções, a especificação [OASIS 2005a] define protocolos gerais de pedido e resposta relacionados com troca de asserções SAML, gerenciamento de contextos de segurança (sessões de autenticação) e gerenciamento de identificadores de usuários. Os protocolos SAML são definidos em duas camadas, sendo a camada superior formada pelos esquemas XML das mensagens e a camada inferior composta de especificações de como usar protocolos subjacentes (SOAP, HTTP, etc.) para transportar essas mensagens [OASIS 2005b]. Essa separação garante ao mesmo tempo a interoperabilidade das aplicações e a possibilidade de utilizar os protocolos SAML em diversos cenários distintos nos quais as aplicações possuem restrições específicas (p.e. um navegador *web* provê suporte a protocolos de transporte diferentes de um cliente SOAP). Os seguintes protocolos são definidos pelas especificações [OASIS 2005a, OASIS 2005b]:

- Protocolos da camada superior (esquemas XML)
  - *Protocolo para pedido de autenticação* – define como um sujeito poderá requerer uma nova asserção de autenticação e, opcionalmente, asserções de atributo;
  - *Protocolo de consulta e pedido de asserção* – define consultas para a obtenção de asserções SAML, previamente existentes ou novas, por meio da especificação de um sujeito, dos tipos de asserções desejadas e de parâmetros de busca e filtragem;
  - *Protocolo para encerramento de sessão* – define um mecanismo para permitir que a sessão associada a um sujeito seja terminada (e os recursos associados a esta sejam liberados) simultaneamente em todas as aplicações do sistema;
  - *Protocolo de resolução de artefatos* – provê mecanismos para passagem de mensagens SAML por referência, usando um identificador de tamanho fixo denominado artefato. De posse do artefato, é possível invocar o emissor da mensagem para obter o conteúdo da mensagem;
  - *Protocolo de gerenciamento de identificador de nome* – usado para indicar que o valor ou formato do identificador de nome de algum sujeito será alterado ou que um identificador de nome não será mais usado para se referir ao sujeito;
  - *Protocolo de mapeamento de identificador de nome* – usado para relacionar identificadores diferentes associados a um mesmo sujeito por aplicações diferentes.
- Protocolos da camada inferior (mapeamentos para protocolos de transporte)
  - *SAML sobre SOAP* – define como mensagens dos protocolos SAML são transportadas em envelopes SOAP sobre HTTP;
  - *Redirecionamento HTTP* – define como mensagens dos protocolos SAML são transportadas em mensagens HTTP de redirecionamento;
  - *HTTP POST* – define como mensagens dos protocolos SAML são transportadas codificadas em *base-64* dentro de formulários HTML;
  - *Artefato HTTP* – define como um artefato é transportado usando HTTP, seja em formulário, seja codificado no texto da URL;
  - *SAML URI* – define como recuperar uma asserção SAML a partir de um identificador URI.

Metadados

Nos perfis de uso da especificação SAML, cenários podem conter diversas entidades com papéis distintos. As diferentes entidades devem entrar em acordo quanto a diversos parâmetros como os identificadores das entidades (URI), os protocolos de transportes suportados, os certificados e chaves criptográficas, entre outros. Para garantir que essas informações sejam descritas e obtidas de maneira padronizada, na especificação [OASIS 2005e]

é definido um formato em XML para expressar os metadados das entidades, bem como os perfis para a troca dinâmica dessas informações entre as entidades do sistema.

Os papéis definidos na SAML para as entidades do sistema são [OASIS 2005e]: provedor de identidade (*identity provider* - IdP), uma autoridade SAML responsável por autenticar sujeitos e atestar seus atributos de identidade; provedor de serviço (*service provider* - SP), uma aplicação que consome asserções SAML emitidas por um IdP e, com base nas informações contidas nestas, controla o acesso do sujeito aos recursos; autoridade de autenticação (*authentication authority*), uma autoridade SAML que implementa o protocolo de consulta de asserções contendo declarações de autenticação; ponto de decisão de política (*policy decision point* - PDP), uma autoridade SAML que implementa o protocolo de consulta de asserções contendo declarações de autorização; autoridade de atributos (*attribute authority* - AA), uma autoridade SAML que implementa o protocolo de consulta de asserções contendo declarações de atributos.

Perfil *Web SSO*

Uma das aplicações mais comuns do gerenciamento de identidades federadas é a autenticação única (*Single Sign-On* - SSO) [Maler e Reed 2008], que permite a um sujeito realizar o processo de autenticação uma única vez, junto ao seu provedor de identidades e usufruir das credenciais obtidas para acessar diferentes provedores de serviços. A SAML define o perfil *Web SSO* para prover a funcionalidade SSO na *web*.

No cenário da *Web SSO*, as aplicações envolvidas podem assumir o papel de provedor de identidades (IdP) ou provedor de serviços (SP). Assume-se que o sujeito usa um navegador *web* comum para se comunicar tanto com o SP quanto com o IdP. O perfil define, basicamente, quais ações um SP deve tomar para iniciar um contexto de segurança (sessão) com um sujeito com base em informações de segurança emitidas pelo IdP. Para isso, o perfil faz uso do protocolo de pedido de autenticação juntamente com um dos seguintes mapeamentos: redirecionamento HTTP, HTTP POST e artefato HTTP.

O funcionamento básico do perfil *Web SSO* está ilustrado na Figura 1.4 [OASIS 2005f]. No passo 1, o sujeito, por meio do navegador, tenta acessar um recurso de um SP que não possui um contexto de segurança com esse sujeito. No passo 2, o SP determina qual IdP usar para pedir informações de segurança sobre o sujeito. Essa etapa é dependente da implementação, mas pode fazer uso de documentos de metadados ou do perfil de descoberta de provedores de identidade [OASIS 2005f]. No passo 3, o SP gera uma mensagem `AuthnRequest` (do protocolo de pedido de autenticação) e passa para o navegador, para que este apresente ao IdP. Nessa etapa, qualquer um dos mapeamentos permitidos para o perfil *Web SSO* pode ser usado. No passo 4, o navegador entra em contato com o IdP para que este autentique o sujeito usando a requisição emitida pelo SP. Nessa etapa, o IdP deve usar mecanismos para autenticar o sujeito e gerar as asserções SAML para enviar ao SP. É possível, nessa etapa, que o IdP já possua um contexto de segurança para o sujeito, não sendo necessário que este passe pelo processo de autenticação. No passo 5, o IdP envia a mensagem `Response`, de acordo com o protocolo de pedido de autenticação, para o SP, por intermédio do navegador, usando um dos mapeamentos permitidos. No passo 6, com base nas informações contidas na resposta

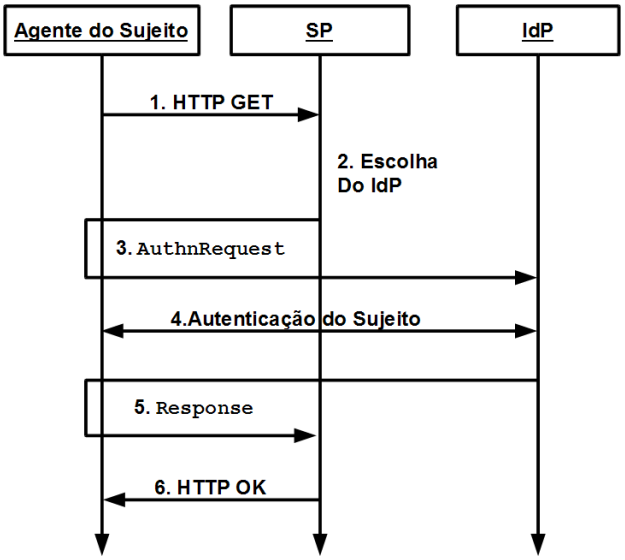


Figura 1.4: Exemplo de funcionamento do perfil *Web SSO*

do IdP entregue pelo sujeito, o SP decide se inicia um contexto de segurança e permite o acesso ao recurso.

Em uma continuação do cenário descrito acima, se o sujeito for acessar um outro SP para o qual também não haja um contexto de segurança, os mesmos passos serão executados, no entanto no passo 4 o IdP poderá responder ao SP sem precisar pedir dados ao sujeito, utilizando o contexto de segurança criado quando o sujeito tentou acessar o primeiro SP.

Uma variação prevista pelo perfil *Web SSO* é a possibilidade de o IdP enviar uma resposta, como no passo 5 do cenário descrito acima, sem a solicitação do SP, para um posterior acesso do sujeito. No cenário anterior, diz-se que ocorreu a autenticação única iniciada pelo SP. Nessa outra variação, ocorreu a autenticação única iniciada pelo IdP.

O perfil *Enhanced Client or Proxy* (ECP) é um perfil para autenticação SSO similar ao *Web SSO*, mas nesse caso o mecanismo de transporte de mensagens usado é o PAOS, ou "SOAP invertido", que permite participação mais ativa do agente do sujeito [OASIS 2005f].

Encerramento Único de Sessão

Quando um sujeito se autentica em um IdP, este último pode estabelecer uma sessão com o sujeito (p.e. por meio de um *cookie*). Além disso, quando o sujeito acessa um SP, este consome asserções emitidas pelo IdP e pode também estabelecer uma sessão com o sujeito. Em um dado momento, o sujeito pode decidir finalizar sua sessão com um SP específico ou pode finalizar todas as sessões de uma só vez. Para o segundo caso, a SAML define o perfil de encerramento único de sessão (*Single log-out* - SLO), baseado no protocolo de SLO [OASIS 2005f].

A Figura 1.5 [OASIS 2005f] ilustra o funcionamento do perfil SLO. Em um dado

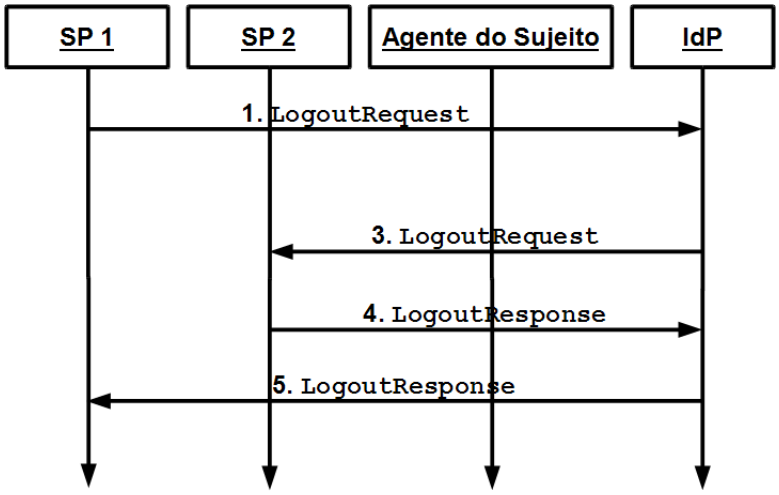


Figura 1.5: Exemplo de funcionamento do perfil SLO

momento, o sujeito indica para o SP que deseja encerrar todas as sessões. O SP em questão enviará uma mensagem `LogoutRequest` (definida no protocolo SLO) para o IdP responsável pela autenticação do sujeito, diretamente ou através do agente do sujeito (p.ex. redirecionamento HTTP no navegador) (etapa 1 da figura). O IdP, então, identifica todos os participantes da sessão do sujeito (etapa 2), que podem ser outros SPs e até outros IdPs que, por sua vez, coordenam sessões de outros SPs. Depois, o IdP envia uma mensagem `LogoutRequest` para esses participantes (etapa 3). Os participantes encerram a sessão localmente e devolvem ao IdP mensagens `LogoutResponse` (etapa 4). O IdP, por sua vez, retorna uma mensagem `LogoutResponse` para o SP que iniciou a desconexão usando o mesmo mecanismo da requisição (diretamente ou via agente do sujeito).

Perfis de atributos

A SAML [OASIS 2005f] define um perfil básico de atributos, que descreve o uso de tipos *XML Schema* como valores de atributos, e perfis que descrevem mapeamentos de formatos e conjuntos de atributos de outras especificações para o formato de atributos do SAML.

Os perfis para mapeamento de atributos permitem o uso de bases de atributos já implantadas para gerar declarações SAML de atributos sem a necessidade de definir os atributos manualmente [OASIS 2005f]. Os mapeamentos incluem transformações de atributos de bases X.500/LDAP [ITU-T 2001, Hodges e Morgan 2002], UUIDs [Leach et al. 2005] e atributos XACML [OASIS 2005c].

SAML e Gerenciamento de Identidades Federadas

A SAML provê suporte a diversas formas de estabelecimento e gerenciamento de identidades federadas [OASIS 2005g]. De maneira geral, a SAML permite que quaisquer mecanismos externos sejam usados para relacionar as diversas identidades de um sujeito.

Por exemplo, duas aplicações podem usar uma sincronização de base de dados para conectar usuários que possuam o mesmo nome de login, ou o mesmo `e-mail`. Esta é a única opção que as versões 1.0 e 1.1 da SAML oferecem suporte.

A SAML 2.0, por outro lado, provê suporte ao uso de pseudônimos, que são identificadores dinâmicos e não relacionados à atributos de identidade do sujeito. Por trás do uso dos pseudônimos estão dois protocolos SAML: o protocolo de gerenciamento de identificador de nome e o protocolo de mapeamento de identificador de nome, bem como os protocolos de transporte e perfis associados. Os pseudônimos servem como identificadores compartilhados entre SP e IdP e podem ser usados de duas formas: persistente e transiente [OASIS 2005g].

O *pseudônimo persistente* é criado uma única vez no IdP e associado permanentemente à identidade do sujeito. Ao receber uma asserção de autenticação contendo o pseudônimo, o SP cria um registro local para o sujeito usando o pseudônimo e outras informações de identidade do sujeito. Em acessos posteriores do mesmo sujeito, o SP receberá o pseudônimo que foi registrado e poderá decidir a autorização com base em dados locais juntamente com informações vindas do IdP e até mesmo poderá requisitar atributos associados ao pseudônimo em uma autoridade de atributos ligada ao IdP. Esse esquema, aliado a políticas de privacidade no acesso a atributos do sujeito, pode garantir a proteção da identidade, no entanto o acesso a diferentes SPs podem ser rastreados, caso esses SP atuem em conluio [OASIS 2005g].

O *pseudônimo transiente* é criado pelo IdP e associado à identidade do sujeito pelo tempo que durar o contexto de segurança. Dessa forma, o SP ainda pode decidir o acesso do sujeito com base em atributos emitidos pelo IdP, mas não pode mais manter informações sobre o sujeito que persistam por mais de uma sessão. Além disso, SPs diferentes não podem correlacionar acessos do mesmo sujeito, garantindo um certo nível de anonimato [OASIS 2005g].

1.4.2. Shibboleth

O projeto *Shibboleth* [Scavo e Cantor 2005] foi uma iniciativa do consórcio americano Internet2 que teve como principal objetivo lançar uma implementação de código aberto, baseada em padrões abertos, para tratar desafios relacionados ao gerenciamento de identidades e controle de acesso em instituições acadêmicas. Em 2003, foi liberada a versão 1.0 e, atualmente, o projeto *Shibboleth* está em sua segunda versão, liberada em 2008. O atual desenvolvimento do *Shibboleth* visa que este seja uma solução genérica para o gerenciamento de identidades federadas, podendo ser adotada por qualquer tipo de organização.

O pacote de *software* desenvolvido está fundamentado sobre padrões abertos como o XML e *Security Assertion Markup Language* (SAML) (ver Seção 1.4.1) e provê uma forma fácil para que aplicações *web* usufruam das facilidades providas pelo modelo de identidades federadas, como o conceito de autenticação única (*Single Sign-On* – SSO) e a troca segura de atributos dos usuários por todos provedores de serviços que compõem a federação. O *Shibboleth* tem como ênfase a privacidade dos atributos dos usuários, sendo que a liberação desses atributos para os provedores de serviços está condicionada a política de privacidade da instituição de origem do usuário e também as preferências

pessoais deste usuário.

Dentro de um domínio *Shibboleth*, existem dois papéis: provedor de identidades (*Identity Provider* – IdP) e provedor de serviços (*Service Provider* – SP). O primeiro é responsável por autenticar seus usuários, antes que estes possam usufruir dos serviços oferecidos pelo segundo. O ponto comum entre estes papéis é que ambos devem implementar toda a pilha de *software* fornecida pelo projeto *Shibboleth*, permitindo assim o transporte das credenciais dos usuários do provedor de identidades até o provedor de serviços [Scavo e Cantor 2005]. No *Shibboleth*, o processo de autenticação sempre é executado na instituição de origem do usuário, através de seu provedor de identidades, fazendo uso dos mecanismos de autenticação presentes nessa instituição. A autenticação de usuários pode ser feita através de nome de usuário e senha, Kerberos, X.509, etc [Chadwick 2009].

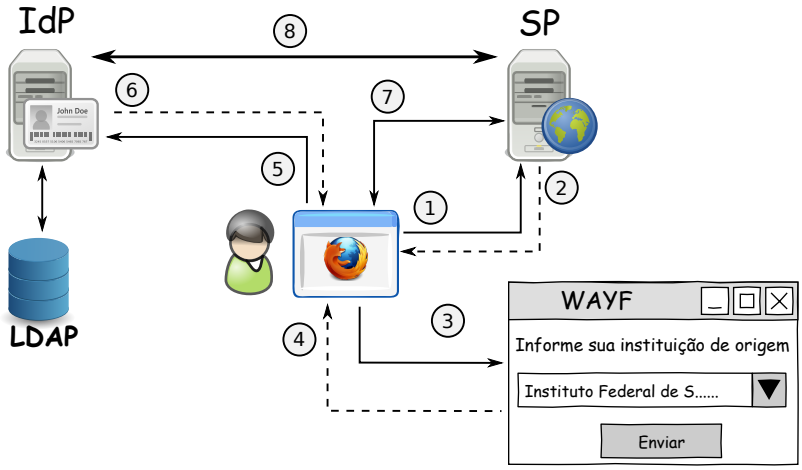


Figura 1.6: Interação de um usuário com um provedor de serviço *Shibboleth*

A Figura 1.6 ilustra os passos para que um usuário, ainda não autenticado, consiga acessar um recurso disponibilizado por um provedor de serviços *Shibboleth*. O usuário, através de seu navegador, aponta para a `URL` da aplicação *web* desejada (passo 1). Este pedido é interceptado pela pilha *Shibboleth*, que verifica que o mesmo não está autenticado e assim deve encaminhá-lo ao provedor de identidades do respectivo usuário para que passe pelo processo de autenticação.

O provedor de serviços desconhece o provedor de identidades do usuário e assim este usuário é encaminhado ao serviço *Where Are You From* (WAYF), através de um redirecionamento HTTP, que permite ao usuário selecionar sua instituição de origem (passo 2). No WAYF são listados somente os provedores de identidades tidos como confiáveis pelos provedores de serviços da federação *Shibboleth*. Após o usuário selecionar sua instituição de origem, este é encaminhado, novamente através de redirecionamentos HTTP, ao provedor de identidade (IdP) de sua instituição (passo 4).

Neste ponto, o usuário realiza o processo de autenticação (passo 5) de acordo com o mecanismo de autenticação presente em sua instituição, podendo tal processo ser realizado através de nome de usuário e senha, estes armazenados em uma base LDAP. Uma vez que o processo de autenticação tenha sido realizado com sucesso, o IdP cria um iden-

tificador aleatório para este usuário o qual persistirá no IdP durante toda a sessão deste usuário. Por fim, o usuário é redirecionado ao recurso *web* desejado (passo 6) e, juntamente com a requisição HTTP ao provedor de serviços (SP), é enviado seu identificador aleatório através de asserções SAML de autenticação.

Cabe ao SP aplicar o controle de acesso, considerando os atributos do usuário que foram fornecidos com essa tentativa de acesso (passo 7). O provedor de serviços pode requisitar outros atributos do usuário junto ao provedor de identidades do usuário para usar no mecanismo de controle de acesso (passo 8), como por exemplo número do registro acadêmico, endereço de *e-mail*, etc. Os provedores de identidades respeitam um conjunto de políticas para revelação de atributos de seus usuários, preservando assim a privacidade dos mesmos. O *Shibboleth* define uma forma padronizada para troca de atributos, através de asserções SAML, porém não especifica como deverão ser tais atributos, deixando tal função livre para os desenvolvedores.

Em um ambiente federado, a padronização destes atributos é fundamental, para que provedores de serviços saibam quais atributos poderão requisitar e para que provedores de identidades saibam quais atributos deverão fornecer. Em [Internet2 2008, Wahl 1997, Smith 2000], foi proposto o `eduPerson`, um conjunto padrão de atributos de identidade comuns para federações acadêmicas, sendo que 6 atributos são altamente recomendados, 10 são sugeridos e 25 são opcionais. A comunidade federada CAFe[5] que reúne instituições acadêmicas brasileiras, além de implementar esse conjunto de atributos, definiu ainda seu próprio conjunto de atributos (chamado `brEduPerson`).

Relações de confiança entre provedores de identidades e de serviços garantem que os provedores de serviços terão certeza que um usuário foi autenticado corretamente junto ao provedor de identidades em questão e que este último fornecerá corretamente os atributos relacionados a este usuário. As asserções emitidas pelo provedor de identidades são assinadas por este, o que permite que o provedor de serviços verifique a autenticidade das mesmas [Chadwick 2009].

Para provedores de serviços cujo público alvo não se restringe exclusivamente à comunidade acadêmica, a implementação da pilha *Shibboleth* pode ser um impeditivo, analisando custos *vs* benefícios. É importante ressaltar ainda que, mesmo partindo do pressuposto de que as relações de confiança já estejam previamente estabelecidas entres os diversos domínios administrativos que representam uma federação, ainda assim, há diversos desafios para transpor as credenciais de autenticação em uma federação, pois provedores de serviços possuem autonomia para decidir quais políticas e tecnologias de segurança utilizar, ou seja, uma federação precisa prover uma infraestrutura que suporte a autenticação SSO mesmo diante de parceiros que usem credenciais de segurança diferentes daquelas usadas no *Shibboleth*.

1.4.3. Projeto Liberty Alliance

O projeto *Liberty Alliance* surgiu como um consórcio formado por empresas de diferentes áreas como telecomunicações, bancos, universidades, etc. com o intuito de criar um conjunto de especificações abertas voltadas para o gerenciamento de identidades federadas

[5] `http://www.cafe.rnp.br`

e sua integração com Serviços *Web* [Liberty 2003]. Atualmente mais de 160 organizações privadas, sem fins lucrativos e governamentais fazem parte do projeto *Liberty Alliance* e um dos principais pontos positivos do projeto é sua influência em padrões como o SAML, cujas extensões propostas pela *Liberty Alliance* são hoje parte do SAML 2.0 [Baldoni 2010]. Os principais objetivos do projeto são [Liberty 2003]:

- Permitir aos usuários garantir a privacidade e a segurança de suas informações pessoais;
- Prover um padrão aberto para permitir uma única autenticação (SSO), o que inclui a autenticação descentralizada e a autorização em múltiplos provedores de serviços;
- Prover especificações compatíveis com uma grande variedade de dispositivos;
- Utilizar em suas especificações, padrões e protocolos existentes e amplamente aceitos;
- Prover meios para que as empresas respeitem os requisitos de segurança e a privacidade dos clientes.

O arcabouço proposto para o gerenciamento de identidades é composto por três componentes principais: *Identity Federation Framework* (ID-FF), *Identity Web Services Framework* (ID-WSF) e *Identity Services Interface Specifications* (ID-SIS).

O ID-FF visa permitir o gerenciamento de identidades federadas através de diversos domínios administrativos, caracterizando o *círculo de confiança*. Um *círculo de confiança* é formado entre organizações através de relações de confiança e acordos comerciais. Dentro de um *círculo de confiança* cada organização pode assumir papéis como provedores de identidades (IdP), como provedores de serviços (SP) ou como ambos [Kallela 2008]. Assim como no *Shibboleth* (ver Seção 1.4.2), o IdP gerencia e autentica os usuários e o SP aceita as informações sobre a identidade de usuários oriundas do IdP de seu *círculo de confiança*.

O ID-FF é formado por três componentes: **redirecionamento HTTP**, que permite que as informações dos usuários, que façam uso de navegadores *web*, sejam trocadas entre o IdP e os SP; **Serviço *Web***, que permite a comunicação entre as entidades do sistema através de trocas de mensagens SOAP; e **metadados e esquemas XML**, os quais indicam como as diversas informações sobre o usuário serão trocadas entre IdPs e SPs [Kallela 2008]. No ID-FF também são descritos mecanismos para ligação entre diferentes contas ou identidades, visando garantir a privacidade e anonimato dos usuários; autenticação única (SSO); e mecanismos para o gerenciamento de sessões de forma simplificada.

O ID-WSF apresenta modelos para a criação de serviços que rodem sobre o arcabouço da *Liberty Alliance*, além de especificar um serviço para a localização de provedores de identidades e mecanismos de segurança. As principais características do ID-WSF são:

- **Permissão baseada no compartilhamento de atributos** – Permite que empresas ofereçam serviços personalizados para os clientes, de acordo com os atributos e preferências que estes clientes escolheram compartilhar;
- **Descoberta do Serviço de Identidades** – Para obter maiores informações sobre a identidade de um cliente, os provedores de serviços podem utilizar do Serviço de Descoberta para encontrar um Serviço de Identidades específico de um cliente;
- **Serviço de Interação** – Um Serviço de Identidades, antes de fornecer as informações de um usuário a um serviço, deve obter a permissão deste usuário. São definidas especificações e protocolos que permitem a interação entre os Serviços de Identidades e os serviços que estão solicitando as informações;
- **Perfis de segurança** – Define perfis e requisitos de segurança para a descoberta e o uso dos Serviços de Identidade;
- **Modelos de Serviços de Identidades** – Provê modelos para a implementação de Serviços de Identidade sobre a ID-WSF.

O componente ID-SIS, que estende o ID-FF e o ID-WSF, provê um conjunto versátil de ferramentas para a construção de serviços interoperáveis sobre o ID-WSF. Tais especificações foram definidas para permitir que organizações possam facilmente, criar ou estender serviços sobre a estrutura do ID-WSF. Uma das especificações propostas foi a *ID-Personal Profile*, que define um serviço para obter informações pessoais de um usuário como nome, endereço, telefone, etc. Tal especificação permite que todas organizações, que estejam de acordo com a *Liberty Alliance*, possuam um conjunto de campos e valores conhecidos, tendo assim um dicionário e uma linguagem padrão para que possam interagir entre si.

Os *identificadores opacos* ou *pseudônimos* foram propostos nas especificações da *Liberty* com o intuito de garantir a privacidade dos usuários dos serviços. Para cada provedor de serviços, o provedor de identidades poderá atribuir diferentes pseudônimos relacionados a um mesmo usuário. Dessa forma, o mesmo usuário será representado por diferentes pseudônimos para cada serviço que for acessar, garantindo assim a proteção contra o rastreamento de suas transações. Identificadores opacos permitem aos provedores de serviços identificar quem são seus clientes, relacionando em suas contas locais, porém não possibilita que os provedores de serviços obtenham informações pessoais dos clientes de forma que possa comprometer a privacidade do mesmo.

1.4.4. Especificações WS-Trust e WS-Federation

A especificação *WS-Security* [OASIS 2004] define mecanismos para garantir a integridade e a confidencialidade de mensagens SOAP, bem como o uso de vários tipos de credenciais de segurança que visam declarar informações de segurança (*claims*). A especificação *WS-Trust* [OASIS 2009b] estende a *WS-Security* com a definição de um protocolo para a troca e disseminação de credenciais de segurança entre diferentes domínios, bem como meios para se verificar se uma credencial é ou não confiável. Dessa forma, as partes envolvidas podem detectar e estender relações de confiança baseadas na emissão e validação de credenciais.

A base do modelo de confiança *WS-Trust* é o serviço de *tokens* de segurança (*security token service* - STS) [OASIS 2009b]. O STS é um Serviço *Web* que implementa uma interface WSDL padrão, que define operações para emissão, renovação, validação e revogação de credenciais. Se duas aplicações de diferentes domínios desejam se comunicar e não possuem uma relação de confiança direta (i.e., as credenciais emitidas em um domínio não são aceitas no outro), estas podem usar um STS de confiança de ambos os domínios para emitir credenciais em nome das aplicações. Dessa forma, o STS serve como mediador de confiança entre domínios de segurança distintos.

De maneira geral, o modelo de confiança da *WS-Trust* [OASIS 2009b] especifica que um serviço *Web* pode exigir que uma mensagem comprove um conjunto de declarações (*claims*) para que seja processada. Essas exigências se traduzem em um conjunto de credenciais de segurança suportadas pelo serviço *Web* e um conjunto de STSs aos quais o serviço confia a emissão dessas credenciais. Para dar dinamismo e interoperabilidade ao serviço, deve-se descrever as exigências de segurança na forma de documentos de políticas em um formato padronizado, como *WS-Policy* [W3C 2007], e disponibilizar essas políticas anexadas à descrição WSDL do serviço.

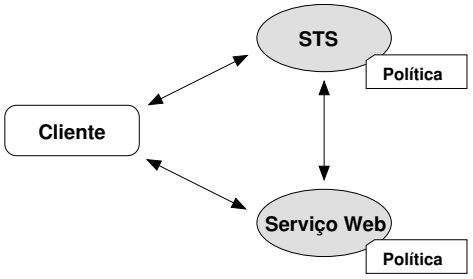


Figura 1.7: Modelo de confiança da *WS-Trust*

A Figura 1.7 ilustra um cenário de mediação de confiança com base em uma terceira parte confiável que implementa um STS [OASIS 2009b]. Quando o cliente deseja acessar o serviço, primeiramente obtém a política desse serviço (passo 1). Por meio dessa política, o cliente descobre o conjunto de exigências do serviço e os STSs de confiança. Caso o cliente não possua credenciais suficientes para satisfazer às exigências, pode pedir as credenciais a um dos STSs listados (passo 2). No entanto, o STS também poderá conter uma política especificando um outro conjunto de exigências e também pode apontar para outros STSs nos quais confie. Caso o cliente possua credenciais suficientes para acessar o STS de confiança do serviço, este pode requerer ao STS que emita as credenciais exigidas. O STS emitirá as credenciais e o cliente apresentará estas juntamente com a requisição ao serviço *Web* (passo 3). O serviço realizará a validação das credenciais passadas pelo cliente, possivelmente invocando o STS que as emitiu (passo 4), para poder permitir o acesso do cliente.

As mensagens trocadas pelo STS são bastante gerais para permitir extensões e composições futuras, cabendo a cada operação (emissão, validação, renovação, revogação, etc.) especificar quais elementos a mensagem deve conter. A mensagem de requisição é composta de um elemento XML `RequestSecurityToken` (RST) e a resposta é formada pelo `RequestSecurityTokenResponse` (RSTR). A RST contém parâmetros gerais, como o tipo de requisição, o tipo de credencial ao qual a requisição se refere, o

serviço ao qual a credencial será apresentada e as exigências desse serviço. Dependendo do tipo da requisição, esta conterá elementos mais específicos, como uma prova de posse de uma chave privada, conteúdo aleatório para geração de chaves, prazo de validade esperado para as credenciais, etc. A RSTR contém, basicamente, a credencial requisitada juntamente com parâmetros da credencial (tipo, validade, contexto de utilização, etc.) descritos de forma independente do tipo de credencial.

WS-Federation

A especificação *WS-Federation* [W3C 2009a] é um padrão OASIS que define mecanismos baseados nos padrões WS-*, em especial *WS-Security*, *WS-Trust* e *WS-Policy*, para a formação de federações. Esses padrões já definem as bases para o gerenciamento federado de identidades, porém a *WS-Federation* propõe extensões que definem como combinar esses modelos de forma a prover funcionalidades mais ricas aos domínios de segurança dentro e entre federações.

Há alguma sobreposição entre as funcionalidades da *WS-Federation* e da tecnologia *SAML* (ver seção 1.4.1) [W3C 2009a]. Ambas soluções permitem gerenciamento federado de identidades e provêm um conjunto de funcionalidades similar. Assim como a SAML, a *WS-Federation* suporta autenticação única, encerramento único de sessão, compartilhamento de atributos (sujeito a políticas de privacidade), pseudônimos permanentes e transientes e documentos de metadados. A principal diferença é que a *WS-Federation* está baseada no modelo de confiança da *WS-Trust* e permite o uso de quaisquer credenciais de segurança, não somente asserções SAML.

A *WS-Federation* define serviços para o gerenciamento de identidades como implementações da interface do STS, definida na *WS-Trust* [W3C 2009a]. Dessa forma, o STS passa a acumular a função de provedor de identidades (*identity provider* - STS/IdP) e a emitir credenciais contendo informações de identidades dos sujeitos do seu domínio de segurança para serem usadas em outros domínios que tiverem uma relação de confiança (i.e. aceitarem credenciais assinadas pelo STS/IdP). As relações de confiança podem ser estabelecidas diretamente, pelo intermédio de um STS/IdP, ou indiretamente por meio de relações de confiança entre STS/IdPs de domínios distintos. A Figura 1.8 apresenta algumas topologias de mediação de confiança previstas na *WS-Federation*, bem como as trocas de mensagens em cenários de acesso a recursos.

No cenário A, o sujeito se autentica no STS/IdP do seu domínio (passo 1, por meio da operação RST) e, em seguida, realiza o acesso aos recursos, enviando junto a credencial emitida (passo 2). O recurso verifica a validade da credencial enviando um pedido de validação para o STS/IdP do seu próprio domínio (passo 3). Como os STS/IdPs do cliente e do serviço possuem uma relação de confiança, a validação terá sucesso e o provedor do recurso poderá decidir sobre o acesso com base na validação das informações contidas na credencial. O cenário B é similar, no entanto, os STS/IdP dos domínios não possuem uma relação direta de confiança, mas uma relação mediada por um terceiro STS/IdP. Além disso, o cliente, antes de tentar acessar o recurso, invoca o STS/IdP do domínio do provedor (passo 2) para que este lhe indique as credenciais aceitas pelo provedor do recurso. O cenário C apresenta uma comunicação direta entre aplicações distribuídas, na qual o

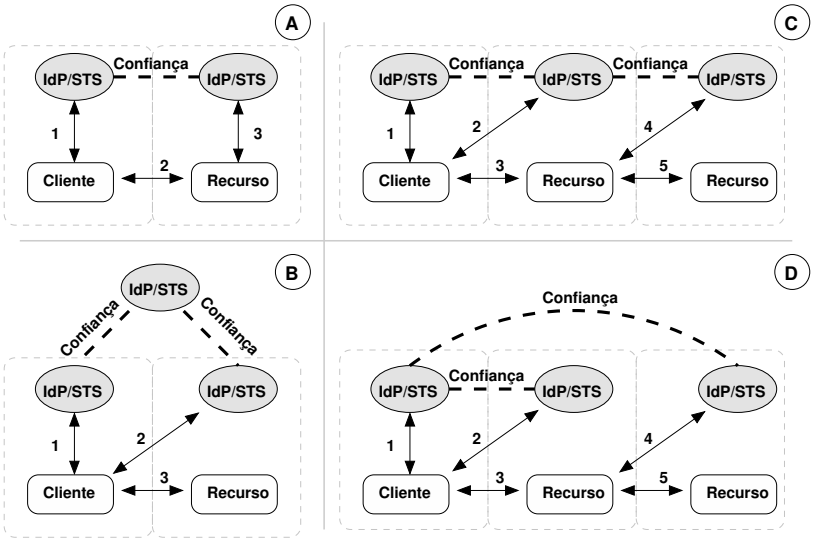


Figura 1.8: Cenários de federações com diferentes topologias de confiança

serviço acessado pelo cliente realiza, por sua vez, o acesso a um segundo recurso de um domínio que possua relação de confiança. O cenário D é similar ao C, no entanto nesse caso o cliente deve enviar ao recurso acessado no passo 3 as credenciais para que esse possa acessar o segundo recurso. A delegação foi necessária pois não há uma relação de confiança entre os domínios dos dois recursos.

Além do provedor de identidades, a *WS-Federation* prevê ainda os papéis de serviço de atributos e serviço de pseudônimos [W3C 2009a]. O serviço de atributos é responsável por emitir atributos de identidade dos sujeitos. A especificação não obriga o uso de nenhuma interface específica para o serviço de atributos, no entanto recomenda para isso o uso do STS, pois o uso do mesmo modelo de confiança e protocolo de comunicação pode facilitar análises de ameaças e a implementação. Além disso, o uso do STS facilita que um mesmo serviço implemente tanto o IdP quanto o servidor de atributos. Os serviços de atributos devem garantir a privacidade das informações dos sujeitos, portanto, a *WS-Federation* prevê que diferentes atributos devam ser associados a diferentes políticas de acesso, de acordo com o consentimento dos sujeitos.

O serviço de pseudônimos é responsável por associar pseudônimos a identidades de sujeitos. Um pseudônimo é um tipo especial de atributo, usado para identificar um sujeito sem revelar diretamente as informações de identidade. Na *WS-Federation*, pseudônimos podem ter diferentes níveis de volatilidade para permitir diferentes níveis de personalização e privacidade [W3C 2009a]. Por exemplo, um sujeito pode ter um pseudônimo diferente para cada provedor de serviço, o que dificulta o seu rastreamento (exceto em caso de conluio entre os serviços) mas ainda permite aos serviços manter informações locais para fins de personalização de acesso. Em outro exemplo, o sujeito pode ter pseudônimos que durem apenas uma sessão de autenticação, aumentando sua privacidade e impedindo que serviços associem qualquer informação persistente. Diferente do IdP e do serviço de atributos, o serviço de pseudônimos usa uma interface diferente, não baseada no STS, mas sim na especificação *WS-Transfer* [W3C 2010], que define métodos para criação, remoção, alteração e obtenção de recursos (no caso, pseudônimos).

Os serviços de atributos, de pseudônimos e IdPs podem trabalhar em conjunto a fim de prover funcionalidades complexas garantindo a privacidade dos sujeitos. Por exemplo, o serviço de atributos pode responder a pedidos de atributos associados a um pseudônimo, para isso invocando o serviço de pseudônimos e obtendo a identidade associada ao pseudônimo. Além disso, esses serviços podem ser implementados no mesmo sistema [W3C 2009a].

Assim como a SAML tem um perfil para clientes capazes de processar mensagens SOAP, a *WS-Federation* tem um perfil para clientes *seb* (i.e. navegadores *web* sem suporte a Serviços *Web*) [W3C 2009a]. O perfil tira a necessidade de o cliente processar mensagens SOAP usando, para isso, mecanismos do protocolo HTTP. Todas as trocas de mensagens são feitas usando somente métodos POST e GET e redirecionamentos são usados para automatizar comunicações entre o STS e a aplicação *web*. Esse perfil permite que navegadores *web* aproveitem os modelos de segurança da *WS-Security* e *WS-Trust*.

Para facilitar a descoberta de serviços e a comunicação entre os participantes da federação, a *WS-Federation* define um formato XML para especificação de metadados da federação [W3C 2009a], que contém descrições de uma ou mais entidades participantes. Essas descrições especificam mecanismos para a descoberta de serviços federados e de metadados (WSDL, políticas, etc.) associados a estes. O formato XML é baseado no modelo de documentos de metadados da especificação SAML [OASIS 2005e] (ver Seção 1.4.1), que associa papéis a entidades. A estrutura do documento é similar, no entanto os papéis que as entidades podem assumir são diferentes e refletem as funcionalidades e os parâmetros dos serviços da *WS-Federation*. A especificação define, ainda, diversos mecanismos para a obtenção de documentos de metadados de maneira segura. Entre os mecanismos estão a incorporação dos documentos em descrições WSDL, uso de URL padrão e resolução de registros DNS.

1.4.5. OpenID

Em 2005, Brad Fitzpatrick, arquiteto-chefe da Six Apart, desenvolveu a tecnologia OpenID [OpenID 2010] para ser utilizada no LiveJournal com o objetivo de autenticar os comentaristas do *blog* da comunidade e evitar o *spam* de comentários. *OpenID Authentication 1.0* começou como um protocolo leve de autenticação de identificadores de usuários (URLs) baseado no HTTP. Conforme [Maler e Reed 2008], a solução OpenID, que fornece ao usuário a possibilidade de ter uma única credencial (um OpenID) para acessar diferentes sítios *web*, está evoluindo rapidamente.

Atualmente, a tecnologia *OpenID Authentication 2.0* é uma plataforma aberta conduzida pela comunidade de desenvolvedores organizada pela *OpenID Foundation*, que permite e incentiva a inovação. Esta suporta tanto URLs[6] quanto XRIs (*Extensible Resource Identifier*)[OASIS 2005d] como identificadores de usuários, acrescenta mais segurança e suporta tanto identificadores públicos quanto privados. Esta última versão, além de adotar o modelo de gerenciamento de identidades centrado no usuário, implementa o conceito de identidade federada [Recordon e Reed 2006].

Uma vasta gama de sítios *web*, especialmente os que tem forte conteúdo gerado

[6]Um exemplo de um identificador do tipo URL é `http://openid-provider.appspot.com/wangham`

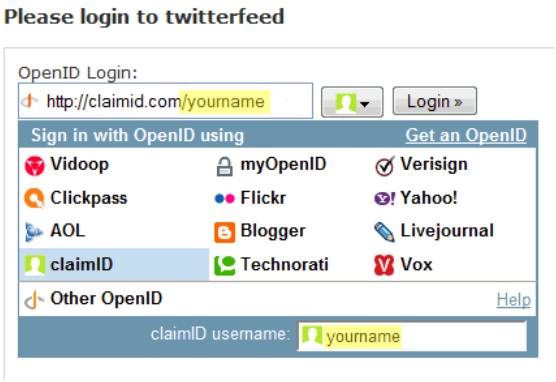


Figura 1.9: Sítio *web* com suporte a *login* OpenID

pelo usuário, adotaram esta tecnologia (usam ou provêm OpenIDs), entre estes destacam-se Google, Six Apart, Yahoo, Flickr, MySpace.com, Facebook, Wordpress, Verisign, AOL e PayPal. Formada em junho de 2007, a *OpenID Foundation* é uma organização internacional sem fins lucrativos constituída de indivíduos e empresas comprometidas com o suporte, promoção e segurança da tecnologia OpenID. A fundação atua como uma organização de confiança do público que representa a comunidade aberta de programadores, fornecedores e usuários [OpenID 2010].

A solução OpenID é descentralizada e nenhuma autoridade central aprova ou registra as partes confiantes (*relying parties*), sítios *web*, ou provedores OpenID (*OpenID providers*). Um usuário pode escolher livremente qual provedor OpenID usará (Google, Yahoo, etc) e pode preservar seu identificador caso deseje futuramente mudar de provedor OpenID (ver Figura 1.9). A distribuição de um identificador OpenID é gratuita e não é necessário qualquer tipo de registro ou aprovação de qualquer organização [Baldoni 2010].

Segundo a especificação [OPENID 2007], o *framework* utiliza apenas pedidos e respostas HTTP, por isso não exige nenhuma capacidade especial do *software* cliente (*User-Agent*), no caso um navegador *web*. O *framework* OpenID não está vinculado à utilização de *cookies*, ou a utilização de qualquer outro mecanismo específico da parte confiante (*relying party*) ou depende da utilização de gerenciamento de sessão do provedor OpenID. Extensões para os navegadores Web podem simplificar a interação com o usuário final, porém não são obrigatórios.

A seguir, uma visão geral das trocas de mensagens do protocolo OpenID 2.0 é descrita e também é ilustrada na Figura 1.10 [OPENID 2007].

1. Através do seu navegador Web, o usuário inicia o processo de autenticação apresentando um identificador para a parte confiante (o sítio *web* que deseja acessar e que suporta *login* OpenID);

2. Com base no identificador fornecido pelo usuário, a parte confiante realiza a descoberta (*Discovery*) da URL do provedor OpenID que o usuário utiliza para autenticação;

3. (Opcional e não ilustrado na Figura) A parte confiante e o provedor OpenID esta-

belecem uma associação - uma chave secreta é estabelecida utilizando o protocolo Diffie-Hellman Key Exchange. Esta associação é estabelecida para facilitar o processo de assinatura e verificação de mensagens trocadas entre o provedor OpenID e o a parte confiante.

4. A parte confiante redireciona o navegador do usuário para o provedor OpenID com um pedido de autenticação OpenID (solicitação de uma asserção ou credencial);

5. O provedor OpenID verifica se o usuário final está autorizado a executar a autenticação OpenID que deseja fazê-lo. A maneira na qual o provedor OpenID autentica o usuário final e as políticas em torno desta autenticação estão fora do escopo da especificação (p.ex: no caso do Google, é utilizada a senha associada a conta google como forma de autenticação);

6. O provedor OpenID redireciona o navegador Web do usuário final de volta para a parte confiante com uma asserção que indica que a autenticação está aprovada (asserções positivas) ou uma mensagem de que a autenticação falhou (asserções negativas);

7. A parte confiante verifica as informações enviadas pelo provedor OpenID, que inclui a verificação da URL retornada, das informações descobertas (provedor OpenId), do *nonce* e da assinatura. Para verificação da assinatura, a parte confiante usa a chave compartilhada estabelecida durante a associação ou a solicita diretamente ao provedor OpenID.

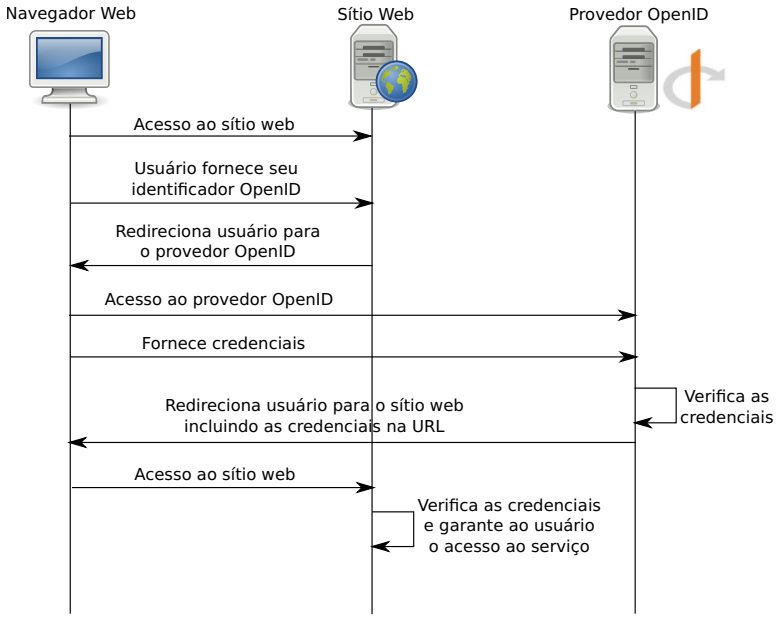


Figura 1.10: Protocolo OpenID Authentication 2.0

Conforme citado no passo 2 do protocolo OpenID 2.0, a descoberta do provedor OpenID se dá quando os usuários fornecem seus identificadores às partes confiantes. Diante disto, provedores OpenID e partes confiantes que não se conhecem podem

se comunicar com sucesso, um tipo de escalabilidade conscientemente modelada dentro dos padrões da própria Web. De acordo com [Maler e Reed 2008], isso pode representar um desafio a privacidade: como uma arquitetura tendenciosa e direcionada ao amplo compartilhamento de informações dos usuários. O OpenID permite e até estimula que diferentes partes confiantes correlacionem atividades de um usuário. No entanto, OpenID 2.0 suporta o login utilizando pseudônimos. O OpenID também permite que o provedor OpenID de um usuário veja todas as partes confiantes (sítios) que o usuário visitou. Para controlar a disseminação dessas informações para um provedor OpenID (de terceiros), a única opção do usuário seria a de executar o seu próprio provedor OpenID. O modelo de descoberta de provedores OpenID também impede uma autenticação única verdadeira, na qual a parte confiante pode visitar diretamente o provedor OpenID sem pedir para que o usuário indique a sua localização [Maler e Reed 2008].

1.4.6. Windows CardSpace (*InfoCard*)

De acordo com [Chappell 2006], nos diferentes tipos de redes colaborativas que utilizam a Internet diferentes tipos de identidades digitais são necessárias e a realidade é que estas identidades são providas por diferentes fontes (IdPs). Isto significa que a solução para o gerenciamento dessas identidades é utilizar sistemas que suportem múltiplas identidades, ou seja, um sistema de sistemas - um meta sistema (*metasystem*) - focado na identidade. O desafio é criar, usar, e gerenciar esta diversidade de identidades de uma forma efetiva.

O meta sistema Windows CardSpace, originalmente chamado de *InfoCard*, é um componente da plataforma .Net da Microsoft projetado para oferecer aos usuários uma experiência consistente do uso de múltiplas identidades digitais, a partir do uso de um agente (*user-agent*) especializado. A Microsoft documentou o protocolo implementado pelo Cardspace na especificação *InfoCard*. A tecnologia CardSpace está disponível por padrão no Windows Vista e no Windows 7 e pode ser incorporada em versões anteriores do sistema operacional Windows. Além disso, a mesma também é suportada no navegador Internet Explorer (desde a versão 7.0).

O Cardspace concentra-se nas coleções de dados do usuário chamados cartões de informação (*InfoCards*), apresentados em uma interface de software, chamado de seletor de identidade (semelhante a uma carteira que contém os cartões que identificam o usuário). Conforme ilustrado na Figura 1.11, cada *InfoCard* representa uma identidade diferente. Quando uma parte confiante (SP) solicita as credenciais do usuário, este escolhe, a partir do seletor, uma de suas identidades [Maler e Reed 2008].

A Figura 1.12 ilustra um cenário no qual um usuário, através de uma aplicação, por exemplo um navegador Web, tenta acessar a parte confiante B que suporta a tecnologia CardSpace. Este usuário também deve ser capaz de escolher, entre um grupo de provedores de identidades, quem será a fonte da identidade digital que este apresentará à parte confiante B. Seja qual for a escolha do usuário, as mensagens trocadas entre as partes serão[Chappell 2006]:

1. A aplicação obtém os requisitos do *token* de segurança da parte confiável que o usuário deseja acessar. Esta informação está contida na política da parte confiável e estas inclui, entre outras informações, qual tipo de *tokens* de segurança que a parte confiável pode aceitar e quais atributos (*claims*) este *token* deve conter;

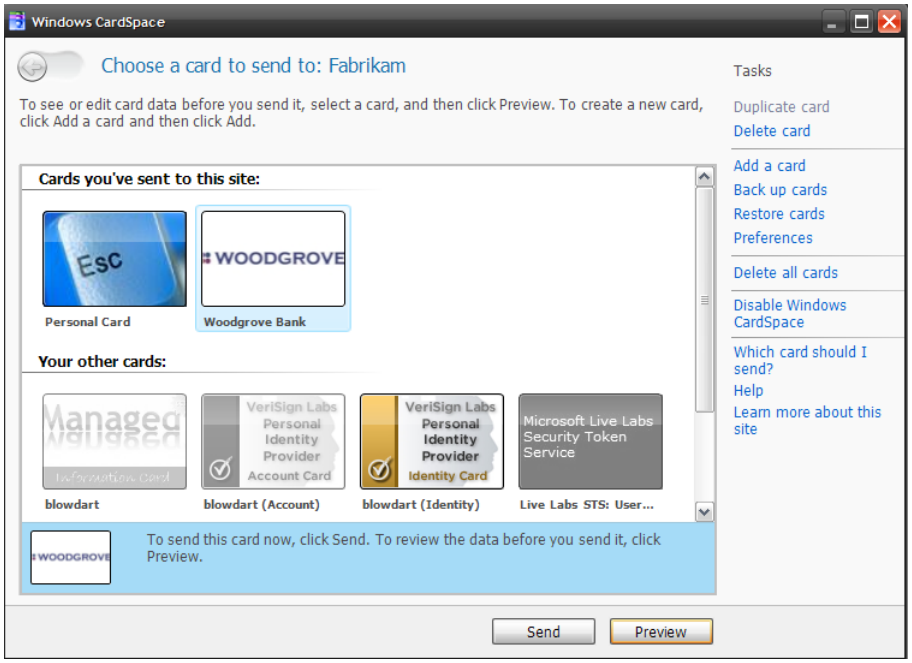


Figura 1.11: Visualização de um Seletor de *InfoCards*

2. Uma vez que estas informações são repassadas para o CardSpace, a aplicação mostra a tela do seletor de identidades, com os cartões de informação que o usuário possui, para que o usuário escolha qual identidade irá usar. Apenas alguns cartões são aplicáveis, os cartões cujos tokens de segurança e os atributos não são compatíveis com os requisitos da parte confiante, estes aparecem na tela esmaecidos e os usuários não podem escolhê-los;

3. Após selecionar o cartão desejado, o CardSpace emite um pedido de *token* de segurança para a o provedor de identidades associado com o cartão. O provedor de identidades então retorna um *token* de segurança;

4. Uma vez que o token é recebido, o CardSpace passa este para aplicação que apresenta para a parte confiante. A parte confiante pode então usar este token para autenticar o usuário ou para outros propósitos.

No passo 3, quando o provedor de identidades retorna o *token* de segurança assinado digitalmente, o conjunto de atributos do *token* corresponde à noção de uma asserção SAML, e, de fato, um dos tipos de token suportados é um *token* SAML. A tecnologia CardSpace suporta dois tipos de cartões [Maler e Reed 2008]:

- *cartões self-asserted* – representam um conjunto de atributos cujos valores são determinados unicamente pelo usuário (semelhantes as identidades OpenID). Na implementação da Microsoft, esses atributos são diretamente armazenados no dispositivo do usuário;

- *cartões administrados* – representam um conjunto (extensível) de atributos dos usuários gerenciado por um provedor de identidade. Tipicamente, cada vez que

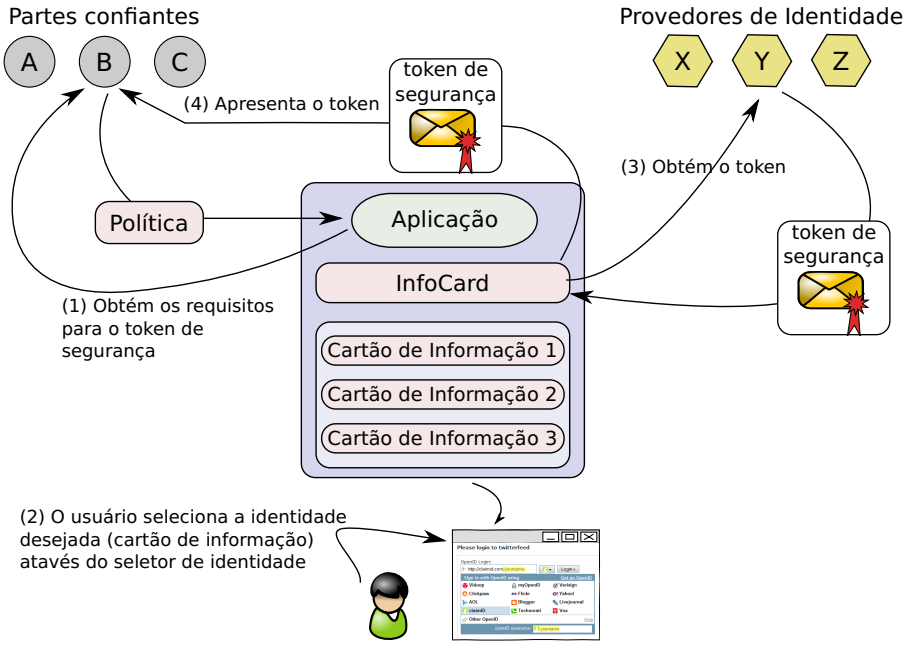


Figura 1.12: Mensagens Trocadas no Windows CardSpace

o usuário seleciona um cartão específico em resposta a um pedido de uma parte confiante, o seletor de identidades recupera os atributos do usuário no IdP que os emitiu. Cartões administrados são típicas identidades SAML-federadas nas quais o IdP rege os seus atributos e validade.

Implementação de tecnologias centradas no usuário impõem um custo, mas também permite soluções mais elegantes para problemas como o da descoberta do IdP. O modelo InfoCard aborda este problema eliminando a necessidade de uma parte confiante se conectar ao IdP. Em cartões *self-asserted*, o dispositivo do cliente pode ser o próprio IdP e, para cartões administrados, os IdPs armazenam seu endereço no cartão para o seletor de identidades usar [Maler e Reed 2008].

Um cartão administrado reflete a estreita relação do usuário com o IdP e um seletor de identidade pode usar isso para aumentar a resistência a ataques de *phishing* de autenticação. Como um intermediário nas comunicações entre IdPs e partes confiantes, um seletor de identidades também permite aos usuários evitar que um IdP identifique os sítios *web* e aplicações *web* visitadas (partes confiantes) pelos usuários. Vale destacar ainda que, um seletor de identidades ao permitir que um usuário selecione a identidade que deseja utilizar possibilita o gerenciamento centrado no usuário [Maler e Reed 2008].

Segundo [Chappell 2006], a tecnologia Windows CardSpace é totalmente agnóstica sobre o formato de token de segurança que é requerido por um provedor de identidade e que é passado para parte confiante. De fato, geralmente o CardSpace não tem consciência do que está dentro do *token* (formato). Por isso, o CardSpace pode trabalhar com qualquer sistema de identidade digital, utilizando qualquer tipo de token de segurança, incluindo simples *usernames tokens*, certificados X.509, *tickets* Kerberos, *tokens* SAML ou qualquer outro *token*. Isso permite que este meta-sistema de identidades possa ser usado junto com qualquer tecnologia de identidades digitais.

Todas as trocas implementadas pelo CardSpace e ilustradas na Figura 1.12, são feitas usando protocolos abertos e padronizados. No cenário mais geral, a política da parte confiante é descrita usando a *WS-SecurityPolicy*[OASIS 2009a], a política é recuperada usando a *WS-MetadataExchange* [W3C 2009b], um token de segurança é adquirido usando *WS-Trust*[OASIS 2009b], e o *token* é transmitido para a parte confiável usando *WS-Security* (todos estes protocolos da família WS são necessários para permitir a troca segura de *tokens* de identidade no meta-sistema de identidades).

1.4.7. Projeto Higgins

A motivação inicial do projeto Higgins foi o desejo de um sistema de gerenciamento de identidades centrado no usuário que permita que este tenha mais controle, comodidade e privacidade sobre a sua identidade e informações de perfil. As pessoas devem ser capazes de decidir quais informações desejam compartilhar e com quais sítios *web*. Higgins trata-se de um *framework* que opera com todos os protocolos de identidade digital, incluindo WS-Trust, OpenID, SAML, XDI, LDAP, entre outros. O objetivo é criar uma identidade única de todas as outras identidades de diferentes domínios [EclipseFoundation 2010].

O *framework* Higgins define uma série de interfaces de programação que os desenvolvedores podem usar para ligar o seu software à função de gerenciamento de identidades Higgins [Le e Bouzefrane 2008]. O projeto Higgins tem recebido contribuições tecnológicas da IBM, Novell, Oracle, CA, Serena, Google, Corisecio, bem como de várias outras empresas e indivíduos. O projeto Higgins aborda cinco áreas [EclipseFoundation 2010]:

1. Proporciona uma experiência consistente ao usuário, baseado em cartões de informação chamados de *i-Card*, para o gerenciamento e divulgação dos seus dados de identidade;

2. Permite aos usuários um maior controle sobre a revelação de suas informações pessoais com os sítios *web* que interagir;

3. Fornece uma API e um modelo de dados para prover identidades federadas, a partir de uma ampla variedade de fontes. Através desta API, o projeto Higgins incentiva os desenvolvedores a criar *plugins* para operar com protocolos e *tokens* de segurança de sistemas legados;

4. Fornece *(plugins*) para que fontes de dados existentes, incluindo diretórios, sistemas de comunicações, sistemas de colaboração e bases de dados, possam ser integradas ao *framework*;

5. Fornece um *framework* para integração de dados de relacionamentos sociais que permite que essas relações sejam persistentes e reutilizáveis, para além das fronteiras da aplicação. Este *framework* organiza as relações em um conjunto de contextos sociais distintos dentro do qual uma pessoa pode expressar diferentes papéis e personalidades.

O modelo de identidades do Higgins segue a abordagem baseada em cliente ativo, ou seja, uma aplicação precisa auxiliar o usuário a controlar as suas múltiplas identidades

e preferências. O Higgins oferece aos usuários três aplicações que atuam como seletores de identidades para a criação, seleção, compartilhamento e gerenciamento de diversos *i-cards* que representam a identidade do usuário em diferentes contextos e relacionamentos. Assim como no CardSpace, os benefícios do *login* centrado em cartões são também válidos para o Higgins. Neste modelo, é possível cruzar contextos e gerenciar qualquer tipo de informação do usuário como canções favoritas, números de identificação do empregado, carteira de habilitação, sua filiação, seu plano de saúde, entre outras que possam ser armazenadas em um cartão. É importante ressaltar que estes seletores são interoperáveis com o Microsoft CardSapce. Estes seletores de identidades estão disponíveis para alguns sistemas operacionais (Mac OSX, Linux e Windows), bem como para os navegadores Firefox e Internet Explorer [EclipseFoundation 2010].

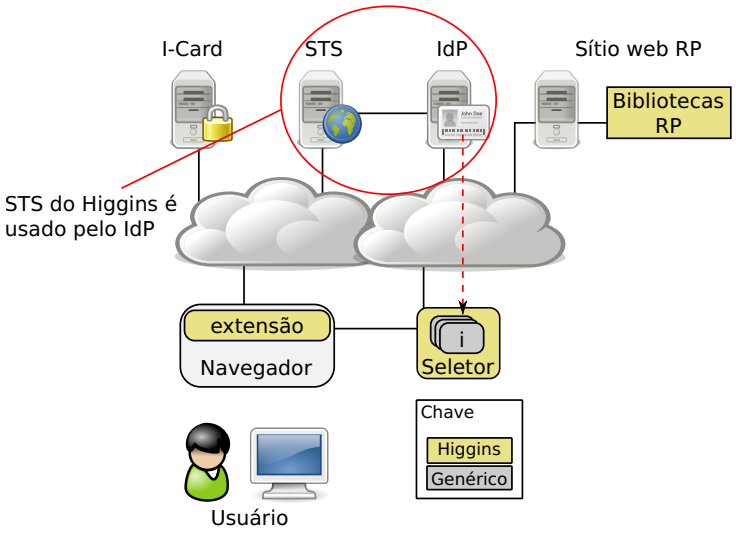


Figura 1.13

Para os desenvolvedores, o Higgins fornece dois provedores de identidades - IdP (que são Serviços Web). O primeiro é um STS (*Security Token Service*), baseado no WS-Trust, e o segundo suporta o padrão SAML 2.0. Higgins também provê bibliotecas para as partes confiantes necessárias para permitir que sítios *web* e sistemas possam solicitar e aceitar cartões de informação (*i-cards*). Os desenvolvedores podem incorporar este código da parte confiante dentro de suas aplicações e sítios *web* para tornar mais fácil para os usuários o processo de autenticação nestes sistemas. As partes confiantes podem prover autenticação OpenID e autenticação através de cartões de informação (*i-card*). A Figura 1.13 apresenta as entidades que participam do processo de autenticação, quando um usuário tenta acessar um parte confiante.

Abaixo das aplicações seletoras e dos Serviços *Web* mencionados anteriormente, encontra-se uma camada de abstração para o gerenciamento de identidades. Esta camada consiste em um *framework* que pode ser estendido através de *plugins*. A camada mais baixa deste *framework* é o serviço de atributos de identidade (*Identity Attribute Service* – IdAS), que fornece interoperabilidade e portabilidade através de federações de dados de identidade (ver Figura 1.14). O IdAS fornece acesso de leitura e escrita a uma ampla variedade de fontes de dados, incluindo diretórios LDAP e arquivos XML, e pode ser estendido usando *plugins* chamados *provedores de contexto*. Ou seja, este serviço torna

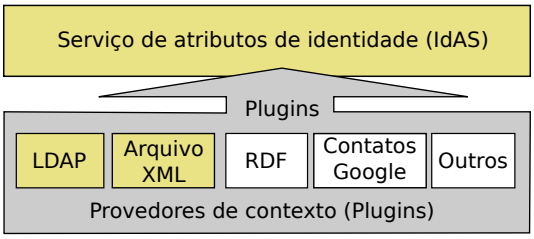


Figura 1.14: Serviço de Atributos de Identidades

possível combinar dados de redes sociais e de identidade através de fontes de dados altamente heterogêneos, incluindo diretórios, bancos de dados relacionais e as redes sociais.

1.4.8. Considerações sobre as soluções de gerenciamento

As soluções para gerenciamento de identidades apresentadas nessa seção compartilham pontos em comum, como a facilidade de autenticação única (SSO), distribuição das tarefas de autenticação e controle, preocupações com a privacidade e anonimato dos usuários. Todas consideram que o usuário pode fazer uso de um navegador *web*, sendo que a troca de informações entre provedores de identidades e de serviços se dá através de redirecionamentos HTTP.

As especificações do SAML apresentam um arcabouço genérico para lidar com identidades federadas, no qual são definidos metadados para representar informações de segurança, protocolos para troca de asserções de segurança, além de casos de uso, com usuários atrás de navegadores *web* ou não. Por se tratar de uma solução genérica, o SAML foi empregado por várias outras soluções para o gerenciamento de identidades, inclusive por todas as soluções apresentadas nessa seção.

O *Shibboleth* surgiu como uma solução aberta para permitir que instituições de ensino e pesquisa ofereçam uma gama maior de serviços para seus usuários, através do compartilhamento de recursos, esses oferecidos através de provedores de serviços. Hoje as principais federações acadêmicas do mundo fazem uso do *Shibboleth* e, em muitas dessas federações, cujo público alvo é formado por alunos e professores, empresas estão se filiando para oferecer serviços personalizados.

O projeto *Liberty Alliance* teve como objetivo facilitar as interações comerciais, usufruindo da Arquitetura Orientada a Serviços (AOS), através do conceito de federações, que em suas especificações são caracterizadas pelos círculos de confiança. Um dos pontos fortes do projeto foi sua participação direta nas especificações do SAML, sendo que muitas sugestões do *Liberty Alliance* são hoje parte do SAML 2.0. A WS-Federation fornece funcionalidades semelhantes àquelas do projeto *Liberty Alliance*, porém está fundamentada sobre uma pilha de especificações para Serviços *Web*, como WS-Trust e WS-Policy [Kallela 2008].

OpenID, CardSpace e Higgins são soluções que seguem a abordagem do gerenciamento de identidades federadas centrado no usuário. Dentre estas soluções, a solução que vem sendo amplamente usada, em especial devido a parceria com empresas que oferecem aplicações Web 2.0, é o OpenID. Uma das vantagens do OpenID é que este não requer software no lado do cliente. O CardSpace e o Higgins adotam o mo-

delo de cliente ativo (chamado de seletor de identidades), sendo que o cliente ativo do Higgins está disponível para diferentes plataformas. Outra diferença é que o OpenID adota a abordagem de identidade baseada no endereço e CardSpace e Higgins adotam a abordagem baseada em cartão (*tokens*). A literatura mostra que esta última abordagem é considerada mais flexível pois suporta identidades providas de diferentes fontes e também por oferecer um experiência consistente ao usuário e por impedir que um provedor de identidade rastreie os provedores de serviços (aplicações) acessados pelo usuário [Maler e Reed 2008, Akram e Hoffmann 2008].

Apesar de prover suporte a qualquer tipo de *token* de segurança, os protocolos adotados no *CardSpace* seguem somente os protocolos de Serviços *Web* da família WS-*, centrados na especificação WS-Trust. No entanto, o projeto Higgins da Fundação Eclipse está focado em uma solução mais independente pois além de oferecer suporte a provedores de identidade baseados na especificação WS-Trust, também oferece suporte a provedores de identidades baseados no SAML 2.0.

Atualmente, soluções de e-gov, como as do Governo dos Estados Unidos, começam a construir suas infraestruturas com suporte a tecnologias de identidades abertas, tais como o OpenID e o CardSpace. O padrão SAML é considerado uma tecnologia de identidade aberta, porém a necessidade de relações de confiança prévias entre IdPs e SPs fazem com que esta tecnologia não seja escalável para aplicações Web 2.0. Diante disto, *frameworks* abertos de confiança (terceiras partes confiáveis) estão sendo desenvolvidos para habilitar sítios *web* do Governo e aplicações a aceitarem credenciais emitidas por diferentes provedores de identidades, comerciais e acadêmicos [Thibeau e Reed 2009].

Segundo [Chadwick 2009], a maior limitação do *Shibboleth* e do CardSpace[7] é que o usuário pode selecionar apenas um provedor de identidades e apresentar apenas uma credencial a um provedor de serviços. Uma solução para este problema, proposto em [Chadwick e Inman 2009], é usar um componente chamado de Serviço de Ligação (*Linking Service*). Este serviço permite aos usuários agregar vários atributos de diferentes IdP preservando a privacidade desses usuários. O projeto Higgins também pretende trabalhar este problema, porém a versão atual ainda não oferece uma solução.

1.5. Privacidade no Gerenciamento de Identidades Federadas

O conceito de identidades federadas fornece aos usuários um modo conveniente para criar identidades e mover-se por vários SPs. Mas não se pode negar que, além de toda a simplicidade e conveniência oferecidas, a gestão dessas identidades federadas torna-se uma tarefa crucial e é necessário levar em consideração as várias ameaças contra a segurança e a privacidade dos dados do usuário. Qualquer infraestrutura de gerenciamento de identidades deve proteger adequadamente as informações do usuário e deve aderir adequadamente às política de privacidade definidas para os dados do mesmo.

Outras propriedades e características são necessárias para manter a privacidade de usuários em uma federação. Medidas de segurança devem garantir que os atributos do usuário não sejam divulgados de forma involuntária. No entanto, os mecanismos adicionais necessários para oferecer resistência aos diferentes tipos de posse indevida ou roubo

[7]Pode-se incluir também o OpenID.

destas identidades e atributos devem levar em conta as diferenças de contextos e as diferenças de políticas nas federações. Por exemplo, se um sistema particular de identidades federadas for centrado no usuário e permitir ao usuário armazenar suas próprias credenciais em um dispositivo de sua propriedade, então, medidas adicionais são necessárias para proteger as credenciais do mesmo o caso este dispositivo seja perdido. Proteger os dados do usuário onde estes estão armazenados é parte da segurança de um sistema e da privacidade do usuário.

O compartilhamento de informações de identificação pessoal é um grande desafio no que se refere à privacidade, à proteção de dados pessoais e à conformidade com aspectos legais que envolvem os direitos individuais das pessoas. Em sistemas de identidades federadas, verifica-se que entre os principais objetivos está o compartilhamento de tais informações.

Pode-se definir a privacidade como a divulgação mínima em nível funcional; isto é, fornecer somente os identificadores e informações necessários para assegurar a execução ou a continuidade de um serviço. Sistemas de identidades federadas, frequentemente, manipulam diferentes tipos de identificadores em diferentes contextos. Tais identificadores podem assumir um caráter *absoluto*, independentes de contexto, ou *relativo*, dependentes do contexto [Ahn e Lam 2005].

Uma técnica importante para a preservação da privacidade é o uso de pseudônimos, que são identificadores de usuários que não permitem inferências em relação à identidade real, propriedades ou atributos dos usuários a quem fazem referência. Pseudônimos podem ter significado *local*, dependente do contexto entre usuário e SP, ou *global*, independente do contexto e sendo válido por toda a federação. A validade pode também ser temporária ou permanente [Ahn e Lam 2005].

Dentre as soluções de gerenciamento de identidades federadas que oferecem mecanismos para prover privacidade, destaca-se a *Liberty Alliance* (ver Seção 1.4.3). Os pseudônimos usados em asserções SAML são construídos com base em valores pseudo-aleatórios que não têm correspondência discernível com os identificadores dos usuários em IdPs ou SPs. Um pseudônimo tem um significado apenas no contexto da relação entre as duas partes que estão se comunicando. A intenção é criar pseudônimos de forma a dificultar a ligação entre usuários e transações (serviços sendo acessados), mantendo assim a privacidade.

O *Liberty Alliance* provê suporte a uma abordagem de compartilhamento de atributos de usuário com o consentimento do mesmo [Aarts e Madsen 2006]. Isto significa que o usuário deve ser colocado no controle da liberação e uso de suas informações armazenadas em um provedor de atributos, papel que pode ser assumido por um IdP. Nas mensagens a serem trocadas neste protocolo a requisição deve especificar o propósito do uso das informações solicitadas e a resposta pode determinar as preferências do usuário em termos de privacidade ou política para o elemento requisitado.

As especificações do *Liberty Alliance* também abordam questões sobre políticas de privacidade multi-nível [Aarts e Madsen 2006, Ahn e Ko 2007], que se faz através de *rótulos de privacidade*. Rótulos de privacidade são semelhantes aos rótulos de segurança nos controles de acesso obrigatórios (*Mandatory Access Control* – MAC). Em controles

do tipo MAC, cada recurso ou objeto é etiquetado com um rótulo de segurança que representa a sensibilidade do recurso considerado. Um usuário (sujeito) desejando fazer um acesso ao recurso considerado deve possuir um nível de autorização (*clearance level*) adequado ao rótulo de segurança do recurso. Os níveis de privacidade são usados nas políticas de privacidade dos provedores de identidades, que também atuam como repositórios de atributos de usuários, e nas requisições de atributos enviadas pelos provedores de serviços aos IdPs.

Em vez de um grande número de políticas de privacidade, variado e personalizado, foi definido um pequeno número (padronizado) destas aos quais, ambos, requisitante e provedor de atributos devem aderir em favor do usuário. Isto leva a uma simplificação nas verificações da política nas requisições de informações. Para preservar a privacidade da informação do usuário, o IdP deve liberar informações de atributos requisitados somente com o consentimento do usuário. O IdP deve ter armazenado as preferências do usuário no que se refere a liberação de suas informações. Estas preferências são expressas na forma da política multi-nível. Ou seja, o usuário classificou suas informações segundo os níveis disponíveis. O IdP precisa só comparar o nível na requisição com o nível definido nas preferências do usuário. No caso de desacordo nestas comparações, o IdP pode tomar algumas ações definidas pelo próprio usuário. É lógico que a definição destas ações e políticas deve considerar vários aspectos do contexto da interação entre usuário e SP e as intenções do usuário em relação à suas informações pessoais.

Os requisitos que devem atender os níveis de privacidade seguem as seguintes regras conforme discutido em [Ahn e Lam 2005]:

- *Os níveis de privacidade devem ser hierárquicos e comparáveis entre as partes envolvidas* – é necessário avaliar cada requisição de atributo pela comparação dos rótulos do SP requerente com a da política do usuário. A informação requisitada é liberada tomando como base esta avaliação;

- *Rótulos de privacidade devem ser amigáveis* – os usuários tendem a usar rótulos para representar conceitos abstratos como níveis de seriedade ou justiça. As pessoas podem não compreender completamente as necessidades exatas da definição destes níveis. Ou seja, talvez estas não consigam dimensionar a importância das informações nos contextos;

- *Os rótulos devem funcionar com um motor de política* – ao invés de avaliar cada descrição de elemento nas políticas de privacidade este motor necessita apenas comparar níveis de privacidade para cada atributo requisitado. Isto reduz consideravelmente o custo do processamento de todas as requisições.

Na abordagem de gerenciamento de identidades federadas centrado no usuário, as soluções de privacidade devem atender alguns pontos chaves [Ahn e Lam 2005]:

- *Notificação* – usuários devem receber *a priori* notificações sobre determinadas liberações de suas informações.

- *Definição de propósitos* – os usuários devem especificar o propósito do uso e quais de suas informações devem ser coletadas;
- *Disponibilidade de suas informações* – os usuários podem acessar e modificar suas informações pessoais quando necessário;
- *Segurança de suas informações* – usuários devem estar certos de que o sistema de gestão de identidades é capaz de proteger suas informações pessoais.

1.6. Ferramentas Computacionais para Implantação de Gerenciamento de Identidades

Nesta seção são apresentadas algumas das principais ferramentas usadas por soluções de gerenciamento de identidades.

1.6.1. Metro

O *framework Metro*[8], componente do projeto *Glassfish* da *Oracle* [9], possui um extenso conjunto de bibliotecas que podem ser facilmente estendidas e implementa padrões e especificações apropriadas ao gerenciamento de identidades, aprovadas e adotadas por diversas empresas e organizações [10], tais como Microsoft, Oracle e OASIS[11]. Estas características o destaca como uma importante opção a ser considerada no desenvolvimento de aplicativos que incluam o gerenciamento de identidades entre seus recursos.

A importância do *framework Metro* no cenário de Serviços *Web* está ligado ao fato deste conter em seu conjunto de bibliotecas, implementações chamadas "implementações de referência" de diversas especificações da plataforma Java. Dentre estas, destaca-se a especificação JAX-WS - *Java API for XML Web Services*[12] - que define as bases da criação de serviços *Web* com foco na linguagem Java e é parte da plataforma Java EE da *Oracle*.

Além da implementação da especificação JAX-WS e de outras implementações auxiliares, destacam-se as bibliotecas *Policy*, responsável pela implementação da especificação *WS-Policy*; XWSS - *XML and Web Services Security* - responsável pela implementação da especificação *WS-Security*; e WSIT - *Web Services Interoperability Technologies* [13] - responsável pela implementação das seguintes especificações: *WS-Trust*, *WS-SecurityConversation*, *WS-SecurityPolicy*, *WS-ReliableMessaging*, *SOAP over TCP* *WS-MetadataExchange* e *WS-AtomicTransactions*.

O *framework Metro* fornece toda funcionalidade básica para construção de um STS, definido na WS-Trust, por meio da classe `BaseSTSImpl`. Essa classe, por padrão, permite a emissão de asserções SAML 1.1 e 2.0. A implementação é extensível por meio das seguintes interfaces: `STSTokenProvider`, para suportar outros tipos

[8] `https://metro.dev.java.net/discover`
[9] `https://glassfish.dev.java.net`
[10] `https://metro.dev.java.net/guide/Metro_Specifications.html`
[11] `http://www.oasis-open.org`
[12] `https://jax-ws.dev.java.net`
[13] `https://wsit.dev.java.net`

de credenciais; `STSAttributeProvider`, para obter atributos de fontes variadas; e `STSAuthorizationProvider`, para emitir credenciais e declarações de autorização.

1.6.2. Shibboleth

A implantação de um sistema de controle de acessos unificado baseado no Shibboleth em uma instituição requer a configuração de alguns serviços distintos, citados na seção 1.4.2

O provedor de identidades (IdP) do Shibboleth [14] consiste de uma aplicação *web*, disponível em formato WAR, que é disponibilizada em um contêiner Java como o *Apache Tomcat*. O contêiner Java por sua vez deve ser executado vinculado a um servidor *web*, por exemplo *Apache HTTP*, o qual terá o papel de deixar o IdP disponível na rede.

```
1 <Location /secure>
2  AuthType shibboleth
3  ShibRequireSession On
4  require valid-user
5  Order allow,deny
6  allow from all
7 </Location>
```

Figura 1.15: Exemplo de configuração do *Apache* para autenticação via Shibboleth

Provedores de serviços do Shibboleth são aplicações *web* comuns que permitem que seus usuários sejam autenticados através dos provedores de identidades. O Shibboleth disponibiliza um módulo próprio para ser integrado ao servidor *web Apache*, permitindo assim que aplicações *web*, disponibilizadas através do Apache HTTP, possam facilmente usufruir da infraestrutura do Shibboleth. A Figura 1.15 ilustra um exemplo de configuração do servidor web Apache usufruindo do módulo Shibboleth para realizar a autenticação dos usuários que acessarem o recurso `/secure`.

1.6.3. WSO2 Identity Server

O *WSO2 Entity Provider*[15] é uma solução completa, que abrange desde a conexão com fontes de dados LDAP e JDBC até a interface com o usuário por meio de telas para o processo de autenticação. O *WSO2 Entity Provider* é uma solução de código aberto baseada no *WSO2 Carbon*, uma plataforma com diversas funcionalidades para a construção de aplicações para *web*. As principais funcionalidades oferecidas pelo *WSO2 Identity Server* são: controle de acesso com XACML 2.0, suporte a asserções SAML 1.1/2.0, bem como implementações para STS WS-Trust (ver Seção 1.4.4), IdP SAML 2.0 (*Web SSO*), provedor OpenID, provedor de *Information Cards* e um serviço XKMS [Hallam-Baker e Mysore 2005].

[14] O Shibboleth foi a tecnologia adotada pela Federação CAFe. Diversos documentos para instalação e configuração dos serviços estão disponíveis na página da federação (`http://cafe.rnp.br`)

[15] `http://wso2.com/products/identity-server`

1.6.4. Lasso

Lasso[16] consiste em um conjunto de bibliotecas para linguagem C que implementam os conceitos definidos pelas especificações *Liberty Alliance* (ver Seção 1.4.3). A versão atual implementa a ID-FF 1.2, SAML 2.0 e boa parte da ID-WSF. Apesar de ser desenvolvido em C, *Lasso* possui diversos mapeamentos para outras linguagens, como Python e Java.

1.6.5. Windows CardSpace

Conforme visto na Seção 1.4.6, O *Windows CardSpace* é um componente da plataforma .NET. Um provedor de identidades compatível com o *CardSpace* pode ser um STS padrão. Portanto, qualquer implementação da *WS-Trust* pode ser usada para construir um provedor *CardSpace*. Os provedores de serviços, por outro lado, são construídos por meio de extensões HTML ou XHTML que indicam para o navegador quando acionar o seletor de identidades.

```
<OBJECT type="application/x-informationCard" name="xmlToken">
  <PARAM Name="tokenType" Value="urn:oasis:names:tc:SAML:1.0:assertion" />
  <PARAM Name="issuer"
     Value="http://schemas.xmlsoap.org/ws/2005/05/identity/issuer/self" />
  <PARAM Name="requiredClaims"
     Value=
     "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
     http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
     http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname" />
</OBJECT>
```

Figura 1.16: Exemplo de uma configuração para invocar o seletor de identidade do *CardSpace*

A Figura 1.16 apresenta um exemplo de elemento HTML que indica o uso do seletor de identidades. Esse elemento contém parâmetros que indicam que a credencial exigida é uma asserção SAML, emitida pelo IdP (elemento `issuer`) e que deve conter os atributos e-mail, nome e sobrenome.

No lado do usuário, se um navegador habilitado a reconhecer um pedido de autenticação por *InfoCard*, receber uma página com o elemento acima, este poderá invocar uma interface para o usuário selecionar seu *InfoCard* apropriado. A ferramenta *CardSpace* possui um módulo responsável por realizar essa interface com o usuário e é distribuída como parte do *framework .Net*[17].

1.6.6. Eclipse Higgins

O projeto *Eclipse Higgins* (ver Seção 1.4.7) é uma solução que visa aumentar o controle das pessoas sobre suas identidades digitais. O desenvolvimento do projeto é dividido em três partes, *Active Client*, *Personal Data Store* e *Identity Services*. O *Active Client* é um módulo integrado ao navegador *web* que automatiza o processo de autenticação do usuário usando credenciais como *InfoCard*, *OpenID* e nome de usuário e senha. Essa

[16] `http://lasso.entrouvert.org`

[17] `http://www.microsoft.com/windows/products/winfamily/cardspace/getitnow.mspx`

funcionalidade apresenta alguma sobreposição com o *CardSpace*, no entanto o *Higgins* provê suporte a mais tecnologias de autenticação e um número maior de plataformas e navegadores.

O *Personal Data Store* (PDS) é um serviço de armazenamento, sincronização e compartilhamento de atributos de identidade do usuário. Esse serviço ainda não é um produto completo, mas um plano para a próxima versão (2.0). O PDS deverá prover um ponto central de controle sobre informações acerca de um usuário e uma maneira para compartilhar dados entre PDSs de diferentes usuários para formar uma espécie de rede social.

O *Identity Services* implementa IdPs de acordo com a *WS-Trust* e a SAML 2.0, bem como bibliotecas Java para implementação de partes confiantes *InfoCard*. Os IdPs são distribuídos como pacotes independentes e a biblioteca para implementação de partes confiantes é distribuída acoplada a um exemplo de aplicação *web* que ilustra o uso de *InfoCards* para controlar o acesso a recursos.

1.7. Considerações finais

As redes colaborativas, que utilizam computadores e dispositivos móveis, oferecem novas possibilidades de conexões, oportunidades e aplicações. No entanto, a forma como as pessoas e as organizações (privadas e públicas) farão uso dessas oportunidades e aplicações, dependerá do progresso da autenticação de identidades digitais e do gerenciamento destas identidades [Lewis 2008].

Conforme visto neste Capítulo, o modelo de gerenciamento de identidades federadas beneficia tanto usuários quanto provedores de serviços. Constata-se que promover identidades federadas apresenta desafios complexos em termos de questões técnicas e necessidades humanas [Maler e Reed 2008]. Requisitos importantes muitas vezes parecem ser mutuamente exclusivos. Alguns aspectos de segurança, tais como auditoria do acesso a recursos do sistema, pode entrar em conflito com questões de privacidade do usuário. Ao mesmo tempo, a capacitação do usuário, tais como possibilitar que este atue como intermediador de fluxos de dados, pode entrar em conflito com as conveniências do usuário, tais como a realização de autenticação única totalmente "silenciosa".

As principais soluções para prover o gerenciamento de identidades federadas foram descritas e analisadas neste texto. Constatou-se que o SAML 2.0 é base para estas soluções, o *Shibboleth* se tornou um padrão de fato nas redes acadêmicas e a solução *Liberty Alliance* está sendo adotada por uma grande comunidade de empresas privadas e também por empresas públicas. As soluções mais recentes do modelo centrado no usuário, em especial OpenID e CardSpace tem despertado muito interesse, em especial dos provedores de serviços que seguem a abordagem Web 2.0 e por governos que desejam incluir ativamente seus cidadãos através das redes sociais e de seus programas de E-Gov.

Para [Maler e Reed 2008], a interoperabilidade é um desafio contínuo para prover identidades federadas. No entanto, muitos desenvolvedores estão começando a combinar diferentes soluções, de acordo como estas crescem em popularidade. Por exemplo, promover a autenticação em um IdP OpenID ou SAML, usando um cartão de informação (*i-Card* ou *InfoCard*) ou usando um OpenID ao invés de uma asserção SAML para então

acessar um Serviço *Web* com suporte a *Liberty Identity*.

O primeiro passo para para resolver os problemas de interoperabilidade é o entendimento das distâncias entre as tecnologias. Alguns projetos estão sendo desenvolvidos visando promover a interoperabilidade em sistemas de gerenciamento de identidades federadas. Entre estes destacam-se: a iniciativa Kantara, que engloba o projeto Concordia e o grupo de trabalho OSIS (*Open Source Identity System*) do *Identity Commons*. A iniciativa *Kantara*[18] constituiu uma organização para resolver os desafios de interoperabilidade e de harmonização que existem entre as empresa que oferecem serviços e aplicações Web. Criada de forma colaborativa, a iniciativa visa promover a inovação necessária para a ampla adoção de soluções interoperáveis de identidades federadas adequadas para todas as indústrias e regiões e alinhada as necessidades das redes móveis. Já o projeto OSIS [19], reúne muitos projetos de gerenciamento de identidades e tem objetivo contribuir com a construção de uma camada de identidade interoperáveis a partir do soluções de código-fonte aberto e soluções comerciais. Os projetos atuais incluem esforços para promover a interoperabilidade entre o Information Card (CardSpace) e OpenID.

Segundo [Chadwick 2009], gerenciamento de identidades federadas é um tema de pesquisa ativo e, provavelmente, diante da sua complexidade e relevância, continuará assim por muito mais anos. Esta constatação decorre das inúmeras questões que os sistemas de identidades federadas devem considerar, tais como: facilidade de uso, privacidade do usuário, segurança forte, autenticação única diante de diferentes tecnologias, custo dos sistemas (*total cost of ownership*), escalabilidade, controle de acesso de granularidade fina (baseado em atributos), personalização dos serviços e anonimato.

Referências

[Aarts e Madsen 2006] Aarts, R. e Madsen, P. (2006). *Liberty ID-WSF Interaction Service Specification v.2*. Liberty Alliance Project. `http://www.projectliberty.org/liberty/content/download/`.

[Ahn e Ko 2007] Ahn, G.-J. e Ko, M. (2007). User-centric privacy management for federated identity management. *International Conference on Collaborative Computing: Networking, Applications and Worksharing*, 0:187–195.

[Ahn e Lam 2005] Ahn, G.-J. e Lam, J. (2005). Managing privacy preferences for federated identity management. In *DIM '05: Proceedings of the 2005 workshop on Digital identity management*, pages 28–36, New York, NY, USA. ACM.

[Akram e Hoffmann 2008] Akram, H. e Hoffmann, M. (2008). Supports for identity management in ambient environments - the hydra approach. In *ICSNC '08: Proceedings of the 2008 Third International Conference on Systems and Networks Communications*, pages 371–377, Washington, DC, USA. IEEE Computer Society.

[Baldoni 2010] Baldoni, R. (2010). Federated Identity Management Systems in e-Government: the Case of Italy. *Electronic Government: An International Journal*, 8(1).

[18] `http://kantarainitiative.org`
[19] `http://osis.idcommons.net`

[Bartel et al. 2002] Bartel, M., Boyer, J., e Fox, B. (2002). *XML-Signature Syntax and Processing*. W3C. http://www.w3.org/TR/xmldsig-core.

[Bhargav-Spantzel et al. 2007] Bhargav-Spantzel, A., Camenisch, J., Gross, T., e Sommer, D. (2007). User centricity: a taxonomy and open issues. *Journal of Computer Security*, 15(5):493–527.

[Burr et al. 2006] Burr, W. E., Dodson, D. F., e Polk, W. T. (2006). Electronic authentication guideline. *NIST Special Publication*, 800:63.

[Camarinha-Matos et al. 2008] Camarinha-Matos, L. M., Afsarmanesh, H., e Ollus, M. (2008). *Methods and Tools for Collaborative Networked Organizations*, chapter Ecolead And Cno Base Concepts, pages 3–32. Springer.

[Camenisch e Pfitzmann 2007] Camenisch, J. e Pfitzmann, B. (2007). *Security, Privacy, and Trust in Modern Data Management*, chapter Federated Identity Management, pages 213–238. Springer Verlag.

[Cameron 2005] Cameron, K. (2005). The laws of identity. http://www.identityblog.com/?p=352/#lawsofiden_topic3.

[Carmody et al. 2005] Carmody, S., Erdos, M., Hazelton, K., Hoehn, W., Morgan, B., Scavo, T., e Wasley, D. (2005). Incommon technical requirements and information. vol. 2005.

[Chadwick 2009] Chadwick, D. (2009). Federated identity management. *Foundations of Security Analysis and Design V*, pages 96–120.

[Chadwick e Inman 2009] Chadwick, D. e Inman, G. (2009). Attribute aggregation in federated identity. *IEEE Computer*, pages 44–53.

[Chappell 2006] Chappell, D. (2006). Introducing windows cardspace. Msnd technical articles, Microsoft Corporation. http://msdn.microsoft.com/en-us/library/aa480189.aspx.

[Clauß e Köhntopp 2001] Clauß, S. e Köhntopp, M. (2001). Identity management and its support of multilateral security. *Computer Networks*, 37(2):205–219.

[Damiani et al. 2003] Damiani, E., di Vimercati, S. D. C., e Samarati, P. (2003). Managing multiple and dependable identities. In *IEEE Internet Computing*, pages 29–37. IEEE.

[Dawes e Pardo 2008] Dawes, S. S. e Pardo, T. A. (2008). *Advances in Digital Government Technology, Human Factors, and Policy*, chapter Building Collaborative Digital Government Systems Systemic: constraints and effective practices, pages 259–273. Springer US.

[de Mello 2009] de Mello, E. R. (2009). *Um modelo para confiança dinâmica em ambientes orientados a serviço*. PhD thesis, Universidade Federal de Santa Catarina.

[de Mello et al. 2009] de Mello, E. R., Wangham, M. S., da Silva Fraga, J., Camargo, E., e da Silva Böger, D. (2009). Model for authentication credentials translation in service oriented architecture. *Transactions on Computational Sciences Journal*, 5430:68–86.

[EclipseFoundation 2010] EclipseFoundation (2010). Higgins open source identity framework. `http://www.eclipse.org/higgins/`.

[Gottschalk e Solli-Saether 2008] Gottschalk, P. e Solli-Saether, H. (2008). Stages of e-government interoperability. *Electronic Government: An International Journal*, 5(3):310–320.

[GOV.BR 2010] GOV.BR (2010). Programa de governo eletrônico brasileiro (gov.br). `http://www.governoeletronico.gov.br`.

[Hallam-Baker e Mysore 2005] Hallam-Baker, P. e Mysore, S. H. (2005). *XML Key Management Specification (XKMS 2.0)*. W3C – Proposed Recommendation.

[Hansen et al. 2008] Hansen, M., Schwartz, A., e Cooper, A. (2008). Privacy and identity management. *Security Privacy, IEEE*, 6(2):38 –45.

[Hodges e Morgan 2002] Hodges, J. e Morgan, R. (2002). *Lightweight Directory Access Protocol (v3): Technical Specification. RFC3377*. IETF.

[Housley et al. 2002] Housley, R., Polk, W., Ford, W., e Solo, D. (2002). *Internet X. 509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. IETF RFC 3280.

[IBM 2005] IBM (2005). *Federated Identity Management and Web Services Security with IBM Tivoli Security Solutions*. IBM, second edition.

[Internet2 2008] Internet2 (2008). eduPerson & eduOrg Object Classes. `http://middleware.internet2.edu/eduperson/`.

[ITU-T 2001] ITU-T (2001). *Information technology - Open Systems Interconnection - The Directory: Overview of concepts, models and services*. ITU-T Recommendation X.500. `http://www.itu.int/rec/recommendation.asp?type=folders&lang=e&parent=T-REC-X.500`.

[Jøsang et al. 2005] Jøsang, A., Fabre, J., Hay, B., Dalziel, J., e Pope, S. (2005). Trust requirements in identity management. In *CRPIT '44: Proceedings of the 2005 Australasian workshop on Grid computing and e-research*, pages 99–108, Darlinghurst, Australia. Australian Computer Society, Inc.

[Jøsang e Pope 2005] Jøsang, A. e Pope, S. (2005). User centric identity management. In *AusCERT Asia Pacific Information Technology Security Conference 2005*.

[Kallela 2008] Kallela, J. (2008). Federated identity management solutions. Technical report, Helsinki University of Technology. `http://www.cse.tkk.fi/en/publications/B/1/papers/Kallela_final.pdf`.

[Kohl e Neuman 1993] Kohl, J. e Neuman, C. (1993). The kerberos network authentication requestor (v5). rfc1510. Technical report, IETF.

[Kürümlüoglu et al. 2005] Kürümlüoglu, M., Nostdal, R., e Karvonen, I. (2005). *Base concepts*, chapter Virtual organisations: Systems and practices, pages 11–28. Springer.

[Le e Bouzefrane 2008] Le, H.-B. e Bouzefrane, S. (2008). Identity management systems and interoperability in a heterogeneous environment. pages 239 –242.

[Leach et al. 2005] Leach, P., Mealling, M., e Salz, R. (2005). *A UUID URN Namespace*. IETF RFC 4122. `http://www.ietf.org/rfc/rfc4122.txt`.

[Lewis 2008] Lewis, J. A. (2008). Authentication 2.0 - new opportunities for online identification. Technical report, Center for Strategic and International Studies.

[Liberty 2003] Liberty (2003). *Introduction to the Liberty Alliance Identity Architecture*. Liberty Alliance.

[Lopez et al. 2006] Lopez, D., Solberg, A., e Stanica, M. (2006). eduGAIN Profiles and Implementation Guidelines.

[Maler e Reed 2008] Maler, E. e Reed, D. (2008). The venn of identity: Options and issues in federated identity management. *Security Privacy, IEEE*, 6(2):16–23.

[Maliki e Seigneur 2007] Maliki, T. E. e Seigneur, J.-M. (2007). A survey of user-centric identity management technologies. In *The International Conference on Emerging Security Information, Systems, and Technologies, 2007. SecureWare 2007*, pages 12–17.

[OASIS 2004] OASIS (2004). *Web Services Security: SOAP Message Security 1.0*. OASIS. `http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf`.

[OASIS 2005a] OASIS (2005a). *Assertions and Protocols for the SAML 2.0*. OASIS.

[OASIS 2005b] OASIS (2005b). *Bindings for the OASIS SAML V2.0*. Organization for the Advancement of Structured Information Standards (OASIS).

[OASIS 2005c] OASIS (2005c). *eXtensible Access Control Markup Language (XACML) version 2.0*. Organization for the Advancement of Structured Information Standards (OASIS). `http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf`.

[OASIS 2005d] OASIS (2005d). *Extensible Resource Identifier (XRI) Syntax V2.0*. OASIS. `http://www.oasis-open.org/committees/download.php/15377/xri-syntax-V2.0-cs.pdf`.

[OASIS 2005e] OASIS (2005e). *Metadata for the OASIS SAML V2.0*. Organization for the Advancement of Structured Information Standards (OASIS).

[OASIS 2005f] OASIS (2005f). *Profiles for the OASIS SAML V2.0*. Organization for the Advancement of Structured Information Standards (OASIS).

[OASIS 2005g] OASIS (2005g). *Security Assertion Markup Language (SAML) 2.0 Technical Overview*. OASIS.

[OASIS 2009a] OASIS (2009a). *WS-SecurityPolicy 1.3*. OASIS. http://docs.oasis-open.org/ws-sx/ws-securitypolicy/v1.3/ws-securitypolicy.html.

[OASIS 2009b] OASIS (2009b). *WS-Trust 1.4*.

[OPENID 2007] OPENID (2007). Openid authentication 2.0. OPENID. http://openid.net/specs/openid-authentication-2_0.html.

[OpenID 2010] OpenID (2010). Openid. http://openid.net.

[Rabelo 2008] Rabelo, R. J. (2008). *Methods and Tools for Collaborative Networked Organizations*, chapter Advanced Collaborative Business ICT Infrastructures, pages 337–365. Springer.

[Recordon e Reed 2006] Recordon, D. e Reed, D. (2006). Openid 2.0: a platform for user-centric identity management. In *DIM '06: Proceedings of the second ACM workshop on Digital identity management*, pages 11–16, New York, NY, USA. ACM.

[RNP 2010] RNP (2010). Federação cafe. http://www.cafe.rnp.br.

[Scavo e Cantor 2005] Scavo, T. e Cantor, S. (2005). *Shibboleth Architecture*. http://shibboleth.internet2.edu/docs/draft-mace-shibboleth-tech-overview-latest.pdf.

[Smith 2000] Smith, M. (2000). *Definition of the inetOrgPerson LDAP Object Class*. IETF RFC 2798.

[TERENA 2008] TERENA (2008). *TERENA Compendium of National Research and Education Networks In Europe*. TERENA.

[Thibeau e Reed 2009] Thibeau, D. e Reed, D. (2009). Open trust frameworks for open government: Enabling citizen involvement through open identity technologies. White paper, OpenID Foudation and Information Card Foudation.

[W3C 2007] W3C (2007). *Web Services Policy 1.5 - Framework*. http://www.w3.org/TR/2007/REC-ws-policy-20070904.

[W3C 2009a] W3C (2009a). *Web Services Federation Language – WS-Federation*.

[W3C 2009b] W3C (2009b). *Web Services Metadata Exchange (WS-MetadataExchange)*. W3C. http://www.w3.org/TR/2009/WD-ws-metadata-exchange-20090317.

[W3C 2010] W3C (2010). *Web Services Transfer (WS-Transfer)*. http://www.w3.org/TR/2010/WD-ws-transfer-20100805.

[Wahl 1997] Wahl, M. (1997). *A Summary of the X.500(96) User Schema for use with LDAPv3*. IETF RFC 2256.