Um Mecanismo Agregador de Atributos Mediado pelo Cliente para um Sistema de Gestão de Identidades Federadas Alinhado ao Programa Gov.br

Marcondes Maçaneiro[1,2], Michelle S. Wangham[1]

[1]Programa de Mestrado em Computação Aplicada – Universidade do Vale do Itajaí (UNIVALI) – Itajaí - SC – Brasil

[2]Centro Universitário par o Desenvolvimento do Alto Vale do Itajaí - UNIDAVI

marcondesmacaneiro@gmail.com, wangham@univali.br

Abstract. *In identity management systems, the use of multiple identity providers (IdPs) can bring benefits to users, mainly for privacy. This paper defines a mechanism able to aggregate the attributes of users available in multiple IdPs. Those attributes can be presented to providers that require attributes that are not in a single IdP. The proposed mechanism innovative since adopts a client-mediated approach, that uses an intelligent client and follows the recommendations of the E-PING architecture Gov.br program.*

Resumo. *Em sistemas de gestão de identidades, o uso de múltiplos provedores de identidades (IdPs) pode trazer vantagens para os usuários, principalmente, para privacidade de seus dados. Este artigo define um mecanismo agregador de atributos capaz de coletar e unir os atributos dos usuários disponibilizados em múltiplos IdPs, para que estes possam ser apresentados para provedores que exigem atributos que não estão em um único IdP. O mecanismo proposto é inovador ao adotar uma abordagem mediada pelo cliente, que faz uso de um aplicativo executado no ambiente do usuário e que segue as recomendações da arquitetura e-PING do Programa Gov.br.*

1. Introdução

Sistemas de gerenciamento de identidades (IdM) federadas permitem o compartilhamento dos atributos do usuário e a autenticação única através de múltiplos domínios, tornando-se facilitadores para os sistemas governamentais [Baldoni 2010]. Nos últimos anos, alguns governos aprovaram estratégias nacionais de gestão de identidades baseadas no modelo federado buscando melhorar seus serviços de governo eletrônico, dentre estes se destacam: Nova Zelândia, Austrália, Canadá e Estados Unidos [OECD, 2011].

A maioria dos sistemas de IdM federadas restringe a fonte de identidade e de atributos a um único provedor de identidades (IdP) em qualquer sessão criada com um provedor de serviços (SP) [Klingenstein 2007]. Com isto, as autorizações são limitadas a um subconjunto de atributos da identidade do usuário. No contexto do Governo Eletrônico, diante das diversas esferas governamentais, observa-se como comum em uma Federação que um usuário possua atributos espalhados em múltiplos IdPs (cada qual mantendo apenas os atributos dos usuários que são de sua responsabilidade), sendo que estes precisam ser coletados. Esta união, muitas vezes processada por uma terceira parte confiável [Chadwick e Inman 2009], é conhecida como agregação de atributos. Nesta abordagem, a terceira parte

mantém o controle das informações e acessos de usuário, o que pode comprometer a sua privacidade.

O objetivo deste trabalho é prover a agregação de atributos dos usuários, que estão distribuídos em múltiplos provedores de identidades, garantindo a privacidade, por meio de um mecanismo agregador de atributos, mediado pelo cliente e alinhado às recomendações da arquitetura E-PING, Padrões de Interoperabilidade de Governo Eletrônico, do Brasil.

2. Solução Proposta

Para concepção do mecanismo proposto, assume-se a existência de uma estratégia nacional de gestão de identidades federadas. A Federação de Serviços reúne as esferas do governo federal, estadual e municipal. Assume-se ainda que a estratégia de IdM segue também o modelo centrado no usuário. Por fim, assume-se que a Federação usa como infraestrutura de autenticação e de autorização o padrão SAML (Security Assertion Markup Language).

De forma a não prejudicar a interoperabilidade das aplicações de e-Gov, o mecanismo agregador de atributos atende as recomendações de interoperabilidade do programa de governo eletrônico brasileiro, contidas na arquitetura e-PING [BRASIL 2011].

Grande parte das implementações de agregação de atributos existentes focam na implementação baseadas em *proxy* que possuem vantagens, tais como a facilidade de implementação e, em especial, o suporte à autenticação SSO (*Single Sing-On*). Porém, a privacidade dos usuários do mecanismo pode ser comprometida nesta abordagem diante da facilidade da terceira parte em poder rastrear as interações entre o usuário e os IdPs e os SPs (provedores de serviços) [Chadwick e Inman 2009]. Já os mecanismos existentes que seguem a abordagem mediada pelo cliente são focados em plataformas específicas. Segundo [Klingenstein 2007], esta abordagem é a mais adequada quando se pretende priorizar a privacidade dos dados.

Para implementar a abordagem de agregação de atributos mediada pelo cliente, o mecanismo está sendo desenvolvido como um cliente ativo, executado no ambiente operacional do usuário. O aplicativo tem a finalidade de coletar os atributos dos usuários, a partir de múltiplos IdPs. Visando ainda prover a privacidade aos usuários, o mecanismo permite que o usuário indique quais provedores ele deseja utilizar e controle todas as trocas de atributos dos usuários, sendo que os atributos agregados pelo mecanismo só serão entregues ao provedor de serviço alvo após o consentimento do usuário.

A segurança durante as trocas de informações realizadas entre os SPs, os IdPs e o mecanismo agregador de atributos é assegurada através de protocolos e mecanismos de segurança amplamente aceitos: protocolo SSL e assinaturas digitais. Em todo processo de agregação, as autoridades de atributos (IdPs) são identificadas nas asserções de atributos por meio de suas assinaturas digitais.

A Figura 1 ilustra a visão geral do mecanismo proposto. Alguns IdPs do Governo são indicados como exemplo: o IdP DETRAN para acesso às informações veiculares e de habilitação do usuário; o IdP do registro de identidade civil (RIC) e o IdP da receita federal, responsável por armazenar informações fiscais de pessoas físicas e jurídicas.

No passo 1, o usuário, por intermédio de seu navegador Web, tenta acessar um serviço no provedor governamental. Por ser um serviço que exige autenticação, o navegador do usuário é redirecionado para o IdP indicado pelo serviço para proceder com a autenticação (passo 2). Após a autenticação bem sucedida, o navegador retorna para o

provedor de serviço que, para concretizar a ação solicitada pelo usuário, indica quais atributos do usuário este necessita (passo 3). Neste momento, o usuário deve confirmar que deseja prosseguir com o processo de agregação de atributos. Para obter o software do cliente ativo homologado por alguma instituição governamental (passo 4), o navegador do usuário é redirecionado para o serviço de descoberta de provedor de cliente ativo (SDPCA[1]) mantido pela federação. O serviço SDPCA deve apresentar ao usuário uma lista de provedores de aplicativos de cliente ativo homologados pelo governo.

Após o usuário selecionar um dos provedores de cliente ativo (passo 5), o navegador do usuário é redirecionado para o provedor selecionado para fazer o *download* da aplicação (passo 6). Após o *download* da aplicação, esta é executada no ambiente operacional do usuário (passo 7). Para efetuar a agregação de atributos, o cliente ativo deve solicitar ao SP a indicação dos atributos necessários (passo 8). Os atributos necessários são apresentados ao usuário para que este indique quais IdPs deseja utilizar (passo 9). Como a autenticação SSO é garantida, o usuário precisará se autenticar, via cliente ativo, apenas no primeiro IdP (passo 10.1), os demais aceitarão o *token* de autenticação emitido pelo IdP e responderão à solicitação de atributos (passo 10.2, 10.3 e 10.4). Finalmente, no passo 11, o cliente ativo efetua a agregação de atributos e encaminha, após o consentimento do usuário, os atributos agregados para o SP (passo 12). O provedor de serviços de posse dos atributos poderá permitir ou não o acesso ao serviço solicitado pelo usuário.

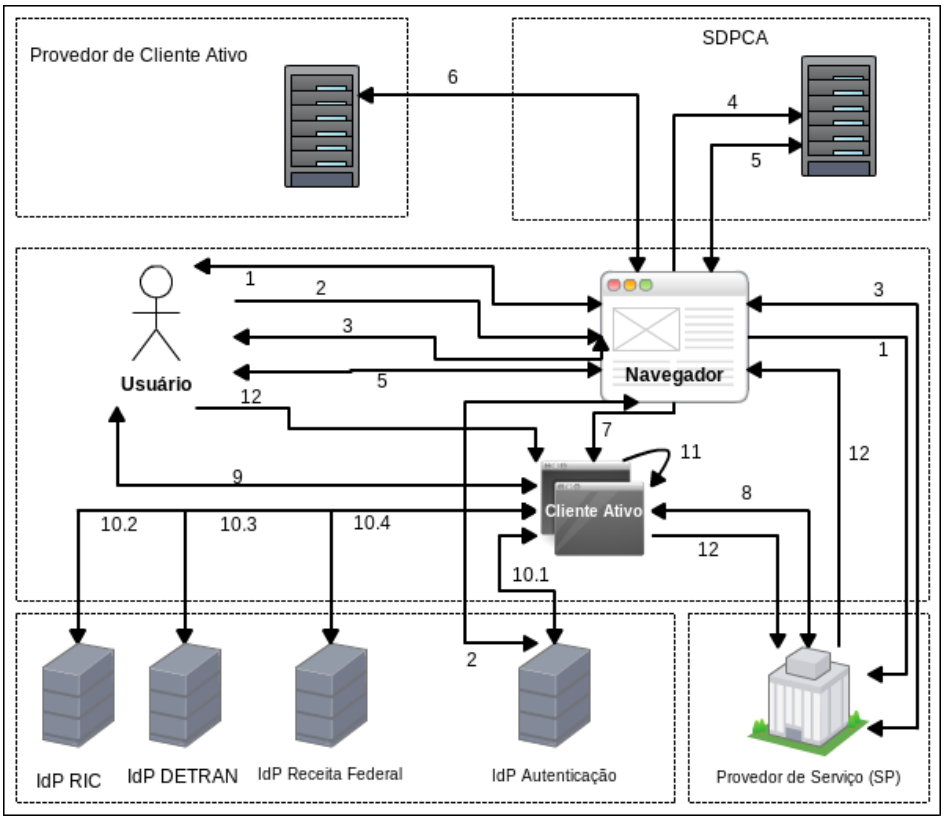

Figura 1. Visão geral do mecanismo agregador de atributos proposto

[1] Este serviço deve estar em um SP confiável administrado, por exemplo, por órgão federal.

Visando prover a interoperabilidade na comunicação entre o mecanismo agregador de atributos e os provedores de serviços da federação, foram definidas duas estruturas de dados (*XML Schemas)* para padronizar as trocas de dados entre estes. A primeira define como um provedor de serviços deve indicar ao Cliente Ativo os atributos que este deseja (lista de atributos). A segunda estrutura padroniza como os atributos agregados (asserções SAML) são compartilhados com os provedores de serviços.

Nos passos da autenticação do usuário (passos 2 e 10), recomenda-se que os provedores de identidades utilizem métodos de autenticação que evitem a adivinhação de senhas e, quando exigido por um SP, recomenda-se o uso de mecanismos de autenticação mais fortes que os baseados em senha, que oferecem maiores garantias de segurança ao sistema, mas que podem ser utilizados na autenticação do cliente ativo.

3. Considerações Finais

A análise e o projeto do mecanismo agregador de atributos e de um cenário de uso do mecanismo (serviço para emissão de passaporte) já foram concluídos. O cliente ativo está sendo desenvolvido na linguagem Java como um aplicativo Java Web Start. Os IdPs e SPs estão sendo desenvolvidos com o *framework* SimpleSAMLPHP e são serviços *restful*.

Com o objetivo de avaliar o atendimento dos requisitos funcionais e não funcionais, testes de software, incluindo os de segurança, serão executados. Em seguida, o cenário de uso do Serviço para Emissão de Passaporte que faz uso do mecanismo agregador proposto, será avaliado por especialistas da área de Governo Eletrônico e da área de gestão de identidades. Um questionário será aplicado (pesquisa de satisfação) para que estes especialistas possam avaliar a solução proposta. Dentre os aspectos a serem avaliados estão: grau de satisfação dos usuários ao fazer uso do mecanismo, aplicabilidade do mecanismo em diferentes serviços de e-Gov, flexibilidade (suporte a múltiplos IdPs), interoperabilidade, portabilidade, privacidade dos usuários, integridade e confidencialidade dos dados sensíveis.

Referências

Brasil (2011). “e-PING – Padrões de Interoperabilidade de Governo Eletrônico”. In: Comitê Executivo de Governo Eletrônico. Brasil.

Baldoni, Roberto. (2010) “Federated Identity Management System in e-Government: the Case of Italy”. In: Electronic Government, An International Journal.

Chadwick, D. e Inman, G. (2009). “Attribute aggregation in federated identity”. In: IEEE Computer, pages 44–53.

Jøsang, A. e Pope, S. (2005), “User centric identity management”. In: AusCERT Asia Pacific Information Technology Security Conference, 22, 2005, Gold Coast. Proceedings…, Springer Berlim Heidelberg, Berlim.

Klingestein, N. (2007) “Attribute Aggregation and Federated Identity”. In: 2007 International Symposium on Applications and the Internet Workshops (SAINTW'07).

OECD. National Strategies and Policies for Digital Identity Management. In OECD Countries. OECD Digital Economy Papers, No. 177, OECD Publishing, 2011.

