Um Mecanismo Agregador de Atributos Mediado pelo Cliente Alinhado ao Programa de E-GOV.BR

Marcondes Maçaneiro[1,2], Fábio Zoz[2], Michelle Silva Wangham[1]

[1]Laboratório de Sistemas Embarcados e Distribuídos (LSED) –

Universidade do Vale do Itajaí (UNIVALI)

[2]Curso de Sistemas de Informação – Centro Universitário para o Desenvolvimento do Alto ale do Itajaí, UNIDAVI.

{marcondes, zozfabio}@unidavi.edu.br, wangham@univali.br

Abstract. *The use of multiple identity providers (IdPs) in IdM systems can bring benefits to users, especially regarding privacy of data. This paper describes an aggregation mechanism able to gather and to join users' attributes that are distributed in multiple IdPs. These attributes can be presented to providers that require attributes, which are not in a single IdP. The proposed mechanism is innovative in adopting a client-mediated approach, which makes use of an active client in the user's environment and follows the recommendations of the ePING architecture of Gov.br's Program. The implementation results and the use of proposed mechanisms demonstrate that it gets more flexibility to a Gov Federation and also assures privacy without prejudicing the interoperability of E.Gov applications.*

Resumo. *O uso de múltiplos provedores de identidades (IdPs) em sistemas de IdM pode trazer vantagens para os usuários, principalmente, para privacidade de seus dados. Este artigo descreve 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 ePING do Programa Gov.br. Os resultados obtidos com a implementação e uso do mecanismo proposto demonstram que este traz mais flexibilidade para um sistema federado e garante a privacidade dos usuários sem prejudicar a interoperabilidade do sistema e de uma aplicação de E.Gov.*

1. Introdução

Sistemas de gerenciamento de identidades (*Identity Management - 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 2012]. 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, destacam-se: Nova Zelândia, Austrália, Canadá e Estados Unidos [OECD 2011].

A maioria dos sistemas de IdM federadas restringe a fonte de identidades e de atributos a um único provedor de identidades (IdP), em qualquer sessão criada com um provedor de serviços (SP) [Chadwick e Inman 2013]. Com isto, as autorizações são limitadas a um subconjunto de atributos da identidade do usuário. Segundo Klingenstein (2007), os sistemas de IdM federadas são sólidos e garantem o acesso federado de seus usuários, porém, muitas vezes, questões referentes à privacidade dos usuários não são devidamente consideradas, já que durante as trocas de informações que ocorrem nesses sistemas, os provedores podem rastrear a identidade do usuário e seus acessos.

No contexto das aplicações de 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. Observa-se ainda que, para algumas aplicações, é necessário que estes sejam coletados. Esta união, muitas vezes processada por uma terceira parte confiável, é um procedimento conhecido como agregação de atributos [Hatakeyma e Shima 2008]. Nesta abordagem, a terceira parte mantém o controle das informações e acessos de usuário, o que pode comprometer a sua privacidade.

Este artigo tem por objetivo descrever um mecanismo agregador de atributos mediado pelo cliente que atende as recomendações da arquitetura ePING (Padrões de Interoperabilidade de Governo Eletrônico do Brasil) [Brasil 2014]. O mecanismo proposto tem como foco garantir a privacidade dos usuários e trazer mais flexibilidade a um sistema de IdM federadas governamental ao possibilitar a agregação de atributos de múltiplos IdPs que seguem o padrão SAML[1], por meio de um cliente ativo executado na máquina do usuário.

Este artigo está organizado em seis seções. A Seção 2 apresenta os principais conceitos envolvidos no problema e na solução proposta. A Seção 3 apresenta e compara os trabalhos relacionados selecionados a partir de uma revisão sistemática da literatura. Na Seção 4, as premissas e o detalhamento do funcionamento do mecanismo agregador de atributos proposto são descritos. Os resultados experimentais relativos à implementação do mecanismo e o seu uso em uma aplicação de e-Gov são discutidos na Seção 5. Por fim, na Seção 6, são apresentadas as considerações finais.

2. Gestão de Identidades Federadas

A gestão de identidades pode ser entendida como o conjunto de processos e tecnologias usados para garantir a identidade de uma entidade (usuário ou um dispositivo), garantir a qualidade das informações de uma identidade (identificadores, credenciais e atributos) e para prover procedimentos de autenticação, autorização e auditoria [ITU 2009]. As entidades envolvidas em um sistema de IdM são: (i) usuário ou dispositivo, entidade que utiliza um serviço fornecido por um provedor de serviços; (ii) provedor de identidades (*Identity Provider* – IdP), responsável por manter a base de dados de usuários do domínio e validar suas credenciais (autenticar usuários); e (iii) provedor de serviços (*Service Provider* – SP), que oferece recursos ou serviços aos usuários.

[1] SAML é o padrão recomendado pela arquitetura E-PING e é o mais adotado por países que seguem o modelo de IdM federadas [OECD 2011][Brasil 2014] .

Dentre os modelos de IdM, no contexto de Governo Eletrônico, destaca-se o federado [OECD 2011]. Neste modelo, a tarefa de autenticação é realizada a partir de múltiplos provedores de identidades, que participam de um círculo de confiança entre diferentes domínios administrativos. Um domínio administrativo pode representar, por exemplo, uma empresa, uma universidade ou uma unidade governamental. Este domínio administrativo é composto de usuários, provedores de serviços (SPs) e um provedor de identidades (IdP). O gerenciamento de identidades federadas possibilita o compartilhamento de atributos do usuário, além da autenticação única[2] (SSO – *Single Sign On*) através de múltiplos domínios [Landau et al 2009].

Segundo [Chadwick e Inman 2013], a maioria dos sistemas de IdM federadas limita o usuário para que este escolha apenas um provedor de identidades por sessão. A introdução de mecanismos agregadores de atributos permite que, de forma segura, usuários possam acessar diferentes IdPs, o que possibilita a agregação de atributos de múltiplas fontes, sem a necessidade do usuário se autenticar separadamente em cada IdP (autenticação SSO nos IdPs). Para atender ao requisito de privacidade dos usuários, um mecanismo agregador de atributos deve inviabilizar o rastreamento das ações dos usuários e dos seus atributos de identidade [Chadwick e Inman 2013].

Na tentativa de evitar o comprometimento das informações do usuário, alguns trabalhos descritos na literatura buscam resolver o problema referente à privacidade dos usuários, por meio de soluções de IdM federadas centradas no usuário, que visam atribuir o controle das informações aos próprios usuários, já que estes são os mais habilitados a liberar os atributos em suas contas nos IdPs. Segundo [Hoellrigl et al. 2010], uma característica importante sobre os sistemas de IdM centrados nos usuários é a capacidade do usuário de poder escolher o IdP que deseja utilizar.

De acordo com [Klingenstein 2007], existem seis abordagens para implementação de mecanismos de agregação de atributos. A primeira assume que o usuário tenha um identificador único comum entre todas as autoridades de atributos. Este identificador é um nome X.500 contido em um certificado X.509, emitido por uma autoridade certificadora [Landau *et al.* 2009]. A segunda abordagem é classificada como *proxy* de identidades. Um IdP *proxy* transforma ou estende uma identidade obtida por um IdP em uma identidade que contém as informações necessárias ao SP. O IdP *proxy*, neste caso, deve ser confiável tanto para o SP que depende deste, como também pelos IdPs que disponibilizam os atributos ao IdP *proxy*. O IdP *proxy* é capaz de identificar todos os atributos sobre qualquer identidade [Chadwick et al 2010].

A terceira abordagem é considerada uma especificação de um *proxy*. Esta abordagem é denominada de proxy de retransmissão de identidade, embora as trocas de atributos no modo de retransmissão de identidade sejam semelhantes ao modelo de IdP *proxy*, neste modelo tem-se a garantia da retransmissão das asserções de atributos. Neste caso, o IdP *proxy* não irá assinar as asserções de atributos, mas sim retransmiti-las no formato original (assinadas pelo IdP original). O SP irá receber as asserções de atributos criptografadas [Chadwick et al 2010].

[2] Na autenticação única (SSO), o usuário autentica-se uma única vez em seu IdP de origem e pode acessar diferentes SPs. No caso da autenticação federada, estes SPs podem estar outros domínios administrativos.

A abordagem de agregação de atributos mediada pelo cliente faz uso de clientes inteligentes (clientes ativos) para criar solicitações de atributos aos múltiplos IdPs. Exemplos destes clientes são o ECP SAML (do inglês *Enhanced Client or Proxy*) e os clientes ativos do *CardSpace* [Klingenstein 2007]. A quinta abordagem é a federação de identidades que depende da capacidade do usuário em associar as identidades que controla fazendo a ligação entre os IdP. Um agente do usuário autenticado com sucesso em dois IdPs diferentes pode controlar ambos os IdPs e criar um identificador unidirecional persistente, permitindo que um IdP aponte para a identidade relacionada no segundo IdP. Por fim, a última abordagem possível é a mediada pelo SP. Apesar da autenticação do usuário ser única para cada IdP, o SP necessita realizar excessivos redirecionamentos para completar a agregação dos atributos [Klingenstein 2007].

3. Trabalhos Relacionados

Após a execução de um protocolo de busca (revisão sistemática), foram identificados nove trabalhos (entre 2008 e 2013) que tratam do problema da agregação de atributos e descrevem mecanismos agregadores.

Em [Lee *et al.* 2008], um modelo de agregação de atributos, que segue a abordagem de mediada pelo provedor de serviços (SP) e que utiliza a avaliação da reputação dos IdPs no processo de agregação dos atributos do usuário, é descrito. Para auxiliar a agregação, cada SP obtém os atributos dos IdPs e os armazena em seu repositório de dados local. Esta solução é simples de ser desenvolvida, mas possibilita o rastreamento das informações dos usuários por parte dos SPs, visto que este irá mediar todo o processo de agregação de atributos e viola a privacidade, ao armazenar no SP os atributos do usuário.

O trabalho proposto por [Hatakeyama e Shima 2008] apresenta uma infraestrutura para a gestão de privilégios em uma federação a fim de vincular todos os tipos de perfis dos usuários. O modelo permite que os usuários conectem suas contas de outros provedores e consigam gerenciar tais contas de forma centralizada. A proposta dos autores está na criação de um novo módulo de segurança (do inglês *Trust Server Provider* – TSP), que segue uma abordagem de *proxy* e que possibilita o rastreamento das informações dos usuários.

Em [Chadwick *et al.* 2010], é descrito um mecanismo agregador de atributos que segue a abordagem baseada em proxy e que permite que SPs autorizem solicitações de acesso dos usuários com base em atributos afirmados por vários provedores de identidade (IdP). O modelo utiliza um componente chamado de serviço de ligação (do inglês – *Linking Service* - LS), que tem por objetivo ligar as contas dos usuários que estão em diferentes IdPs. A solução proposta está baseada no protocolo SAML 2.0, porém, por se tratar de uma solução de proxy, possui as desvantagens em relação à privacidade apontadas anteriormente.

O modelo proposto por [Hoellrigl *et al*. 2010] apresenta um mecanismo de delegação de identidades controlado pelo usuário. Este delegado de identidade atua em nome do usuário quando um SP deseja acessar seus atributos, mesmo que o usuário não esteja conectado. Apesar de seguir uma abordagem centrada no usuário, o mecanismo implementa uma abordagem de agregação de retransmissão, pois este é responsável por

mediar todas as requisições do usuário, porém não armazena os atributos e não está no ambiente computacional do cliente (é uma aplicação Web).

A proposta de [Vossaert *et al.* 2010] define uma abordagem para um sistema de gestão de identidades centrada no usuário, que aborda a privacidade dos usuários. No modelo de agregação de atributos proposto pelos autores, alguns atributos do usuário podem estar disponíveis no cache do elemento seguro temporariamente. No modelo, tem-se um módulo de segurança (*Trusted Module* - TM) para cada usuário, que é representado por um cartão inteligente (*smart card*) que fica de posse do usuário. Esse cartão permite que os usuários possam interagir com o sistema. Esta proposta, por ser centrada no usuário e mediada pelo cliente, favorece a garantia de privacidade dos usuários, mas é apenas uma abordagem conceitual que não foi implementada e avaliada. Além disso, a solução não adota nenhum padrão de interoperabilidade para lidar com identidades de IdPs heterogêneos (solução proprietária implementada no *smartcard*).

O trabalho proposto por [Hulsebosh *et al*. 2011], apresenta uma plataforma de colaboração virtual (do inglês *Virtual Collaboration Platform* - VCP) para a *SURFnet*. A plataforma aproveita a infraestrutura da federação acadêmica já existente, que se baseia no padrão *SAML2*. Esta plataforma implementa um mecanismo agregador de atributos no formato de *proxy* ou retransmissão, conforme desejado.

[Chadwick et al 2011] estendem o seu trabalho anterior para integrar ao projeto *Logins4Life* que visa o uso das contas sociais dos usuários da comunidade acadêmica para obter acesso às ferramentas disponibilizadas pelas instituições. No mecanismo proposto, os autores definiram um provedor de serviço confiável (*Trusted Service Provider* - *TSP*) responsável por ligar as diferentes contas dos usuários. O TSP visa ainda prover segurança à base de dados com os atributos do usuário e contêm um *proxyIdP*. Semelhante ao trabalho anterior, este trabalho segue a abordagem baseada em *proxy* e possibilita ainda o armazenamento de atributos dos usuários (de diferentes IdPs), o que prejudica o requisito de privacidade dos usuários.

Com objetivo de aprimorar a preservação de privacidade no processo de agregação de atributos, [Chadwick et al 2003] definiram o *Trusted Attribute Aggregation Service – TAAS*, responsável por coletar e agregar os atributos de um usuário a ser entregue para o SP. Ao contrário dos trabalhos anteriores, este serviço não armazena os atributos dos usuários e, de forma semelhante, a um seletor de identidades do CardSpace permite que um usuário selecione quais atributos de quais IdPs serão encaminhados a um dado SP. A diferença está que o TAAS não é um cliente ativo, mas sim uma aplicação web (*proxy*). Outra característica desta solução é que o usuário precisará se autenticar em cada IdP para que este emita a asserção SAML com seus atributos para evitar a rastreabilidade dos atributos do usuário por parte de um IdP.

A Tabela 1 apresenta um resumo comparativo dos trabalhos relacionados considerando as seguintes características: (1) se a proposta foi implementada e avaliada, (2) as tecnologias de IdM adotadas na definição da proposta, (3) o padrão de interoperabilidade utilizado e (4) qual a abordagem de agregação de atributos que a proposta implementa. Dentre os modelos e mecanismos de agregação de atributos apresentados, a abordagem de *proxy* de identidades se mostrou a mais comum.

Como visto anteriormente, a abordagem mediada pelo cliente busca evidenciar a privacidade dos usuários no uso do mecanismo agregador [Klingenstein, 2007]. A

justificativa para a pouca adoção desta abordagem se deve à dificuldade de prover a autenticação SSO, uma vez que nas soluções citadas que fazem uso desta abordagem, o usuário deve se autenticar várias vezes em diferentes provedores de identidades. Somente o trabalho de [Vossaert *et al* 2010] apresenta uma proposta que segue a abordagem mediada pelo cliente (faz uso de um cliente ativo) baseada no uso de *smartcards*, porém, esta proposta não foi implementada e avaliada. O mecanismo agregador proposto neste trabalho e o seu diferencial diante das soluções apresentadas estão indicados na Tabela 1 e descritos nas próximas seções.

Tabela 1: Tabela comparativa dos Trabalhos Relacionados

TRABALHOS RELACION.	IMPL.	TECNOLOGIAS DE IDM ADOTADAS	PADRÃO DE INTEROPERABILID.	ABORDAGEM DA AGREGAÇÃO DE ATRIBUTOS
Lee et al. (2008)	Não	Apenas modelo conceitual	XML	Mediado pelo SP
Hatakeyama e Shima (2008)	Não	OpenID, CardSpace, SAML, OAuth	SAML	Proxy
Chadwick *et al.* (2010)	Sim	SAML	SAML	Proxy
Hoellrigl *et al.* (2010)	Sim	CardSpace, Active Directory Federation Services	WS-Trust	Retransmissão
Vossaert et al. (2010)	Não	OpenID, Shibboleth, CardSpace	-	Mediado pelo Cliente
Chadwick et al. (2010)	Sim	SAML, OpenID, OAuth	SAML	Proxy
Hulsebosch (2011)	Sim	SAML, OAuth	SAML, Protocolo *OpenSocial*	Proxy ou Retransmissão
Chadwick et al (2011)	Sim	SAML, Facebook Connect, OAuth, OpenID	SAML	Proxy
Chadwick et al (2013)	Sim	SAML	XML e SAML	Retransmissão
Modelo Proposto	**Sim**	**SAML**	**SAML e Schemas XML**	**Mediado pelo Cliente**

4. Mecanismo Agregador de Atributos Baseado em Cliente Ativo

O governo brasileiro ainda não definiu a estratégia nacional de gestão de identidades a ser adotada nas aplicações de Governo Eletrônico. O que existe é apenas a arquitetura ePING, que traz algumas diretrizes para definição de estratégias de interoperabilidade entre sistemas [Brasil 2014]. Dentre estas, destacam-se o uso do SAML como padrão para a troca de informação sobre autenticação e autorização entre domínios, da especificação WS-Security 1.1 para o fornecimento de segurança às mensagens trocadas e WS-Trust 1.4 para a gestão de relacionamentos confiáveis (intermediação).

Para conceber uma estratégia nacional de gestão de identidades federadas para o governo brasileiro, um dos problemas que precisa ser solucionado é a agregação de atributos de identidades de um usuário (cidadão). Poder agregar de forma segura atributos que estão distribuídos em diferentes IdPs proverá uma maior flexibilidade a esta estratégia. É comum um cidadão possuir atributos de identidade distribuídos em diferentes provedores, tais como os do DETRAN, polícia federal, receita federal, sistema único de saúde entre outros. Alguns serviços governamentais, como a emissão de passaportes, exigem que um usuário apresente atributos que podem estar distribuídos

em múltiplos IdPs. Este trabalho descreve um mecanismo agregador de atributos mediado pelo cliente que atende as recomendações da arquitetura ePING, que garanta a privacidade dos usuários e que visa trazer mais flexibilidade a um sistema de gerenciamento de identidades federadas governamental.

Visando impedir a rastreabilidade dos atributos de identidade do usuário, possível nas soluções baseadas em *proxy*, o mecanismo agregador proposto segue a abordagem mediada pelo cliente, com o diferencial de ser alinhado à arquitetura ePING. O procedimento de agregação é executado por um aplicativo no ambiente operacional do usuário, chamado de cliente ativo. O mecanismo agregador gerencia ainda pseudônimos, conforme definido na especificação SAML, para aumentar a privacidade do usuário e dificultar o rastreamento de suas informações nos SPs.

O mecanismo agregador proposto assume algumas premissas. A primeira está na existência de uma federação governamental. Esta federação deve envolver todas as esferas governamentais, tais como: governos federal, estadual e municipal. Nesta federação, existem provedores de identidades (IdPs) e provedores de serviços governamentais (SPs) que possuem relações de confiança e que estão em conformidade com a especificação SAML. E, por fim, considera-se como premissa que o código do mecanismo agregador foi homologado e assinado por uma entidade confiável da federação. IdPs e SPs devem ainda seguir outras diretrizes de interoperabilidade da arquitetura ePING, como o uso de Serviços *Web RESTful*, o uso do protocolo SSL e o padrão XML (como linguagem de intercâmbio de dados).

Dentro da federação governamental considerada, um usuário (cidadão) tem atributos distribuídos em múltiplos IdPs. Um SP que oferece serviços governamentais via Internet pode requerer um subconjunto desses atributos de um usuário para prover determinados serviços. Para coletar esse subconjunto de atributos, utiliza-se do mecanismo agregador de atributos, que em nome e com a aprovação do usuário coleta os atributos em diversos IdPs e os compartilha com o SP. O mecanismo agregador não compartilha qualquer informação sem o consentimento do usuário.

A Figura 1 ilustra a visão geral do mecanismo agregador proposto. Alguns novos serviços foram definidos para integração do mecanismo agregador de atributos aos serviços de uma federação. O SDPCA, Serviço de Descoberta de Provedor de Cliente Ativo, é responsável por apresentar ao usuário uma lista de provedores de aplicativos de cliente ativo[3] homologados pelo governo. Caberá ao usuário indicar o provedor de cliente ativo (PCA) em que confia para fazer o download do aplicativo. É importante destacar que tanto o SDPCA, quanto os PCAs devem ser SPs da federação (estão no círculo de confiança da federação). Em todas as trocas, utiliza-se o protocolo SSL para estabelecer um canal seguro de comunicação entre as entidades envolvidas.

No passo 1 da Figura 1, o usuário, por intermédio de seu navegador Web, tenta acessar um serviço da federação. 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 usuário informar os dados para a autenticação (passo 2a), o IdP autentica o usuário, emite uma asserção de atributos para este (passo

[3] O software de cliente ativo pode ser desenvolvido por órgãos do governo ou também por empresas privadas, porém, estes precisarão passar por um processo de homologação.

2b) e redireciona o navegador para o SP (passo 3a). Para concretizar a ação solicitada pelo usuário, o SP indica quais atributos do usuário este necessita (passo 3b). Neste momento, o usuário deve confirmar que deseja prosseguir com o processo de agregação de atributos. Para obter o software do cliente ativo, responsável pela agregação (passo 4), o navegador do usuário é redirecionado para o SDPCA mantido pela federação.

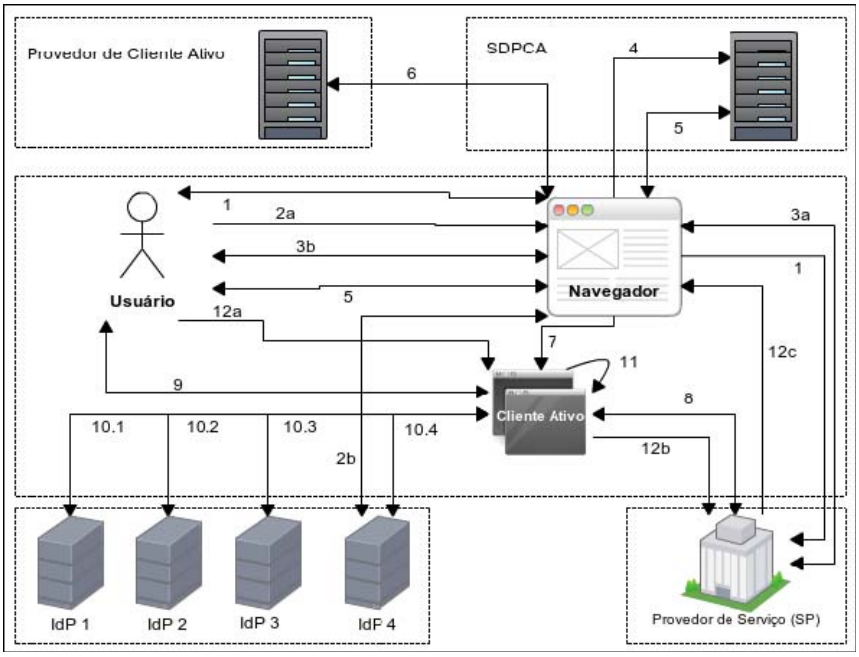

Figura 1- Visão geral do mecanismo agregador de atributos proposto.

Após o usuário selecionar um dos PCAs (passo 5), o navegador do usuário é redirecionado para o provedor selecionado para fazer o *download* da aplicação de cliente ativo (passo 6). Após o *download* do cliente ativo, este é executado no ambiente operacional do usuário (passo 7). Para efetuar a agregação de atributos, o cliente ativo deve solicitar ao SP a asserção assinada que indica os atributos necessários (passo 8). Os atributos necessários são apresentados ao usuário para que este indique quais IdPs deseja utilizar para cada atributo (passo 9). Como a autenticação SSO é garantida, o usuário precisa se autenticar, via cliente ativo, apenas no primeiro IdP indicado (passo 10.1), os demais aceitam o *token* de autenticação emitido pelo IdP e respondem à solicitação de atributos (passo 10.2, 10.3 e 10.4).

No passo 11, o cliente ativo efetua a agregação de atributos. No passo 12a, o cliente ativo solicita que o usuário confirme a liberação dos atributos e então encaminha (passo 12b) os atributos agregados para o SP. De forma semelhante a abordagem de retransmissão, o cliente ativo não irá assinar as asserções de atributos, mas sim retransmiti-las no formato original (assinadas pelo IdP original). Logo, qualquer violação das asserções recebidas feita na máquina do usuário[4] pode ser detectada pelo SP. O SP de posse dos atributos enviados (passo 12c) poderá permitir ou não o acesso ao serviço solicitado pelo usuário.

Nos passos da autenticação do usuário (passos 2 e 10), recomenda-se que os IdPs utilizem métodos de autenticação que evitem a adivinhação de senhas (ataque de

[4] Considerando que o ambiente de execução do usuário possa ser malicioso.

força bruta). Recomenda-se o uso de mecanismos de autenticação mais fortes que os baseados em senha, mas que podem ser utilizados implementados via cliente ativo. Por exemplo, certificados digitais ou autenticação de dois fatores que combinem uma prova de posse (e.g. celular). Para algumas aplicações governamentais, o uso de uma identidade digital (*smartcard*) ou o novo RIC (Registro de Identidade Civil Brasileiro) pode ser exigido para prover esta autenticação forte baseada em certificados digitais.

O processo de agregação de atributos pode ser classificado como dinâmico ou estático e transitório ou permanente [Chadwick et al. 2010]. O mecanismo agregador proposto oferece três modos de funcionamento. O primeiro modo é o transitório dinâmico. Neste modo, não há uma política de liberação de atributos pré-definida para os SPs (dinâmico) e o usuário precisará se autenticar em cada IdP que solicitar atributos (transitório). Neste modo, a autenticação SSO nos IdPs[5] não é suportada.

O segundo modo é o permanente dinâmico. Neste modo, ainda não há uma política de liberação de atributos pré-definida para os SPs (dinâmico). Além disso, neste modo, a autenticação SSO é garantida para solicitar atributos em múltiplos IdPs (permanente). Neste caso, o *token* de autenticação do primeiro IdP é compartilhado e aceito nos demais IdPs. E, por fim, o terceiro modo que é o permanente estático. Neste modo, o usuário pode criar uma política de liberação de atributos após o processo de agregação, assim como pode salvar informações sobre quais escolhas de IdP foram feitas pelo cliente ativo. Além disso, a autenticação SSO nos IdPs é garantida. Todos os modos exigem o consentimento do usuário para liberação de atributos.

Um padrão para as trocas de mensagens entre os provedores de serviço e o Cliente Ativo foi definido com estruturas de esquemas de dados XML (*XML Schemas*). Estes esquemas padronizam as requisições de atributos enviadas ao cliente Ativo (ver exemplo na Figura 2.a) e também a resposta da agregação de atributos com as asserções SAML (ver exemplo na Figura 2.b) que devem sem compartilhadas com os SPs.

```
1  <?xml version="1.0" encoding="UTF-8"?>
2  <SAMLAgregator>
3    <SAMLRequest>
4      <attribute>CPF</attribute>
5    </SAMLRequest>
6    <SAMLRequest>
7      <attribute>TITULOELEITOR</attribute>
8    </SAMLRequest>
9    <SAMLRequest>
10     <attribute>RG</attribute>
11   </SAMLRequest>
12 </SAMLAgregator>
```

a. *XML Request*

```
1  <?xml version="1.0" encoding="UTF-8"?>
2  <SAMLAgregator>
3    <SAMLResponse>
4      <attribute>CPF</attribute>
5      <SAML>SAML...SAML</SAML>
6    </SAMLResponse>
7    <SAMLResponse>
8      <attribute>RG</attribute>
9      <SAML>SAML...SAML</SAML>
10   </SAMLResponse>
11   <SAMLResponse>
12     <attribute>TITULOELEITOR</attribute>
13     <SAML>SAML...SAML</SAML>
14   </SAMLResponse>
15 </SAMLAgregator>
```

b. *XML Reply*

Figura 2- Exemplos de um pedido e de uma resposta de atributos

5. Implementação e Resultados

Com o objetivo de avaliar (1) a flexibilidade proporcionada com o uso do mecanismo agregador de atributos proposto, (2) o impacto sobre a interoperabilidade do sistema de

[5] Vale ressaltar que a autenticação SSO nos SPs é garantida.

gerenciamento de identidades adotado, (3) a privacidade e a (4) usabilidade dos usuários ao fazer uso do cliente ativo, um protótipo do mecanismo agregador de atributos foi desenvolvido e integrado a um cenário fictício de solicitação de emissão de passaporte.

O processo de emissão de passaporte é demorado e burocrático. A Polícia Federal exige a apresentação de alguns documentos que comprovem a identidade do cidadão, tais como: Registro de Geral (RG), Título de Eleitor, Documento de Cadastro de Pessoa Física (CPF). Após efetuar o cadastro das informações e pagar a taxa do serviço, o cidadão deve apresentar seus documentos originais em uma agência de atendimento, para então, recolher as digitais e fotografia do cidadão. Este procedimento não evita a apresentação de documentos falsificados. Pode-se tornar este procedimento automático e mais seguro se os atributos do usuário forem coletados diretamente nos IdPs da Federação Governamental com o uso do mecanismo agregador de atributos.

O uso do mecanismo agregador, neste cenário, contemplou os seguintes passos: (1) o usuário, por meio do navegador Web, acessa o SP da Polícia Federal (PF). Como o serviço exige que o usuário se autentique, o navegador é redirecionado para o IdP de confiança do SP da PF; (2) o usuário se autentica no provedor de identidades (login e senha) e o seu navegador é redirecionado de volta para o SP da PF; (3) após o usuário indicar que consente com o processo de agregação de atributos, o navegador é redirecionado para o provedor SDPCA; (4) o usuário seleciona o provedor para realizar o *download* do cliente ativo e o seu navegador é redirecionado para o site do provedor escolhido; (5) o usuário efetua o download da aplicação e executa o aplicativo de cliente ativo em sua máquina. Em seguida, o cliente ativo obtém a lista de atributos requeridos pela aplicação (conforme Figura 2.a); (6) o cliente ativo apresenta os atributos e solicita que o usuário indique quais IdPs contêm os atributos requeridos; (7) após indicar os IdPs para cada atributo, o usuário se autentica em cada IdP para que o cliente ativo recolha e reúna as asserções de atributos; e (8) por fim, o cliente ativo agrega as asserções SAML (sem modificá-las) e as envia para o SP da polícia federal (Figura 2.b).

Para o desenvolvimento do protótipo de cliente ativo, foi escolhida a plataforma Java por oferecer portabilidade e por oferecer uma solução robusta para o desenvolvimento de códigos de execução remota (aplicativos *Java Web Start* - JWS). A tecnologia JWS permite que um aplicativo, que está disponível em um provedor, seja migrado para a máquina do usuário e seja executado em seu ambiente operacional[6]. Vale destacar ainda que o aplicativo JWS é assinado digitalmente pelo PCA. Os provedores de serviços SPDCA, PCA e o serviço para emissão de passaporte que foram utilizados nos experimentos de avaliação do mecanismo proposto foram desenvolvidos em PHP e o Apache foi o servidor Web utilizado. Todos os SPs fazem uso de certificados digitais SSL. Os IdPs utilizados nos experimentos estão de acordo com a especificação SAML2 e foram implementados utilizado o *framework simpleSAMLPHP*.

Após a execução de testes de software funcionais e não funcionais (incluindo os de segurança), realizou-se um experimento que envolveu especialistas que trabalham ou prestam serviços para o governo e a aplicação. Estes especialistas, após o uso do protótipo, responderam uma pesquisa de satisfação (teste de usabilidade). Nesta

[6] O *Java Web Start* é iniciado automaticamente quando é feito o primeiro *download* do aplicativo Java que utiliza essa tecnologia.

primeira fase de avaliação qualitativa (e subjetiva) do mecanismo, foi utilizado o modo transitório dinâmico sem autenticação SSO nos IdPs.

A pesquisa de satisfação foi respondida por quinze (15) profissionais de TI que trabalham em instituições governamentais e por vinte e quatro (24) de profissionais de TI que trabalham em empresas que prestam serviços de TI para o governo, totalizando trinta e nove (39) avaliadores. A aplicação dos questionários serviu para detectar o nível de satisfação dos avaliadores no que tange a utilização do mecanismo agregador de atributos. A seguir, alguns dos resultados obtidos são analisados.

A primeira parte da pesquisa foi dedicada a identificar o conhecimento dos avaliadores em relação a alguns conceitos sobre gestão de identidades (autenticação SSO, IdPs, autenticação federada, SAML, OpenID, OAuth). Com relação a autenticação SSO, 76.9% dos avaliadores responderam ter conhecimento, outros 56.4% sabem o significado de autenticação federada e 66.7% responderam ter conhecimento sobre o que é um IdP. A respeito do SAML, apenas 35.5% dos avaliadores responderam conhecer a tecnologia. Constatou-se que o conhecimento geral dos avaliadores que participaram da pesquisa é limitado, em especial, referente aos conceitos e tecnologias relacionados à gestão de identidades federadas (e.g. SAML).

A pesquisa identificou se as ações no protótipo partiram de uma ação do avaliador (ver Figura 3.a) e se as mensagens de erro (caso tenham ocorrido) ajudaram a resolver o problema (ver Figura 3.b). Os resultados apresentados demonstram que a maioria dos avaliadores respondeu que o protótipo exigiu sua ação. Este resultado é positivo uma vez que o usuário precisa ter consciência de suas ações sobre o sistema e confirma que o protótipo é centrado no usuário. Referente aos erros do sistema, apenas 7.7% dos avaliadores responderam que as mensagens de erros não foram suficientes para contornar o problema. Logo, diante da ocorrência de erros, na maioria das vezes, o sistema contribui para resolução destes.

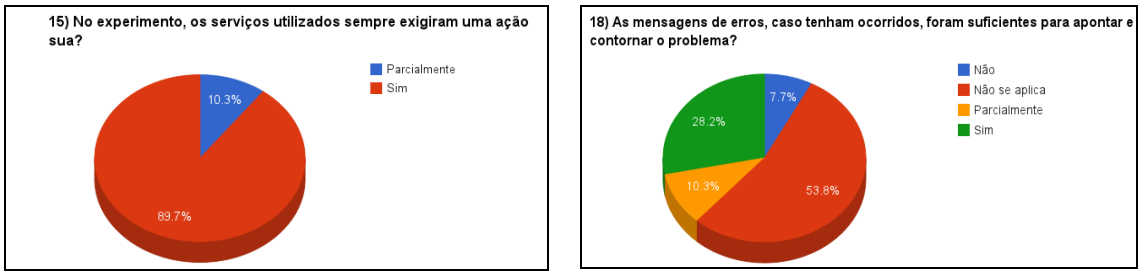

Figura 3 – Resultados da Pesquisa de Satisfação (ações do usuário e msgs de erro)

A Figura 4.a aponta que 76.9% dos avaliadores se sentiram confortáveis durante o uso do mecanismo, o que demonstra uma boa satisfação dos usuários. Alguns dos avaliadores que não se sentiram confortáveis foram os que não conseguiram executar todo o experimento. Outros por acharem o processo “burocrático” diante da necessidade de tantos consentimentos do usuário e de autenticação em todos os IdPs (ausência da autenticação SSO). Outro motivo reportado pelos avaliadores se refere ao uso de

certificados autoassinado[7]. Por fim, um avaliador apontou que o uso do aplicativo executado na máquina do usuário não lhe agrada, que este prefere que todo o processo de agregação seja executado em páginas Web. Não é possível na abordagem mediada pelo cliente esta solicitação do avaliador.

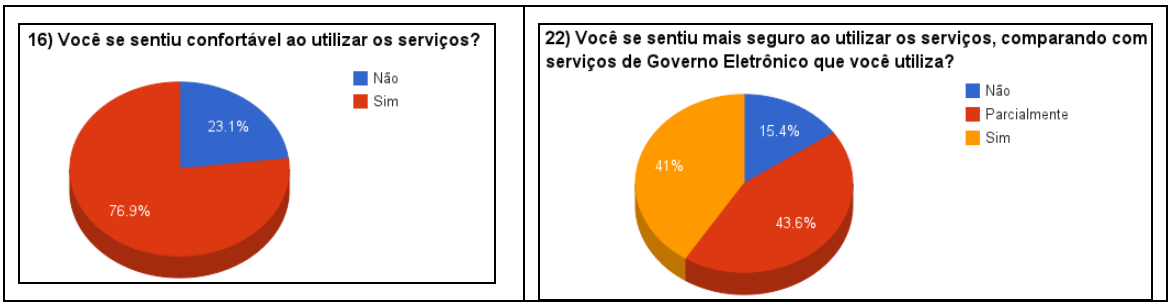

Figura 4 – Resultados da Pesquisa de Satisfação (uso e segurança da aplicação)

Dentre os avaliadores do protótipo do mecanismo, apenas seis responderam não se sentirem seguros ao usar o serviço (Figura 4.b). Dentre estes, quatro não conseguiram completar a execução do experimento e os demais não apontaram seus motivos. É possível que estes consideram os atuais serviços de e.gov seguros ou que o uso de certificados autoassinados prejudicaram este item de avaliação.

Conforme a Figura 5a, a maioria, 97.4% das pessoas que participaram da pesquisa responderam que gostariam de utilizar o mecanismo agregador de atributos em aplicações de governo eletrônico. Verificou-se ainda que apenas um avaliador respondeu que não indicaria a ferramenta. Este avaliador não conseguiu executar todo o experimento e não indicou seus motivos.

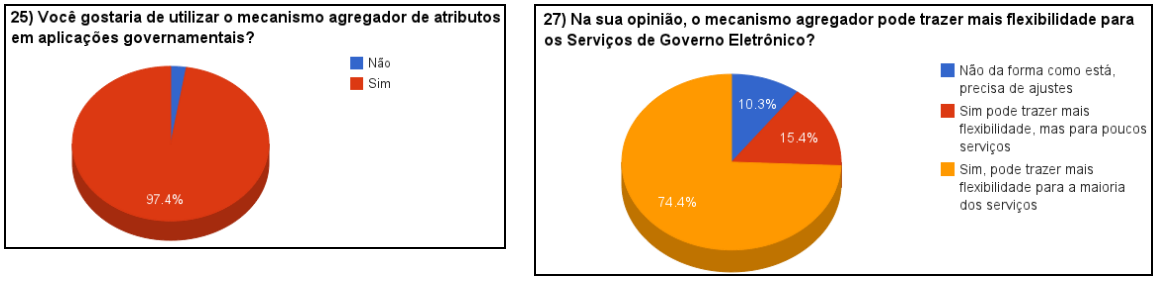

Figura 5: Resultados da Pesquisa (Uso e flexibilidade em serviços de e-Gov)

Em relação à flexibilidade do mecanismo proposto (ver Figura 5b), a maioria dos avaliadores responderam que a solução proposta pode trazer mais flexibilidade para a maioria dos serviços de e-Gov. Os 10,3% que indicam que o sistema necessita de ajustes foram os que não conseguiram executar todos os passos do experimento ou foram os que indicaram a necessidade da autenticação SSO nos IdPs.

Referente à privacidade dos usuários (ver Figura 6), a maioria dos avaliadores respondeu que o mecanismo agregador de atributos pode garantir a privacidade dos

[7] Foi indicado que estes certificados estavam sendo usados por ser tratar de um protótipo experimental e que em um serviço real seriam usados certificados confiáveis, mesmo assim alguns avaliadores criticaram o uso destes certificados.

usuários no processo de coleta de seus atributos. Alguns dos que não avaliam como possível, tiveram problemas na execução do experimento.

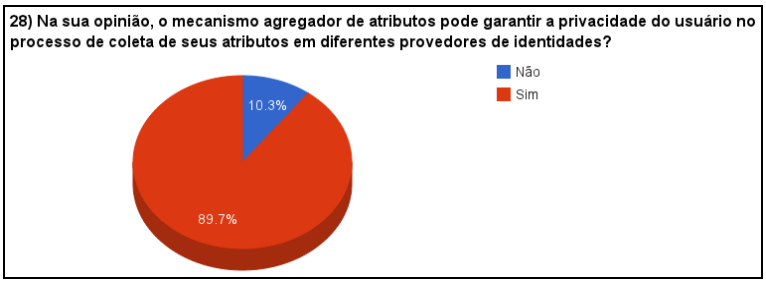

Figura 6: Resultados da Pesquisa de Satisfação (Privacidade dos Usuários)

Em relação à portabilidade do cliente ativo, todos os avaliadores que seguiram as instruções (e.g. não usar *tablets* ou *smartphones*, navegadores web atualizados e máquina virtual Java – JRE 7) executaram com sucesso o experimento.

Segundo os avaliadores existem alguns impactos negativos para os desenvolvedores de aplicação de e.gov na utilização do mecanismo agregador de atributos proposto, tais como: o "Redesenvolvimento" dos mecanismos de autenticação, o que estaria concentrado nos IdPs e não nos SPs como ocorre hoje; a necessidade de aprender uma nova tecnologia, o SAML; a barreira em aceitar que atributos de outros IdPs possam ser utilizados, o que identifica-se uma falta de conhecimento dos benefícios da autenticação SSO federada. Quanto as sugestões do que pode ser melhorado no mecanismo, os avaliadores indicaram: (1) autenticação SSO nos IdPs; (2) política de liberação de atributos para SPs; (3) criação de uma API e documentação para integração e uso do mecanismo agregador de atributos em aplicações de e-Gov.

Na segunda fase de avaliação, foi implementado o modo permanente dinâmico que oferece a autenticação SSO nos IdPs. Na solução, um IdP central é o responsável por autenticar os usuários e prover o *token* de autenticação que é repassado aos demais IdPs. Após a autenticação bem sucedida do usuário, o IdP central, conforme suportando no *simpleSAMLPHP*, indica ao cliente ativo os redirecionamentos que precisam ser efetuados para os IdPs que detêm os atributos requeridos e indicados pelo usuário. De forma semelhante a um navegador, o cliente ativo implementa os redirecionamentos HTTP. Após a implementação, novos testes de software foram executados para verificar o atendimento aos requisitos funcionais e não funcionais de segurança e portabilidade.

6. Conclusão

Diante do desenvolvimento do mecanismo agregador de atributos mediado pelo cliente, da comprovação da aplicabilidade do mecanismo agregador de atributos no cenário de emissão de passaportes, das análises em relação à privacidade, flexibilidade e usabilidade realizadas, é possível afirmar que os objetivos desse trabalho foram atingidos e que a abordagem mediada pelo cliente é viável no cenário de e-Gov.

O mecanismo agregador de atributos apresentado neste artigo inova em relação aos trabalhos relacionados, ao prover uma solução que evita a rastreabilidade dos atributos do usuário, por meio de uma abordagem mediada pelo cliente alinhada à arquitetura ePING. O mecanismo proposto tem como objetivo trazer mais flexibilidade para uma estratégia nacional de gestão de identidades federadas e centrada no usuário.

Por fim, como trabalhos futuros, pretende-se implementar e avaliar o modo permanente dinâmico (definição de uma política de liberação de atributos. Pretende-se ainda implementar o cliente ativo em um cartão inteligente (*tamper-resistant smartcard*) para proteger contra ataques de plataformas de execução maliciosas (ambiente de execução do cliente ativo).

Referências

Baldoni, R. (2012).Federated Identity Management System in e-Government: the Case of Italy, *Electronic Government, an International Journal*, v. 9, no. 1, pp. 64-84.

BRASIL, Comitê Executivo de Governo Eletrônico (2014). ePING – Padrões de Interoperabilidade de Governo Eletrônico. Disponível em: <http://www.governoeletronico.gov.br/acoes-e-projetos/e-ping-padroes-de-interoperabilidade>. Acesso em: 04 Jul. 2014.

Chadwick, D; Innman, G. Klingenstein, N. (2010). A Conceptual model for Attribute Aggregation, *Future Generation Computer Systems*. vol. 26, no.7, pp.1043-1052.

Chadwick, D.; Inman. G. Siu, K. W . S. Ferdous, M. S (2011). Leveraging Social Networks to Gain Access to Organisational Resources. Proceedings of the 7th ACM workshop on Digital identity management. p. 43-52.

Chadwick, D.; Inman, G., (2013). The Trusted Attribute Aggregation Service (TAAS) - Providing an Attribute Aggregation Layer for Federated Identity Management. Eighth International Conference on Availability, Reliability and Security (ARES), pp.285-290.

Hatakeyma, M.; Shima, S. (2008). Privilege Federation between Different User Profiles for Service Federation, *ACM Conference on Computer and Communications Security*, pp.41-50, New York.

Hoellrigl, T., Kühner, H.; Dinger, J.; Hartenstein, H. (2010). User-Controlled Automated Identity Delegation, *Network and Service Management*, pp. 230-233, Niagara Falls.

Hulsebosch, B.; Wegdam, M.; Zoetekouw, B; Dijk, N.; Poortinga, R. (2011). Virtual collaboration attribute management, *Surf Net: GigaPort3*, vol.1, Sep, 2011.

ITU (2009). Ngn identity management framework. Recommendation Y.2720.

Klingenstein, N. (2007). Attribute Aggregation and Federated Identity, *International Symposium on Applications and the Internet Workshops (SAINTW'07)*, pp. 15-19.

Landau, S.; Gong, H.; Wilton, R. (2009). Achieving Privacy in a Federated Identity Management System, *Financial Cryptography and Data Security*, pp. 51-70, Barbados.

Lee, J. W.; Kim, H.; Hong, J. S.; (2008). An Attribute Aggregation Architecture with Trust-Based Evaluation for Acess Control, *Network Operations and Management Symposium*. pp. 1011-1014, Salvador, 2008.

OECD (2011), National Strategies and Policies for Digital Identity Management in OECD Countries, *OECD Digital Economy Papers*, no. 177, OECD Publishing, 2011.

Vossaert, J.; Lapon, J.; Decker, B. D.; Naessens, V. (2010). User-Centric Identity Management Using Trusted Modules, *European Workshop*, pp.155-170, Atenas.

