

**MARCONDES MAÇANEIRO**

**UM MECANISMO AGREGADOR DE ATRIBUTOS MEDIADO  
PELO CLIENTE ALINHADO AO PROGRAMA DE EGOV.BR**

Itajaí (SC), Agosto de 2013



**UNIVALI**

**UNIVERSIDADE DO VALE DO ITAJAÍ**  
**CURSO DE MESTRADO ACADÊMICO EM**  
**COMPUTAÇÃO APLICADA**

**UM MECANISMO AGREGADOR DE ATRIBUTOS MEDIADO  
PELO CLIENTE ALINHADO AO PROGRAMA DE EGOV.BR**

por

**Marcondes Maçaneiro**

Dissertação apresentada como requisito parcial à  
obtenção do grau de Mestre em Computação  
Aplicada.

Orientadora: Michelle Silva Wangham, Dr.

Itajaí (SC), Agosto de 2013

## **AGRADECIMENTOS**

Gostaria de agradecer aos meus familiares, minha esposa Greice Niggemann, minha filha Letícia Maçaneiro e minha mãe Cecília Maçaneiro que acompanharam de perto todas as angustias e esforços para realizar este mestrado. São os agradecimentos de um Marido, Pai e Filho que em muitos momentos deve que ficar distantes devido às necessidades de estudo.

Gostaria de agradecer imensamente a minha orientadora Michelle Silva Wangham, que contribuiu muito para a melhoria do meu conhecimento. Uma pessoa muito especial, dedicada, uma segunda mãe.

Gostaria também de agradecer a todos meus amigos, colegas de mestrado, de trabalho, que acompanharam muitas das fases para a conclusão desse mestrado.

# **UM MECANISMO AGREGADOR DE ATRIBUTOS MEDIADO PELO CLIENTE ALINHADO AO PROGRAMA DE EGOV.BR**

Marcondes Maçaneiro

Agosto / 2013

Orientadora: Michelle Silva Wangham, Dr.

Área de Concentração: Computação Aplicada

Linha de Pesquisa: Sistemas Embarcados e Distribuídos

Palavras-chave: Agregação de Atributos, Identidades Federadas, Governo Eletrônico.

Número de páginas: 193

## **RESUMO**

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 as aplicações de Governo Eletrônico. A agregação de atributos é um mecanismo que pode ser utilizado em conjunto com os sistemas de gerenciamento de identidades federadas para promover o compartilhamento dos atributos dos usuários coletados de múltiplos provedores de identidades. Dentre as propostas de mecanismos agregadores de atributos, destacam-se as baseadas em *proxy*. Estas soluções têm vantagens quanto à sua implementação, porém, devido ao uso de uma terceira parte confiável que possa rastrear as interações entre o usuário e os provedores de identidade e de serviço, estas soluções não garantem a privacidade dos usuários. O objetivo deste trabalho é prover a agregação de atributos de 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 a recomendações da arquitetura E-PING (Padrões de Interoperabilidade de Governo Eletrônico do Brasil). A pesquisa realizada envolveu: (1) uma revisão bibliográfica sobre IdM; (2) a análise dos trabalhos relacionados; (3) a concepção de um mecanismo agregador de atributos implementado em um cliente ativo; (4) o desenvolvimento de um protótipo que faz uso do mecanismo proposto, e, por fim, (5) a avaliação do mecanismo por meio de testes de software, da aplicação de uma pesquisa de satisfação de usuários e comparação do mecanismo proposto com os trabalhos relacionados. Os resultados obtidos demonstram que o mecanismo agregador proposto traz mais flexibilidade para um sistema gestão de identidades federadas ao permitir que provedores de serviços possam exigir atributos de múltiplos provedores de identidades. Comprovou-se também nos experimentos que o mecanismo, implementado em um aplicativo executado no ambiente do usuário, garante a privacidade dos usuários sem prejudicar a interoperabilidade do sistema de IdM e da aplicação de E.Gov analisada. Entretanto, observou-se nos experimentos que a usabilidade da aplicação de E.Gov pode ser afetada devido à necessidade de o usuário ter consciência do processo de agregação.

# **A CLIENT-MEDIATED ATTRIBUTE AGGREGATION MECHANISM ALIGNED WITH THE EGOV.BR PROGRAM**

Marcondes Maçaneiro

August / 2013

Advisor: Michelle Silva Wingham, Dr.

Area of Concentration: Applied Computer Science

Research Line: Embedded System

Keywords: Aggregation, Federated Identities, Electronic Government.

Number of pages: 193

## **ABSTRACT**

Federated Identity Management Systems (IdM) allow sharing of user attributes and single authentication across multiple domains, becoming facilitators for Electronic Government Applications. Attribute aggregation is a mechanism that can be used in conjunction with the management systems of federal entities, to promote a sharing of user attributes collected from multiple identity providers. Among the proposed attribute aggregation mechanisms are proxy-based ones. These solutions have advantages in terms of their implementation, however, due to the fact that they use a trusted third party that can track the interactions between the user and the identity providers and the service, these solutions do not guarantee users' privacy. The objective of this work is to provide aggregation of user attributes, which are distributed in multiple identity providers, ensuring privacy, through an attribute aggregation mechanism that is mediated by the client and is in line with the recommendations of the E- PING architecture (Standards of Interoperability of Electronic Government in Brazil). The research involved: (1) a literature review of IdM, (2) analysis of related works, (3) designing an attribute aggregation mechanism to be implemented in an active client, (4) developing a prototype that uses the proposed mechanism, and, finally, (5) evaluating the mechanism by means of software testing, applying a user satisfaction survey and comparing the proposed mechanism with other, related works. The results demonstrate that the proposed aggregator mechanism brings more flexibility for management systems of the federal entities, enabling service providers to request attributes from multiple identity providers. It was also shown, in the experiments, that the mechanism, implemented in an application running in the user environment ensures users' privacy, without sacrificing the interoperability of the IdM system or the E.Gov application analyzed. However, it was observed in experiments that the usability of the E.Gov application may be affected by the need for the user to be aware of the aggregation process.

## LISTA DE ILUSTRAÇÕES

Figura 1. Propensão ao uso da internet na obtenção de um serviço de governo no Brasil. ....	30
Figura 2. Classificação dos modelos de gerenciamento de identidade. ....	35
Figura 3. Exemplo de pseudônimo de atributo SAML .....	43
Figura 4. Banco de Dados SP.....	48
Figura 5. Coleta de Atributos.....	55
Figura 6. Fluxo de mensagens do modo permanente estático para a agregação de atributos.....	58
Figura 7. Exemplo de autorização inicial, para um cenário com <i>três IdPs</i> .....	60
Figura 8. Exemplo de atualização dos atributos de usuário, em um cenário com três IdPs .....	61
Figura 9. Visão geral da arquitetura.....	63
Figura 10. Fluxo de Informações necessários para acessar o ShinTau portal DAMES.....	64
Figura 11. Visão geral do funcionamento com o proxyIdP .....	66
Figura 12. Modelo de federação de privilégios.....	69
Figura 13. Visão geral do mecanismo agregador de atributos proposto .....	78
Figura 14. Diagrama de sequência modo transitório dinâmico .....	83
Figura 15. Diagrama de sequência modo permanente dinâmico .....	84
Figura 16. Diagrama de sequência modo permanente estático .....	85
Figura 17. XML Schema de requisição da lista de atributos .....	86
Figura 18. XML Request .....	87
Figura 19. XML <i>Schema</i> de resposta com os atributos agregados .....	87
Figura 20. XML de resposta .....	88
Figura 21. Diagrama de Sequência Parcial 1 .....	99
Figura 22. Diagrama de Sequência Parcial 2 .....	100
Figura 23. Diagrama de Sequência Parcial 3 .....	100
Figura 24. Diagrama de sequência Parcial 5.....	102
Figura 25: Sequência de mensagens para a primeira utilização do mecanismo com SSO nos IdPs	105
Figura 26. Tela de alerta de certificado ssl não confiável.....	110
Figura 27. Tela inicial do Provedor de Serviço da Polícia Federal.....	110
Figura 28. Tela de certificado de segurança inválido .....	111
Figura 29. Tela de autenticação do provedor de identidade da Polícia Federal.....	111
Figura 30. Tela de atributos requeridos pelo provedor da Polícia Federal .....	112
Figura 31. Mensagem de alerta de certificado no SDPCA .....	113
Figura 32. Tela do SDPCA com a lista de provedores de Cliente Ativo.....	114
Figura 33. Tela de certificado não confiável do PCA.....	114
Figura 34. Tela do PCA para realização do download do Cliente Ativo.....	115
Figura 35. Alerta de segurança ao executar o Cliente Ativo .....	115
Figura 36. Alerta de segurança ao executar o Cliente Ativo com certificado desconhecido.....	116
Figura 37. Tela inicial do Cliente Ativo .....	116
Figura 38. Tela de autenticação inicial no Provedor de Identidade da Polícia Federal .....	118
Figura 39. Tela de autenticação e agregação do CPF .....	119
Figura 40. Tela de autenticação e agregação do RG.....	119
Figura 41. Tela de autenticação para agregação do Título de Eleitor.....	120
Figura 42. Tela de resumo dos atributos agregados no Cliente Ativo .....	120
Figura 43. Tela final da Polícia Federal após receber os atributos do Cliente Ativo.....	121
Figura 44. Log de requisições na porta 443 ( <i>ssl</i> ) .....	123

## LISTA DE QUADROS

Quadro 1. Requisitos do usuário para agregação de atributos .....	45
Quadro 2. Análise comparativa dos Trabalhos Relacionados.....	72
Quadro 3. Lista de documentos e respectivos IdPs para a emissão de passaporte .....	89
Quadro 4. Lista de documentos e respectivos IdPs para o financiamento habitacional .....	91
Quadro 5. Detalhamentos do caso de teste CT 01 .....	109
Quadro 6. Detalhamentos do caso de teste CT 02 .....	112
Quadro 7. Detalhamentos do caso de teste CT 03 .....	117
Quadro 8. Detalhamentos do caso de teste CT 04 .....	121
Quadro 9. Detalhamentos do caso de teste CT 05 .....	122
Quadro 10. Detalhamentos do caso de teste CT 06 .....	123

## LISTA DE ABREVIATURAS E SIGLAS

ABAC	Attribute-based Access Control
ACL	Access Control List
ADFS 2.0	Active Directory Federation Services
AOS	Arquitetura Orientada a Serviços
ARP	Account Release Policy
B2B	Business to Business
DETRAN	Departamento Estadual de Trânsito
ECP	Enhanced Client or Proxy
e-GIF	e-Government Interoperability Framework
e-Gov	e-Government
e-Gov.br	Governo Eletrônico Brasileiro
e-PING	Padrões de Interoperabilidade de Governo Eletrônico
FIDM	Federated Identity Management
G2B	Government to Business
G2C	Government to Citizen
G2G	Government to Government
ID-FF	Identity Federation Framework
IdP	Identity Provider
ID-WSF	Identity Web Services Framework
ID-WSF	Liberty's Identity Web Services Framework
IEEE	Institute of Electrical and Electronics Engineers
IMD	Federated Identity Management
LoA	Level of Assurance
LS	Linking Service
NSTIC	National Strategy for Trusted Identities in Cyberspace
PId	Permanente Identifier
RBAC	Role-Based Access Control
RIC	Registro de Identidade Civil
SAML	Security Assertion Markup Language
SP	Service Provider
SSO	Single Sign-on
STS	Security Token Service
TSP	Trusted Serve Provider
UA	User Assertion
UCAID	User-Controlled Automated Identity Delegation
UK	United Kingdom
VCP	Virtual Collaboration Platform
VO	Virtual Organizations
WSS	Web Services Security
XACML	eXtensible Access Control Markup Language
XML	eXtensible Markup Language



## SUMÁRIO

<b>1 INTRODUÇÃO.....</b>	<b>12</b>
<b>1.1 PROBLEMA DE PESQUISA.....</b>	<b>15</b>
1.1.1 Solução proposta .....	18
1.1.2 Delimitação de escopo .....	19
1.1.3 Justificativa.....	20
<b>1.2 OBJETIVOS .....</b>	<b>22</b>
1.2.1 Objetivo geral .....	22
1.2.2 Objetivos específicos .....	22
<b>1.3 METODOLOGIA.....</b>	<b>22</b>
1.3.1 Metodologia da pesquisa .....	23
1.3.2 Procedimentos metodológicos .....	24
<b>1.4 ESTRUTURA DO DOCUMENTO.....</b>	<b>25</b>
<b>2 FUNDAMENTAÇÃO TEÓRICA.....</b>	<b>27</b>
<b>2.1 GOVERNO ELETRÔNICO .....</b>	<b>27</b>
2.1.1 A arquitetura e-PING .....	31
<b>2.2 SISTEMAS DE GERENCIAMENTO DE IDENTIDADE .....</b>	<b>34</b>
<b>2.3 A ESPECIFICAÇÃO SAML.....</b>	<b>38</b>
2.3.1 Componentes da especificação SAML .....	41
2.3.2 Uso de Pseudônimos.....	43
<b>2.4 AGREGAÇÃO DE ATRIBUTOS.....</b>	<b>43</b>
2.4.1 Modelos de associação .....	45
<b>2.5 ABORDAGENS PARA IMPLEMENTAÇÃO DE AGREGAÇÃO DE ATRIBUTOS.....</b>	<b>46</b>
2.5.1 Banco de dados da aplicação.....	47
2.5.2 <i>Proxying</i> de identidade.....	48
2.5.3 Proxy de retransmissão de identidade .....	49
2.5.4 Agregação de atributos mediada pelo cliente.....	49
2.5.5 Federação de identidade.....	50
2.5.6 SP mediando a agregação de atributos .....	51
<b>2.6 CONSIDERAÇÕES SOBRE ABORDAGENS DE AGREGAÇÃO DE ATRIBUTOS.....</b>	<b>51</b>
<b>3 TRABALHOS RELACIONADOS .....</b>	<b>54</b>
3.1 LEE, KIM E HONG (2008) .....	54
3.2 CHADWICK, INAMAN E KLINGESTEIN (2010) .....	56
3.3 HOELLRIGL, KUHNER, DINGER E HARTENSTEIN (2010) .....	59
3.4 VOSSAERT, LAPON, DECKER E NAESSENS (2010) .....	61
3.5 WATT E SINNOTT (2011).....	64
3.6 CHADWICK, INMAN, SIU E FERDOUS (2011).....	65

3.7 HATAKEYAMA E SHIMA (2008) .....	67
3.8 HULSEBOSCH, WEGDAM, ZOETEKOUW, DIJK E POORTING (2011) 69	
3.9 COMPARAÇÃO DOS TRABALHOS RELACIONADOS .....	71
3.10 CONSIDERAÇÕES FINAIS DO CAPÍTULO .....	72
<b>4 MECANISMO AGREGADOR DE ATRIBUTOS BASEADO EM CLIENTE ATIVO .....</b>	<b>74</b>
4.1 VISÃO GERAL E PREMISSAS.....	74
4.2 DETALHAMENTO DO MECANISMO PROPOSTO E DOS FLUXOS DE COMUNICAÇÃO .....	79
4.2.1 Modo transitório dinâmico.....	80
4.2.2 Modo permanente dinâmico .....	81
4.2.3 Modo permanente estático .....	81
4.2.4 Padronização da Interação entre Cliente Ativo e Provedor de Serviços...	86
4.3 DESCRIÇÃO DE DOIS CENÁRIOS DE USO DO MECANISMO AGREGADOR DE ATRIBUTOS .....	88
4.3.1 Emissão de passaporte.....	88
4.3.2 Financiamento de imóveis .....	90
4.4 ANÁLISE DE REQUISITOS DO MECANISMO AGREGADOR DE ATRIBUTOS.....	92
4.4.1 Requisitos funcionais e Não Funcionais Associados .....	92
4.5 PROTÓTIPO DESENVOLVIDO.....	95
4.5.1 Ferramentas e tecnologias utilizadas .....	96
4.5.2 Detalhamento do Cenário de Uso .....	97
4.5.3 Configuração dos Serviços da Federação Governamental .....	98
4.5.4 Diagrama de Sequência Detalhado.....	98
4.5.5 Implementação do modo permanente dinâmico .....	103
<b>5 RESULTADOS .....</b>	<b>106</b>
5.1 PROJETO DOS EXPERIMENTOS DE AVALIAÇÃO DO MECANISMO AGREGADOR DE ATRIBUTOS PROPOSTO .....	106
5.2 RESULTADOS OBTIDOS E ANÁLISE DOS RESULTADOS.....	108
5.2.1 Resultados da Execução dos casos de teste.....	109
5.2.1 Análise da Execução dos Casos de Testes.....	124
5.2.2 Resultados e Análise da Pesquisa de Satisfação.....	124
5.3 AVALIAÇÃO DOS RESULTADOS .....	125
5.3.1 Avaliação da pesquisa de satisfação .....	125
5.3.2 Comparação com os trabalhos relacionados .....	132
<b>6 CONCLUSÕES .....</b>	<b>134</b>
6.1 CONTRIBUIÇÃO DA DISSERTAÇÃO .....	136
6.2 TRABALHOS FUTUROS .....	136

<b>REFERÊNCIAS .....</b>	<b>138</b>
<b>APÊNDICE A – REVISÃO SISTEMÁTICA.....</b>	<b>143</b>
<b>APÊNDICE B – CONFIGURAÇÃO DO FRAMEWORK SIMPLESAMPLPHP .....</b>	<b>148</b>
<b>APÊNDICE C – MENSAGEM CONVITE PARA PARTICIPAÇÃO DA AVALIAÇÃO .....</b>	<b>152</b>
<b>APÊNDICE D – QUESTIONÁRIO DE PESQUISA – GOVERNO... .....</b>	<b>153</b>
<b>APÊNDICE E – QUESTIONÁRIO DE PESQUISA – EMPRESAS.. .....</b>	<b>162</b>
<b>APÊNDICE F – OPINIÃO DOS USUÁRIOS NOS FORMULÁRIO DE PESQUISA .....</b>	<b>163</b>
<b>APÊNDICE G – DETALHES DE DESENVOLVIMENTO DO PROTÓTIPO .....</b>	<b>184</b>
<b>APÊNDICE H – RESULTADOS DA PESQUISA DE SATISFAÇÃO .....</b>	<b>187</b>

# 1 INTRODUÇÃO

No Brasil e no mundo, a Internet torna-se cada vez mais indispensável. Diariamente, novas aplicações e serviços surgem seguindo a tendência da *Web 2.0*. Algumas aplicações *Web* interativas, tais como *Twitter*, *Facebook*, blogs, têm como finalidade facilitar a comunicação entre as pessoas e empresas e a divulgação de conteúdo. Outras aplicações, como as de Governo Eletrônico, procuram agilizar a prestação de serviços governamentais tanto para o cidadão quanto para as empresas.

A Organização das Nações Unidas (ONU) destaca que o desenvolvimento e implantação de programas de governo eletrônico em vários países é uma das consequências mais viáveis da rápida e intensa adoção das TICs, com impacto significativo na forma como o governo gere o relacionamento entre prestadores de serviços públicos e o cidadão (UNDP, 2004).

No contexto de governo eletrônico, garantir que as interações entre o governo e o cidadão (do inglês *Government to Citizen* - G2C) ou entre governos (do inglês *Government to Government* - G2G) sejam interoperáveis, seguras e fáceis são alguns dos objetivos na utilização da internet pelos governos (THIBEAU, 2009).

Segundo Baldoni (2009), alguns países desenvolveram portais de serviços participativos para a população. A Dinamarca, por exemplo, foi um dos primeiros países a adotar o portal do cidadão. Contudo, neste cenário dinâmico e participativo, surge o problema relacionado à gestão das novas identidades criadas pelos usuários em cada novo serviço que eles utilizam.

Para prover a gestão de identidades é fundamental o uso de tecnologias que auxiliem o usuário nesta tarefa, assim como a aplicação de políticas para a definição das regras relacionadas ao ciclo de vida das identidades digitais (JOSANG; POPE, 2005).

Para Chadwick (2009), a gestão de identidades (do inglês *Identity Management* - IdM) consiste de um conjunto de funções e habilidades para a administração, descoberta e troca de informações, usadas para garantir a consistência das identidades, permitindo assim que transações possam ocorrer com segurança.

Segundo Bhargav-Spantzel *et al.* (2006), a gestão de identidades consiste de softwares e protocolos que gerenciam o ciclo de vida das identidades dos usuários. Segundo esse autor, além

dos usuários, um sistema de IdM é composto de três partes principais, que são: o provedor de identidades (do inglês *Identity Provider* – IdP), que é responsável por gerenciar as identidades dos usuários; o provedor de serviços (do inglês *Service Provider* – SP), que é responsável por prestar serviços aos usuário com base em seus atributos; e as identidades que são o conjunto de atributos dos usuários.

No modelo isolado ou tradicional de gestão de identidades, amplamente utilizado nos atuais sistemas computacionais presentes na Internet, a identificação do usuário é tratada de forma isolada pelo provedor de serviços, o qual também atua como provedor de identidades. Cabe ao usuário criar uma identidade digital para cada provedor de serviços com o qual deseja interagir, não havendo assim o compartilhamento das identidades desses usuários entre diferentes provedores de serviços (JOSANG; POPE, 2005).

Além do modelo tradicional, Lips e Pang (2008) classificam o gerenciamento de identidades (IdM) em outros três modelos, que são:

- Modelo IdM centrado na organização (do inglês *organization centric IdM*): neste modelo, as organizações mantêm e gerenciam as informações dos usuários. Este está fundamentado no compartilhamento de identidades dos usuários entre provedores de serviços de uma mesma organização e no conceito de autenticação única (*Single Sign On* – SSO). Neste modelo, o provedor de identidades da organização é responsável por autenticar os usuários e fornecer aos provedores de serviços informações sobre estes, sendo que todos os provedores de serviços devem confiar plenamente nas informações fornecidas pelo provedor de identidades (BHARGAV-SPANTZEL *et al.*, 2007);
- Modelo IdM federado (do inglês *federated IdM*): a tarefa de autenticação no modelo federado é realizada a partir de múltiplos provedores de identidade, que participam de um círculo de confiança entre diferentes domínios administrativos. Um domínio administrativo pode representar, por exemplo, uma empresa ou uma universidade. Este domínio administrativo é composto de usuários, provedores de serviços e provedores de identidades. Segundo Landau *et al.* (2009), o gerenciamento de identidades federadas possibilita o compartilhamento de atributos do usuário, além da autenticação única através de múltiplos domínios; e

- Modelo IdM centrado no usuário (do inglês *user-centric IdM*): neste modelo, os usuários controlam as suas informações. Lips e Pang (2008) afirmam que somente o usuário conhece e controla todas as suas identidades, sendo o único capaz de realizar a ligação de todas as suas contas. O modelo tem como objetivo fornecer ao usuário o total controle sobre suas identidades digitais. Contudo, as principais propostas e implementações deste modelo fazem uso de um dos modelos anteriores, sendo que o modelo de identidade federado é o mais usado. Por exemplo, na solução proposta em Jøsang e Pope (2005), as identidades de um usuário, 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.

Para Bhargav-Spantzel *et al.* (2007), outro modelo de gestão de identidades é o centralizado, que surgiu devido à inflexibilidade do modelo tradicional. Neste modelo, existe um único provedor de identidades responsável por autenticar os usuários para que estes acessem provedores de serviços de diferentes organizações. Segundo Maliki e Seigneur (2007), o ponto fraco do modelo centralizado é que o provedor de identidades possui controle absoluto sobre as informações de seus usuários, podendo assim usá-las da forma que bem entender.

Segundo Baldoni (2009), os sistemas de gerenciamento de identidades federadas no governo eletrônico podem ser utilizados para tornar os serviços fornecidos pelo governo mais eficientes e participativos. 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).

Os sistemas de IdM federadas podem ser utilizados em sistemas de todas as esferas governamentais (federal, estadual e municipal) e podem também ser utilizados para a colaboração entre o governo e as empresas privadas e do terceiro setor. No entanto, nem todos os países decidiram adotar uma abordagem federada, alguns destes adotaram regimes de acordo com a cultura e com sua relação com os governos locais, por exemplo, Coreia do Sul, Holanda e Reino Unido adotaram o modelo centralizado (BALDONI, 2009; OECD, 2011).

Dentro deste contexto, este trabalho procura contribuir para a área de gestão de identidades federadas em programas de governo eletrônico, conforme o que será analisado na seção a seguir.

## 1.1 PROBLEMA DE PESQUISA

Um sistema de gerenciamento de identidades federadas pode fornecer recursos para a implementação de mecanismos de gestão dos atributos dos usuários em aplicações de Governo Eletrônico. Segundo Klingenstein (2007), os sistemas que seguem o modelo de identidades federadas são sólidos e garantem o acesso federado de seus usuários, porém, muitas vezes, questões referentes à privacidade dos usuários não são devidamente consideradas. O autor mencionado afirma ainda que durante as trocas de informações que ocorrem nesses sistemas, os provedores podem rastrear a identidade do usuário e seus acessos. Esta prática pode comprometer a privacidade dos usuários. Algumas trocas podem exigir que um provedor de identidades emita asserções referentes à identidade do usuário sem a associação de um destinatário, o que é uma prática perigosa quando os dados não são criptografados.

Na tentativa de evitar o comprometimento das informações do usuário, alguns trabalhos descritos na literatura buscam resolver o problema referente à privacidade dos usuários (BARTON *et al.*, 2005; CHADWICK, 2006; GEMMILL *et al.*, 2009). Esses trabalhos descrevem soluções de IdM federados centrados 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 diversas contas em provedores de identidades. Segundo Hoellrigl *et al.* (2010), uma característica importante sobre os sistemas de gerenciamento de identidades centrados nos usuários é a capacidade do usuário de poder escolher o provedor de identidades que deseja utilizar. O usuário pode optar por utilizar um determinado provedor e, a qualquer momento, trocá-lo, sem a preocupação de perder acesso aos serviços que costuma utilizar, com a possibilidade, ainda, de utilizar múltiplos provedores de identidade. Os autores apontam três razões para que os usuários optem pela utilização de múltiplos provedores de identidade (IdPs), que são:

- Os atributos do usuário normalmente estão em diferentes fontes confiáveis de autoridade;
- Provedores de serviços (SPs) e os usuários não confiam em um IdP centralizador; e
- Muitos SPs não confiam em informações fornecidas por IdPs auto-hospedados, ou seja, que possam ser criados pelos próprios usuários.

Múltiplos IdPs podem trazer vantagens para os usuários, principalmente para segurança de seus dados no contexto do Governo Eletrônico, diante das diversas esferas governamentais, observa-se como comum em uma Federação Governamental que um usuário possua atributos espalhados em múltiplos IdPs (cada qual mantendo apenas os atributos dos usuários que são de sua responsabilidade).

Hoellrigl *et al.* (2010) afirmam que em consequência da utilização de múltiplos IdPs, os atributos dos usuários podem ser armazenados de forma redundante. Isto resulta na replicação das informações dos usuários em múltiplos esquemas de dados heterogêneos, o que, nestes casos, requer que as alterações de atributos dos usuários sejam disseminadas para todas as suas cópias.

Para esclarecer o problema de pesquisa a ser tratado neste trabalho, pode-se considerar o seguinte cenário: “Supondo que um professor queira comprar pela Internet cartões de estacionamento para utilizar nos locais indicados pela Prefeitura para este fim. Este serviço de governo eletrônico, mantido pela Prefeitura, oferece descontos especiais para funcionários e professores municipais. Para efetuar a compra com desconto e com cartão de crédito, o professor deverá provar as seguintes informações: (i) que é professor em uma instituição da rede de ensino municipal; (ii) que é proprietário de um veículo; e (iii) que é titular de um cartão de crédito”.

No cenário descrito, como os atributos do usuário encontram-se armazenados em múltiplos provedores de identidades, estes precisam ser coletados. Esta união, muitas vezes processada por uma terceira parte confiável, é conhecida como agregação de atributos. Para solicitar os cartões de estacionamento, o professor precisará de um mecanismo que solicite aos diferentes provedores de identidades (IdP da Instituição de ensino, IdP da operadora de cartão de crédito e IdP do DETRAN) asserções que comprovem os atributos de identidade do usuário exigidos pelo provedor do serviço.

Klingenstein (2007) comenta que a complexidade para garantir a interoperabilidade sempre vai existir na agregação de atributos devido à natureza do problema, isto porque as tecnologias adotadas nos provedores de serviços e as adotadas pelos usuários e pelos provedores de identidades podem sempre sofrer variações.

Dentro do cenário apresentado, constata-se a necessidade do uso de um mecanismo agregador de atributos capaz de coletar e unir os atributos dos usuários disponibilizados em



múltiplos provedores de identidade, para que estes possam ser apresentados para provedores de serviços que exigem um conjunto de atributos que não estão em um único IdP.

A maioria dos trabalhos que tratam do problema da necessidade de agregação de atributos descrevem mecanismos implementados por uma terceira parte confiável (*proxies*) (CHADWICK *et al.*, 2010; HOELLRIGL *et al.*, 2010; VOSSAERT *et al.*, 2010;). Nesta abordagem, a terceira parte mantém o controle das informações e acessos de usuário o que pode comprometer a sua privacidade. 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. Para isto, uma possível solução é conceber um mecanismo agregador de atributos que seja executado no próprio cliente, abordagem conhecida como mediada pelo cliente.

Conforme mencionado anteriormente, com o objetivo de incentivar a utilização de serviços de governo eletrônico, em todas as esferas governamentais (federal, estadual, e municipal), e promover a segurança, diversos países estão implantando suas estratégias nacionais de gestão de identidades tendo como base o modelo de identidades federados (OECD, 2011). Contudo, estes sistemas de IdM não permitem que provedores de serviços exijam dos usuários atributos que estejam em múltiplos provedores de identidades, por não oferecer um suporte a coleta e agregação de atributos distribuídos em diferentes IdPs.

Neste contexto, este trabalho busca garantir a privacidade dos usuários no processo de agregação de atributos distribuídos em múltiplos provedores de identidades e tem por objetivo trazer mais flexibilidade a uma estratégia brasileira de gestão de identidades federadas. Em especial, busca-se responder às seguintes questões de pesquisa:

1. O emprego de um mecanismo agregador de atributos mediado pelo cliente traz mais flexibilidade para um sistema de gestão de identidades federadas, ao permitir que provedores de serviços possam exigir atributos de múltiplos provedores de identidade?
2. É possível garantir a privacidade do usuário com o uso de um mecanismo agregador de atributos que segue uma abordagem mediada pelo cliente sem prejudicar a interoperabilidade do sistema de IdM e da aplicação de e-GOV?
3. Quais os impactos na usabilidade decorrentes do uso do mecanismo agregador de atributos mediado pelo cliente pelas aplicações de Governo Eletrônico no Brasil?

### 1.1.1 Solução proposta

A solução proposta neste trabalho consistiu no desenvolvimento de um mecanismo agregador de atributos, mediado pelo cliente, que garante a privacidade dos cidadãos em seus acessos a serviços de governo eletrônico.

Para concepção do mecanismo proposto, assumiu-se a existência de uma estratégia nacional de gestão de identidades federadas. A Federação Governamental de Serviços reúne as esferas do governo federal, estadual e municipal. Assumiu-se ainda que a estratégia nacional de gestão de identidades segue também o modelo centrado no usuário. Por fim, assumiu-se que a Federação Governamental usa como infraestrutura de autenticação e de autorização o padrão SAML (*Security Assertion Markup Language*) (OASIS, 2013).

Dentro da federação governamental, um cidadão terá atributos espalhados por diversos provedores de identidade, sendo que um provedor de serviços pode requerer um subconjunto desses atributos de um usuário para conceder o acesso.

De forma a não prejudicar a interoperabilidade das aplicações de e-Gov, o mecanismo agregador de atributos proposto, além de atender aos requisitos do sistema de gerenciamento de identidades federadas e centrado no usuário, atende às recomendações de interoperabilidade do programa de governo eletrônico brasileiro, contidas na arquitetura e-PING (BRASIL, 2011).

A segurança durante as trocas de informações realizadas entre os provedores de serviço, os provedores de identidades, que fazem parte da federação governamental, e o mecanismo agregador de atributos é assegurada através de protocolos e mecanismos de segurança amplamente aceitos, o protocolo SSL e assinaturas digitais.

Para implementar a abordagem de agregação de atributos mediada pelo cliente, o mecanismo foi 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 provedores de identidade. Visando ainda prover a privacidade aos usuários, o mecanismo permite que o usuário indique quais provedores deseja utilizar e como controlar todas as trocas de seus atributos, sendo que os atributos agregados pelo mecanismo só serão entregues ao provedor de serviços alvo após o consentimento do usuário (autorização de liberação de atributos).

Outro requisito importante para o mecanismo agregador de atributos é a garantia da autenticidade dos atributos enviados aos provedores de serviços. Ou seja, é necessário que os provedores de serviços tenham garantias sobre os atributos recebidos, no que diz respeito à fonte originadora dos atributos, conhecida também como autoridade de atributos ou provedor de identidades (IdP). Em todo processo de agregação de atributos, as autoridades de atributos são identificadas através das asserções de atributos assinadas digitalmente.

Como hipótese, tiveram-se as seguintes afirmações:

- H1 - Um mecanismo agregador de atributos mediado pelo cliente, alinhado à arquitetura E-PING e que segue o padrão SAML, traz mais flexibilidade para um sistema de gestão de identidades federadas ao permitir que provedores de serviços possam exigir atributos de múltiplos provedores de identidade;
- H2 - Com o uso de uma abordagem mediada pelo cliente, é possível conceber um mecanismo agregador de atributos que garanta a privacidade dos usuários; e
- H3 - O uso de um mecanismo agregador de atributos mediado pelo cliente impacta na usabilidade das aplicações de governo eletrônico alinhadas ao programa e.Gov.br.

### **1.1.2 Delimitação de escopo**

O escopo deste trabalho englobou o desenvolvimento do mecanismo agregador de atributos para ser usado com um sistema de gerenciamento de identidades federadas, centrado no usuário e baseado no padrão SAML. Este mecanismo atende às recomendações de interoperabilidade do programa de governo eletrônico brasileiro (e-PING).

É importante destacar que o trabalho não abordou aspectos sobre a criação de federações governamentais e nem a concepção de uma estratégia nacional de gestão de identidades (uso de um sistema de gestão de identidade). Porém, assumiu-se, como premissa, a existência desta estratégia nacional. Para avaliar o mecanismo proposto, um protótipo do mecanismo agregador de atributos foi desenvolvido como prova de conceito e este foi avaliado tendo como base um cenário de uso de solicitação de passaportes que também foi desenvolvido no escopo deste trabalho. Alguns especialistas em aplicações de governo eletrônico avaliaram a flexibilidade, a privacidade e a usabilidade da solução proposta, por meio de uma pesquisa de satisfação.

### 1.1.3 Justificativa

Segundo Wingham *et al.* (2010), as redes colaborativas governamentais possuem uma série de requisitos de interoperabilidade e de segurança. A interoperabilidade é necessária para tratar vários aspectos de heterogeneidade entre os provedores, dentre estes: a heterogeneidade das plataformas computacionais utilizadas e as várias políticas administrativas e de segurança implantadas. A segurança, por sua vez, é fundamental para que os membros de uma rede colaborativa possam depositar confiança nas interações com outros membros.

Uma limitação de alguns sistemas de gerenciamento de identidades federadas atuais está em limitar que os usuários possam selecionar apenas um de seus IdPs em qualquer sessão criada com um provedor de serviços (SP). Segundo Chadwick, Inman e Klingenstein (2010), a maioria dos sistemas de identidades federadas sofre dessa limitação significativa, ou seja, a falta de uma abordagem padronizada para agregar atributos de usuários afirmados por múltiplas fontes, viabilizando o uso desses atributos pelo SP na decisão do acesso a seus recursos/serviços.

Para Chadwick e Inman (2009), um mecanismo que permite a agregação dos atributos do usuário, a partir de múltiplos IdPs em uma única sessão, mostra-se mais flexível para serviços oferecidos em Programas de Governo Eletrônico.

As soluções de agregação de atributos baseadas em *proxy* (HATAKEYAMA; SHIMA, 2008; CHADWICK; INAMAN; KLINGESTEIN, 2010; HOELLRIGL *et al.*, 2010; CHADWICK *et al.*, 2011; WATT; SINNOT, 2011; HULSEBOSCH *et al.*, 2011), que utilizam uma terceira parte confiável, possuem vantagens quanto à facilidade de implementação e suporte a autenticação SSO, porém, não favorecem a garantia da privacidade do usuário. Esta desvantagem ocorre já que a terceira parte pode rastrear as interações entre o usuário e os provedores de identidades e de serviços (CHADWICK; INMAN, 2009).

A solução proposta por Lee, Kim; Hong (2008) segue uma abordagem de agregação mediada pelo próprio provedor de serviços. Este tipo de abordagem favorece a rastreabilidade das informações do usuário, visto que o próprio provedor de serviço irá realizar os procedimentos de agregação de atributos. Ou seja, o provedor de serviço será capaz de identificar todas as contas e atributos que o usuário possui, o que fere fortemente as regras de não rastreabilidade das informações dos usuários, conforme afirmado no trabalho de Chadwick e Inman (2009).

Para garantir a privacidade do usuário, a agregação de atributos deve evitar a rastreabilidade dos atributos do usuário, sendo que a estratégia baseada em cliente ativo contribui para o provimento deste requisito. A abordagem de cliente ativo é pouco utilizada (HOELLRIGL *et al.*, 2010; VOSSAERT *et al.*, 2010), mas é recomendada quando se necessita priorizar a privacidade dos atributos do usuário. Sua baixa adoção é justificada pela dificuldade de promover a autenticação SSO e de garantir a interoperabilidade (KLINGENSTEIN, 2007).

O trabalho apresentado por Hoellrigl *et al.* (2010) descreve uma proposta de implementação que segue uma abordagem baseada em *proxy* e mediada pelo cliente, capaz de seguir políticas e regras determinadas pelo usuário. A grande desvantagem deste trabalho está nas tecnologias utilizadas para concepção da abordagem mediada pelo cliente. O mecanismo proposto está baseado em soluções proprietárias, tais como o *Card Space* da Microsoft, que impede que a solução funcione de forma adequada em diferentes sistemas operacionais e navegadores *Web* existentes. Logo, a portabilidade e interoperabilidade destes mecanismos estão comprometidas.

A solução de agregação proposta por Vossaert *et al.* (2010) segue a abordagem mediada pelo cliente. Os autores definem um novo módulo de segurança, no formato de um *smart card*, baseando-se na implementação utilizada na Alemanha, que criou identidades conhecidas como eID (do inglês *Electronic Identity*), o que promove a interoperabilidade e a segurança.

O problema maior da solução proposta por Vossaert *et al.* (2010) está na utilização dos cartões inteligentes (*smart cards*) que podem se tornar onerosos para a criação e manutenção, tanto para o governo quanto para o usuário. Outra questão que dificulta a utilização de cartões, é que para serviços que exigem autenticação, embora sejam simples<sup>1</sup>, como por exemplo, uma pesquisa que o governo venha a realizar com a população, se o usuário não estiver de posse de seu dispositivo ou de seu leitor, este não poderá participar. Além disso, poucos leitores de cartões inteligentes podem ser utilizados com dispositivos móveis como *smartphones* e *tablets* ou *smartTVs*, o que restringirá a participação dos usuários por estes meios.

De acordo com as considerações apresentadas anteriormente, constata-se a necessidade dos sistemas de gestão de identidades usados em aplicações de governo eletrônico proverem a

---

<sup>1</sup> Nível de garantia baixo.

agregação de atributos a partir de múltiplos provedores de identidade, sendo que o processo de agregação de atributos deve evitar a rastreabilidade dos atributos do usuário com o objetivo de preservar a sua privacidade sem prejudicar a interoperabilidade das aplicações envolvidas.

## **1.2 OBJETIVOS**

### **1.2.1 Objetivo geral**

Prover a agregação de atributos dos usuários que estão distribuídos em múltiplos provedores de identidades, garantindo a privacidade dos usuários, 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.

### **1.2.2 Objetivos específicos**

1. Prover mais flexibilidade para uma estratégia nacional brasileira de gestão de identidades federadas e centrada no usuário ao permitir que provedores de serviços possam exigir atributos de múltiplos provedores de identidade, por meio de um mecanismo agregador de atributos, alinhado à arquitetura E-PING;
2. Prover privacidade ao processo de agregação de atributos, por meio de um mecanismo agregador de atributos mediado pelo cliente que faz uso de um aplicativo executado no ambiente operacional do usuário; e
3. Identificar os impactos na interoperabilidade e na utilização decorrentes do uso do mecanismo agregador de atributos das aplicações de governo eletrônico alinhadas ao programa e.Gov.br., considerando o seu uso em um estudo de caso.

## **1.3 METODOLOGIA**

Esta seção apresenta a metodologia de pesquisa e os procedimentos metodológicos adotados nessa dissertação de mestrado.

### 1.3.1 Metodologia da pesquisa

Um método científico é o conjunto de processos ou operações mentais que devem ser adotados na investigação, permitindo que seja definida uma linha de raciocínio para o processo de pesquisa (SILVA; MENEZES, 2001).

Foi utilizado nesta pesquisa o método hipotético-dedutivo, que consiste na construção e verificação de hipóteses (LAKATOS; MARCONI, 2000). Estas hipóteses foram submetidas à avaliação (desenvolvimento e uso do mecanismo agregador), à crítica de especialistas (em parte subjetiva) e à análise comparativa com trabalhos relacionados, a fim de verificar quais foram as hipóteses válidas.

A pesquisa realizada neste trabalho é de natureza aplicada, pois teve como objetivo investigar, comprovar ou rejeitar as hipóteses apresentadas na solução proposta. A pesquisa aplicada teve como objetivo gerar conhecimento para a aplicação prática, dirigida à solução de problemas específicos. Neste contexto, este trabalho teve como objetivo solucionar problemas em relação à privacidade, usabilidade e flexibilidade do processo de agregação de atributos a ser usado em uma estratégia nacional de gestão de identidades.

Do ponto de vista de seus objetivos, esse trabalho se enquadra em uma pesquisa exploratória (LAKATOS; MARCONI, 2000), pois visou investigar o tema de agregação de atributos em estratégias de identidades federadas por meio de levantamento bibliográfico e de trabalhos correlacionados.

Em relação ao ponto de vista da forma de abordagem do problema, este trabalho enquadra-se como uma pesquisa qualitativa<sup>2</sup> no que se refere ao problema da garantia da privacidade do usuário e do aumento da flexibilidade sem prejuízos em relação à interoperabilidade. Neste caso, a avaliação da abordagem foi dada de forma descritiva, através da análise e comparação de trabalhos e da análise do atendimento de alguns requisitos. Porém, para avaliar o problema da usabilidade

---

<sup>2</sup> Este tipo de pesquisa considera que há uma relação dinâmica entre o mundo real e o sujeito, isto é, um vínculo indissociável entre o mundo objetivo e a subjetividade do sujeito que não pode ser traduzido em números. A interpretação dos fenômenos e a atribuição de significados são básicas no processo de pesquisa qualitativa, tornando o uso de métodos e técnicas estatísticos facultativos (SILVA; MENEZES, 2001)

(impacto) da solução proposta, uma pesquisa quantitativa foi empregada. Dentro deste contexto, foi realizada uma análise da privacidade, flexibilidade e usabilidade da solução proposta para agregação de atributos.

### 1.3.2 Procedimentos metodológicos

Esta seção apresenta os procedimentos metodológicos que foram utilizados para cumprimento dos objetivos da dissertação, que são:

- **Pesquisa bibliográfica:** O objetivo da pesquisa bibliográfica foi de fortalecer o conhecimento técnico que circunda os objetivos da dissertação. Foi realizado para isso um levantamento bibliográfico sobre as questões de governo eletrônico, segurança da informação, gestão de identidades, arquitetura de padrões de interoperabilidade de governo eletrônico brasileiro (e-PING), bem como sobre as abordagens para implantação do processo de agregação de atributos. Estudou-se também a especificação SAML tão importante para o contexto da solução proposta. Foram utilizados também materiais publicados em livros, teses, dissertações e artigos de periódicos e de conferências científicas.
- **Análise de trabalhos relacionados:** A partir da execução de um protocolo de busca (ver Apêndice A) foram encontrados alguns trabalhos relacionados ao tema da pesquisa desta dissertação. Estes trabalhos foram analisados de forma a identificar suas características e limitações. Esta atividade foi muito importante para identificar algumas características que foram também seguidas no mecanismo proposto e para delinear a sua contribuição diante dos trabalhos relacionados.
- **Definição do Mecanismo Agregador de Atributos:** Após o levantamento bibliográfico e a análise dos trabalhos relacionados, buscou-se definir um novo mecanismo agregador de atributos, que fosse relevante e contribuísse para a comunidade acadêmica. Para a definição do mecanismo agregador foi necessário estudar de forma aprofundada a ferramenta que implementa a especificação SAML e que possibilitou a criação da federação governamental e a tecnologia *Java Web Start* adotada para o desenvolvimento do aplicativo do cliente ativo. Para esta definição foram utilizados também diagramas de



UML, técnicas para o levantamento de requisitos funcionais (RF) e não funcionais (RNF), bem como a definição de casos de uso (USC) e casos de testes (CT).

- **Implementação do mecanismo proposto:** o mecanismo agregador de atributos proposto foi implementado (prova de conceito) de forma a comprovar as hipóteses levantadas. É importante frisar que todas as escolhas tecnológicas estão alinhadas à arquitetura e-PING, buscando com isso uma maior flexibilidade para uma estratégia nacional de gestão de identidades federadas, sem prejudicar a interoperabilidade.
- **Avaliação do mecanismo proposto:** Na avaliação do mecanismo agregador de atributos, procurou-se analisar o atendimento aos requisitos funcionais e não funcionais e as hipóteses de pesquisa (em relação à privacidade, flexibilidade e usabilidade da solução proposta), através de testes de *software*, uma pesquisa de satisfação de usuários e da comparação com trabalhos relacionados. Com a pesquisa de satisfação de usuários, foi possível avaliar os impactos decorrentes do uso do mecanismo agregador, bem como comprovar o seu funcionamento correto em diferentes ambientes operacionais e navegadores *Web*.

## 1.4 ESTRUTURA DO DOCUMENTO

O trabalho está organizado em seis capítulos correlacionados. O Capítulo 1, Introdução, apresentou, por meio de sua contextualização, o tema proposto neste trabalho. Da mesma forma, foram estabelecidos os resultados esperados por meio da definição de seus objetivos e foram apresentadas às limitações do trabalho, permitindo uma visão clara do escopo proposto.

O Capítulo 2, Fundamentação Teórica, apresentou uma revisão bibliográfica sobre governo eletrônico, a arquitetura e-PING, os conceitos e modelos de gestão de identidades; a especificação SAML; agregação de atributos e as abordagens e implementações de agregação de atributos. Por fim, foram apresentadas algumas considerações sobre as abordagens de agregação de atributos.

O Capítulo 3, Trabalhos Relacionados, tratou dos trabalhos encontrados na literatura que utilizam agregação de atributos em mecanismos de identidades federadas e de uma análise comparativa destes trabalhos. Estes trabalhos relacionados foram utilizados como base para a definição do novo mecanismo agregador de atributos proposto neste trabalho.

O Capítulo 4 apresentou a visão geral do mecanismo agregador de atributos proposto e o detalhamento dos modos de funcionamento do mecanismo. Além disso, neste capítulo, foram descritos os requisitos funcionais e não funcionais do mecanismo agregador de atributos, bem como a modelagem do protótipo implementado (Serviço de Emissão de Passaporte que faz uso do mecanismo agregador de atributos). As ferramentas e tecnologias utilizadas e o detalhamento do desenvolvimento do protótipo foram também descritos.

No Capítulo 5, foram apresentados os experimentos de avaliação realizados, bem como os resultados obtidos na aplicação de tais experimentos. Por fim, uma análise comparativa entre os trabalhos relacionados e a solução proposta foi descrita.

Por fim, no Capítulo 6, foram tecidas as conclusões do trabalho, relacionando os objetivos identificados, inicialmente com os resultados que se espera alcançar, bem como a descrição dos trabalhos futuros.

## 2 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo são apresentados os conceitos de governo eletrônico, a arquitetura E-PING, os conceitos e modelos relacionados a gestão de identidades e a especificação SAML. Ainda neste capítulo são descritos os modelos de agregação de atributos existentes, bem como as abordagens de implementação do processo de agregação de atributos. Por fim, as considerações sobre este capítulo são apresentadas.

### 2.1 GOVERNO ELETRÔNICO

Segundo Barbosa (2008), os programas de governo eletrônico – e-Gov (do inglês *e-government*), resultam do avanço na utilização das Tecnologias de Informação nos setores públicos. A tecnologia no setor público tem como objetivo aumentar o desempenho e a eficácia da administração. Sua adoção, quando focada na melhoria do relacionamento com a população, ou na promoção do governo participativo, normalmente, é direcionada ao oferecimento de novos serviços via Internet. 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 (do inglês *government to business* - G2B) e entre o governo e o cidadão (do inglês *government to citizen* - G2C), (DAWES; PARDO 2008).

A contribuição principal no desenvolvimento dos programas de governo eletrônico está diretamente ligada à transparência do governo perante a população. Inúmeros países estão atualmente adotando políticas de relacionamento para abertura e para transparência de seus governos. Um governo aberto ou participativo (do inglês *open government*) tem como objetivo principal aumentar a participação do cidadão nas decisões governamentais (THIBEAU, 2009).

O presidente dos Estados Unidos da América, Barack Obama, redigiu no início de seu mandato um memorando no qual afirmava que sua administração seria baseada na transparência, tendo como objetivo principal conquistar a confiança pública, trabalhando com o envolvimento de toda a população e estabelecendo um sistema de participação e colaboração. Esse documento foi escrito pelo presidente a fim de fortalecer a democracia e promover a eficiência do governo. O presidente afirmou ainda que buscava encontrar medidas para divulgar as informações com a maior

agilidade possível e de fácil acesso para toda a população, para que o governo consiga tomar suas decisões com base no pensamento da maioria. (OBAMA, 2009).

Segundo o relatório de 2010 das Nações Unidas sobre governo eletrônico (ONU, 2010), um programa de e-Gov é uma poderosa ferramenta para o desenvolvimento humano e social, sendo essencial para conquistar todos os objetivos de desenvolvimento de um país. Muitos países estão direcionando suas forças no aprimoramento de seus programas de governo eletrônico, como por exemplo: revitalizando a administração pública; reformulando a gestão pública; promovendo as lideranças inclusivas e os serviços mais eficientes; melhorando constantemente a transparência e a responsabilidade pública (ONU, 2010).

No Brasil, existem inúmeras linhas de ação em termos de políticas públicas, para que o uso de e-Gov possa se consolidar e produzir benefícios, assumindo a premissa fundamental de governo eletrônico centrado no cidadão (CGI.br, 2010).

O relatório das Nações Unidas de 2010 posiciona o Brasil em 61º lugar no ranking mundial de desenvolvimento de aplicações para governo eletrônico. Em 2008, ano do relatório anterior, o Brasil se encontrava na 45º posição (ONU, 2010), o que indica a falta de desenvolvimento de aplicações de governo eletrônico no país durante o período das avaliações.

Muitos governos estão encorajando sua população a utilizarem suas ferramentas on-line. Estas ferramentas possuem mecanismos de interação com os usuários, como por exemplo, enquetes, questionários e ferramentas de *feedback*, o que resulta no recebimento de críticas e sugestões da população para os serviços prestados pelo governo (ONU, 2010).

O termo tecnológico “Web 2.0” marca o surgimento da segunda geração de serviços *Web*, ou a “Web 3.0”, em um futuro próximo. Estas tecnologias podem proporcionar ao cidadão avanços e melhorias na organização dos serviços oferecidos pelo governo. As tecnologias da “Web 2.0” e as redes sociais criam um ambiente para os políticos e gestores públicos incorporarem ao seu dia a dia. Nos Estados Unidos, por exemplo, mais de vinte milhões de seguidores assinam as notícias escritas pelo presidente Barack Obama na ferramenta *Twitter*.

O relatório da ONU analisa ainda o índice de e-Participação (do inglês *e-Participation*), que define a prestação de serviços on-line aos cidadãos. Muitos governos têm reforçado suas ferramentas de e-Participação, e como o cidadão tem poder, estas ferramentas criam uma forma

diferente de relacionamento com o governo (ONU, 2010). Com maior eficácia no relacionamento com a população, o governo é capaz de direcionar suas ações conforme as necessidades da população. Segundo o relatório das ONU (2010), o Brasil está na 42<sup>a</sup> posição no índice de e-Participação.

O relatório da ONU (2010) mostra ainda a necessidade de melhorias no formato de participação do governo brasileiro. Observando-se este índice de participação, verifica-se a necessidade do entendimento do cenário atual de utilização da internet no Brasil. Segundo o comitê gestor da internet no Brasil, (CGI.br, 2010), o avanço no uso da internet pela população brasileira na área urbana aumentou de 30,5 milhões de internautas em 2005, para 58,5 milhões em 2009. Isso fortalece a hipótese de que cada vez mais o cidadão utilizará a Internet como meio de comunicação com o Governo.

Segundo a pesquisa sobre utilização da tecnologia de informação no Brasil, o relatório (CGI.br, 2010) aponta um cenário positivo para o uso de serviços público pela internet no país, pois mais da metade da população, especificamente 56% dos entrevistados, escolheu a Internet como forma de acessar os serviços governamentais (ver Figura 1). A proporção de cidadãos propensa a utilizar o governo eletrônico na internet é superior a 35% daqueles que utilizam algum serviço na rede, o que indica uma demanda reprimida no uso desse importante serviço. Tal percentual é ainda superior para os usuários de e-Gov, chegando à marca de 93% de pessoas que escolheriam a Internet para usar serviços governamentais. Isso mostra que aqueles que usam hoje a tecnologia continuarão usando no futuro e que cada vez mais pessoas poderão ser incluídas digitalmente no relacionamento com o governo.

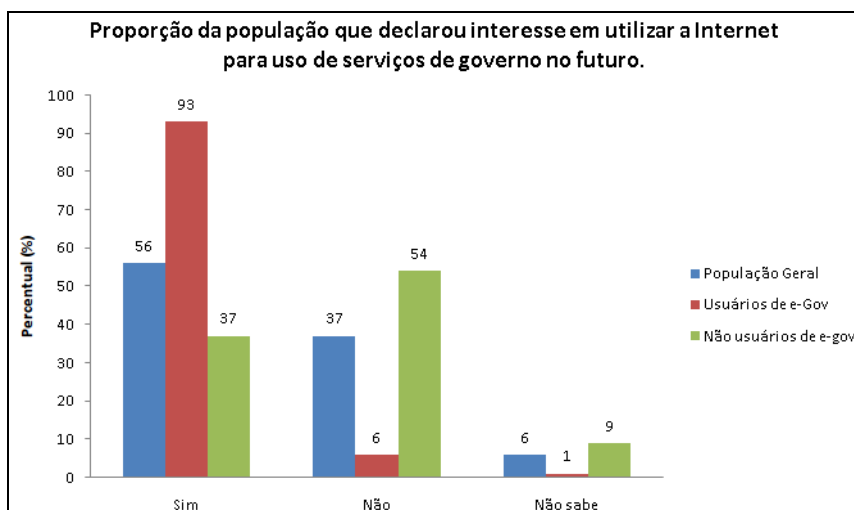


Figura 1. Propensão ao uso da internet na obtenção de um serviço de governo no Brasil.

Fonte: CGI.br, (2010, p31).

Alguns fatores que limitam o uso efetivo das ferramentas de e-Gov estão diretamente ligados a fatores de segurança da informação. Segundo a pesquisa do comitê gestor, os usuários de e-Gov apontam uma preocupação na proteção e segurança dos dados do cidadão. O mesmo relatório de 2010 aponta que trinta e nove por cento (39%) dos entrevistados declararam a sua desconfiança com a segurança de suas informações.

Há grandes desafios para o avanço do governo eletrônico no Brasil. Segundo o CGI.br (2010), uma premissa fundamental do governo eletrônico está na necessidade da formulação de serviços utilizando novas tecnologias. O relatório do CGI.br (2010) apresenta ainda o conceito de governo focado no cidadão, que foi tema de discussão em muitos países, como Canadá, Estados Unidos, Inglaterra e Austrália. Este conceito torna o cidadão o centro da dinâmica dos processos do governo.

Segundo o CGI.br (2010, p 49), as aplicações de e-Gov devem ser simples, intuitivas e até mesmo lúdicas, facilitando o uso da ferramenta, para aqueles de pouco conhecimentos. O uso de aplicações *Web 2.0*, tais como as redes sociais, *blogs* e *wikis*, vêm crescendo bastante. Estas ferramentas proporcionam o uso inclusivo nas diversas camadas da sociedade. Existe ainda uma linha paralela que se refere à qualidade do serviço de e-Gov, relacionada a questões de segurança da informação, do desempenho das aplicações, da infraestrutura dos sistemas, da interoperabilidade entre as aplicações e da acessibilidade das ferramentas.

O CGI.br (2010) afirma que, de forma complementar, outra possibilidade está na utilização de serviços digitais como cartões inteligentes (do inglês *smart cards*) ou outros dispositivos que garantam maior segurança na utilização do serviço oferecido pelo governo.

### 2.1.1 A arquitetura e-PING

Visando tratar alguns aspectos de interoperabilidade, o programa de e-Gov do Brasil definiu a arquitetura e-PING. Segundo o programa BRASIL (2011), que define o Comitê Executivo do Governo Eletrônico, a arquitetura e-PING (Padrões de Interoperabilidade de Governo Eletrônico) é o conjunto mínimo de premissas, políticas e especificações técnicas que regulamentam a utilização da tecnologia da informação e comunicação (TIC) na interoperabilidade de serviços de governo eletrônico. A arquitetura estabelece as condições de interação com os demais poderes da esfera governamental e com a sociedade de modo geral.

A adoção da arquitetura e-PING não pode ser imposta aos cidadãos, diferentes esferas governamentais, no país ou fora dele. A arquitetura e-PING estabelece um padrão de especificações definido pelo governo brasileiro. Logo, como essa arquitetura não está sendo imposta, a adesão se dará de forma voluntária. No entanto, para os órgãos do governo federal – Poder Executivo brasileiro – a adoção dos padrões e políticas contidos na e-PING é obrigatória (Portaria SLTI/MP número 5 de 14 de julho de 2005) (GOV.BR, 2013).

A arquitetura e-PING (BRASIL, 2011, p. 9) não tem como foco trabalhar com todos os assuntos relacionados à área de tecnologia da informação e comunicação. Apenas especifica aspectos relevantes para garantir a conectividade de sistemas, integração de dados, acesso seguro a serviço de governo eletrônico e gerenciamento de conteúdo.

O conceito de interoperabilidade também é definido em BRASIL (2011), tendo como base as definições utilizadas em outros países e organizações, conforme segue:

- Reino Unido: “Intercâmbio coerente de informações e serviços entre sistemas. Deve possibilitar a substituição de qualquer componente ou produto usado nos pontos de interligação por outro de especificação similar, sem comprometimento das funcionalidades do sistema.” (BRASIL, 2011);

- Austrália: “Habilidade de transferir e utilizar informações de maneira uniforme e eficiente entre várias organizações e sistemas de informação.” (BRASIL, 2011);
- ISO: “Habilidade de dois ou mais sistemas (computadores, meios de comunicação, redes, software e outros componentes de tecnologia da informação) de interagir e de intercambiar dados de acordo com um método definido, de forma a obter os resultados esperados.” (BRASIL, 2011); e
- Lichun Wang, Instituto Europeu de Informática - Cobra Workshops: “Interoperabilidade define se dois componentes de um sistema, desenvolvidos com ferramentas diferentes, de fornecedores diferentes, podem ou não atuar em conjunto.” (BRASIL, 2011).

Segundo BRASIL (2011), a arquitetura e-PING se divide em cinco áreas, que são:

1. Interconexão;
2. Segurança;
3. Meios de Acesso;
4. Organização e Intercâmbio de Informações; e
5. Áreas de Integração para Governo Eletrônico.

Cada uma das cinco áreas apresentadas anteriormente é estudada a partir de grupos de trabalho definidos pela coordenação geral da e-PING. No contexto deste trabalho, apresentam-se, a seguir, algumas recomendações da e-PING para o desenvolvimento de sistemas, intercâmbio de informações e segurança que são:

- Para o protocolo de transferência de hipertexto adota-se o protocolo HTTP/1.1 (RFC 2616);



- Para a transferência de dados em redes inseguras, recomenda-se a utilização da especificação TLS (*Transport Layer Security*)<sup>3</sup> RFC 52463 (atualizada pela RFC 5746 e RFC 5878). Caso seja necessário o protocolo TLS v1 pode emular o SSL v3;
- Para os mecanismos internos inerentes à utilização do TLS v1, a e-PING recomenda múltiplas alternativas de algoritmos, para cada caso: RSA, Diffie-Hellman RSA, Diffie-Hellman DSS, DHE\_DSS e DHE\_RSA (definição de chaves de cifração), RC4, IDEA, 3DES e AES (troca de chaves durante o *handshake* de uma sessão), SHA-256 ou SHA-512 (implementação de funções de hash) (BRASIL, 2011).
- Para o componente de Certificado Digital, recomenda-se a utilização da especificação X.509 v3. Esses certificados devem ser emitidos por entidades pertencentes à rede da entidade certificadora conhecida como ICP-Brasil (BRASIL, 2011); e
- Para a complementação dos serviços oferecidos pelo TLS v1, a e-PING recomenda a utilização do SASL (*Simple Authentication and Security Layer*). O SASL possibilita o desacoplamento entre mecanismos de autenticação e protocolos de aplicação, e também viabiliza um procedimento conhecido como *proxy authorization* (um usuário assume a identidade de outro, em um contexto de alta confiabilidade) (BRASIL, 2011);

Algumas recomendações sobre segurança no desenvolvimento de sistemas são feitas pela e-PING. Para o componente de autenticação e autorização de acesso XML, recomenda-se a adoção da especificação SAML. E para a intermediação ou federação de identidades, recomenda-se a utilização das especificações WS-Security 1.1 e WS-Trust 1.4.

Segundo a arquitetura e-PING, o padrão SAML (*Security Assertion Markup Language*) deve ser utilizado para a troca de informação sobre autenticação e autorização entre domínios. O Ws-Security 1.1 deve ser utilizado para o fornecimento de segurança às mensagens SOAP (*Simple Object Access Protocol*) e o WS-Trust 1.3 deve ser utilizado para a gestão de relacionamentos confiáveis entre os envolvidos na troca de mensagens seguras (BRASIL, 2011).

---

<sup>3</sup> Com as modificações introduzidas na versão 3.1, o SSL passou a ser chamado de TLS (*Transport Layer Security*) ou Segurança da Camada de Transporte. A e-PING recomenda a utilização do TLS v1 (BRASIL, 2011).

Ainda no segmento de segurança no desenvolvimento de sistemas, a arquitetura e-PING define como protocolo a serem adotados para o acesso a *Web Services* as especificações SOAP v1.2 e HTTP/1.1 (REST). Este segundo é considerado muito importante para o contexto da proposta deste trabalho, por se tratar de um protocolo de comunicação leve e relativamente fácil de ser implementado em relação à especificação SOAP.

## 2.2 SISTEMAS DE GERENCIAMENTO DE IDENTIDADE

Como visto anteriormente, o governo eletrônico só é possível com a utilização de sistemas de gerenciamento de identidades. Existem alguns modelos que podem ser implementados em sistemas de gerenciamento de identidades e que serão apresentados nesta seção.

Segundo Wingham *et al.* (2010), o modelo tradicional é amplamente utilizado nos sistemas computacionais presentes na Internet. Neste modelo, a identificação do usuário é tratada de forma isolada no provedor de serviços, o qual também atua como provedor de identidades (ver Figura 2a). Cabe ao usuário criar uma identidade digital para os provedores de serviços que deseja interagir, sem que haja o compartilhamento das identidades dos usuários entre diferentes IdPs.

Apesar de o modelo tradicional ser amplamente adotado, seu uso tende a ser custoso tanto para usuários quanto para provedores de serviços é custoso para os usuários, pois estes precisam controlar separadamente suas múltiplas identidades em diferentes provedores. E é custoso para os provedores de serviços, pois exige que estes mantenham um conjunto próprio de atributos para compor a identidade digital dos usuários que utilizam seus serviços. Por outro lado, um conjunto comum de atributos pode ser exigido por diversos provedores de serviços, como nome, senha, endereço, data de nascimento, entre outros (JOSANG; POPE, 2005).

Um sistema de gerenciamento de identidades define tecnologias que permitem às organizações a manipulação das identidades (atributos de identidades), assim como tecnologias integradas de políticas e de processos de negócios (JOSANG; POPE, 2005). A gestão de identidades trata também de alguns aspectos de certificação e gerenciamento do ciclo de vida das identidades digitais (JOSANG; POPE, 2005).

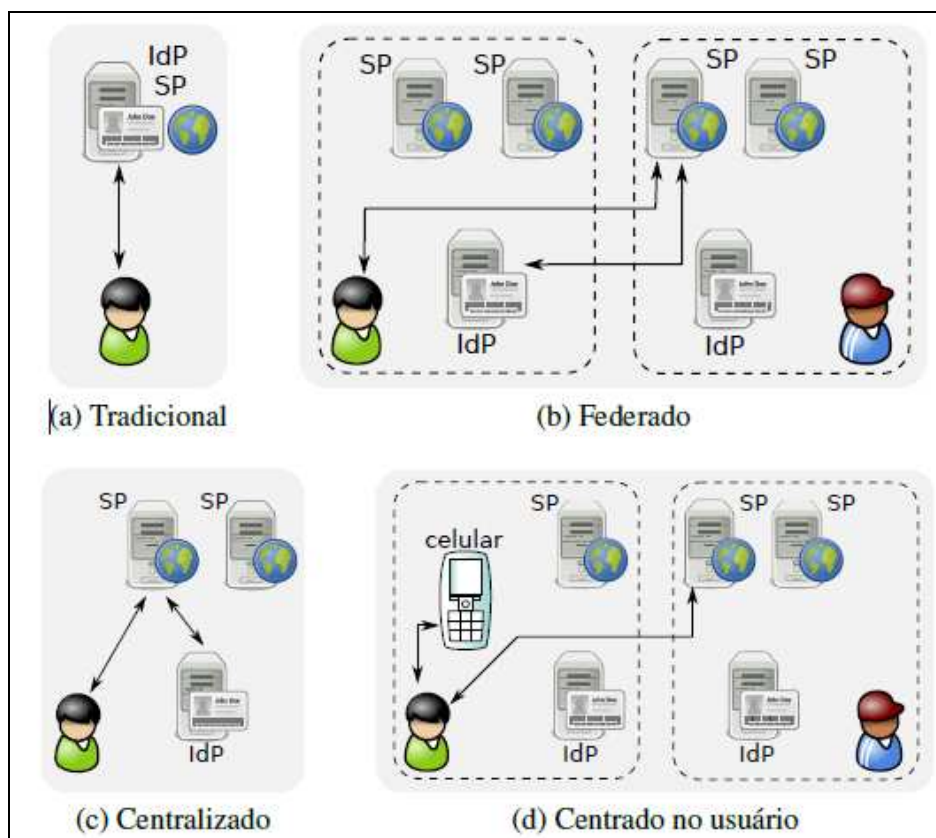


Figura 2. Classificação dos modelos de gerenciamento de identidade.

Fonte: Wingham *et al.*, (2010).

Para Chadwick (2009), o gerenciamento de identidades consiste em um conjunto de funções e habilidades para a administração, descoberta e troca de informações. Estas funções são usadas para garantir a consistência das informações contidas na identidade e permitem que as relações comerciais possam ocorrer de forma segura.

É dentro deste contexto de descoberta e troca de informações que surgiram três modelos para o gerenciamento de identidades. O primeiro a ser citado é o modelo centralizado (ver Figura 2c) implementado dentro do contexto de uma organização que deseja compartilhar as identidades dos seus usuários ou clientes para seus diversos provedores de serviço. Nota-se que este modelo é uma evolução do modelo tradicional, no sentido de centralizar a manutenção das identidades dos utilizadores, mas ainda mantém o fluxo de informações apenas no contexto da organização.

Com a evolução da tecnologia, pensou-se na possibilidade de compartilhamento de identidades entre contextos de organizações. Diante deste cenário, surge o modelo de identidades federadas (ver Figura 2b). Este modelo provê o compartilhamento das informações e atributos dos

usuários entre contextos de organizações separados, promovendo a reutilização e compartilhamento de identidades entre organizações participantes do círculo de confiança (JOSANG; POPE, 2005).

Seguindo ainda a evolução do modelo federado, observou-se a necessidade do consentimento do usuário para o compartilhamento de suas informações. Então surge o modelo centrado no usuário (ver Figura 2d). Este modelo pode prover as mesmas funcionalidades do modelo federado, mas com garantias adicionais para os usuários, sendo que estes se tornam o centro do mecanismo e são os responsáveis por liberar ou não o acesso as suas informações para determinados provedores de serviços.

Conforme mencionado anteriormente, o gerenciamento de identidades federadas é uma abordagem para aperfeiçoar a troca de informações da identidade através de relações de confiança, construídas entre as organizações que compõem a federação (CAMENISCH; PFITZMANN, 2007). Acordos estabelecidos entre os provedores de identidades garantem que as identidades emitidas em um domínio sejam aceitas por provedores de serviços em outros domínios, garantindo, assim, o funcionamento do conceito de autenticação única (do inglês - *Single Sign On* - SSO) (JOSANG; POPE, 2005).

É comum que as organizações governamentais criem e gerenciem os atributos das identidades dos usuários em duplicidade no sistema de autenticação. Essa duplicidade muitas vezes está ligada à utilização de um modelo tradicional de gerenciamento de identidades conforme descrito anteriormente. Os sistemas governamentais, formados por diversas instâncias governamentais, agrupadas em instâncias municipais, estaduais e federais, favorecem a criação de identidades e atributos dos usuários em duplicidade, e isto pode se tornar um caos para o gerenciamento e manutenção dessas identidades.

Segundo Baldoni (2010), uma solução para o problema descrito anteriormente é o modelo de gerenciamento de identidades federadas (do inglês *Federated Identity Management* - FIDM), que possibilita a integração de instituições parceiras. Uma federação pode facilitar a integração, reduzir custos e aumentar a velocidade de implantação de sistemas e melhorar a disponibilidade de serviços para a população.

Segundo Chadwick e Inman (2000), os sistemas de gerenciamento de identidades federadas tipicamente adotam o modelo ABAC (do inglês *Attribute-based Access Control*). Os sistemas de

gerenciamento de identidades federadas são implementados a partir de múltiplos IdPs remotamente distribuídos e são utilizados para conceder acessos aos provedores de Serviço (SPs). Assim, nos sistemas de identidades federadas, a confiança deve ser estabelecida entre os IdPs e SPs, constituindo um círculo de confiança. As autorizações para o uso dos serviços federados são baseadas nos atributos dos usuários.

Mesmo sendo comum que os usuários tenham atributos em múltiplos provedores de identidade, para Chadwick, Inaman e Klingenstein (2010), a maioria dos sistemas de gerenciamento de identidades federadas tem limitação no que diz respeito à abordagem de agregação de atributos dos usuários em múltiplos provedores de identidade.

A fim de mapear os trabalhos realizados em outros países, a pesquisa da Organização para Cooperação e Desenvolvimento Econômico - OECD (*Organization for Economic Co-operation and Development*) procurou identificar as principais tecnologias e aplicações que estão sendo adotadas. Segundo a OECD (2011), dois países (Austrália e Estados Unidos) consideram o aspecto da segurança como o objetivo fundamental de sua estratégia de IdM. Para a maioria dos outros países, o objetivo primordial do desenvolvimento de uma estratégia nacional de IdM é possibilitar o governo eletrônico no uso das aplicações de e-Gov. A estratégia de IdM da maioria dos países também inclui transações com o setor privado buscando promover a inovação na Internet de forma mais ampla. Um relato importante da pesquisa afirma que todos os países reconhecem a necessidade do gerenciamento de diversas camadas da administração pública (federal, estadual e municipal), independentemente do seu nível de autonomia. Entretanto, este aspecto é muitas vezes apontado como um desafio.

De acordo com a OECD (2011), diversos países estão desenvolvendo e implementando as suas estratégias nacionais de gestão de identidades (IdM) utilizando serviços de governo eletrônico. O Brasil não especificou ainda a sua estratégia nacional de gestão de identidades. O que existe são apenas as recomendações da arquitetura e-PING do Brasil, conforme apresentado anteriormente. Analisando as recomendações do E-PING, pode-se apontar que o modelo mais alinhado ao programa de governo eletrônico é o de identidades federadas.

## 2.3 A ESPECIFICAÇÃO SAML

Segundo a comissão de segurança de serviços técnicos da organização para o avanço de padrões de informação estruturada (do inglês *Security Services Technical Committee of the Organization for the Advancement of Structured Information Standards*), OASIS (2005a), o SAML é um *framework* baseado em XML usado para comunicar de forma segura a autenticação do usuário, seus direitos e seus atributos entre os parceiros de negócio on-line. Este *framework*, composto por um conjunto de especificações, permite a geração de afirmações de identidades, de autorização e atributos informados pelos usuários.

As asserções SAML são portáteis, ou seja, podem ser compartilhadas entre os parceiros de confiança conforme implementado pelo sistema de compartilhamento SAML. O padrão SAML define a sintaxe e regras claras para solicitação, criação, comunicação e utilização das asserções SAML (OASIS, 2008).

Como já descrito anteriormente, as asserções SAML são codificadas em arquivos XML que geralmente são incorporados em outras estruturas para o transporte, como por exemplo, o HTTP POST ou mensagens SOAP (*Simple Object Access Protocol*) codificadas. Esse tipo de transporte é denominado na especificação como *binding* e fornece um conjunto base de perfis para o uso de afirmações e protocolos, visando possibilitar a interoperabilidade ao se utilizar dos recursos SAML OASIS (2005b).

Segundo OASIS (2005a), o SAML versão 1.0 tornou-se um padrão em novembro de 2002. Em setembro de 2003, ganhou força, sendo utilizado por serviços financeiros, na educação, nos governos, na indústria e em outros segmentos.

Em 2005, foi lançada a especificação SAMLv2.0 que fortalece a construção de federações de identidades, com maior utilização na área da educação como no caso do *Shibboleth* e da *Iniciativa Kantara*. Esta versão foi um passo fundamental para implantação do modelo de identidades federadas. O SAML 2.0 tem sido bastante adotado nas estratégias nacionais de gestão de identidades OECD (2011).

Segundo OASIS (2005a), existem alguns **benefícios na utilização da especificação SAML**, quando utilizada como mecanismo de troca de informações de identidades digitais dos usuários e das organizações. Estes benefícios são:

- Neutralidade da plataforma: Independente da lógica da aplicação, a segurança da especificação SAML é garantida. Isso é um princípio importante da arquitetura orientada a serviços. Este benefício é garantido por abstrair da estrutura de segurança a arquitetura determinada;
- Liberdade no acoplamento de diretórios: O SAML não requer que as informações do usuário sejam mantidas e sincronizadas entre os diretórios;
- Melhora da experiência on-line dos usuários finais: SAML permite o SSO (*single sign-on*), possibilitando que os usuários se autentiquem em um determinado provedor de identidade e, em seguida, possa acessar os demais provedores de serviço da federação sem a necessidade de se identificar novamente. Desta forma o SAML promove a privacidade e melhora a experiência dos usuários na personalização em cada serviço;
- Redução dos custos administrativos para o serviço de provedores: A utilização de uma única forma de identificação viabilizada pelo SAML pode reduzir os custos de manutenção e gerenciamento das contas dos usuários, isso porque os custos são transferidos para o provedor de identidade, o que não é possível no modelo tradicional de gerenciamento; e
- Transferência de risco: O SAML transfere a responsabilidade pela gestão das identidades do usuário para o provedor de identidades. O provedor de identidade tem o foco na gestão das referidas identidades, e geralmente possui o modelo de negócio mais compatível do que um provedor de serviços.

Segundo OASIS (2005a), a versão 2.0 do SAML introduz um grande número de características importantes, que são:

- Pseudônimos: o SAMLv2.0 define um identificador aleatório, sem relação correspondente com os identificadores significativos da identidade real. Essa técnica foi criada para inibir o rastreamento das informações das identidades dos usuários entre seus múltiplos provedores de identidade;
- Identificadores de Gestão: o SAMLv2.0 define como dois provedores podem estabelecer e, posteriormente, gerenciar os identificadores aleatórios aos quais eles estão ligados;

- Metadados: os metadados do SAML definem como expressar as configurações de confiança dos dados relacionados para tornar a implantação de SAML mais fácil. Ao fazer isso, este identifica os atores envolvidos nos diversos perfis, como o provedor de identidade e o provedor de serviço;
- Criptografia: o SAMLv2.0 permite a criptografia de declaração de atributos, os identificadores de nome ou as asserções inteiras. Esta característica assegura a confidencialidade das trocas de mensagens;
- Perfis de Atributos: este perfil simplifica que a configuração e a implantação de sistemas para a comunicação de atributos, incluindo o suporte, a sequência de nomes e de valores de atributos extraídos de esquemas XML. O perfil de atributos é subdividido em duas categorias conforme segue:
  - Perfis de atributos X.500/LDAP suportam que: nomes de atributos e valores X.500/LDAP; e
  - Perfis de atributos XACML que: definem formatos adequados para o processamento por XACML;
- Gerenciamento de sessão: o protocolo de *logout* único (do inglês *Single Logout*) do SAMLv2.0 fornece padrão em que todas as sessões de uma autoridade de sessão podem ser quase que simultaneamente finalizadas. Como por exemplo, se um usuário, após a autenticação em um provedor de identidade, usa a mesma autenticação em outros provedores de serviço, ele pode ter suas sessões iniciadas em todos os provedores, automaticamente encerradas, a pedido do provedor de autenticação inicial;
- Dispositivos: o SAMLv2.0 introduz um novo suporte para o ambiente móvel, abordando os desafios e restrições de largura de banda e as oportunidades possibilitadas pelos dispositivos inteligentes ou ativos;
- Mecanismos de privacidade: o SAMLv2.0 inclui mecanismos que permitem aos provedores comunicarem políticas de privacidade e configurações. Por exemplo, o SAML torna possível obter e expressar o consentimento de um usuário para que uma operação de consulta de atributos do usuário possa ser realizada; e
- Descoberta de provedores de identidade: em soluções com múltiplos provedores de identidade, os provedores de serviço necessitam de meios para descobrir o provedor real



da identidade do usuário. O perfil de descoberta de provedores de identidade se baseia em *cookies* gravados em um domínio comum entre a identidade e o provedor de serviços.

### 2.3.1 Componentes da especificação SAML

Segundo a OASIS (2005a), uma asserção é um pacote de informação que fornece uma ou mais declarações feitas por uma autoridade SAML. O SAML define três tipos diferentes de declarações de afirmações que podem ser criadas por uma autoridade SAML, que são:

- autenticação – esse tipo de declaração é normalmente gerada por um provedor de identidade SAML, que é encarregado de autenticar o usuário e manter o controle das suas informações;
- atributo – tem a ver com a associação dos atributos com um determinado usuário; e
- aecisão de autorização – tema ver com uma autorização de serviço a uma solicitação específica de acesso a um recurso que pode ser permitida ou negada.

A estrutura de uma asserção é genérica, provendo informações comuns para todas as declarações. Dentro de uma asserção existe uma série de elementos que descrevem a autenticação, os atributos ou as declarações definidas pelo usuário.

Segundo OASIS (2005a), o SAML define um número de protocolos (*protocols*) de solicitações e respostas que os provedores de serviços podem utilizar para:

- solicitar a uma determinada autoridade SAML uma ou mais asserções;
- solicitar a autenticação de um usuário em um provedor de identidade e receber a asserção correspondente;
- solicitar que um identificador de nome seja registrado;
- solicitar que a utilização de um identificador seja encerrada;
- recuperar uma mensagem do protocolo que foi solicitada por meio de um artefato;
- solicitar a saída simultânea de uma coleção de asserções, bem como o conhecido desconectar de tudo, ou “single logout”; e

- solicitar o mapeamento de um identificador de nome.

O SAML se utiliza de protocolos para a troca das asserções SAML entre os sistemas. Esse modelo de uso de protocolo é denominado comumente na especificação como ligações. Segundo OASIS (2005b), há uma variedade de ligações (*bindings*) possíveis para o transporte de mensagens entre as partes do sistema que se utilizam do SAML. Especificamente as ligações do SAML versão 2.0 são:

- *SOAP Binding*: na utilização desse tipo de *binding*, as mensagens SAML podem ser transmitidas utilizando-se o protocolo SOAP;
- *SOAP Reverso (Reverter Binding SOAP)*: assim como o *SOAP Binding*, as mensagens SAML também podem ser trocadas via SOAP reverso;
- *HTTP Redirect Binding*: o *binding* HTTP Redirect fornece um meio para transmitir as asserções SAML dentro da URL de uma solicitação HTTP. Essa opção pode ser utilizada quando não é possível um caminho direto entre um provedor de identidade e um provedor de serviços. Nesse caso a mensagem SAML será transportada de maneira indireta, normalmente, via o navegador *web* do usuário final;
- *HTTP POST Binding*: nesse modelo de *binding*, as mensagens SAML são transmitidas dentro do conteúdo de um formulário HTML, utilizando do método HTTP POST para postar o SAML em um provedor de serviços;
- *HTTP Artifact Binding*: este modelo de *binding* denominado de “Artefato HTTP SAML” fornece um mecanismo que permite a comunicação por intermédio de um agente do usuário HTTP intermediário. Esta ligação tem o objetivo de reduzir o fluxo de mensagens através do SAML; e
- *URI Binding*: este modelo de *binding* possibilita que uma asserção SAML específica seja repassada ao provedor de serviço por intermédio de uma HTTP URI.

Existem alguns perfis disponíveis no SAML. Os perfis possibilitam que os protocolos do SAML e suas asserções trabalhem em fluxos de dados específicos, por exemplo, com a finalidade de promover a funcionalidade de gerenciamento de identidades e autenticação única (SSO). Um perfil bastante utilizado é o *Web SSO profile*, que especifica o perfil como federação de identidades, habilitado para a sessão do navegador *web* do usuário, especificando a maneira pela qual as

afirmações de autenticação SAML são comunicadas entre um Provedor de Identidade e um Provedor de Serviços.

### 2.3.2 Uso de Pseudônimos

A Figura 3 ilustra um pseudônimo de atributo criado e adicionado à resposta SAML do Provedor de Identidade. O atributo, conforme exposto na linha 4, representa o pseudônimo para o atributo do usuário que foi criado no IdP, e pode ser relacionado a apenas este usuário. Neste caso, para o SAML, este atributo é um transiente ou transitório (*urn:oasis:names:tc:SAML:2.0:nameid-format:transiente*), e foi criado no IdP especificamente para expressar a troca de atributos realizada em nome do usuário para com o provedor de identidade.

```
1. <saml:NameID  
2. SPNameQualifier=https://sample/default-sp  
3. Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient">  
4. _cadebabdb3fe04d6cd86f6dc210bc253ff1ef71801  
5. </saml:NameID>
```

Figura 3. Exemplo de pseudônimo de atributo SAML

## 2.4 AGREGAÇÃO DE ATRIBUTOS

Segundo Chadwick, Inaman e Klingesteisn (2010), a autenticação do usuário em um provedor de identidade é o mais comum para o funcionamento dos sistemas de identidades federadas, sendo que este envia uma asserção de autenticação para o provedor de serviço, que em seguida concede acesso aos recursos como se baseando nos atributos do usuário. Nota-se que apenas um conjunto de atributos de identidade do usuário é envolvido durante a autenticação, porém, é comum que os usuários tenham atributos em múltiplos provedores de identidade.

Para Chadwick, Inaman e Klingesteisn (2010), a maioria dos sistemas de gerenciamento de identidades federadas tem limitação no que diz respeito à abordagem de agregação de atributos dos usuários em múltiplos provedores de identidade. Segundo os autores, a maioria dos sistemas de gerenciamento de identidades 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 provedores de identidade, possibilitando a agregação de atributos de múltiplas fontes, sem a necessidade de o usuário se autenticar separadamente em cada IdP.

Para Chadwick *et al.* (2010), muitas organizações estão fazendo experiências no uso de federações. Os autores apresentam alguns exemplos práticos como as federações acadêmicas, como por exemplo, a *Incommon* (EUA).

Nas federações acadêmicas, o provedor de serviços precisa ter garantias suficientes para confiar nas informações recebidas. As identidades contendo atributos agregados devem ser associadas de alguma maneira, sendo que uma asserção deve ser estabelecida em um contexto seguro no provedor de serviços (KLINGENSTEIN, 2007).

Chadwick, Inaman e Klingesteisn (2010) apresentam alguns requisitos considerados importantes pelos usuários para a construção de um modelo de agregação de atributos. Estes requisitos foram consolidados de resultados obtidos com a aplicação de um questionário<sup>4</sup>. São sete as categorias principais que classificam os requisitos e dentro dessa classificação apresentam-se doze requisitos considerados importantes, conforme pode ser observado no Quadro 1.

---

<sup>4</sup> As informações sobre o questionário aplicado e os resultados podem ser encontrados em: <http://sec.cs.kent.ac.uk/shintau/pages/requirements.html>

Quadro 1. Requisitos do usuário para agregação de atributos

<b>Categoria</b>	<b>Requisitos</b>
Requisitos Gerais	1. A agregação de atributos pode ser utilizada por uma variedade de formas, como: por seres humanos através do navegador <i>Web</i> ; por aplicações por intermédio das APIs ( <i>Application Programming Interface</i> ); por usuários de rede, através dos clientes de rede.
Requisitos relacionados à privacidade	2. A proteção da privacidade dos atributos do usuário é importante e isso pode ser feito através do uso de técnicas de controle que são independentes dos meios legais. 3. Os provedores de serviço podem ser capazes de rastrear os usuários entre suas sessões, se necessário. 4. Em circunstâncias excepcionais, os provedores de serviço podem identificar a verdadeira identidade dos usuários, no entanto, somente solicitando a identificação junto aos IdPs do usuário.
Requisitos de Consentimento do Usuário	5. IdPs e SPs podem se comunicar para unir os atributos do usuário e este processo deve ser de conhecimento e aprovação do usuário. 6. Somente com a aprovação dos usuários, os SPs podem consultar seus múltiplos IdPs, a fim de agregar os atributos adicionais dos usuários.
Exigências do Protocolo	7. Os protocolos devem ser capazes de funcionar através de <i>firewalls</i> utilizando-se de portas de comunicação já existentes, usando preferencialmente os protocolos HTTP e HTTPS. 8. O protocolo SAML é a escolha mais usual em sistemas de gerenciamento de identidades federadas. 9. O <i>proxy</i> de informação deve ser suportado através de múltiplos saltos ( <i>redirects</i> ).
Requisitos de Confiança	10. A capacidade opcional para assinar todas as asserções deve ser suportada em todas as trocas de mensagens. 11. O SP deve ser capaz de exigir que todas as asserções sejam assinadas pelas autoridades de atributos.
Requisitos de Usabilidade	12. O sistema deve ser fácil de utilizar e exigir o mínimo de interação do usuário.

Fonte: Adaptado de Chadwick, Inaman e Klingestein (2010).

## 2.4.1 Modelos de associação

A agregação de atributos precisa demonstrar que as informações contidas em duas identidades distintas referem-se a uma entidade. O modelo de identidades federadas precisa de um identificador comum para se referir a mesma entidade (principal), com isso identidades diferentes devem ser associadas durante o processo de agregação de atributos. Os modelos de associação descritos por Klingenstein (2007) são: associações contextuais; compartilhamento de identificadores; e federação de identidades.

### 2.4.1.1 Associações contextuais

Segundo Klingenstein (2007), as próprias transações de identidades federadas podem ser aproveitadas para criar um contexto de associação de uma entidade (principal). Quando duas ou mais asserções forem apresentadas, simultaneamente, por uma única asserção de usuário (*User Assertion* - UA), as asserções são implicitamente consideradas verdadeiras e ligadas pelo contexto.

Essa ligação é suficiente para que qualquer provedor associe o sujeito de uma asserção com uma representação local criada anteriormente.

#### **2.4.1.2 Compartilhamento de identificadores**

Para Klingenstein (2007), as contas em diferentes provedores de identidades podem ser associadas ao se transmitir um identificador utilizado em um IdP, através de uma asserção de usuário. Se o segundo IdP “reautenticar” o usuário, este irá detectar um identificador já associado com uma conta estabelecida anteriormente, então o IdP irá saber que ambos os identificadores são válidos para o usuário. O novo identificador pode ser armazenado com a identidade existente. Se o usuário ainda não tem uma identidade no segundo IdP, mas este provedor deseja manter informações sobre a identidade do usuário, este pode usar o identificador enviado pelo primeiro IdP como um identificador para a criação de uma nova identidade local, sem a necessidade de “reautenticar” o usuário.

#### **2.4.1.3 Federação de identidades**

O conceito de federação de identidades é diferente do conceito de identidades federadas, sendo que o primeiro conceito é conhecido como ligação de contas, que permite que um IdP crie um novo identificador para uma identidade (conta) e ligue este identificador a contas que estejam em outros provedores. Este identificador, que pode ser um pseudônimo, é unidirecional e pode ser revogado a qualquer momento pelo criador ou por qualquer critério do destinatário e por si só não revela nenhuma informação sobre um usuário. A complexidade adicionada preserva a privacidade e flexibilidade para o maior grau possível, associando permanentemente as identidades (KLINGENSTEIN, 2007).

### **2.5 ABORDAGENS PARA IMPLEMENTAÇÃO DE AGREGAÇÃO DE ATRIBUTOS**

Nesta seção serão apresentados os conceitos sobre as abordagens para implementação de agregação de atributos.

### 2.5.1 Banco de dados da aplicação

Os primeiros trabalhos sobre agregação de atributos assumem 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. Nesta abordagem o usuário precisa se autenticar uma única vez com seu certificado de chave pública, para que o processo de agregação dos atributos possa ser executado. Porém, atualmente, poucos usuários possuem certificados X.509. É mais comum que estes tenham diferentes nomes de usuário e diferentes atributos em seus vários IdPs (CHADWICK; INMAN, 2009).

Segundo Hulsebosch *et al.* (2011), a forma mais simples de agregação de atributos permite que o SP colete as informações sobre o usuário nos IdPs a partir de atributos informados pelo usuário, ficando por conta do SP gerenciar os atributos adicionais do usuário. A Figura 4 ilustra a sequência do fluxo de agregação dos atributos da proposta conforme segue:

1. O agente do usuário requisita o uso do serviço no SP;
2. O SP requisita a afirmação de autenticação;
3. O agente do usuário é redirecionado para o IdP 1;
4. O IdP 1 autentica usuário através de seu agente;
5. O IdP 1 retorna a asserção de autenticação;
6. O agente do usuário encaminha a afirmação de autenticação para o SP;
7. O SP busca os atributos adicionais do usuário a partir de um repositório de identidades (banco de dados); e
8. Por fim, é concebido o acesso ao serviço para o agente do usuário.

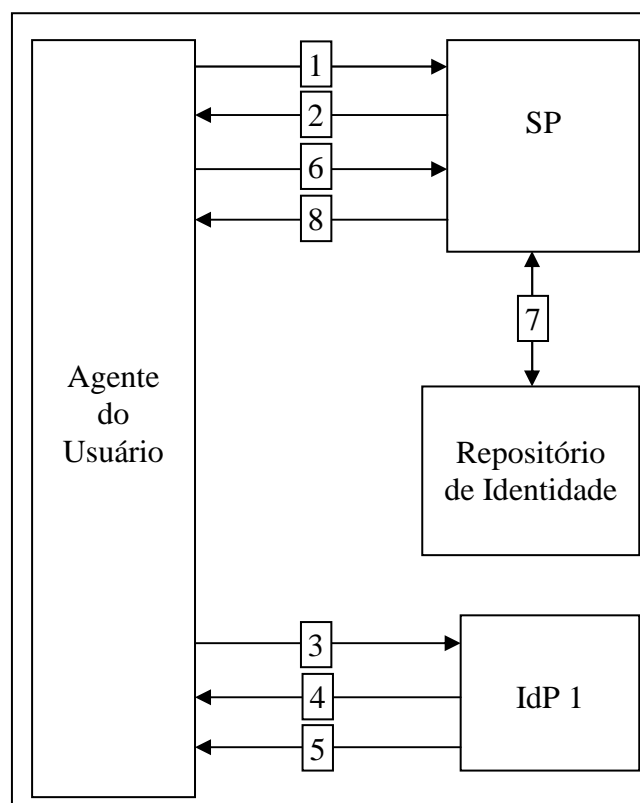


Figura 4. Banco de Dados SP

Fonte: Adaptado de Hulsebosch *et al.*, (2011).

### 2.5.2 Proxying de identidade

De acordo com Klingenstein (2007), as comunidades formam organizações virtuais (do inglês *Virtual Organizations* - VO). Estas organizações mantêm as informações sobre seus membros. 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, mas também pelos IdPs que disponibilizam os atributos ao IdP *proxy*.

Segundo Klingenstein (2007), o IdP *proxy* é capaz de identificar todos os atributos sobre qualquer identidade. As soluções *myVocs* (GEMMILL; LYNN; ROBINSON, 2005) e *I AM Suite* (BARTON *et al.*, 2006) implementam o modelo *IdP Proxy*.

Outras soluções, tais como *Grid-Shib* e *D-Grid*, também estão sendo estudadas, mas são capazes de agregar atributos de apenas duas autoridades. *MyVocs* é uma solução alternativa que coloca um servidor *myVocs* entre o IdP e o SP, além de suportar a comunicação entre vários IdPs



para a agregação de atributos. Apesar de ser uma vantagem considerável, o sistema *myVocs* tem sérias limitações em seu modelo de confiança. As limitações estão na imposição da confiança dos atributos enviados do IdP *myVocs* aos SPs, sem garantias sobre a fonte autenticadora destes atributos, já que o IdP *myVocs* parece ser a fonte oficial dos atributos. (CHADWICK; INAMAN; KLINGESTEISN, 2010).

### 2.5.3 Proxy de retransmissão de identidade

Segundo Hulsebosch *et al.* (2011), a técnica de retransmissão de identidade pode ser considerada uma especificação de um *proxy*. Embora as trocas de atributos no modo de retransmissão de identidade seja semelhante ao modelo de IdP *proxy*, no modelo de retransmissão tem-se a garantia 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 afirmações de atributos criptografadas.

Este modelo requer uma relação de confiança entre os IdPs e os SPs. O modelo de retransmissão de identidade é seguro, mas compromete um pouco a privacidade do usuário, já que o IdP retransmissor poderá monitorar todas as ligações de identidades e seus serviços utilizados.

### 2.5.4 Agregação de atributos mediada pelo cliente

Para Klingenstein (2007), o modo de agregação de atributos mediado pelo cliente se aproveita do uso de clientes inteligentes (clientes ativos) que podem criar solicitações, mantendo o estado e agregando informações sobre o usuário. Exemplos destes clientes são o ECP SAML (do inglês *Enhanced Client or Proxy*) e os clientes ativos do *CardSpace*<sup>5</sup>. A coleta de atributos feita por estes clientes garante a privacidade dos usuários e a segurança contra os ataques de *phishing*<sup>6</sup>, além de tornar o fluxo simples. Este modelo em alguns casos não pode ser considerado SSO, uma vez que o usuário deve se autenticar várias vezes em diferentes IdPs para a agregação dos atributos. No

---

<sup>5</sup> 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 (do inglês *user-agent*) especializado (WANGHAM *et al.*, 2010).

<sup>6</sup> Em computação significa uma tentativa de fraude eletrônica, caracterizada por tentativas em adquirir informações pessoais, ao se fazer passar por uma pessoa confiável.

entanto, tais identificadores nunca poderão ser ligados, mantendo a segurança e a privacidade implícita no sistema.

### 2.5.5 Federação de identidade

A federação de identidade depende da capacidade do usuário em associar as identidades que controla. Um agente do usuário autenticado com sucesso em duas entidades diferentes pode controlar ambas as entidades e criar um identificador unidirecional persistente, permitindo que um IdP aponte para a identidade relacionada no segundo IdP. Isso pode ser repetido pelo provedor para criar uma ligação bidirecional (KLINGENSTEIN, 2007).

Este identificador contém informações limitadas sobre a ligação com a identidade. É possível codificar grandes quantidades de informação em um identificador, como por exemplo, um *NameID*. Por ser uma prática com limitações, torna-se necessária a utilização de asserções para associar as informações da identidade do usuário. Para permitir que terceiros utilizem este *link* de associação e agregar os atributos do usuário, este mapeamento precisa ser incorporado em uma afirmação. Além disso, o provedor pode requerer informações adicionais, tais como validade, qualidade de autenticação e evidência de intenção. SAML e ID-WSF<sup>7</sup> (do inglês *Identity Web Services Framework*) possibilitam a incorporação de valores adicionais nas afirmações. Na prática, esta técnica pode se tornar confusa ao necessitar de grandes trocas de informações (KLINGENSTEIN, 2007).

Segundo Chadwick e Inman (2000), os sistemas de gerenciamento de identidades federadas - FIM (do inglês *Federated Identity Management*) tipicamente adotam o modelo ABAC (do inglês *Attribute-based Access Control*). Os sistemas de gerenciamento de identidades federadas são implementados a partir de múltiplos IdPs, remotamente distribuídos, e são utilizados para conceder acessos aos prestadores de Serviço (SPs). Assim, nos sistemas FIM a confiança deve ser estabelecida entre os IdPs e os SPs, constituindo um círculo de confiança. As autorizações para o uso dos serviços federados são baseadas nos atributos dos usuários.

---

<sup>7</sup> Segundo Aarts *et al.*, (2006), ID-WSF é uma especificação que define uma série de protocolos que permitem a qualquer serviço interagirem com Web Services, um provedor de serviços Web, ou ambos.

### 2.5.6 SP mediando a agregação de atributos

Dependendo da capacidade do SP, é possível que este seja o mediador da agregação de atributos e isso é feito através da obtenção de informações de vários IdPs. Apesar da autenticação do usuário ser única para cada IdP, o SP realizará excessivos redirecionamentos para completar a agregação de atributos. Esta solução é das mais simples de ser desenvolvida, mas possibilita o rastreamento das informações dos usuários, visto que o SP irá mediar todo o processo de agregação de atributos (KLINGENSTEIN, 2007).

## 2.6 CONSIDERAÇÕES SOBRE ABORDAGENS DE AGREGAÇÃO DE ATRIBUTOS

Klingenstein (2007) comenta que a complexidade sempre vai existir na agregação de atributos devido à natureza do problema, e provavelmente não existirá uma solução perfeita para este problema. O autor comenta ainda que muitas comunidades estão dispostas a alterar os modelos de confiança tornando as trocas de informações mais complexas. Os mecanismos concebidos para a agregação de atributos podem implementar uma forma complexa para a formatação de afirmações, e as especificações de perfis para esta técnica podem ser necessárias para assegurar a interoperabilidade.

Para Chadwick e Inman (2009), o projeto *Liberty Alliance* foi o primeiro que tentou solucionar o problema da agregação de atributo no cenário federado, através do seu conceito de federação de identidade. Neste modelo, como o usuário se transfere entre os serviços da federação, o primeiro IdP autentica o usuário e pergunta se este gostaria de ser identificado em outros IdPs da federação. Caso o usuário queira ser identificado e, posteriormente, se autenticar em um segundo IdP, este será convidado a adicionar sua identidade à federação de identidades a partir do IdP de autenticação inicial. Ao federar a identidade do usuário, os dois IdPs criam um *alias* randômico e trocam este identificador nos bastidores da aplicação. Desta forma, nenhum dos IdPs sabe o identificador de acesso do usuário, mas cada um pode se referenciar a um mesmo usuário, e assim agregar os atributos.

Embora este modelo proteja de forma eficaz os identificadores dos usuários e não permita a troca de dados sem o consentimento dos mesmos, cada IdP ainda sabe que o usuário tem alguns atributos em outros IdPs. Isso não é o que acontece na vida real: a operadora de cartão de crédito

não precisa saber que o usuário é membro da IEEE, ou vice e versa, ainda assim o usuário poderia usar ambos os atributos em uma transação, por exemplo, para compra de um livro de uma loja online e ganhar desconto por ser membro da IEEE. O uso de múltiplos IdPs deve fornecer o conjunto de atributos agregados a um SP, sem que o mecanismo possa identificar o envolvimento de outros provedores de identidade (CHADWICK; INMAN, 2009).

O contexto de múltiplos IdPs pode trazer vantagens para os usuários, principalmente para segurança de seus dados. Pois manter os atributos de um usuário em um único IdP pode favorecer o acesso direto a todas as suas informações e também impossibilitar o anonimato e rastreabilidade das informações do usuário. No que diz respeito à implantação da federação governamental, manter um único IdP centralizado é algo irrealista devido à quantidade de sistemas e serviços utilizados. Logo, conclui-se que há a necessidade de se manter múltiplos IdPs, cada qual gerenciando apenas os atributos dos usuários que lhes são de responsabilidade.

Segundo Chadwick *et al.* (2010), o modo de operação típico nos mais modernos sistemas federados é que o usuário se autentique em um provedor de identidade (IdP) e este envie uma declaração de autenticação e os atributos para autorização para o provedor de serviços (SP), que em seguida, concede acesso a seu sistema com base nos atributos do usuário. Observa-se que apenas um IdP e um conjunto de atributos de identidade do usuário são tipicamente envolvidos nesta troca.

No entanto, a maioria dos usuários tem atributos espalhados em diversos provedores de identidade. A maioria dos sistemas de organizações virtuais federadas sofre com a limitação da falta de uma abordagem padrão para agregar atributos de usuários (CHADWICK *et al.*, 2010).

Diante do exposto, nota-se que a utilização de sistemas de gerenciamento de identidades, em organizações privadas, na educação e no governo, estão ganhando força, promovendo a reutilização das identidades dos usuários, que compartilham seus atributos dentro do círculo de confiança da federação de identidades.

A utilização destes mecanismos nos governos está ganhando força principalmente porque existe um apelo mundial para as melhorias e aplicação dos governos participativos, o que pode ser notado no relatório da ONU (2010), relatório este que não posiciona o Brasil dentre os melhores classificados. E pior, avaliando os dois últimos relatórios, nota-se perda de posições para o país na classificação, e que países vizinhos ao Brasil, notadamente, estão mais bem classificados.

Para proporcionar ao governo federal opções em se tornar um governo mais participativo e visando oferecer uma estratégia de agregação de atributos para um modelo de gerenciamento de identidades nacional, buscou-se, principalmente, uma solução que promova a segurança das informações trocadas entre os provedores de identidades e os serviços oferecidos no país. A segurança está ligada também ao usuário do mecanismo, em oferecer a privacidade aos usuários, inviabilizando o rastreamento das informações de cada usuário no uso do mecanismo agregador.

Essas questões de segurança das informações dos usuários são muito importantes para um mecanismo agregador de atributos, pois conforme o exemplo exposto por Chadwik e Inman (2009), uma companhia de cartão de crédito não precisa saber que o usuário é membro da IEEE, ou vice e versa, e mesmo assim o usuário poderia usar ambos os atributos em uma transação, por exemplo, para comprar um livro de uma loja *on-line* e ganhar desconto por ser membro da IEEE.

Esta questão de não permitir a rastreabilidade das informações do usuário deve ser considerada em um ambiente governamental, pois para os usuários é importante manter o sigilo de suas informações, e que estas sejam utilizadas por provedores somente com seu consentimento. Para evidenciar o consentimento do usuário durante o processo de agregação de atributos, é necessário que o mecanismo agregador de atributos seja centrado no usuário. Este requisito é considerado importante para a composição do modelo proposto neste trabalho.

### 3 TRABALHOS RELACIONADOS

Este capítulo apresenta os trabalhos relacionados, que foram selecionados após a execução de um protocolo de busca (ver APÊNDICE A →) que visou identificar os trabalhos que tratam do problema da agregação de atributos. Os trabalhos analisados seguem uma ordem cronológica a partir do ano de publicação.

#### 3.1 LEE, KIM E HONG (2008)

Lee, Kim e Hong (2008), propõem um modelo de agregação de atributos que segue a abordagem de agregação de atributos mediada pelo provedor de serviço (SP) e que utiliza a avaliação da reputação dos provedores de identidade no processo de agregação dos atributos do usuário. Para auxiliar no processo de agregação, cada SP obtém os atributos dos IdPs e os armazena em seu repositório de dados local. A Figura 5 ilustra o processo de agregação proposto por estes autores com os seguintes passos:

1. Suponha-se que inicialmente os pares se confiam, formando um círculo de confiança;
2. O usuário (solicitante) requisita um serviço;
3. Para cada atributo necessário no controle de acesso, o provedor de serviços coleta os valores dos atributos nos IdPs;
4. As consultas aos IdPs pelos provedores de serviços requer a confiança entre os pares;
5. Para cada valor de atributo coletado, o SP avalia a confiabilidade do IdP; e
6. De acordo com a avaliação de confiança, os valores dos atributos obtidos a partir dos pares não confiáveis são filtrados. O provedor agrega os atributos não filtrados e, em seguida verifica a permissão de acesso do usuário.

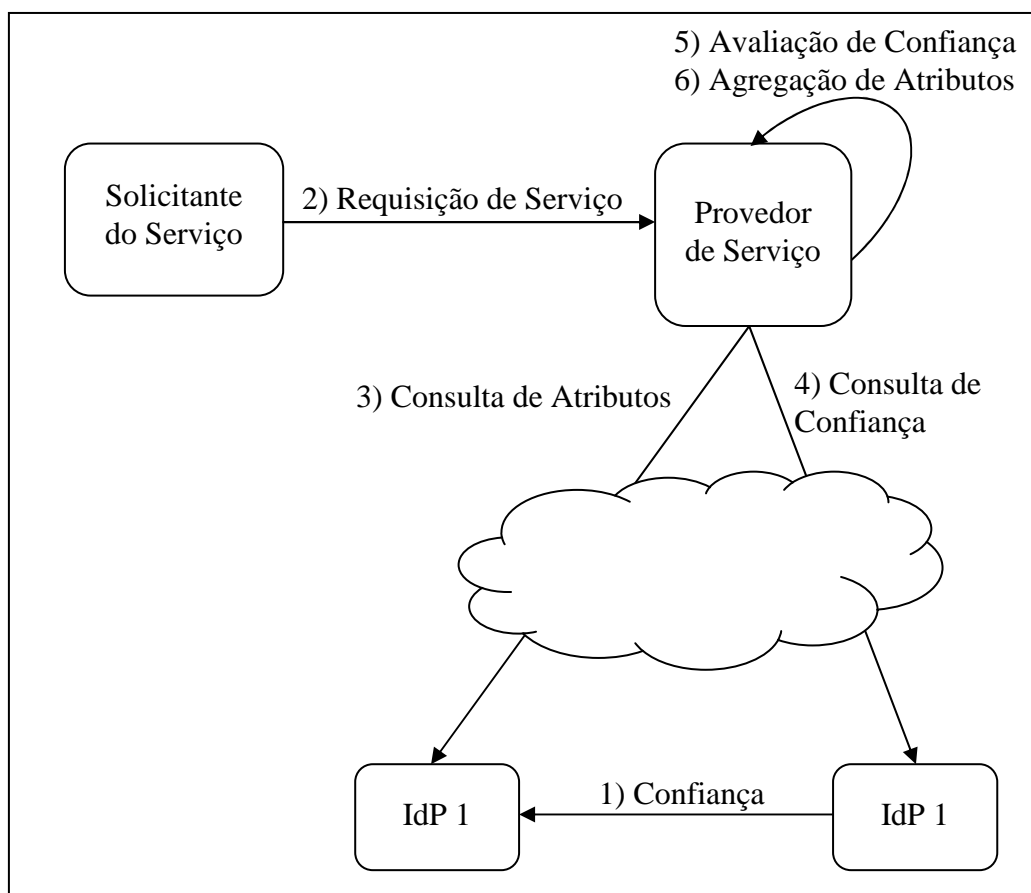


Figura 5. Coleta de Atributos

Fonte: Adaptado de Lee; Kim; Hong, (2008).

Basicamente, o modelo de agregação de atributos proposto por Lee, Kim e Hong (2008) se divide em três fases.

A primeira fase que é a de descoberta de atributos, onde o mecanismo recebe a requisição de um SP. O provedor recupera e classifica os atributos do usuário de seu repositório local, caso o mesmo SP já tenha realizado um acesso anterior. Caso contrário, durante a primeira solicitação de atributos de um provedor de serviço o mecanismo realiza uma consulta de atributos de seus pares, dentro do círculo de confiança. Para a recuperação dos atributos em seus pares o mecanismo de utiliza de um protocolo de consulta de múltiplos provedores.

A segunda fase, que é a fase de avaliação de confiança, onde o modelo adota uma avaliação da confiança de seus pares para solucionar o problema de pares maliciosos.

A terceira fase é a de agregação de atributos. Nesta fase os atributos dos usuários são agregados dos provedores. Os valores dos atributos aceitos devem ser agregados para obter um

valor representativo, que serão utilizados no modelo de controle de acesso baseado em atributos (ABAC).

### 3.2 CHADWICK, INAMAN E KLINGESTEIN (2010)

Chadwick, Inaman e Klingestein (2010) descrevem um modelo conceitual para a agregação de atributos que permite os provedores de serviços (SP) autorizarem solicitações de acesso dos usuários com base em atributos afirmados por vários provedores de identidade (IdP). O modelo utiliza um novo componente chamado de serviço de ligação (do inglês – *Linking Service* - LS), que tem por objetivo, ligar as contas dos usuários que estão em diferentes provedores de identidade (IdPs). A solução proposta pelos autores está baseada no protocolo SAML versão 2.0.

O modelo proposto requer que, no momento do registro do usuário, o IdP gere um nível de garantia (do inglês *Level of Assurance* - LoA) do processo de registro e este nível seja atribuído tendo como base o nível de verificação das informações fornecidas pelo usuário. Os atributos auto afirmados, que são os que o usuário informa, tais como nome, idade, endereço, qualificação, etc., que são verificados pelo IdP, devem receber a LoA de registro igual um (1). No modelo proposto, o IdP pode suportar diversos mecanismos de autenticação, com níveis de garantia diferentes (LoA de autenticação). Quando o usuário se autentica em uma sessão de serviço, este receberá um LoA de autenticação, que mesmo sendo uma autenticação de alto nível irá respeitar o LoA de registro. Ou seja, se o usuário se autenticar em um IdP com LoA de autenticação quatro (4), porém com LoA de registro um (1), este terá um LoA de sessão igual um (1), evitando assim problemas de segurança ou de liberação de atributos indevida.

Chadwick, Inaman e Klingestein (2010) classificam que o processo de agregação de atributos pode ser dinâmico ou estático e transitório ou permanente e que este processo deve ser do consentimento e aprovação do usuário. O modo transitório dinâmico (*Dynamic-Transient*) significa que a ligação dos atributos (contas do usuário) é feita durante cada solicitação de acesso a um serviço (SP) e é esquecida após o serviço ser executado. O modo permanente estático (*Static-Permanent*) significa que a ligação é feita antes de qualquer requisição a um serviço (SP) e que poderá ser usada nas próximas requisições ao serviço. O modo permanente dinâmico (*Dinamic-Permanent*) significa que a ligação é estabelecida durante uma solicitação ao serviço (SP), e é armazenada para uso nas próximas requisições ao serviço. O modo transitório estático (*Static-Transient*) é incomum e não foi considerado no modelo proposto. O modo transiente dinâmico pode



ser implementado a partir de alguns sistemas já existente como o *Shibboleth*<sup>8</sup> e também não foi considerado, pois necessita da autenticação múltipla do usuário em vários IdPs para efetuar a agregação de atributos.

O modo permanente estático de agregação de atributos leva em consideração que o usuário já realizou a ligação de suas contas e criou a sua política de liberação de atributos. Conforme descrito anteriormente, o usuário acessa o SP e é redirecionado para o IdP escolhido para a autenticação. O SP envia um pedido de autenticação e os atributos desejados ao IdP de autenticação. Este questiona o usuário se ele pretende usar a agregação de atributos nesta sessão. Este procedimento será possível somente se, anteriormente, o usuário estabeleceu a ligação do IdP com o LS do usuário. Se não houver este vínculo entre o IdP e o SP então a agregação de atributos não será realizada.

A Figura 6 representa os fluxos de requisições entre os vários componentes do processo de agregação de atributos na proposta de implementação dos autores (CHADWICK; INMAN; KLINGENSTEIN, 2010).

Em seguida no passo três (3), ocorre as trocas de autenticação entre o IdP de autenticação e o agente do usuário. Isso viabiliza o SSO, pois o token de autenticação poderá ser utilizado subsequentemente. No passo quatro (4) o IdP de autenticação faz o redirecionamento do usuário para o provedor de serviço e indica o serviço (passo 5) de ligação que fará a ligação das contas do usuário.

O agente do usuário é redirecionado para o LS (passo 6) que solicita ao SP os atributos que este necessita. Após obter a indicação dos atributos requeridos, o LS redireciona o agente do usuário para o IdP configurado previamente (contém o atributo do usuário). Todos os IdPs previamente ligados aos atributos requeridos do usuário, retornarão ao SP as asserções de atributos. As asserções de atributos emitidas possuem um identificador aleatório atribuído pelo IdP de autenticação na asserção de autenticação. Isto prova ao SP que todos os atributos pertencem ao

---

<sup>8</sup> *Shibboleth* é um sistema que viabiliza o acesso único em sistemas em rede na internet. Ele possibilita que o usuário acesse os sistemas fornecidos pela federação utilizando apenas uma única identidade. Frequentemente utilizado por universidades ou serviços públicos.

mesmo usuário autenticado, sem revelar os IdPs do usuário para o SP. Todas as afirmações de atributos serão assinadas por suas fontes autorizadoras.

No passo sete (7), de posse da referência do IdP ligado, o SP e das asserções de atributos, o SP sabe requisitar ao IdP ligado os atributos desejados. As afirmações de autenticação e de atributo e do conjunto de referências são devolvidos ao SP pelo IdP ligado (passo 8). No passo nove (9) o provedor de serviço deve decidir sobre o serviço solicitado e responder ao usuário (passo 10).

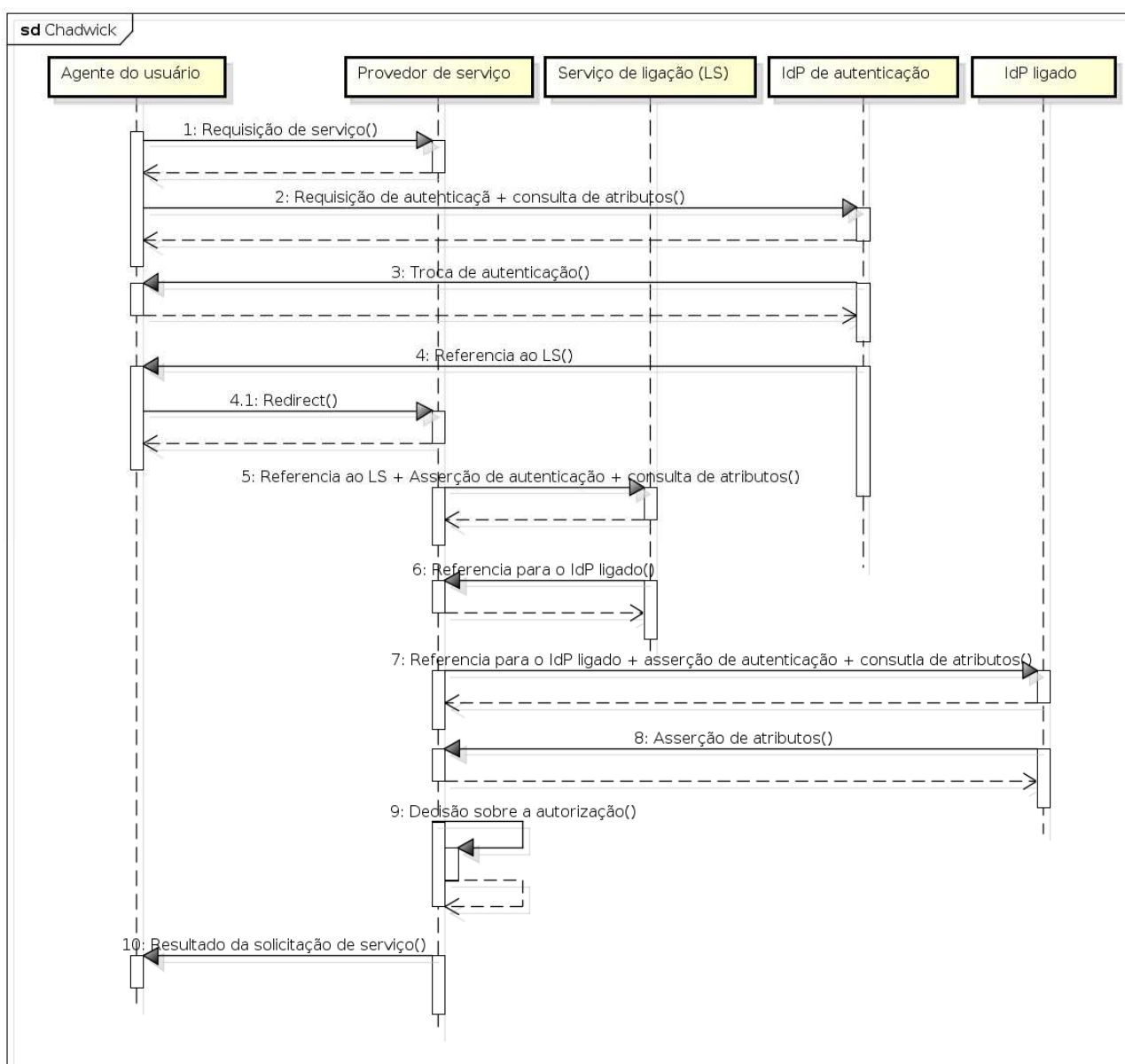


Figura 6. Fluxo de mensagens do modo permanente estático para a agregação de atributos

Fonte: Adaptado de Chadwick; Inman; Klingenstein, (2010).

No modo permanente dinâmico o usuário acessa o SP e, neste caso deve escolher o seu serviço de ligação (LS), no lugar do IdP de autenticação como no modo permanente estático. A vantagem desse modo, está em o usuário pode escolher dinamicamente os IdPs que serão usados para cada sessão de serviço, enquanto que no permanente estático, apresentado anteriormente, uma política deve ser previamente configurada no LS, para que o provedor de serviços tenha acesso aos atributos dos usuários nos mais diversos provedores de identidades.

### 3.3 HOELLRIGL, KUHNER, DINGER E HARTENSTEIN (2010)

Hoellrigl *et al.* (2010), afirmam que os atuais sistemas para o gerenciamento de identidades (FIM) centrados no usuário oferecem apenas a troca de atributos entre um IdP e um SP, ou seja a troca de atributos entre múltiplos IdPs e SPs não é possível. Toda a comunicação entre um IdP e SP deve ser processada pelo *client* do usuário, este componente permite que o usuário aprove a troca de informações.

Um fluxo de atributo direto de IdP para SP é evitado. Assim, inconsistências entre um IdP e SP só podem ser resolvidas durante a utilização do serviço. O SP somente irá ter acesso aos atributos do usuário, quando este estiver efetivamente utilizando o serviço e manualmente aprovar a troca de dados.

A abordagem adotada no modelo proposto por Hoellrigl *et al.* (2010) viabiliza a criação de um mecanismo de delegação de identidade automatizado e controlado pelo usuário. O modelo introduz um novo componente denominado de delegado de identidade (do inglês *Identity Delegate*), que atua em nome do usuário quando algum provedor de serviço desejar acessar os atributos do usuário, mesmo que o usuário não esteja conectado.

Na proposta de Hoellrigl *et al.* (2010), o delegado torna-se a terceira parte confiável do modelo, com a vantagem da automatização do fluxo de liberação dos atributos através da criação de políticas. O delegado atua como um replicador de identidade (do inglês *Identity Relay*), que apenas recolhe e encaminha os atributos e não os armazena localmente. Assim, no caso de uma invasão, se o atacante controlar o delegado ele não será capaz de capturar, armazenar ou alterar os atributos do usuário.

O uso do delegado envolve diferentes etapas. Na fase de preparação, o delegado, é concebido como um serviço prestado por um terceiro confiável e deve ser configurado (IdPs, SPs e a padronização dos metadados de federação) para ser utilizado pelo usuário. O próximo passo, chamado etapa de registro, permite ao usuário indicar os IdPs que o delegado pode recuperar os atributos e criar sua identidade (*information card*) no delegado.

Na etapa de autorização (ver Figura 7), o usuário habilita o SP a recuperar os atributos do delegado de identidade. A política de divulgação é configurada para cada atributo do usuário e o SP que terá acesso ao atributo. É de responsabilidade do delegado de identidade administrar as políticas criadas pelo usuário. Essencial para alcançar a consistência é a última etapa, denominada etapa de atualização (ver Figura 8), nos quais os atributos são solicitados pelo SP ao delegado, sem necessidade de qualquer intervenção manual (HOELLRIGL *et al.*, 2010).

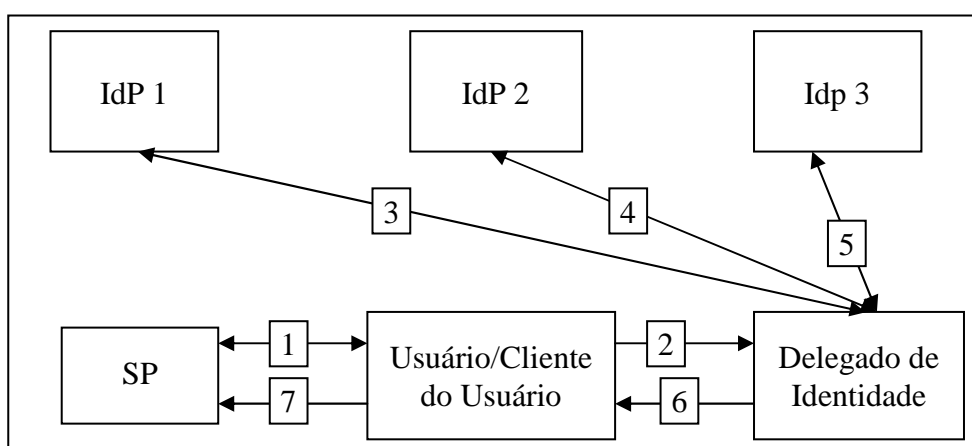


Figura 7. Exemplo de autorização inicial, para um cenário com *três IdPs*

Fonte: Adaptado de Hoellrigl *et al.*, (2010).

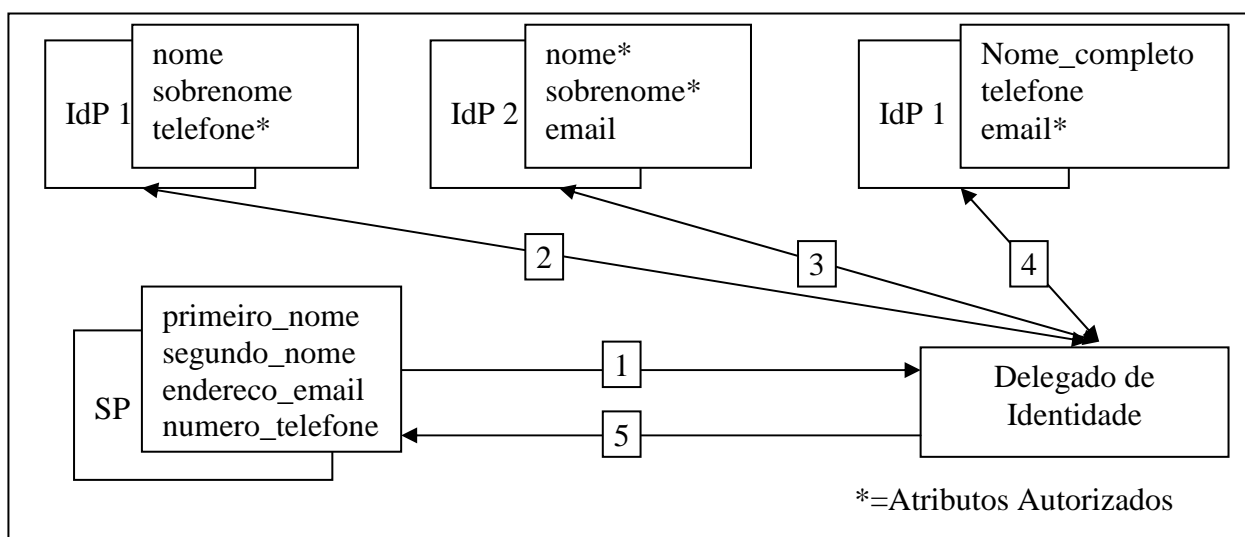


Figura 8. Exemplo de atualização dos atributos de usuário, em um cenário com três IdPs

Fonte: Adaptado de Hoellrigl *et al.*, (2010).

A implementação do protótipo está baseada no padrão *Windows CardSpace 2.0* e *Active Directory Federation Services (ADFS 2.0)*. Instâncias não modificadas do ADFS 2.0 foram usados como IdPs. Um *Active Directory (AD)* foi implantado como armazenamento de identidade. Não foram feitas alterações ao seletor de identidade.

O delegado foi construído com uma aplicação *Web ASP.NET*, com a tecnologia *WS-Trust Security Token Service (STS)* e com funcionalidade de emissão do *Information Card*. Este é configurado inicialmente com uma lista de IdPs confiáveis, uma lista de SPs conhecidos que vão também confiar no delegado e nas regras de transformação para mapear os esquemas correspondentes. O usuário se registra com o delegado de identidade e no uso da interface *Web* adiciona suas identidades no IdPs a federação. Após finalizar a configuração, é emitido um *Information Card* que pode ser utilizado para autorizar SPs ou IdPs a recuperar os atributos a partir do delegado.

### 3.4 VOSSAERT, LAPON, DECKER E NAESSENS (2010)

O mecanismo agregador de atributos proposto por Vossaert *et al.* (2010) segue abordagem mediada pelo cliente.

Vassaert *et al.* (2011) apresentam uma abordagem para um sistema de gestão de identidades centrada no usuário, que aborda a privacidade e vários problemas de segurança. No mecanismo

proposto pelos autores alguns atributos do usuário podem estar disponíveis no cache do elemento seguro temporariamente. Tornando o sistema mais eficiente e utilizável em ambiente off-line. O mecanismo é baseado em um serviço de validação que atualiza regularmente as informações sobre o estado do elemento seguro. A abordagem é flexível e escalável no sentido de que novos provedores de serviço e de identidade podem ser facilmente adicionados ao ambiente.

No modelo proposto por Vossaert, *et al.* (2010), tem-se um módulo de segurança (do inglês *trusted module* - TM) para cada usuário, que é representado por um cartão inteligente (*smart card*) que fica de posse do usuário. Esse cartão inteligente permite que os usuários possam interagir com o sistema.

A Figura 9 representa a visão geral da arquitetura proposta por Vossaert *et al.* (2010). Observa-se a existência do módulo de segurança que liga diretamente as trocas de mensagem realizadas pelos diversos provedores de serviço e pelos diversos provedores de identidade. Este módulo de segurança é responsável por realizar e controlar o processo de agregação de atributos. Os módulos contêm um tratador de requisições (*Service Request Handle*) que é responsável por realizar a agregação dos atributos do usuário provenientes de suas múltiplas identidades (IDx, IDy, IDz, etc.).

A Figura 9 demonstra ainda que os módulos de comunicação dos provedores de serviço são passíveis de auditoria, podendo assim detectar falhas e possíveis tentativas inapropriadas de utilização do mecanismo.

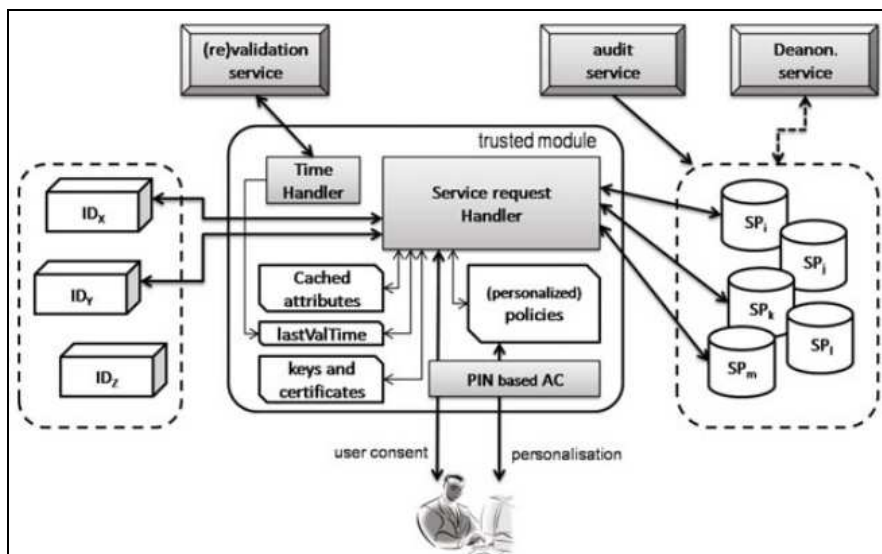


Figura 9. Visão geral da arquitetura

Fonte: Vossaert *et al.*, (2010).

A liberação das informações das pessoas é controlada em dois níveis. Uma autoridade de auditoria define as regras de todo o sistema de acesso. Os usuários podem restringir ainda mais as regras de acesso ou explicitamente solicitar seu consentimento. Futuras pesquisas se concentrarão em descobrir como o sistema pode ser implantado em um ambiente do mundo real e avaliar o impacto no desempenho, segurança e privacidade.

### 3.5 WATT E SINNOTT (2011)

No trabalho de Watt e Sinnott (2011), apresenta-se um novo *middleware*, denominado *ShinTau*, que permite que os usuários criem um conjunto de licenças externas, permissões e funções que lhes permite acessar vários dados seguros disponíveis no portal do projeto DAMES<sup>9</sup>, aderindo a políticas de segurança rigorosas.

A implementação do *ShinTau*, no lado do serviço, consiste de um SP *Shibboleth* padrão que controlará o acesso ao portal DAMES. Este SP está hospedado em um servidor *Web apache*, com um diretiva extra para permitir que a autorização para acesso a área protegida seja realizada pela aplicação de políticas da aplicação PERMIS, conforme ilustrado na Figura 10.

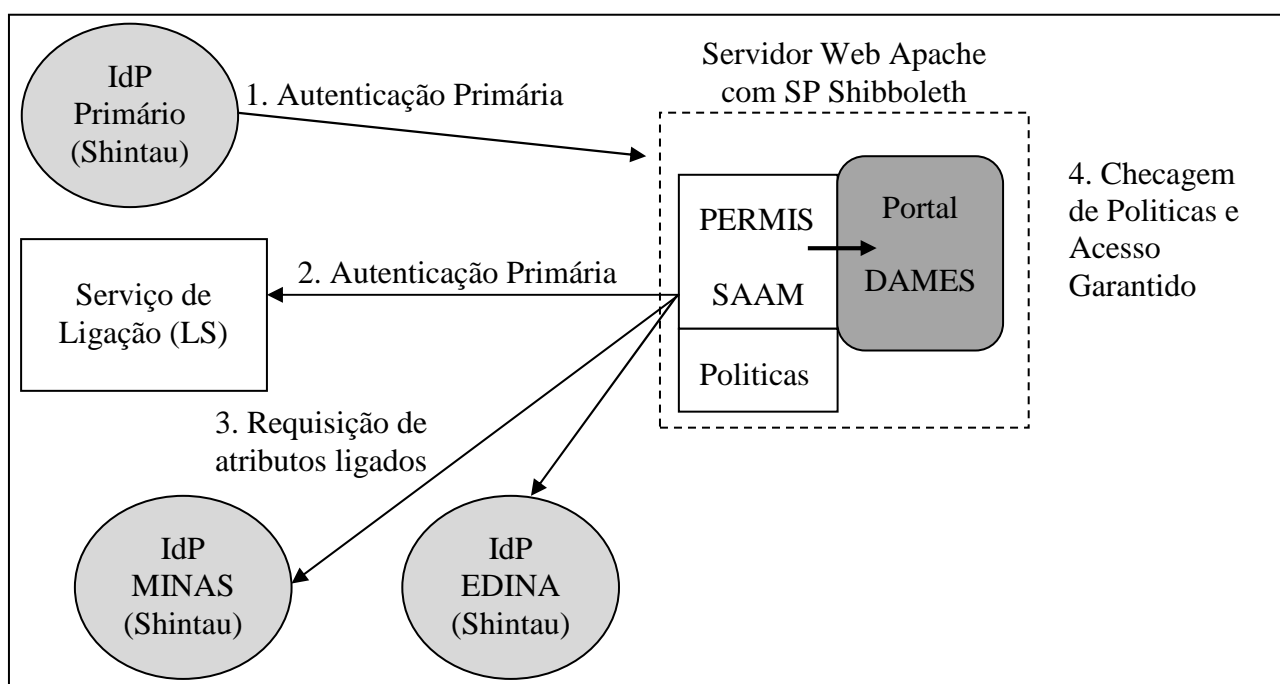


Figura 10. Fluxo de Informações necessários para acessar o ShinTau portal DAMES

Fonte: Adaptado de Watt e Sinnott, (2011).

A fim de conseguir efetuar a ligação dos atributos solicitados pelo usuário é realizada no LS. Essa nova entidade que fora necessária para efetuar a ligação de atributos foi concebida como uma

<sup>9</sup> Segundo Watt e Sinnott (2010), o projeto DAMES foi desenvolvido para a gestão de dados através das ciências sociais e pode ser acessado no endereço [www.dames.org.uk](http://www.dames.org.uk).



solução com interface *Web* e foi desenvolvida com a linguagem de programação PHP. A solução permite aos usuários efetuarem acesso nos IdPs que implementam o *ShinTau* internamente e criar mapeamentos entre SPs e múltiplos IdPs.

### 3.6 CHADWICK, INMAN, SIU E FERDOUS (2011)

A proposta de implementação de Chadwick *et al.* (2010) parte do princípio que muitas organizações gostariam de criar laços mais fortes de relacionamento com seus clientes, fornecendo-lhes acesso personalizado aos seus serviços *Web*. Dentro desse contexto os autores afirmam que as universidades não são diferentes. Com a finalidade de manter maiores relações com seu público universitário, projeto *Logins4Life* foi concebido, permitindo que todos os interessados tenham acesso aos recursos da universidade com seu *login* de universitário durante toda a sua vida.

O projeto *Logins4Life* procura viabilizar a utilização das contas sociais dos usuários para obter acesso às ferramentas disponibilizadas pelas instituições. Um dos problemas apontados pelos autores na utilização das contas sociais dos usuários para autenticação em seu sistema, para realização do SSO, está na pouca ou falta de verificação dos dados dos usuários durante o registro de sua conta.

Os mecanismos propostos no projeto tem por objetivo permitir que os usuários acessem facilmente os recursos da universidade usando suas contas existentes em IdPs de redes sociais, sem ter a necessidade de se registrar na universidade para criar uma nova conta. Além disso, os alunos podem optar por vincular tais contas com a conta interna da instituição, para que possam acessar os recursos internos da universidade acessíveis somente para alunos.

No mecanismo proposto, os autores definiram um provedor de serviço confiável (*Trusted Service Provider* - TSP) responsável por ligar as diferentes contas dos usuários, conforme ilustrada na Figura 11. O TSP visa ainda prover segurança à base de dados com os atributos do usuário e contém um *proxyIdP* (CHADWICK; INAMAN e KLINGESTEIN, 2010).

O usuário pode unir várias contas sempre que acessar o TSP no SP da instituição. O TSP da mesma maneira que todos os outros SPs exige que o usuário efetue o *login* por intermédio do *proxyIdP*. Uma vez autenticado, o usuário pode optar por vincular qualquer outra conta de IdP que possua.

Quando o usuário deseja ligar uma conta de IdP, ele deve solicitar isto ao TCP por meio do proxyIdP, que irá autoriza-lo a escolher entre os IdPs do círculo de confiança. Uma vez que o usuário foi autenticado pelo IdP escolhido, os atributos e o registro LoA do usuário serão armazenados na base de dados do TSP.

O usuário escolhe o IdP que deseja usar para se autenticar no site da instituição. O *proxyIdP* então se comunica com o IdP utilizando o protocolo adequado para isto, dependendo das tecnologias disponíveis no IdP. O *proxyIdP* mapeia todas a resposta de autenticação em uma nova asserção SAMLv2 e envia ao SP que requisitou inicialmente.

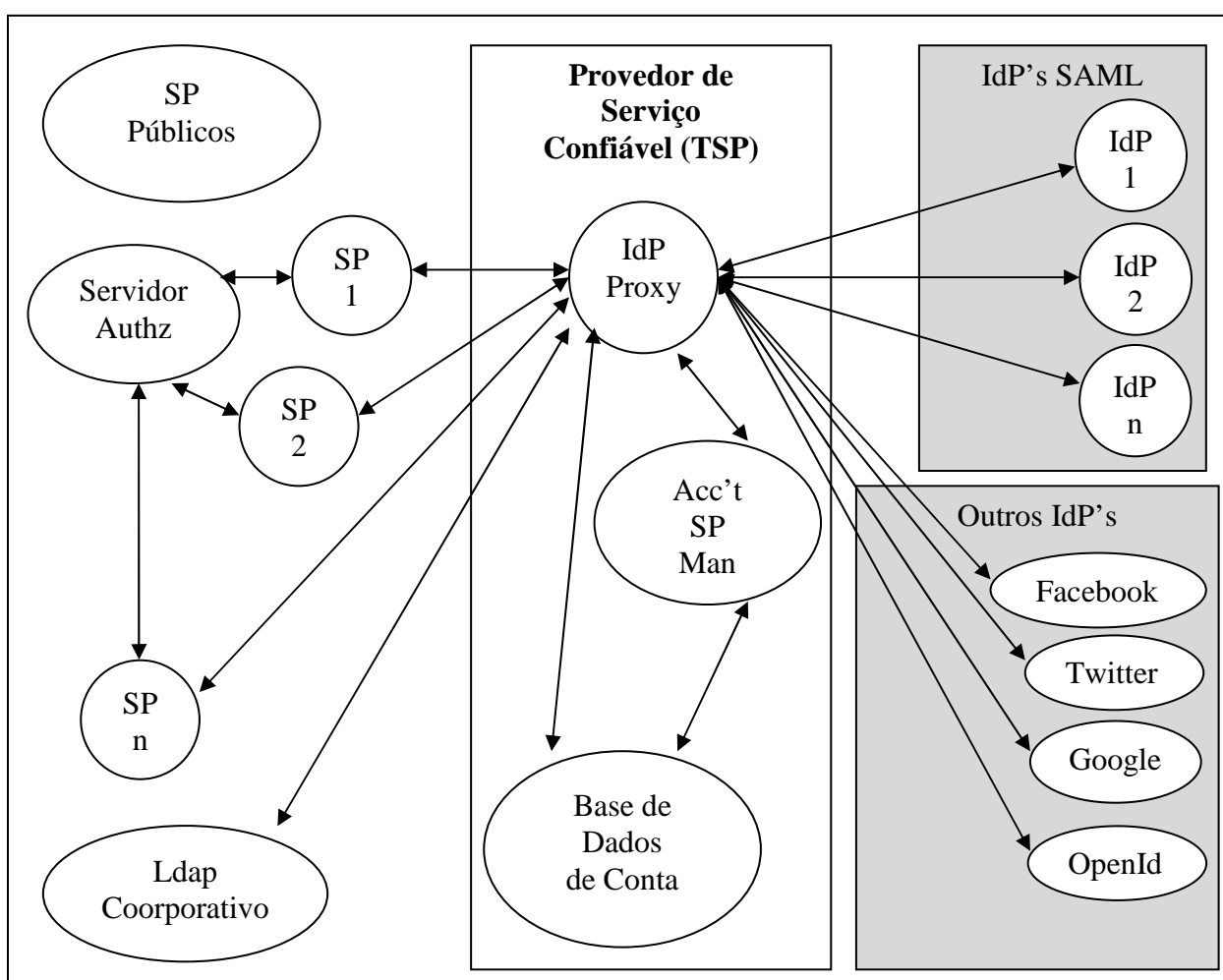


Figura 11. Visão geral do funcionamento com o proxyIdP

Fonte: Adaptado de Chadwick *et al.*, (2010).

De forma mais detalhada os autores explicam que antes de um usuário ser conhecido pelo TSP, este não terá qualquer registro do banco de dados do *proxyIdP*, independentemente de ele existir no serviço LDAP da organização ou não. A primeira vez que um usuário desconhecido interage com o TSP e escolhe o IdP para autenticação, o *proxyIdP* receberá um identificador persistente (Pid) do IdP que o autenticou. O Pid pode ser um nome de usuário (por exemplo o nome do usuário no *Twitter*), ou um identificador uni direcional (por exemplo de um IdP SAML).

### 3.7 HATAKEYAMA e SHIMA (2008)

O trabalho proposto por Hatakeyama e Shima (2008) apresenta uma infraestrutura para a gestão dos 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. O modelo ilustrado na Figura 12 é composto por três partes principais:

- O provedor de identidade (IdP) – que gerencia as informações do usuário para autorização, autenticação, contabilização e privilégios. O IdP também é responsável por resolver os identificadores com base em uma conta de ligação. O modelo permite que o usuário tenha várias contas em provedores de identidade, e este IdP principal gerencia as ligações com as demais contas do usuário, agindo assim como um *proxyIdP*;
- O provedor de serviços *Web* (do inglês *Web Service Provider* - **WSP**) – que gerencia os atributos do usuário e oferece o serviço de identidades a outros provedores. Quando o WSP recebe uma solicitação de outro provedor, ele julga a solicitação aplicando as regras com base na aplicação da política de privilégios; e
- Consumidor de serviços *Web* (do inglês *Web Service Consumer* - **WSC**) – o WSC requisita os atributos dos usuários para o WSP. Este pode oferecer alguns serviços para os usuários, com a finalidade de trocar os atributos dos usuários. Para o fornecimento deste serviço o WSC solicita uma afirmação de acesso ao WSP.

A Figura 12 ilustra também a federação de privilégios proposto. No exemplo, o WSC gerencia os perfis do usuário, e o IdP é responsável por federar as perfis do usuário, conforme o fluxo a seguir:

1. O usuário determina o privilégio de federação entre os provedores. Nesse momento o usuário determina as permissões para o WSC agregar as informações da identidade no WSP;
2. O usuário acessa o WSC que o autentica, obtendo as informações de autenticação do IdP. O WSC pode usar SAML ou OpenID para protocolo de *login*;
3. Quando o WSC necessitar de mais atributos do WSP, ele solicita a permissão para obtenção dos atributos do IdP;
4. O IdP confirma os privilégios de acesso. Se o WSC tiver permissão ele pode acessar o WSP e agregar os atributos do IdP correspondente;
5. O IdP envia um token para o WSC;
6. O WSC requisita os atributos do usuário com o *token* de privilégio. Neste momento não importando o protocolo utilizado, podendo ser ID-WSF, SAML, OAuth, etc.;
7. Quando o WSC receber o *token* com o pedido de atributos, ele solicita uma afirmação de privilégio de acesso com o *token* a um IdP, porque sem isso ele não consegue identificar quem é o usuário ligado ao *token* recebido;
8. O IdP responde a afirmação de privilégio de acordo com o *token*, quando o pedido for válido. O IdP confirma o *token*, e o solicitante tem acesso a obter a afirmação;
9. O WSP verifica os privilégios do WSC recebidos do IdP. Se o WSC tem permissão para acessar os atributos do usuário, ele os retorna para o WSC; e
10. O WSP envia os atributos para o WSC, utilizando-se de qualquer protocolo de comunicação, a exemplo do passo seis.

As trocas de informações são realizadas com o uso do protocolo SAML no mecanismo da federação. O IdP que gerencia uma conta específica do usuário cria identificadores únicos para a identidade, e para a troca de informações com os demais provedores ele cria identificadores diferentes e aleatório, evitando identificar a verdadeira identidade do usuário.

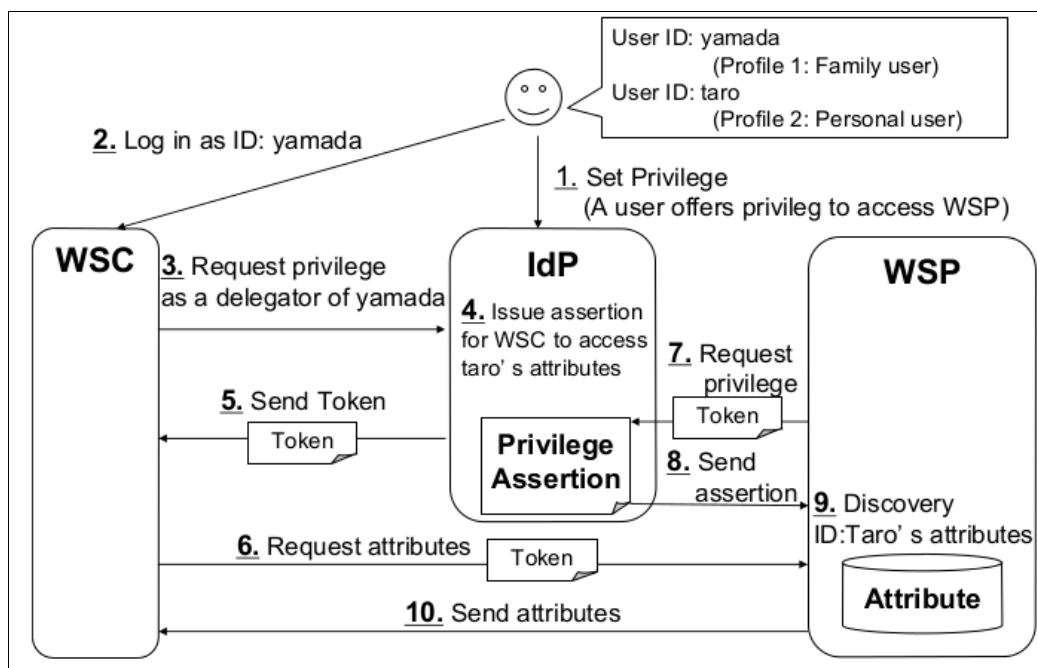


Figura 12. Modelo de federação de privilégios

Fonte: Hatakeyama; Shima, (2008).

### 3.8 HULSEBOSCH, WEGDAM, ZOETEKOUW, DIJK E POORTING (2011)

Hulsebosh *et al.* (2011) apresentam uma plataforma de colaboração virtual (do inglês *Virtual Collaboration Platform* - VCP) para a *SURFnet*, no contexto de um projeto que faz parte do programa *GigaPort3*. A plataforma aproveita a infraestrutura da federação de identidades já existente, que se baseia no padrão *SAML2*. Esta plataforma agrega atributos por meio de uma solução baseada em *proxy* ou retransmissão conforme desejado.

Os componentes centrais da *SURFnet* são o *Engineblock* e o *OpenSocial*. O container *OpenSocial* expõe as informações das pessoas e grupos utilizando do protocolo *OpenSocial REST* e *APIs JavaScript* que lida com a criação de complementos *OpenSocial* a serem utilizados em sites portal. O container *OpenSocial* adquire suas informações sobre os usuário, identidades, grupos e atributos do *Engineblock*.

Segundo Hulsebosch *et al.* (2011), no *Engineblock*, as identidades, grupos e atributos de várias fontes externas são agregadas. Este pode atuar como um retransmissor de identidade (*identity rely*, nas quais as asserções *SAML* recebidas são retransmitidas para o SP de forma inalteradas) de

identidades ou como um proxy de identidade (as asserções SAML são modificadas). Porém, a abordagem baseada em proxy não tem sido feita pela *SURFnet*.

O *Engineblock* recupera dados das identidades de múltiplos IdPs. A maioria das identidades são ligadas dos IdPs institucionais a partir da *SURFfederatie*. Além disso, dois IdPs estão disponíveis para os não-membros da *SURFederation*: O IdP proxy, para identidades on-line já existentes em provedores como o *Google*, *Twitter* e *Linkedin*, e um IdP convidado pelo *SURFguest* (HULSEBOSCH *et al.*, 2011).

O *Engineblock* agrega as informações sobre os grupos e membros de grupos da *SURFteams* e de membros e grupos externos (de fora do *SURFconext*). Estes grupos de provedores externos podem ser entre instituições (ou seja, fornecendo apenas grupos de usuário dentro de uma única instituição) ou interinstitucional (por exemplo, proporcionando aos grupos em um contexto de uma Organização Virtual). O provedor de atributos *SURFattributes* permite entender os perfis de usuários com atributos que não são definidos pelo IdP. Este recurso pode ser utilizado, por exemplo, no contexto de uma organização virtual para prover regras específicas (HULSEBOSCH *et al.*, 2011).

Segundo Hulsebosch *et al.* (2011), os provedores de serviço podem interagir com os serviços do *SURFconext* de três pontos diferentes de entrada:

- Engineblock SAML;
- Interface REST OpenSocial; e
- Portal OpenSocial/Javascript API.

O *Engineblock* SAML é usado principalmente para autenticação e troca de informações de identidade, ou seja, atributos. Asserções SAML gerados por *SURFconext* incluem os atributos emitidos por IdP do usuário, bem como os armazenados na *SURFattributes*. Atributos de membros do grupo não estão incluídos na declaração SAML, o que poderia conduzir a problemas de escalabilidade (HULSEBOSCH *et al.*, 2011).

As interfaces *OpenSocial* podem ser utilizadas para consultar as informações sobre os usuários e seus grupos. Essa interface é protegida através de protocolo *OAuth*, assim os usuários terão de conceder permissão para que um SP possa recuperar as suas informações pessoais através

desta interface. Além disso, os SPs podem fornecer dispositivos *OpenSocial*, que funcionam em um site portal *OpenSocial*, estes aparelhos podem acessar diretamente os dados do *OpenSocial* através da API *OpenSocial* em *JavaScript* (HULSEBOSCH *et al.*, 2011).

### 3.9 COMPARAÇÃO DOS TRABALHOS RELACIONADOS

O Quadro 2 apresenta um resumo comparativo dos trabalhos relacionados. Dentre os modelos de agregação de atributos apresentados, a abordagem de *proxy* de identidades se mostrou a mais comum, por estar presente na maioria dos estudos que envolveram o estado da arte apresentado anteriormente. Apenas os trabalhos de Lee *et al.* (2008) e Vossaert *et al.* (2010) não seguem esta abordagem.

Hoellrigl *et al.* (2012) e Vossaert *et al.* (2010) apresentam uma proposta de implementação que segue a abordagem mediada pelo cliente (faz uso de um cliente ativo). Como visto anteriormente, esta abordagem busca evidenciar a privacidade dos usuários no uso do mecanismo agregador. Sobre a abordagem apresentada por Hoellrigl *et al.* (2012), destaca-se a utilização de apenas uma plataforma operacional diante da escolha pelo *CardSpace* como solução de gestão de identidade.

Além da liberdade de plataforma operacional, outro requisito que se busca seguir para a definição do mecanismo aqui proposto é que este, preferencialmente, seja independente de fornecedor de *software*. No Brasil, existe um apelo do governo federal para adoção de solução de *software* livre. Em virtude deste apelo, busca-se para implementação do modelo de agregação utilizando-se de soluções e ferramentas livres.

Quadro 2. Análise comparativa dos Trabalhos Relacionados

<b>Modelo</b>	<b>Implementado?</b>	<b>Tecnologias de IdM Utilizadas.</b>	<b>Privacidade</b>	<b>Nível de Interoperabilidade</b>	<b>Abordagem de Implementação da Agregação de Atributos</b>
Lee <i>et al.</i> , (2008).	Não	Não se aplica	Centrado no Usuário	XML	SP
Chadwick <i>et al.</i> , (2010).	Sim	SAML2	Centrado no Usuário	SAML	Proxy
Hoellrigl <i>et al.</i> , (2010).	Sim	CardSpace, Active Directory Federation Services	Centrado no Usuário	Card Space	Cliente e Proxy
Vossaert <i>et al.</i> , (2010).	Não	OpenID, Shibboleth, CardSpace	Centrado no Usuário	<i>Smart Card</i>	Mediado pelo Cliente
Watt e Sinnott, (2011).	Sim	PERMIS, Shibboleth,	Centrado no Usuário	SAML, XML	Proxy
Chadwick <i>et al.</i> , (2011).	Sim	SAML2, OpenID, OAuth	Centrado no Usuário	SAML	Proxy.
Hatakeyama e Shima, (2008).	Não	OpenID, CardSpace, SAML, OAuth	Centrado no Usuário	SAML	Proxy
Hulsebosch <i>et al.</i> , (2011).	Não	SAML, OpenID, OAuth	Centrado no Usuário	SAML	Proxy Retransmissão
<b>Este trabalho</b>	<b>Sim</b>	<b>SAML</b>	<b>Centrado no Usuário</b>	<b>SAML</b>	<b>Cliente</b>

O Quadro 2 apresenta de forma introdutória o posicionamento deste trabalho em relação aos demais trabalhos relacionados que abordam a agregação de atributos em identidades federadas. No quesito de flexibilidade as propostas aqui avaliadas são contempladas, em virtude de todas trabalharem com dados compartilhados de diferentes provedores de identidade.

### 3.10 CONSIDERAÇÕES FINAIS DO CAPÍTULO

Sendo assim, compreender os mecanismos de agregação existentes, bem como avalia-los e compará-los é um passo importante para a construção de um novo modelo. Este capítulo apresentou



os trabalhos encontrados na literatura, a partir da aplicação de um protocolo de busca, e referenciados por diversos autores pesquisados. Os trabalhos aqui estudados e descritos serviram de embasamento para o desenvolvimento do mecanismo agregador de atributos proposto.

As explicações mais detalhadas sobre o a proposta de implementação do mecanismo agregador de atributos proposto encontram-se no Capítulo 4.

## 4 MECANISMO AGREGADOR DE ATRIBUTOS BASEADO EM CLIENTE ATIVO

Inicialmente, este capítulo apresenta a visão geral do mecanismo agregador de atributos proposto e uma descrição detalhada dos modos de funcionamento deste mecanismo agregador (fluxos de comunicação de dados). Em seguida, com o objetivo de exemplificar a aplicabilidade do mecanismo agregador, dois cenários de uso são apresentados. Para avaliar o mecanismo agregador, um protótipo de um dos cenários de uso e o mecanismo agregador foram desenvolvidos. Por fim, a modelagem do protótipo e o detalhamento do seu desenvolvimento são apresentados na Seção 4.5.

### 4.1 VISÃO GERAL E PREMISSAS

O governo brasileiro ainda não definiu a estratégia nacional de gestão de identidades a ser adotada nas aplicações de Governo Eletrônico<sup>10</sup>. O que existe é apenas uma definição de padrões de interoperabilidade de sistemas, conhecida como arquitetura e-PING, que traz algumas diretrizes para definição de estratégias para a interoperabilidade de sistemas. 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 entre os envolvidos na troca de mensagens seguras.

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 provedores de identidades, esse 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 provedores de identidades. Este trabalho teve como objetivo desenvolver um mecanismo agregador de atributos mediado pelo cliente que atenda

---

<sup>10</sup> Até a data da elaboração deste documento (Novembro de 2013).

as recomendações da arquitetura E-PING, que garanta a privacidade dos usuários e que traga mais flexibilidade a um sistema de gerenciamento governamental de identidades federadas.

Garantir a privacidade é um grande desafio no compartilhamento de informações de identificação pessoal (atributos de identidade). Em sistemas de identidades federadas, o compartilhamento seguro de tais informações é essencial para se usufruir dos benefícios da federação.

Visando impedir a rastreabilidade dos atributos de identidade do usuário (garantir a privacidade), possível nas soluções baseadas em *proxy*, o mecanismo agregador de atributos proposto neste trabalho segue a abordagem mediada pelo cliente, e que segue o modelo de retransmissão seletiva de asserções SAML, com o diferencial de ser alinhado à arquitetura E-PING e de prover o suporte à autenticação SSO. O procedimento de agregação será executado por um *software* aplicativo no ambiente operacional do usuário, chamado de cliente ativo. O mecanismo agregador de atributos gerencia pseudônimo, conforme provido pela especificação SAML, para aumentar a privacidade do usuário e dificultar o rastreamento de suas informações nos provedores de serviços.

A arquitetura e-PING enfatiza o uso da tecnologia de Serviços Web (*Web Services*) para propiciar a interoperabilidade entre sistemas heterogêneos do Governo, o que implica também na busca por uma arquitetura de *software* mais alinhada aos conceitos de serviços em ambientes distribuídos. Nesse contexto, a Arquitetura Orientada a Serviços ou simplesmente SOA (*Service-Oriented Architecture*) oferece diversas vantagens à aderência aos padrões tecnológicos propostos pela e-PING. Diante desta recomendação, a solução proposta segue a arquitetura orientada a serviços, e utiliza-se dos Serviços Web como tecnologia integradora. A e-PING recomenda tanto a utilização de Serviços Web que usam mensagens XML (*eXtensible Markup Language*), seguindo o padrão SOAP, padrão este mais adotado nas soluções atuais, quanto a utilização do protocolo HTTP para projetos baseados em REST (*Representational State Transfer*).

Para o uso do mecanismo agregador de atributos, assume-se como premissas:

- A existência de uma federação governamental, ou seja, uma rede colaborativa governamental. Esta federação deve envolver todas as esferas governamentais, tais como: governos federal, estadual, distrital e municipal. Nesta federação existem provedores de identidades (IdPs) e provedores de serviços (SPs) governamentais que

possuem relações de confiança. O governo poderá ainda homologar empresas privadas e do terceiro setor para fornecer serviços à população (SPs);

- A federação governamental está baseada na especificação SAML e tanto IdPs, quanto SPs implementam esta especificação e suportam e aceitam a autenticação única (*Single Sign On-SSO*) como provida por esta especificação;
- Provedores de identidades e de serviços devem ainda seguir outras diretrizes de interoperabilidade da arquitetura e-PING, como o uso de Serviços *Web RESTful*, o uso do protocolo SSL e o padrão XML (linguagem de intercâmbio de dados); e
- Não poderão ser geradas estatísticas e efetuadas comunicações entre provedores que não são necessárias para agregação de atributos. Para isto, o código do mecanismo agregador precisará ser homologado por uma entidade confiável da federação.

É possível que provedores de empresas privadas ou do terceiro setor façam parte de uma federação governamental de provedores de identidades, mas para isso será necessário que o governo defina regras para a homologação de tais provedores e permita que estes façam parte de seu círculo de confiança.

Dentro de uma federação governamental, um usuário (cidadão) tem atributos distribuídos por múltiplos provedores de identidades. Um provedor de serviços 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 provedores de identidade e os compartilha com o provedor de serviços. O mecanismo agregador não compartilha qualquer informação sem o consentimento do usuário.

Na concepção do mecanismo agregador, visando garantir a interoperabilidade na federação governamental, a especificação SAML e Serviços *Web RESTful*, recomendações da arquitetura e-PING, também foram adotados.

A Figura 13 ilustra a visão geral do mecanismo agregador de atributos. Conforme ilustrado, 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

homologados pelo governo. 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. 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 provedores de serviços da federação (estão no círculo de confiança da federação).

No passo 1 da Figura 13, 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 provedor de identidades indicado pelo serviço para proceder com a autenticação (passo 2). Após o usuário informar os dados para a autenticação (passo 2a), o provedor de identidade autentica o usuário, emite uma asserção de atributos para este (passo 2b), e redireciona o navegador para o provedor de serviços (passo 3a). Para concretizar a ação solicitada pelo usuário, o provedor de serviços 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 homologada por alguma instituição governamental (passo 4), o navegador do usuário será redirecionado para o serviço de descoberta de provedor de cliente ativo (SDPCA) mantido pela federação governamental<sup>11</sup>.

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 de cliente ativo (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 provedor de serviços a asserção que indica os 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 indicado (passo 10.1), os demais irão aceitar a *token* de autenticação emitido pelo IdP e responderão à solicitação de atributos (passo 10.2, 10.3 e 10.4).

---

<sup>11</sup> Este serviço deve estar em um SP confiável, administrado, por exemplo, por órgão federal.

No passo 11, o cliente ativo efetua a agregação de atributos. No passo 12<sup>a</sup>, o cliente ativo solicita que o usuário confirme a liberação dos atributos e então encaminha (passo 12b) os atributos agregados para o provedor de serviços. O provedor de serviços de posse dos atributos enviados pelo provedor de serviços (passo 12c) poderá permitir ou não o acesso ao serviço solicitado pelo usuário.

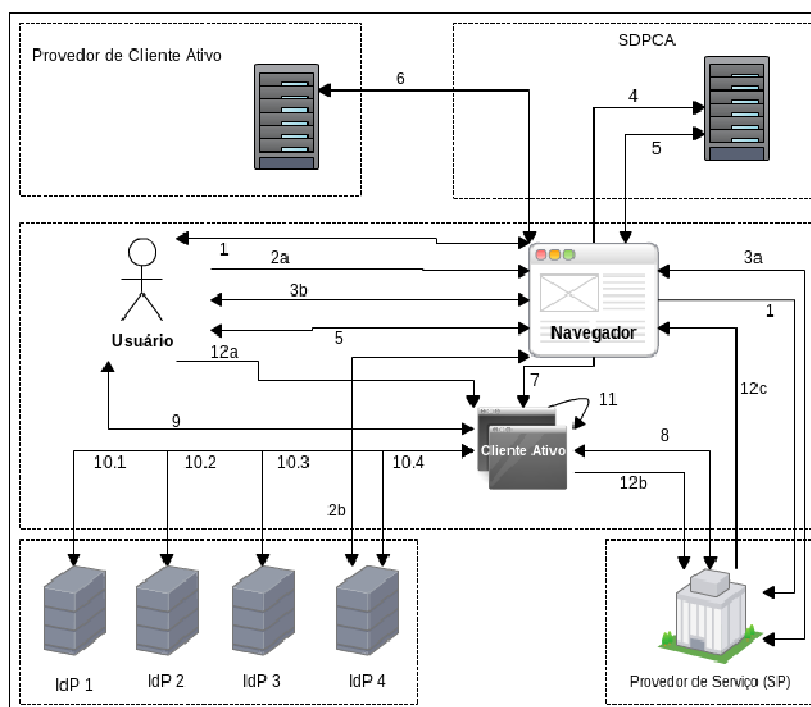


Figura 13. Visão geral do mecanismo agregador de atributos proposto

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 (ataque de quebra de senha com força bruta) 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 (por exemplo, certificados digitais ou autenticação de dois fatores).

Visando prover a interoperabilidade na comunicação entre o mecanismo agregador de atributos e os provedores de serviços da federação, padronizaram-se duas estruturas de dados (*XML Schemas*) que serão trocadas entre estes. A primeira padroniza como um provedor de serviços deve indicar os atributos que este deseja (lista de atributos) com o Cliente Ativo. A segunda estrutura

padroniza como os atributos agregados (asserções SAML) são compartilhados com os provedores de serviços. Estas duas estruturas XML (*XML Schema*<sup>12</sup>) estão descritas na Seção 4.2.4 .

Outra funcionalidade importante para o mecanismo agregador de atributos está na criação de políticas de liberação dos atributos. Esta funcionalidade foi baseada na proposta de implementação apresenta por Chadwick; Inman; Klingenstein (2010), conforme descrito na Seção 3.2. A política de liberação de atributos pode se tornar útil na utilização subsequente do mecanismo agregador, pois, com esta, é possível que os usuários registrem suas políticas de liberação de atributos para determinados provedores de serviços com quem já interagiu.

## 4.2 DETALHAMENTO DO MECANISMO PROPOSTO E DOS FLUXOS DE COMUNICAÇÃO

O processo de agregação de atributos pode ser classificado como dinâmico ou estático e transitório ou permanente (CHADWICK; INAMAN; KLINGESTEISN, 2010). O mecanismo agregador proposto oferece os seguintes modos de funcionamento:

- Modo transitório dinâmico: neste modo não há uma política de liberação de atributos pré-definida para o provedor de serviço em questão (dinâmico) e o usuário precisará se autenticar em cada IdP que solicitar atributos (transitório). Neste modo, a autenticação SSO não é suportada;
- Modo permanente dinâmico: neste modo, ainda não há uma política de liberação de atributos pré-definida para o provedor de serviços em questão (dinâmico), porém, a liberação de atributos concedida ao SP poderá ser usada nas próximas requisições ao serviço (permanente). Além disso, neste modo, a autenticação SSO é garantida para solicitar atributos em múltiplos IdPs (permanente); e
- Modo permanente estático: neste modo há uma política de liberação de atributos para um provedor de serviços específico definida antes mesmo de qualquer requisição ao serviço (estático). Além disso, a autenticação SSO é garantida.

---

<sup>12</sup> Segundo a W3C (World Wide Web Consortium), os esquemas em XML são designados a descrever um arquivo XML, e são utilizados para validar o formato de arquivos XML compartilhados entre servidores, assim evitando-se o mal funcionamento dos procedimentos que recebem os arquivos XML mal formatos de provedores externos.

Destaca-se que o modo transitório estático não é suportado, pois não faz sentido a definição de políticas de liberação de atributos sem que estas sejam mantidas no sistema como ocorre no modo transitório.

O modo transitório dinâmico é o mais simples de ser implementado, porém oferece menor usabilidade aos usuários; já o modo permanente estático é o mais complexo, mas oferece uma melhor experiência de uso. Todos os modos exigem a aprovação e consentimento dos usuários para liberação de atributos. As seções a seguir detalham estes modos de funcionamento.

#### 4.2.1 Modo transitório dinâmico

A Figura 14 ilustra o funcionamento do modo transitório dinâmico. O mecanismo agregador deve ser obtido e executado após a invocação ao SP. No passo 1, o usuário, por intermédio de seu navegador Web, tenta acessar um serviço do SP. Como este exige a autenticação do usuário, este é redirecionado para o provedor de identidade (IdP) confiável para que o usuário realize a sua autenticação. Após autenticação bem sucedida, o navegador do usuário é redirecionado para o SP para que então este informe ao usuário quais os atributos necessários para concretizar a solicitação e para que solicite ao usuário o seu consentimento para continuar o procedimento de agregação de atributos.

No passo 2, após verificar os atributos necessários e o usuário confirmar que deseja continuar o processo, este será redirecionado para o serviço de descoberta de cliente ativo (SPDCA). Neste passo (2.1), o usuário deverá selecionar um provedor de cliente ativo na lista de provedores do SDPCA. Após realizada a seleção pelo usuário, este será redirecionado (passo 2.2) ao provedor de cliente ativo (PCA), para que possa realizar o *download* do aplicativo cliente ativo (passo 3).

De posse do aplicativo, este será executado na máquina do cliente, caso isto não ocorra, o usuário deve executá-lo (passo 4). O cliente ativo, ao tentar acessar o SP para obter a lista de atributos, é redirecionado para IdP para se autenticar (passo 4.1).

No passo 4.3, a lista de atributos é apresentada ao usuário. Este deve selecionar um provedor de identidade (passos 5) para cada um dos atributos requisitados. Deve informar as suas credenciais



de acesso (passo 6, 6.1, 7 e 7.1) para se autenticar no provedor e receber a asserção SAML (passo 6.2 e 7.2) com os atributos do usuário.

Após a coleta das asserções SAML em todos os provedores de identidade, o cliente ativo irá realizar a agregação dos atributos (passo 8) e apresentar um resumo do trabalho realizado ao usuário (passo 9).

No passo 10, o usuário deverá autorizar que seus atributos sejam enviados ao provedor de serviço. Após esta autorização (passo 11), os atributos serão enviados ao SP no formato de um XML de resposta (conforme descrito na Seção 4.2.4). No passo 12, o usuário poderá verificar que seus atributos foram compartilhados e obterá a resposta do provedor de serviço sobre o sucesso ou cancelamento da liberação do serviço solicitado inicialmente no passo 1.

É importante observar que o SPDCA e o provedor de cliente ativo são serviços hospedados em SPs confiáveis da federação governamental que confiam nos provedores de identidades apresentados pelo SP no passo 1; logo, caso a autenticação tenha sido bem sucedida (passo 1.1.1), o usuário não precisa se autenticar no SPDCA e no provedor de cliente ativo (autenticação SSO). Neste modo dinâmico, como não há uma política de liberação de atributos configurada para o SP, o usuário precisará indicar quais IdPs contêm os atributos do usuário solicitados durante o acesso ao serviço e não salvará os atributos agregados. O modo transitório indica que a autenticação SSO, via aplicativo de cliente ativo, não é suportada.

#### **4.2.2 Modo permanente dinâmico**

De forma semelhante à Figura 14, a Figura 15 ilustra o funcionamento do modo permanente dinâmico. As diferenças são, basicamente, a inexistência dos passos 6 e 6.1, pois neste modo o funcionamento do SSO é garantido. Neste caso, o *token* de autenticação de um provedor de identidade é compartilhado e aceito nos demais provedores de identidade. O *token* de autenticação emitido pelo primeiro IdP deve ser apresentado para os demais IdPs, para obtenção dos atributos solicitados.

#### **4.2.3 Modo permanente estático**

No modo estático, 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. Conforme os modos anteriores, o usuário deve solicitar um aplicativo homologado caso este usuário não tenha o cliente ativo em seu ambiente computacional. Este deve solicitar um aplicativo homologado em um dos provedores indicados no SPDCA (passos 1, 2 e 3 da Figura 16). No passo 4, o usuário executa o cliente ativo, seleciona um IdP para correspondente ao atributo que deseja agregar as políticas de seu cliente ativo (passo 5 e 6). Após esta seleção de provedor de identidade, o aplicativo irá coletar os atributos em cada um dos provedores selecionados (passo 5.1 e 6.1). Este procedimento pode ser realizado inúmeras vezes, dependendo de quantos forem os provedores de identidade de um determinado usuário. Além disso, após a liberação dos atributos para o SP, o usuário pode solicitar que o cliente ativo armazene seus atributos para serem utilizados em futuras invocações a este SP (passo 9). A política de liberação de atributos deve ser salva (passo 11), para que estas informações estejam acessíveis em futuras invocações de serviço.

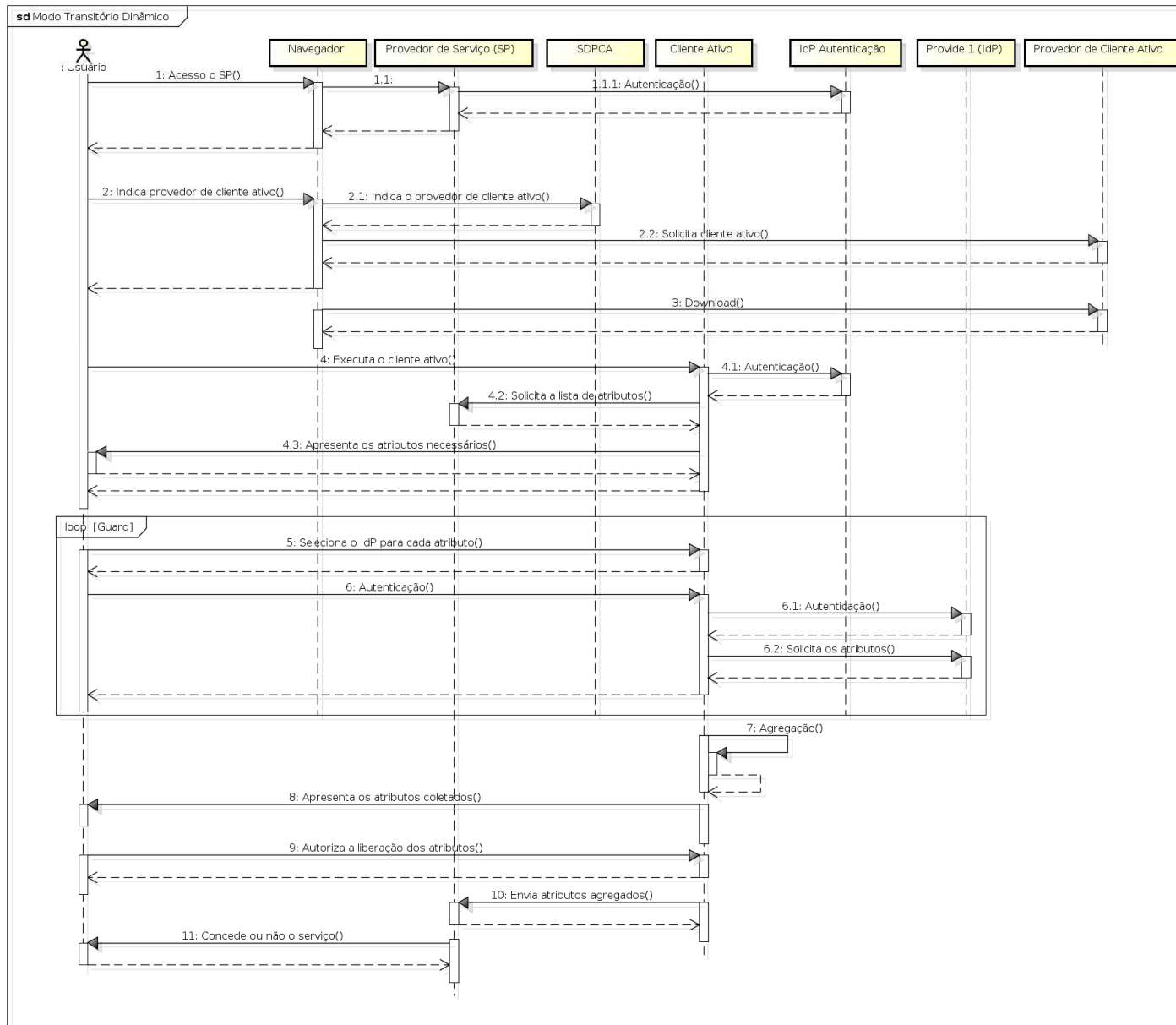


Figura 14. Diagrama de sequência modo transitório dinâmico

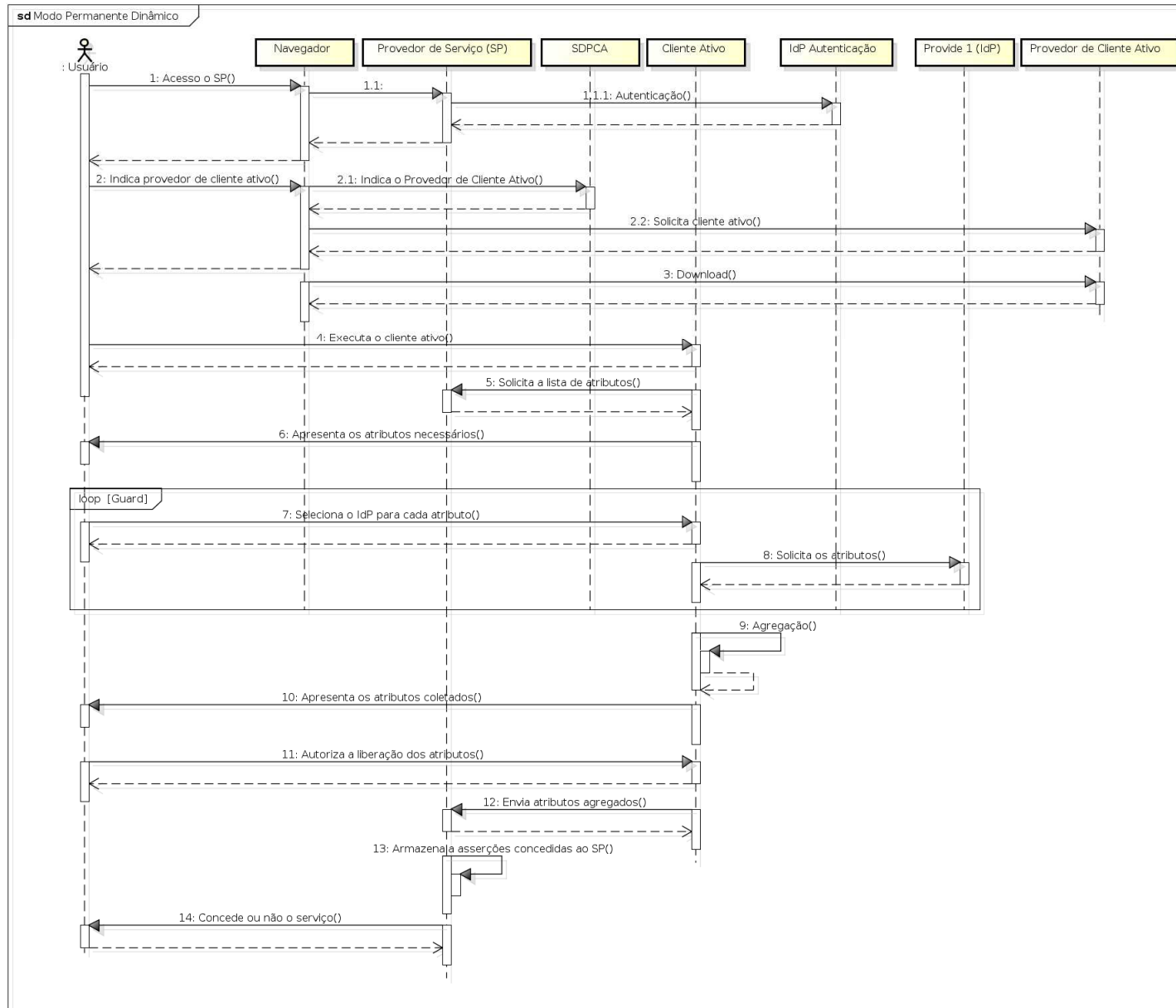


Figura 15. Diagrama de sequência modo permanente dinâmico

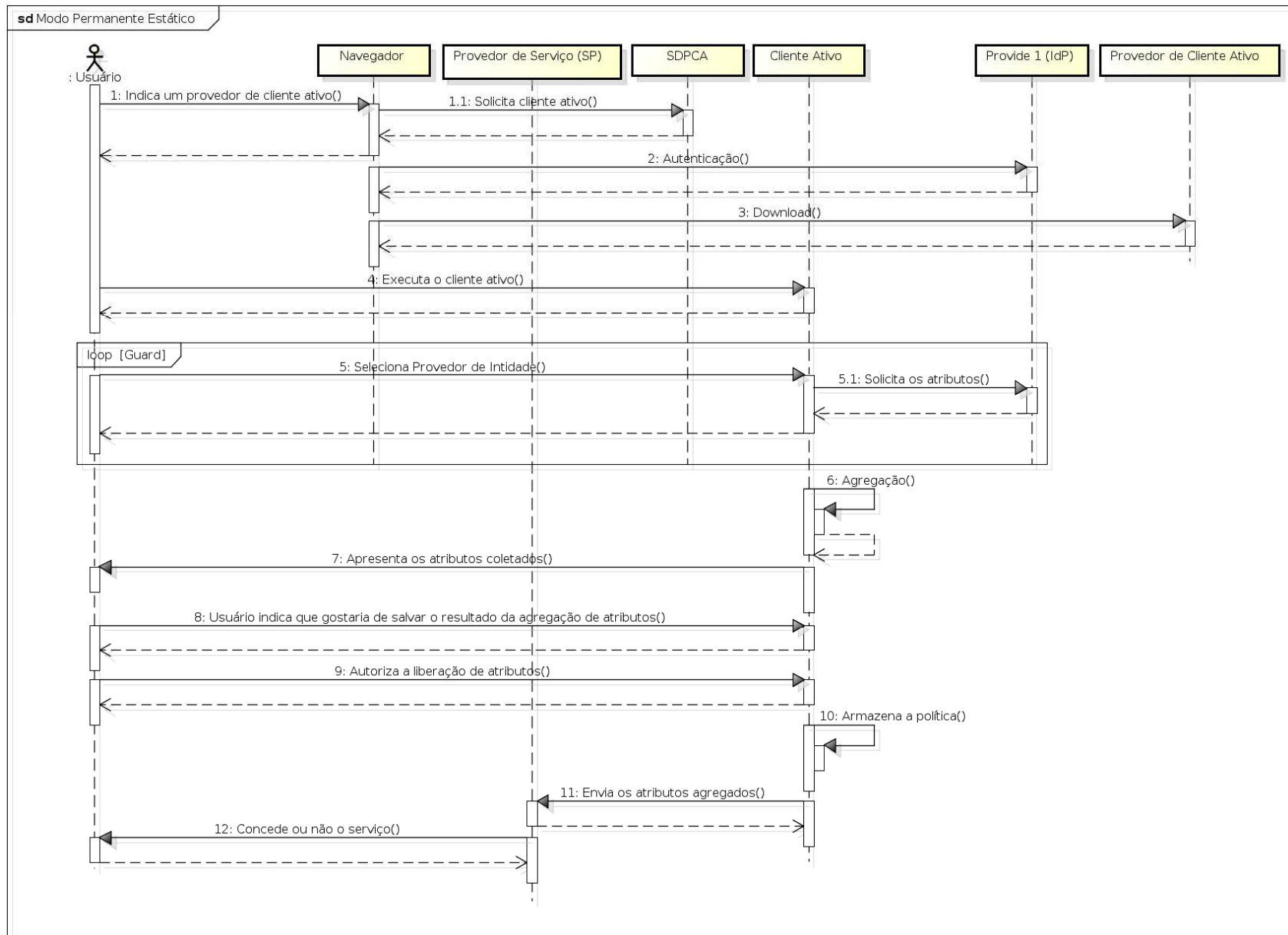


Figura 16. Diagrama de sequência modo permanente estático

#### 4.2.4 Padronização da Interação entre Cliente Ativo e Provedor de Serviços

Para definição de um padrão de troca de mensagens entre os provedores de serviço e o cliente ativo, definiram-se dois *Schemas* XML. O primeiro (ver Figura 17) deverá ser utilizado para compartilhar com o cliente ativo a lista de atributos necessários para a prestação do serviço. Este XML será utilizado no passo 8 da Figura 13.

```

1  <?xml version="1.0" encoding="UTF-8"?>
2  <xs:schema attributeFormDefault="unqualified"
3          elementFormDefault="qualified"
4          xmlns:xs="http://www.w3.org/2001/XMLSchema">
5      <xs:simpleType name="NonEmptyString">
6          <xs:restriction base="xs:string">
7              <xs:minLength value="1" />
8              <xs:pattern value=".*[^\s].*" />
9          </xs:restriction>
10     </xs:simpleType>
11     <xs:complexType name="componentType">
12         <xs:sequence>
13             <xs:element name="attribute"
14                 type="NonEmptyString" />
15         </xs:sequence>
16     </xs:complexType>
17     <xs:element name="SAMLAggregator">
18         <xs:complexType>
19             <xs:sequence>
20                 <xs:element maxOccurs="unbounded"
21                     name="SAMLRequest"
22                     type="componentType" />
23             </xs:sequence>
24         </xs:complexType>
25     </xs:element>
26 </xs:schema>

```

Figura 17. XML Schema de requisição da lista de atributos

Conforme pode ser observado na Figura 18, tem-se um XML que pode ser validado com o XML Schema descrito na Figura 17. Basicamente esse XML representa os atributos (linha 4, 7 e 10) que o provedor de serviço necessita para a autorização do serviço requisitado pelo usuário. Os atributos aqui exemplificados são baseados no cenário da solicitação de passaporte que será descrito com mais detalhes na Seção 4.3.1 .

```

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>

```

Figura 18. XML Request

Com a finalidade de padronizar mensagem de resposta do cliente ativo para o provedor de serviços que contêm os atributos agregados, definiu-se um *XML Schema*, (ver Figura 19). Este *Schema* define que, para cada resposta do cliente ativo, o XML deve conter um elemento composto (linhas 11 a 18). Este elemento composto está subdividido em dois elementos do tipo *String*. O primeiro deles (linha 13) deve receber o nome dos atributos e o segundo (linha 15), o SAML, correspondente a este atributo. Como o SAML por si só é um elemento complexo, a resposta para o provedor de serviço deve ser enviada com esse elemento codificado em *Base64*<sup>13</sup>.

```

1  <?xml version="1.0" encoding="UTF-8"?>
2  <xs:schema attributeFormDefault="unqualified"
3    elementFormDefault="qualified"
4    xmlns:xs="http://www.w3.org/2001/XMLSchema">
5    <xs:simpleType name="NonEmptyString">
6      <xs:restriction base="xs:string">
7        <xs:minLength value="1" />
8        <xs:pattern value=".*[^\s].*" />
9      </xs:restriction>
10   </xs:simpleType>
11   <xs:complexType name="componentType">
12     <xs:sequence>
13       <xs:element name="attribute"
14         type="NonEmptyString" />
15       <xs:element name="SAML"
16         type="NonEmptyString" />
17     </xs:sequence>
18   </xs:complexType>
19   <xs:element name="SAMLAgregator">
20     <xs:complexType>
21       <xs:sequence>
22         <xs:element maxOccurs="unbounded"
23           name="SAMLResponse"
24           type="componentType" />
25       </xs:sequence>
26     </xs:complexType>
27   </xs:element>
28 </xs:schema>

```

Figura 19. XML Schema de resposta com os atributos agregados

A Figura 20 representa o XML de resposta a ser enviado ao provedor de identidade após o processo de agregação dos atributos e com a autorização do usuário. Pode-se observar os blocos de

<sup>13</sup> O padrão de codificação Base64 é comumente utilizado na Internet para transmitir dados no formato binário por meios de transmissão que lidam apenas com texto, como por exemplo para enviar arquivos anexos por email.

respostas (linhas 3 a 6), onde cada um dos blocos representa o atributo (linha 4) e a resposta SAML (linha 5) em *Base64* correspondente ao atributo. Os SAMLs (linhas 5, 9 e 13) estão abreviados na Figura 20, pois seus conteúdos são bem extensos.

```

1  <?xml version="1.0" encoding="UTF-8"?>
2  <SAMLAggregator>
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 </SAMLAggregator>

```

Figura 20. XML de resposta

### 4.3 DESCRIÇÃO DE DOIS CENÁRIOS DE USO DO MECANISMO AGREGADOR DE ATRIBUTOS

Com o objetivo de elucidar a aplicabilidade e flexibilidade do mecanismo agregador de atributos, esta seção descreve dois cenários de uso relacionados a procedimentos comumente oferecidos pelo Governo ao cidadão. Todos os provedores de identidades e de serviços mencionados devem pertencer à federação governamental.

#### 4.3.1 Emissão de passaporte

O procedimento de emissão de passaporte exige a apresentação de diferentes documentos que comprovem os dados fornecidos pelo cidadão, conforme pode ser observado no Quadro 3.



Quadro 3. Lista de documentos e respectivos IdPs para a emissão de passaporte

<b>Documento</b>	<b>IdP que pode conter o atributo</b>
Documento de Identidade ou Registro Geral (RG), para maiores de 12 anos	IdP RG (RIC) - Secretaria de Segurança Pública
Título de Eleitor comprovando que compareceu na última eleição	IdP TSE – Tribunal Superior Eleitoral
Documento de Quitação do Serviço Militar (p/ homens)	IdP do Ministério da Defesa
Comprovante Bancário de Pagamento da Guia de Recolhimento da União – GRU	IdP do Ministério da Fazenda
Documento de Cadastro de Pessoa Física, CPF	IdP da Receita Federal

Fonte: BRASIL, 2013.

Atualmente, o processo de emissão de passaporte é demorado e burocrático. O cidadão para emitir o seu documento precisa informar manualmente suas informações pessoais no site de cadastro fornecido pela Polícia Federal. Após efetuar o cadastro e pagar a taxa cobrada, o cidadão deve agendar a apresentação de seus documentos originais em um posto de atendimento. Na data marcada, os documentos são recebidos e conferidos, para então, recolher as digitais e fotografia do cidadão.

Apesar de o cidadão ser obrigado a entregar seus documentos originais, isso não evita a apresentação de documentos falsificados. Este processo pode ser automatizado e mais seguro se os atributos do usuário forem coletados diretamente em seus provedores de identidade originais com o uso do mecanismo agregador de atributos proposto. Somente provedores de identidades pertencentes à Federação Governamental podem ser utilizados no processo.

O uso do mecanismo agregador neste cenário pode ser resumido nos seguintes passos:

1. O usuário, através do navegador Web, acessa o provedor de serviços (SP) da Polícia Federal. Como o provedor de serviço exige que o usuário se autentique, o navegador é redirecionado para o provedor de identidade de confiança do SP;
2. O usuário se autentica no provedor de identidades e o seu navegador é redirecionado para o SP da polícia federal;
3. Após indicar que consente com o processo de agregação de atributos, o navegador é redirecionado para o provedor SDPCA (Serviço de Descoberta de Provedor de Cliente Ativo);

4. O usuário seleciona um 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;
6. O cliente ativo apresenta os atributos e solicita que o usuário indique qual IdP contém o atributo requerido;
7. Após indicar os IdPs para cada atributo, o usuário deve se autenticar 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.

#### **4.3.2 Financiamento de imóveis**

O segundo exemplo de cenário de uso do mecanismo agregador de atributos é um serviço que verifica informações dos clientes para prover financiamento de imóveis. Este serviço pode ser de uma empresa privada, mas que pertence à Federação do governo brasileiro.

Para este exemplo de cenário foram consideradas algumas informações de financiamento habitacionais disponíveis no site da Caixa Econômica Federal. A “CAIXA”, como é comumente conhecida, é uma instituição financeira sob a forma de empresa pública, diretamente ligada ao Ministério da Fazenda do governo brasileiro e que está disponível em todo o território nacional.

O Quadro 4 apresenta a lista dos principais documentos necessários para solicitar empréstimos habitacionais da CAIXA, bem como o respectivo IdP que poderá fornecer a afirmação da validade do atributo do usuário.

Quadro 4. Lista de documentos e respectivos IdPs para o financiamento habitacional

<b>Documento</b>	<b>IdP que pode conter o atributo</b>
Carteira de Identidade ou Registro Geral - RG	IdP RG (RIC) – Secretária de Segurança Pública
Cadastro de Pessoa Física – CPF	IdP Receita Federal
Certidão Negativa de Débito com a Receita Federal	IdP Receita Federal
Declaração Negativa de Propriedade de Imóvel	IdP do Cartório de Imóveis
Declaração de Imposto de Renda ou Isento	IdP Receita Federal
Carteira de Trabalho e Previdência Social CTPS	IdP Ministério do Trabalho e Emprego
Número do Imposto Sobre a Propriedade Predial e Territorial Urbana – IPTU	IdP da Prefeitura Municipal

Fonte: BRASIL, 2013.

O procedimento para realização de um financiamento habitacional é realizado da mesma forma que o processo de emissão de passaporte, esse processo pode ser ainda mais burocrático, visto que envolve grandes quantidades monetárias. Porém os documentos necessários podem ser mais bem afirmados para a instituição bancária, evitando a necessidade de comprovação dos documentos, visto que emitindo estes diretamente da fonte de autoridade do atributo evita-se os processos de falsificação.

Como apresentado no Quadro 4, para cada atributo desejado, um IdP será responsável pela autenticidade do mesmo. Mas um provedor de identidade pode tranquilamente responder por mais atributos do usuário. É o caso do IdP da Receita Federal, que, neste cenário, é responsável pela validação de três atributos necessários, a saber: CPF; certidão negativa de débito com a Receita Federal; e declaração de isento do Imposto de Renda.

Outra peculiaridade deste cenário de estudo está ligada ao atributo IPTU. Na atualidade as informações de propriedades predial e territorial urbanas estão diretamente ligadas às prefeituras dos municípios, que fazem parte da esfera municipal da federação. Para o correto funcionamento, é necessário que as esferas municipais implantem a infraestrutura necessária para a criação de seus próprios provedores de identidade, ou que isso seja centralizado na esfera estadual, ou até mesmo federal. Mas esse problema não condiz com os objetivos deste trabalho. O que se pretende é demonstrar que é necessário criar uma infraestrutura de federação que englobe todas as esferas da administração do país, ou uma federação de federações (confederação).

## 4.4 ANÁLISE DE REQUISITOS DO MECANISMO AGREGADOR DE ATRIBUTOS

Esta seção apresenta os requisitos funcionais e não funcionais do mecanismo agregador. A descrição dos autores, o diagrama de casos e a descrição detalhada dos casos de usos elaborados na fase de análise estão no APÊNDICE H –.

### 4.4.1 Requisitos funcionais e Não Funcionais Associados

Esta seção apresenta os requisitos funcionais (RF) do mecanismo agregador de atributos proposto (cliente ativo) para uma federação governamental e os requisitos não funcionais associados (RNF), que são:

- RF 01: O cliente ativo deve permitir a passagem de parâmetro na inicialização do sistema. Esse parâmetro irá especificar a URL do serviço *Web* do provedor de serviço;
- RF 02: O cliente ativo deve ser capaz de autenticar o usuário no provedor de identidade (IdP) indicado pelo provedor de serviço (SP);
  - RNF 01: O cliente ativo deve ser capaz de enviar, juntamente com o login e senha do usuário, um CAPTCHA (*Completely Automated Public Turing test to tell Computers and Humans Apart*) para os provedores de identidades;
- RF 03: O cliente ativo deve ser capaz de solicitar a um SP a lista de atributos exigidos para acessar o serviço;
  - RNF 02: O cliente ativo deve ser capaz de solicitar a lista de atributos conforme o *XML Schema* de requisição de lista de atributos (ver Seção 4.2.4 e Figura 17);
- RF 04: O cliente ativo deve ser capaz de apresentar a lista de atributos que o SP necessita e solicitar o consentimento do usuário para prosseguir com o processo de agregação dos atributos;
- RF 05: O cliente ativo deve permitir que o usuário informe os seus provedores de identidades capazes de atestar os atributos exigidos pelo SP;

- RF 06: O cliente ativo deve ser capaz de autenticar o usuário no IdP que contém o atributo solicitado;
  - RNF 03: O cliente ativo deve ser capaz de apresentar o endereço do IdP que o usuário está se autenticando;
- RF 07: O cliente ativo deve ser capaz de, em nome de usuário autenticado, solicitar uma asserção de atributos a um IdP que contém o(s) atributo(s) solicitado (s);
  - RNF 04: O cliente ativo deve ser capaz de encaminhar o *token* de autenticação (asserção SAML), obtido na autenticação do usuário;
- RF 08: O cliente ativo deve ser capaz de realizar a agregação de atributos de múltiplos IdPs no ambiente operacional do usuário;
- RF 09: O cliente ativo deve ser capaz de apresentar o resultado da agregação de atributos para o usuário para que este libere o seu uso (consentimento do usuário);
- RF 10: O cliente ativo deve ser capaz de salvar, no ambiente operacional do usuário em um local definido por este, o resultado da agregação de atributos (asserções de atributos do usuário);
- RF 11: O cliente ativo deve ser capaz de enviar ao SP os atributos agregados e liberados pelo usuário;
  - RNF 05: O cliente ativo deve ser capaz de enviar os atributos agregados, conforme o *XML Schema* de resposta dos atributos (ver Seção 4.2.4 Figura 19);
- RF 12: O cliente ativo deve ser capaz de gerenciar os pseudônimos do usuário;
- RF 13: O cliente ativo deve permitir que o usuário registre, em uma política de liberação de atributos, o resultado da agregação de atributos para que este possa ser usado novamente pelo usuário em um próximo acesso ao SP;
- RF 14: O cliente ativo deve ser capaz de salvar, no ambiente operacional do usuário em um local definido por este, a política de liberação de atributos;
  - RNF 06: A política de liberação de atributos deve ser salva em um arquivo criptografado por senha no local indicado pelo usuário;

- RF15: O cliente ativo deve permitir que o usuário remova um item da política de liberação de atributos;
  - RNF 07: Antes de remover qualquer item, o cliente ativo deve solicitar que o usuário confirme a ação.

Esta seção apresenta os requisitos não funcionais (RNF) do mecanismo agregador de atributos (cliente ativo) para uma federação governamental, que são:

- RNF 08: O cliente ativo deve utilizar o protocolo SSL (HTTPS) na comunicação com os IdPs e SPs para prover um canal de comunicação seguro;
- RNF 09: O cliente ativo deve ser independente de sistema operacional (portabilidade);
- RNF 10: O cliente ativo deve suportar o protocolo SAML para trocas de mensagens com os provedores de identidade e de serviços;
- RNF 11: O cliente ativo deve utilizar REST para acesso aos serviços *Web* dos provedores de serviço e provedores de identidade;
- RNF 12: O cliente ativo deve seguir as recomendações do Governo Federal e fazer uso de softwares e bibliotecas livres;
- RNF 13: O protocolo HTTP/1.1 deve ser utilizado para transferência de hipertexto;
- RNF 14: O cliente ativo deve possuir registros históricos (logs) das asserções SAML resultantes do processo de agregações de atributos realizadas pelo usuário, para permitir auditorias e provas materiais, bem como a utilização de mecanismos que garantam a autenticidade dos registros armazenados, se possível, com assinatura digital;
- RNF 15: O sistema deve utilizar o conjunto de caracteres e alfabetos: UNICODE standard, versão 4.0, latin-1, UTF8, ISBN 0-321-18578-1;
- RNF 16: O sistema deve somente utilizar o formato XML para intercâmbio de hipertexto;
- RNF 17: O sistema deve somente utilizar os seguintes formatos para as imagens:

- a. PNG (.png), gerado conforme especificações do W3C - ISO/IEC 15948:2003;
- b. TIFF (.tif);
- c. SVG (.svg), gerado conforme especificações do W3C;
- d. JPEG File Interchange Format (.jpeg, .jpg ou .jfif);
- e. BMP (.bmp); e
- f. GIF (.gif), gerado conforme as especificações GIF87a e GIF89a.

## 4.5 PROTÓTIPO DESENVOLVIDO

Com o objetivo de avaliar a flexibilidade proporcionada com o uso do mecanismo agregador de atributos proposto, o impacto sobre a interoperabilidade do sistema de gerenciamento de identidades adotado e a privacidade e usabilidade dos usuários ao fazer uso do cliente ativo, um protótipo do mecanismo agregador de atributos foi desenvolvido integrado ao cenário de uso de solicitação de emissão de passaporte. Neste cenário, os objetivos do serviço são:

- agilizar o processo de solicitação de passaporte, disponibilizando à Polícia Federal os atributos de identidade dos solicitantes, atestados por seus provedores de identidades;
- permitir a agregação de atributos dos usuários (CPF, RG e Título de Eleitor) que estão em diferentes Provedores de Identidades (Receita Federal, Tribunal Superior Eleitoral e Polícia Federal/RIC).

### 4.5.1 Ferramentas e tecnologias utilizadas

Na escolha das ferramentas e tecnologias utilizadas no protótipo do mecanismo agregador de atributos e no experimento construído para avaliação do mecanismo agregador, foram priorizadas soluções de *software livre*, conforme recomendado pelo governo brasileiro.

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 direto de navegadores *Web* (aplicativo em *Java Web Start* - JWS). Esta tecnologia permite que um aplicativo, que está disponível em um provedor, seja migrado para a máquina do usuário e seja executado em seu ambiente operacional<sup>14</sup>.

Os serviços de descoberta de provedor de cliente ativo (SPDCA), de provedor de cliente ativo (PCA) e o serviço para emissão de passaporte que foram utilizados nos experimentos de avaliação do mecanismo agregador de atributos foram, desenvolvidos em PHP, por ser uma tecnologia mais simples (o que agilizou o desenvolvimento do protótipo). Além disso, esta tecnologia oferece suporte a todas as tecnologias necessárias, tais como o protocolo SSL, especificação SAML, serviços *Web* e REST.

Para atender aos requisitos da arquitetura e-PING, os provedores de identidades necessários para execução dos experimentos estão de acordo com a especificação SAML. Para isto, foi utilizado o *framework simpleSAMLPHP*. Além de possuir uma boa documentação, este *framework* foi escolhido por seu amplo uso em muitas soluções que fazem uso da especificação SAML e por ser um *software livre*.

Para relação dos testes de segurança, foi utilizado a ferramenta Wireshark<sup>15</sup>. Esta ferramenta funciona como um *sniffer*. Esta ferramenta é capaz de interceptar e registrar o tráfego de dados em uma rede de computadores. Ela ajudou no entendimento do funcionamento da aplicação

---

<sup>14</sup> O *Java Web Start* é iniciado automaticamente quando é feito o primeiro *download* de um aplicativo Java que utiliza essa tecnologia. O *Java Web Start* armazena todo o aplicativo localmente, na memória cache do computador. Assim, todas as inicializações subsequentes são quase instantâneas, pois todos os recursos necessários já estão disponíveis localmente.

<sup>15</sup> <http://www.wireshark.org/>



SimpleSAMLPHP e também para comprovar que as trocas de mensagem entre as aplicações desenvolvidas para o protótipo do mecanismo agregador de atributos estava sendo executada por um canal de segurança criptografado.

#### 4.5.2 Detalhamento do Cenário de Uso

De forma a avaliar a aplicabilidade do mecanismo agregador de atributos proposto, o mecanismo agregador de atributos foi integrado ao cenário para solicitação de emissão de passaporte descrito na Seção 4.3.1. O modo de funcionamento suportado na primeira versão do mecanismo de agregação de atributos foi o modo transitório dinâmico, ou seja, sem suporte para registro de política de liberação de atributos e para autenticação SSO para acesso aos IdPs. Para este experimento, foram implementados um serviço *Web* para emissão de passaporte simples, porém, funcional, quatro IdPs SAML, uma aplicação PHP denominada de Serviço de Descoberta de Provedor de Cliente Ativo (SDPCA), uma aplicação *Web* para realizar o *download* do cliente ativo (provedor de cliente ativo - PCA). A seguir, têm-se algumas informações mais detalhadas a respeito das aplicações:

- a aplicação *Web* PHP *Restful* para solicitação de emissão de passaporte implantada como um módulo no SP SimpleSAMLPHP da Polícia Federal;
- a aplicação *Web* PHP *Restful* que apresenta uma lista de provedores de cliente ativo homologados, implantado como um módulo no SP SimpleSAMLPHP SDPCA;
- aplicação *Web* PHP *Restful*, responsável por disponibilizar para *download* o aplicativo de cliente ativo implantada como um módulo no SP SimpleSAMLPHP PCA<sup>16</sup>;

As aplicações *Web* desenvolvidas seguem a especificação SAML e as mesmas fazem parte de uma federação, ou seja, a autenticação, realizada inicialmente no Provedor de Identidade da Polícia Federal, é aceita nos demais provedores. Os *tokens* SAML são aceitos em todos os provedores da federação, isso se faz necessário para realizar a autenticação SSO.

---

<sup>16</sup> É possível acessar esta aplicação e testar todo o protótipo desenvolvido no endereço <http://goo.gl/PH30Ks>.

Foram desenvolvidos também quatro provedores de identidades SAML: IdP Polícia Federal, IdP Receita Federal, IdP Tribunal Superior Eleitoral e IdP RIC. Os outros três provedores de identidade são utilizados durante o processo de agregação dos atributos, ou seja, quando o Cliente Ativo solicita os atributos.

### **4.5.3 Configuração dos Serviços da Federação Governamental**

Para constituir a federação e o círculo de confiança, foi necessário configurar os metadados para cada serviço (SPDCA, PCA e Serviço de Emissão de Passaporte) para estabelecer as relações de confiança com os IdPs. Da mesma forma, os metadados dos IdPs foram configurados para confiarem nos SPs. Além disso, o mecanismo de autenticação utilizado em cada IdP foi definido com o baseado em senha, porém nenhuma base de dados foi configurada. As contas utilizadas nos IdPs foram criadas estaticamente. Foram definidos ainda a chave e o certificado utilizado por cada IdP nas assinaturas digitais. As configurações citadas, realizadas no Framework SimpleSAMLPHP, estão no Apêndice B.

Cada serviço desenvolvido foi acrescentado a um SP SimpleSAMLPHP como um módulo e suas páginas foram protegidas, exigindo a autenticação do usuário. As configurações citadas, realizadas no Framework SimpleSAMLPHP, estão no Apêndice B.

### **4.5.4 Diagrama de Sequência Detalhado**

A seguir, a Figura 21, Figura 22, Figura 23 e Figura 24 apresentam o diagrama de sequência detalhado para acesso ao provedor de serviços da Polícia Federal. A Figura 21 apresenta no diagrama de sequência das interações até o momento em que o usuário indica que deseja executar o processo de agregação de atributos e é redirecionado para o SPDCA.

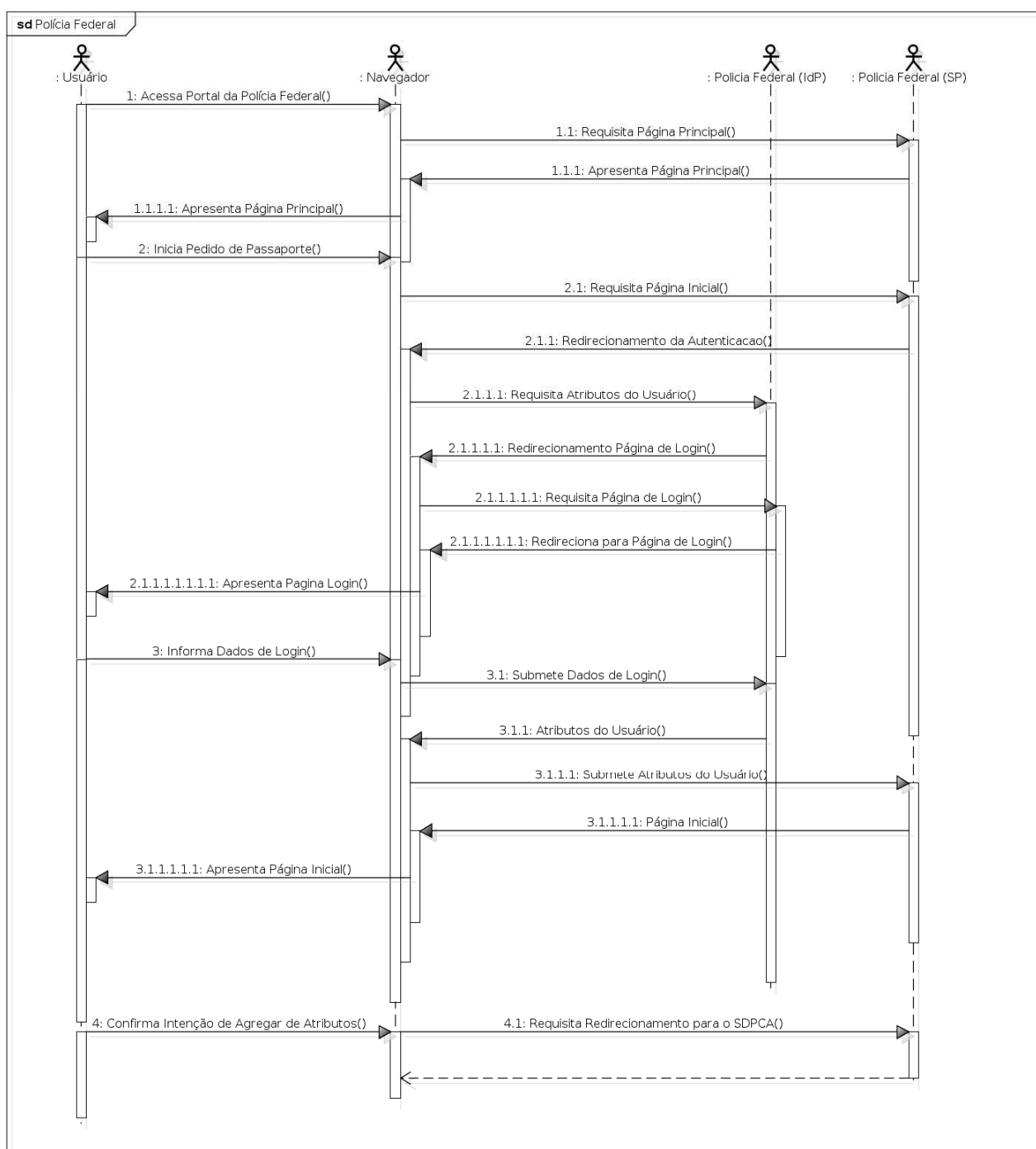


Figura 21. Diagrama de Sequência Parcial 1

A Figura 22 apresenta as trocas de mensagens ocorridas quando da utilização do SDPCA. Vale destacar que o usuário não precisou se autenticar no SDPCA, pois este serviço aceita o *token* de autenticação enviado juntamente com a requisição (mensagem 1). O SDCA confere junto ao IdP a autenticação e atributos do usuário antes de liberar a página para seleção do provedor de cliente ativo.

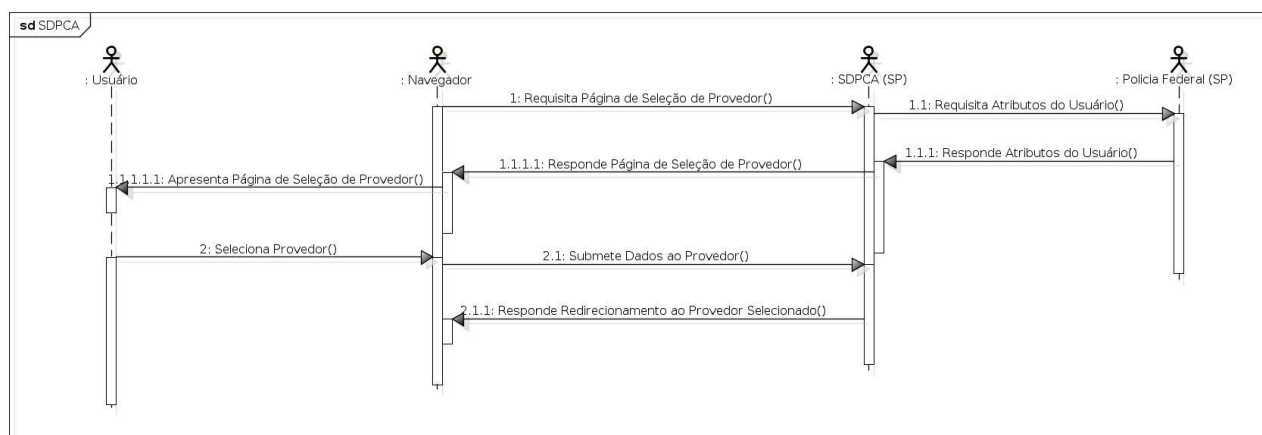


Figura 22. Diagrama de Sequência Parcial 2

A Figura 23 apresenta o fluxo de mensagens quando o Provedor de Cliente Ativo (PCA) é acessado.

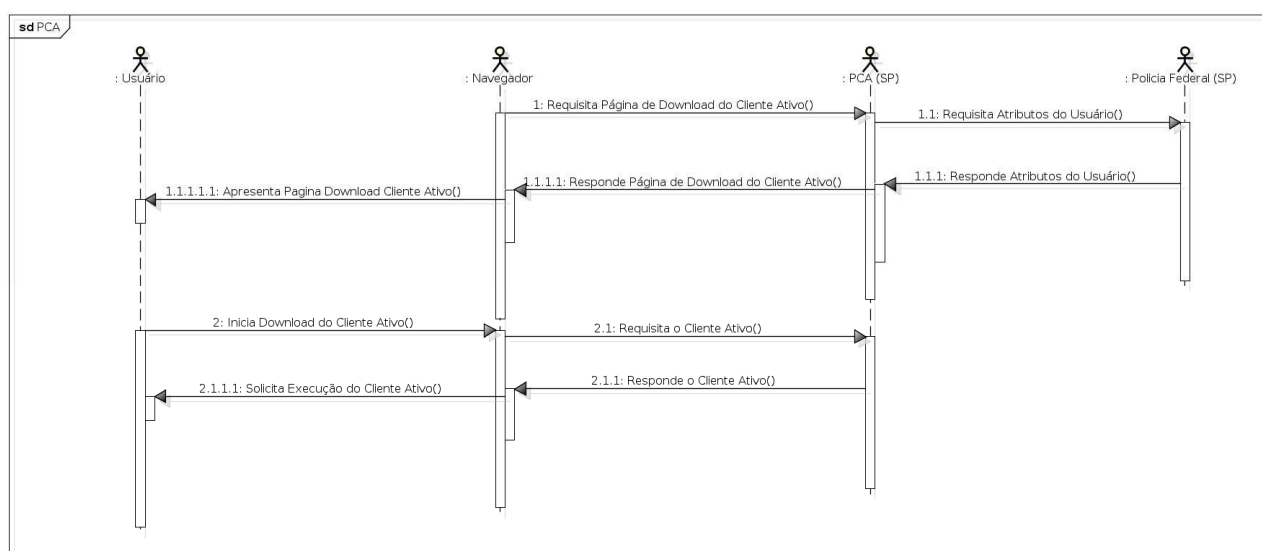


Figura 23. Diagrama de Sequência Parcial 3

O diagrama de sequência da Figura 24 representa as trocas de mensagens quando o Cliente Ativo (mecanismo agregador de atributos) é utilizado. Inicialmente, o usuário deverá estar executando o Cliente Ativo em seu computador (passo 1).

No passo 2, o usuário irá indicar que deseja continuar a execução do cliente ativo, para obter do SP da Polícia Federal a lista de atributos. Neste momento, o cliente ativo é redirecionado para a página de autenticação do Idp da Polícia Federal. Em seguida, o cliente ativo apresenta uma tela de login para que o usuário se autentique no IdP da Polícia Federal. No passo 3, o usuário deverá

informar suas credenciais de acesso. O cliente ativo irá encaminhá-las para o IdP da Polícia Federal para que o mesmo autentique o usuário. Após a autenticação bem sucedida, o SP encaminha para o cliente ativo os atributos necessários (passo 3.1.2). Em seguida, o cliente ativo solicita que o usuário indique em qual IdP este deseja obter o atributo CPF (passo 3.2).

Como no protótipo não foi implementada autenticação SSO no processo de agregação de atributos (modo transiente dinâmico), no passo 4, o usuário deve indicar os dados (credenciais de acesso) para autenticação no IdP da Receita Federal. O mesmo ocorre nos passos 5 e 6 para o IdPs do TSE e do RIC/Polícia Federal.

Na configuração de cada IdP utilizado pelo cliente ativo para obter os atributos, foi configurado também um SP que é o responsável por receber a requisição do cliente ativo e encaminhar para o IdP. Isto é necessário uma vez que o cliente ativo não é um SP da federação e, portanto, não possui relação de confiança com os IdPs para solicitar atributos de usuários.

No passo 7, o usuário poderá optar por salvar os XML gerados pelo cliente ativo em seu computador. No passo oito (8), o usuário deverá confirmar seus atributos agregados e então permitir que o sistema encaminhe as asserções SAML de atributos ao provedor de serviço da Polícia Federal. Por fim, o navegador do usuário é iniciado e é redirecionado para o SP, que envia o resumo dos atributos recebidos e um número de protocolo gerado para aquele pedido do usuário.

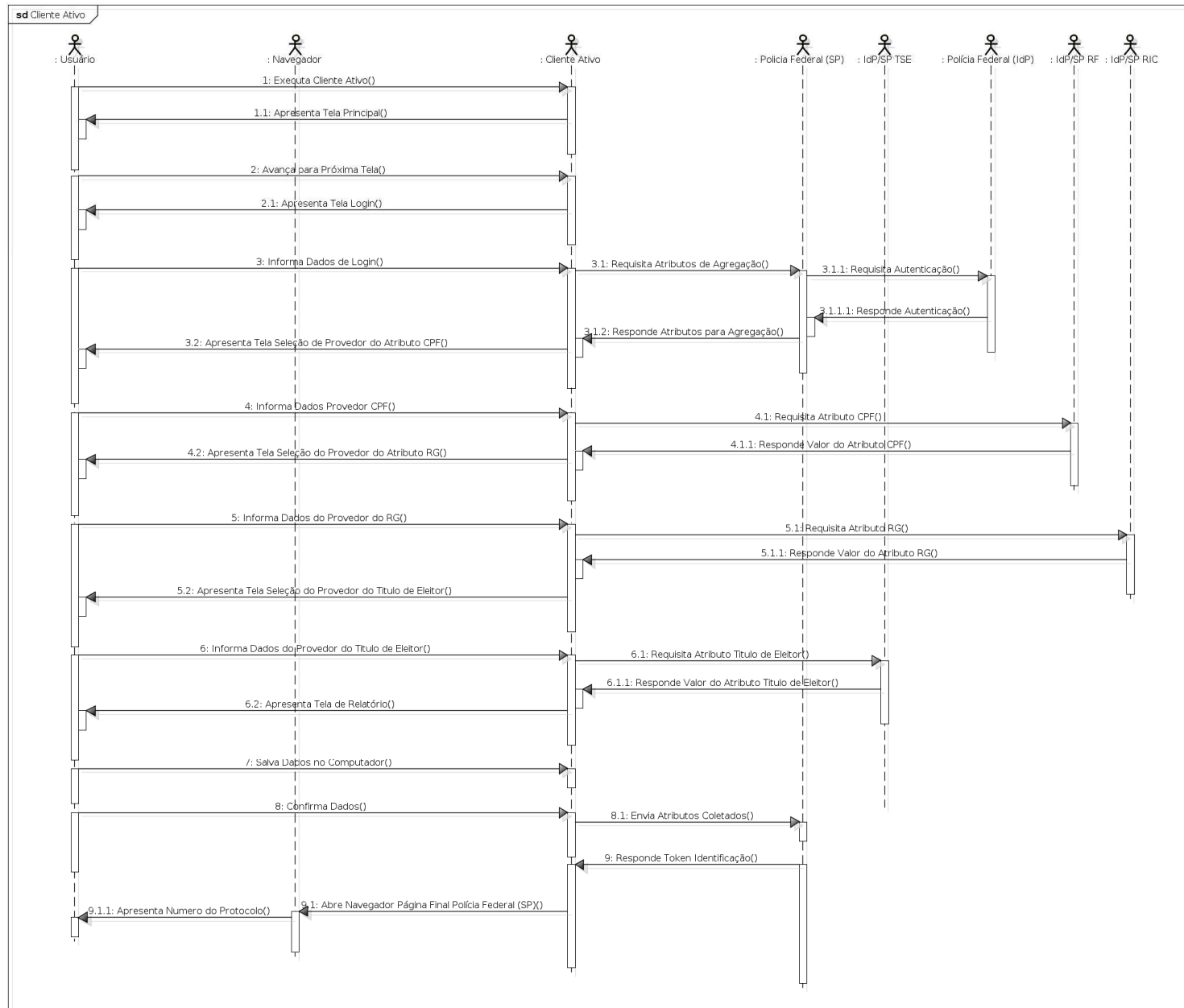


Figura 24. Diagrama de sequência Parcial 5

Pela análise dos diagramas de sequência apresentados, pode-se verificar que somente o requisito funcional (RF) 11 não foi implementado.

O diagrama de classes do mecanismo agregador de atributos e uma breve descrição de suas classes e da biblioteca de classes da Apache utilizada encontram-se disponíveis no APÊNDICE G –.

#### **4.5.5 Implementação do modo permanente dinâmico**

O modo permanente dinâmico provê aos usuários uma funcionalidade bastante facilitadora, visto que este modo elimina a necessidade de repetidas autenticações nos provedores de identidade para que os atributos possam ser coletados.

Como prova de conceito, a autenticação SSO dos IdP foi implementada em uma aplicação *Web* (SP). 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 redireciona o navegador do usuário para os IdPs que detêm os atributos requeridos e indicados pelo usuário.

A Figura 25 representa as trocas de mensagens realizadas entre os provedores de serviço, provedores de identidade, navegador e usuário. Estas mensagens demonstram o correto funcionamento do mecanismo de autenticação e compartilhamento de atributos com a autenticação SSO no nível dos provedores de identidade.

Conforme pode ser observado no passo 1 e 2 da ilustração, o usuário primeiramente deve acessar a página do provedor de serviços por intermédio de seu navegador *Web*. O provedor de serviço redireciona (passo 3 e 4) o navegador do usuário para o IdP que necessita dos atributos. Este provedor de identidade identifica que o usuário não está ainda autenticado no mecanismo e então redireciona (passo 5 e 6) o navegador do usuário para o IdP de autenticação central. Vale destacar que os atributos dos usuários não são compartilhados com o IdP central e nem mesmo este sabe para qual provedor de serviço o atributo será compartilhado.

Após a navegação chegar ao IdP Central, este irá identificar que o usuário ainda não está autenticado e então irá apresentar a tela de login para o usuário (passo 7 e 8). No passo 9, o usuário

irá informar seus dados de acesso ao IdP Central. E então irá solicitar ao seu navegador que os dados sejam submetidos (passo 10).

Após receber os dados de autenticação e validar os mesmos, o IdP Central irá redirecionar (passo 11 e 12) a navegação e encaminhará a asserção de autenticação do usuário para o IdP 1 que requisitou a autenticação inicialmente. O IdP 1 então identifica a autenticação do usuário, e a seguir encaminha os atributos do usuário que estão em seu poder para o SP (passo 13 e 14) por intermédio do navegador de internet do usuário.

O SP, por sua vez, após receber os atributos (passo 15) compartilhados do provedor de identidade, irá apresentar a página restrita com o resultado da agregação dos atributos do usuário compartilhados do IdP (passo 16).

No passo 17, o usuário poderá novamente acessar um serviço a partir de seu navegador (passo 18) que, então, irá redirecionar sua navegação para o IdP 2 (passo 19 e 20). Este verifica que ainda não existe uma sessão anteriormente criada para este usuário, e solicita a autenticação no IdP Central (passo 21 e 22), redirecionando a navegação do usuário para este.

O IdP Central irá identificar que o usuário já está autenticado no sistema, e irá gerar uma nova asserção de autenticação que será encaminhada ao IdP 2 (passo 23 e 24) por intermédio do navegador do usuário. O IdP 2 então recebe a asserção de autenticação e encaminha o atributos armazenados em sua base de dados para o SP (passo 25 e 26) por intermédio do navegador do usuário.

Por fim, o SP exibe ao usuário, por intermédio de seu navegador, o resultado da agregação de atributos do IdP 2 (passo 27 e 28). Percebe-se que no segundo processo de agregação dos atributos do IdP 2 a navegação do usuário foi redirecionada para o IdP central. E como o usuário já possuía uma sessão de autenticação neste IdP, este pode gerar uma nova asserção de autenticação que foi compartilhada com o IdP 2, sem a necessidade de autenticação do usuário. Neste caso pode-se observar o correto funcionamento da autenticação SSO no nível dos Provedores de Identidade.



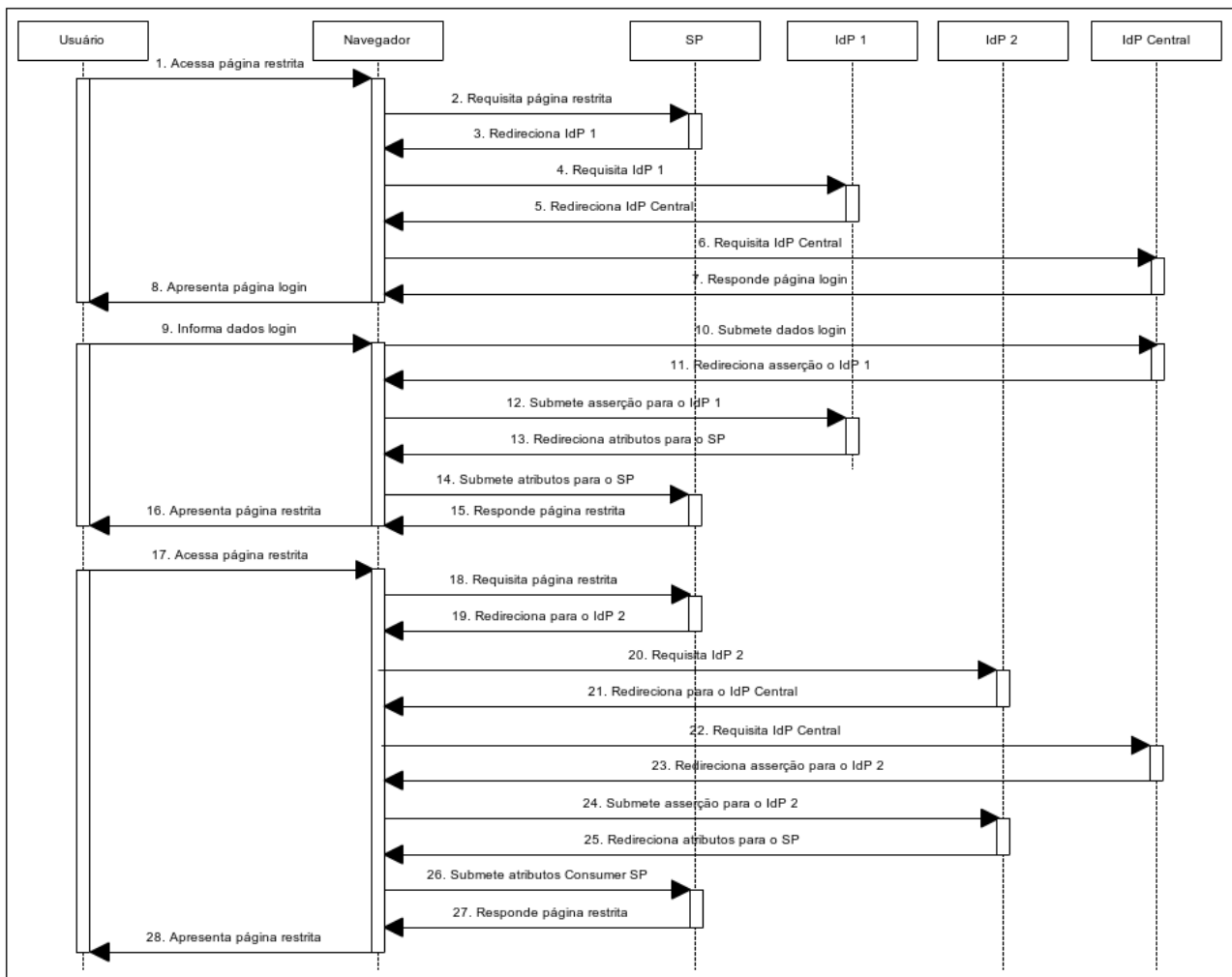


Figura 25: Sequência de mensagens para a primeira utilização do mecanismo com SSO nos IdPs

## 5 RESULTADOS

Neste capítulo, são apresentados os resultados obtidos na fase de avaliação do mecanismo agregador de atributos. Nesta fase de avaliação, procurou-se analisar o atendimento aos requisitos funcionais e não funcionais do mecanismo agregador de atributos e as hipóteses de pesquisa (em relação à privacidade, flexibilidade e usabilidade da solução proposta). A avaliação foi dividida em três etapas. A primeira refere-se aos testes de *software* executados pelo próprio desenvolvedor e por um aluno de graduação; a segunda refere-se a um experimento que envolveu o uso do protótipo implementado por especialistas de TI do Governo e à aplicação de um questionário com uma pesquisa de satisfação, e a terceira etapa foi a comparação do mecanismo proposto com os trabalhos relacionados.

A Seção 5.1 apresenta o projeto dos experimentos de avaliação. A Seção 5.2 apresenta os resultados obtidos e análise dos experimentos e a Seção 5.3 apresenta a comparação com os trabalhos relacionados.

### 5.1 PROJETO DOS EXPERIMENTOS DE AVALIAÇÃO DO MECANISMO AGREGADOR DE ATRIBUTOS PROPOSTO

Após a conclusão da implementação do protótipo, este passou por testes funcionais e testes não funcionais (portabilidade e segurança) nos níveis de sistema e integração. Para esta primeira etapa, foram escritos seis casos de testes (estratégia de caixa preta).

Dentre os aspectos que foram avaliados estão:

- funcionalidades (implementação correta dos casos de uso);
- portabilidade (comportamento do protótipo em ambientes operacionais e navegadores diferentes); e
- segurança (atendimento das propriedades de privacidade, integridade e confidencialidade).

Para segunda etapa de avaliação, um teste de usabilidade foi definido. Foram elaborados dois roteiros (ver APÊNDICE D – e APÊNDICE E –) para que os profissionais soubessem dos

objetivos do mecanismo agregador e do cenário de uso (Serviço de Emissão de Passaporte), porém nenhuma informação referente à estrutura interna de funcionamento do *software* foi passada. Vale destacar que as únicas diferenças entre os dois roteiros elaborados são algumas questões do perfil do avaliador, já que um roteiro foi direcionado para os prestadores de serviços e o outro para funcionários do Governo. Os questionários tiveram como objetivo:

1. Identificar o conhecimento do avaliador em relação a alguns conceitos sobre gestão de identidades (autenticação SSO, provedores de identidades, autenticação federada, SAML, OpenID, OAuth);
2. Identificar se estes trabalharam direta ou indiretamente no desenvolvimento de *software* de governo eletrônico;
3. Identificar qual sistema operacional e navegador os avaliadores usaram nos testes;
4. Identificar se os avaliadores conseguiram executar todo o experimento conforme descrito no roteiro e quais problemas ocorreram;
5. Identificar se o que estava sendo executado no protótipo partiu de uma ação do avaliador e se as mensagens de erros (caso tenham ocorrido) o ajudaram a resolver o problema;
6. Identificar se os avaliadores se sentiram confortáveis (satisfação do usuário) quanto ao uso do protótipo, e em quais situações eles não tiveram a sensação de conforto;
7. Verificar se os avaliadores ficaram satisfeitos em relação à apresentação das informações;
8. Verificar o grau de satisfação dos avaliadores em relação ao uso do protótipo;
9. Verificar se os avaliadores ficaram satisfeitos em relação ao tempo de resposta;
10. Verificar se os avaliadores se sentiram mais seguros ao utilizar os serviços do protótipo, em relação a outros serviços de Governo Eletrônico;
11. Verificar se os avaliadores, em algum momento, não souberam o que fazer e se estes tiveram dificuldades para entender as funções dos serviços;
12. Verificar se os avaliadores gostariam de utilizar o mecanismo agregador de atributos em aplicações de governo eletrônico.

13. Verificar se os avaliadores constataram que o uso do mecanismo agregador de atributos pode agilizar o processo de obtenção e apresentação dos atributos do usuário em aplicações de e.gov;
14. Verificar se os avaliadores constataram que o uso do mecanismo agregador de atributos pode trazer mais flexibilidade para os serviços de e.gov;
15. Verificar se os avaliadores constataram que o mecanismo agregador de atributos pode garantir a privacidade dos usuários;
16. Identificar quais os impactos negativos do uso do mecanismo proposto pode trazer para os desenvolvedores de aplicações e.gov;
17. Verificar se os avaliadores recomendariam o mecanismo agregador de atributos para ser usado em serviços de e.gov;
18. Identificar o que os avaliadores avaliaram como melhor no experimento executado; e
19. Identificar o que pode ser melhorado no mecanismo agregador de atributos;

Com o objetivo de alcançar os avaliadores, uma mensagem de correio eletrônico (ver APÊNDICE C – e APÊNDICE D –) foi encaminhada para cinquenta e oito (58) pessoas que trabalham em instituições governamentais e para quarenta e quatro (44) pessoas que prestam serviços de TI para o Governo. Obteve-se com a pesquisa de avaliação um total de trinta e nove respostas. Os resultados obtidos serão apresentados na próxima seção.

## **5.2 RESULTADOS OBTIDOS E ANÁLISE DOS RESULTADOS**

Esta seção apresenta os resultados obtidos na execução dos casos de teste e os resultados e análise referentes à pesquisa de satisfação aplicada. A descrição detalhada dos resultados obtidos na pesquisa de satisfação encontra-se no APÊNDICE F –.

### 5.2.1 Resultados da Execução dos casos de teste

Quadro 5. Detalhamentos do caso de teste CT 01

Tipo de teste:	Funcional
Descrição (passos)	Ao acessar a página do provedor de serviço, serão apresentadas informações referentes às necessidades do provedor sobre o serviço. Será possível iniciar o processo de agregação de atributos. Neste momento o navegador será redirecionado para a tela de autenticação no provedor de identidade. Após o usuário realizar a autenticação com sucesso, o navegador será novamente redirecionado para o provedor de serviço que poderá listar os atributos necessários para a prestação do serviço requisitado.
Contexto/pré-requisitos	Federação governamental configurada com todos os SPs e IdPs do protótipo.
Dados do teste (entrada)	URL para acesso ao Serviço de Emissão de Passaportes: <a href="http://goo.gl/PH30Ks">http://goo.gl/PH30Ks</a> Dados para acesso: Usuário: user Senha: userpass
Resultados Esperados	Usuário autenticado e ciente dos atributos solicitados pelo SP (lista).

**Execução do teste:** Em um computador pessoal, com acesso à Internet e um navegador *Web* instalado, foi acessado o endereço <http://goo.gl/PH30Ks>. Ao acessar o endereço do provedor de aplicação, o navegador *Web* apresentou uma mensagem de alerta (ver Figura 26) informando que o certificado de segurança contido na aplicação não é confiável. Essa mensagem era esperada, visto que os certificados *ssl* utilizados nas aplicações do experimento são todos auto assinados. Após aceitar o certificado, o sistema apresentou a tela inicial do portal de solicitação de passaportes da Polícia Federal (ver Figura 27). Esta tela não requer autenticação e exibe apenas textos explicativos e um botão de ação para iniciar o processo de solicitação de passaporte.

Após clicar em “iniciar o procedimento de solicitação de passaporte”, o navegador *Web* do usuário foi redirecionado para a página de autenticação do IdP da Polícia Federal e um novo alerta de certificado de segurança não confiável apareceu (ver Figura 28). Após aceitar o uso deste tipo de certificado, o sistema apresentou a tela de autenticação conforme pode ser observado na Figura 29. Nesta tela de autenticação, o usuário entrou com os dados de acesso para proceder com a autenticação.

Após a autenticação ser realizada com sucesso, o IdP redirecionou o navegador *Web* para o serviço de Emissão de Passaporte da PF que apresentou uma tela informando a lista de atributos necessários para a realização do serviço de solicitação de passaporte (Figura 30).

**Resultado do teste:** Usuário autenticado e ciente dos atributos solicitados pelo SP (lista).



Figura 26. Tela de alerta de certificado ssl não confiável



Figura 27. Tela inicial do Provedor de Serviço da Polícia Federal

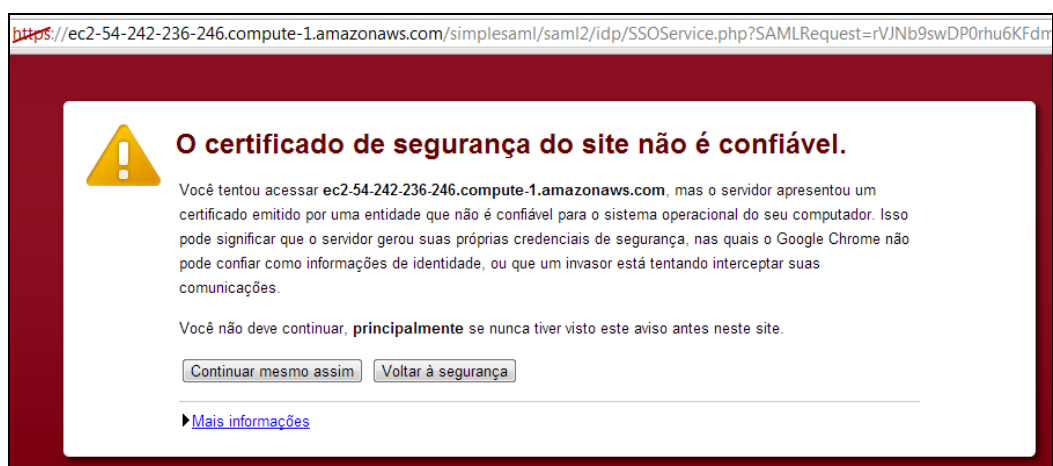


Figura 28. Tela de certificado de segurança inválido



Figura 29. Tela de autenticação do provedor de identidade da Polícia Federal



Figura 30. Tela de atributos requeridos pelo provedor da Polícia Federal

#### Quadro 6. Detalhamentos do caso de teste CT 02

Tipo de teste	Funcional
Descrição (passos)	Após realizar os passos descritos no CT 01, o usuário deverá dar continuidade, aceitando o início do processo de agregação de atributos. O navegador do usuário deverá ser redirecionado para a tela do Serviço de Descoberta de Cliente Ativo (SDPCA) que solicitará ao usuário a seleção de um provedor de Cliente Ativo de sua preferência. Ao selecionar um dos provedores da lista, e confirmar o acesso ao provedor, o navegador do usuário será redirecionado para a tela do Provedor de Cliente Ativo, onde o usuário deverá efetuar o <i>download</i> da aplicação e executar a mesma em seu computador.
Contexto/pré-requisitos	Usuário deve estar autenticado no sistema
Dados do teste (entrada)	Sem entradas
Resultados Esperados	<i>Download</i> do cliente ativo e execução automática do mesmo.

**Execução do teste:** Após executar os mesmos passos descritos no CT 01, o usuário confirma o desejo de executar a agregação de atributos pressionando o botão avançar. O navegador foi redirecionado para o Serviço de Descoberta de Provedor de Cliente Ativo (SDPCA) e mais uma mensagem de alerta referente ao certificado autoassinado (Figura 31). Após aceitar o uso deste tipo de certificado, o sistema apresenta a tela do SDPCA com as instruções de acesso, listando os Provedores de Cliente Ativo (Figura 32).



Após selecionar um provedor e clicar em avançar, o navegador foi redirecionado para a tela do Provedor de Cliente Ativo (PCA) e neste momento um novo alerta referente ao certificado autoassinado foi apresentado (Figura 33). Após aceitar o uso do certificado, o sistema exibiu a tela do PCA para efetuar o *download* do Cliente Ativo (ver Figura 34). O *download* do arquivo jnpl do cliente ativo foi realizado e ao tentar executar o cliente ativo, o *software Java Web Start* acessou o serviço de provedor de cliente ativo para verificar se havia uma nova versão disponível. Como esta conexão é segura (SSL), o navegador informa que o certificado do servidor não é confiável (Figura 35). Após aceitar o certificado como confiável, outra mensagem de alerta aparece indicando que o código do cliente ativo (.jar) foi assinado por uma entidade não confiável (Figura 36). Após confiar na assinatura, o cliente ativo foi executado e a tela inicial deste foi apresentada (Figura 37).

**Resultado do teste:** Aplicativo do cliente ativo na máquina do usuário e em execução.

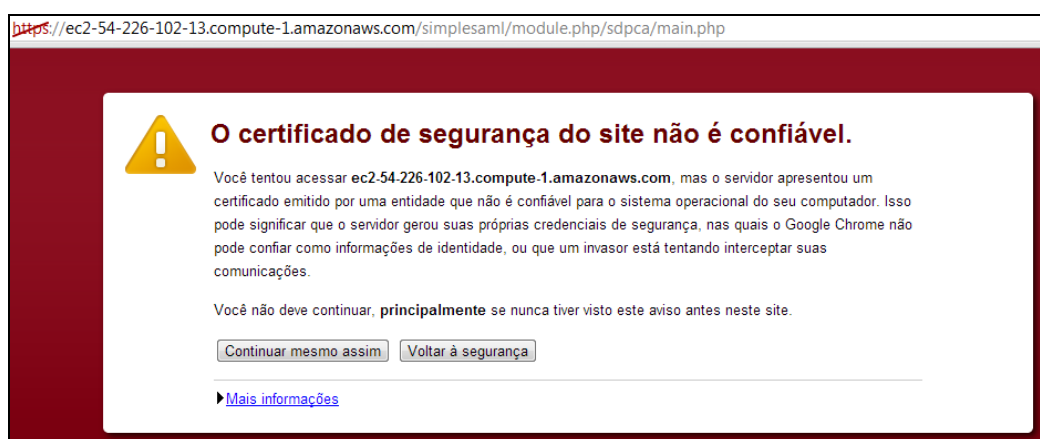


Figura 31. Mensagem de alerta de certificado no SDPCA



Figura 32. Tela do SDPCA com a lista de provedores de Cliente Ativo



Figura 33. Tela de certificado não confiável do PCA



Figura 34. Tela do PCA para realização do download do Cliente Ativo

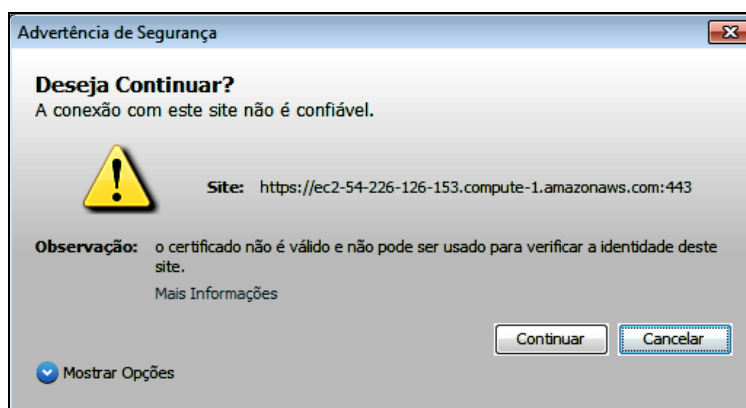


Figura 35. Alerta de segurança ao executar o Cliente Ativo

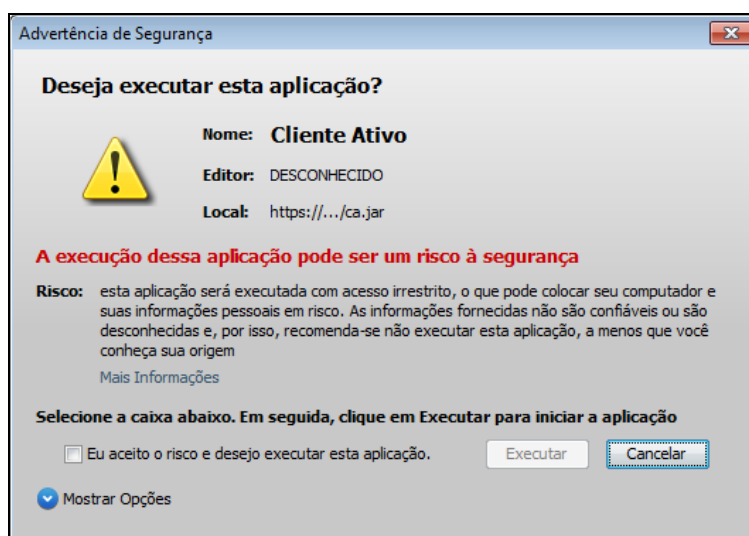


Figura 36. Alerta de segurança ao executar o Cliente Ativo com certificado desconhecido

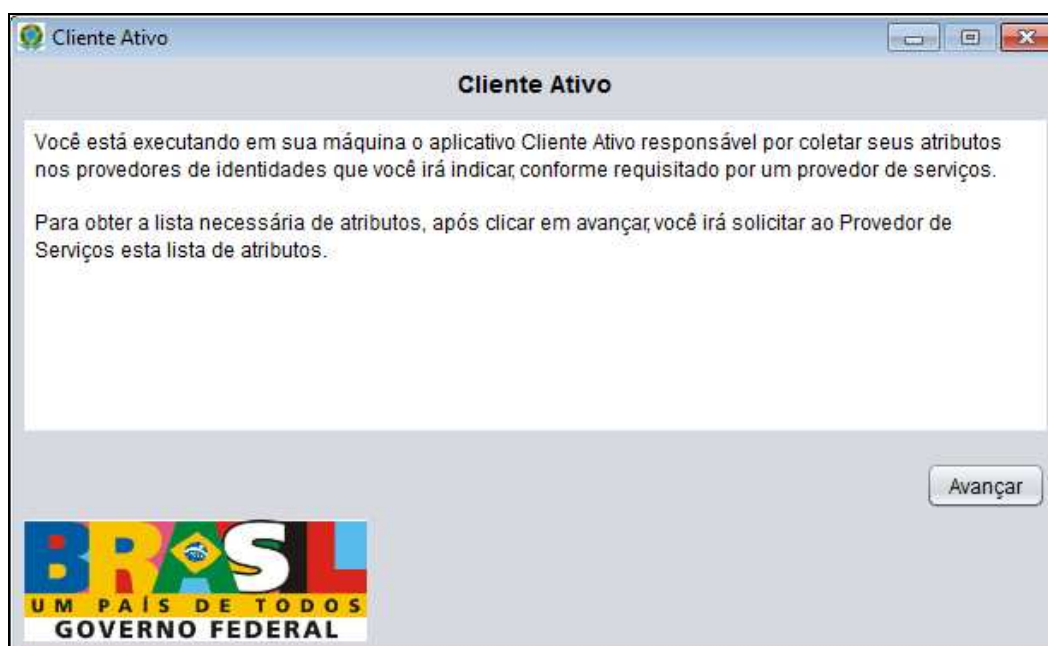


Figura 37. Tela inicial do Cliente Ativo

Quadro 7. Detalhamentos do caso de teste CT 03

Tipo de teste	Funcional
Descrição (passos)	<p>Após executar corretamente o CT 02, o aplicativo de Cliente Ativo é executado no computador do usuário.</p> <ol style="list-style-type: none"> <li>1. Primeiramente o aplicativo irá solicitar que o usuário se autentique no Provedor de Identidade da Polícia Federal para que este tenha acesso ao XML com a lista de atributos necessários neste provedor;</li> <li>2. Depois da autenticação, o usuário deverá selecionar um provedor para cada um dos atributos solicitados e efetuar a autenticação neste para ter acesso a asserção SAML de atributos do usuário;</li> <li>3. Após o procedimento de agregação de atributos, deve-se exibir uma tela contendo um resumo dos atributos coletados, bem como seus valores e uma opção solicitando que o usuário aceite que seus atributos sejam compartilhados com o Provedor da Polícia Federal;</li> <li>4. Na tela de resumo, o usuário poderá optar por salvar os arquivos SAML em seu computador, e também por aceitar que o aplicativo envie seus atributos agregados para o provedor de serviço; e</li> <li>5. Após o aceite do usuário para o compartilhamento de suas informações, o aplicativo irá enviar os dados para o provedor e fará com que seja aberto automaticamente o navegador padrão do usuário, e uma tela do provedor de serviço, com o resumo da agregação e o protocolo, confirmando a solicitação do serviço, será apresentada.</li> </ol>
Contexto/pré-requisitos	Cliente ativo em execução
Dados do teste (entrada)	<p>Dados para acesso ao IdP da Polícia Federação: Usuário: user Senha: userpass</p> <p>Provedor da Receita Federal (para obter o CPF): Usuário: user1; Senha: userpass1</p> <p>Provedor da Polícia Federal/RIC (para obter o RG) Usuário: user2; Senha: userpass2</p> <p>Provedor do Tribunal Superior Eleitoral (para obter o Título de Eleitor) Usuário: user3 e Senha: userpass3</p>
Resultados Esperados	Agregação dos atributos realizada com sucesso. Resultado da agregação entregue ao Serviço de Emissão de Passaporte e protocolo do pedido gerado no SP.

**Execução do teste:** Primeiramente, executou-se os passos descritos no CT 02. Na primeira tela do cliente ativo, após clicar em avançar, o cliente ativo foi direcionado para o IdP da Polícia Federal e os dados para autenticação foram solicitados na tela do cliente ativo (ver Figura 38). Após entrar com os dados da autenticação, o usuário clicou em autenticar. A autenticação ocorreu com sucesso conforme ilustrado na tela do cliente ativo (ver Figura 38). Após o usuário clicar em avançar, iniciou-se o processo de coleta dos atributos nos provedores de identidade. O usuário

selecionou um provedor de identidade para cada atributo (apenas uma opção é apresentada) e indicou seus dados de acesso para cada IdP (ver Figura 39, Figura 40 e Figura 41). Em seguida, um resumo da agregação de atributos (ver Figura 42) é apresentada. Após analisar os atributos coletados, o usuário clicou em confirmar para aceitar o compartilhamento dos atributos agregados com o serviço da Polícia Federal. Nesse momento, o cliente ativo abriu o navegador *Web* (ver Figura 43) e o redirecionou para o serviço de Emissão de Passaportes. Essa última página apresenta os atributos coletados pelo Cliente Ativo e encaminhados ao SP.

**Resultado do teste:** Agregação dos atributos realizada com sucesso. Resultado da agregação entregue ao Serviço de Emissão de Passaporte e protocolo do pedido gerado no SP.

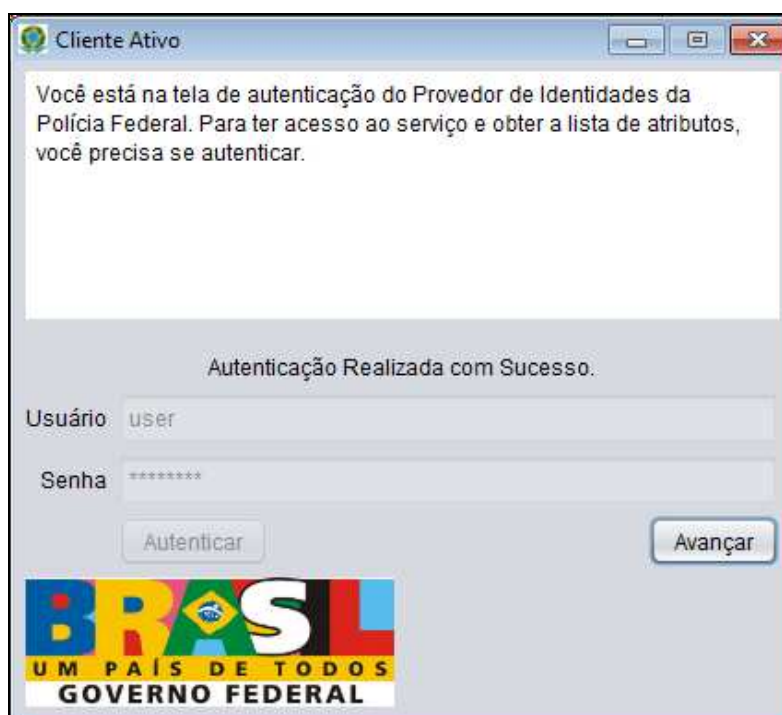


Figura 38. Tela de autenticação inicial no Provedor de Identidade da Polícia Federal

Cliente Ativo

Indique qual Provedor de Identidade você deseja usar para obter o atributo:

**cpf**

Para obter este atributo, você precisa se autenticar no provedor selecionado.

Autenticação Realizada com Sucesso.

Usuário: user1

Senha: \*\*\*\*\*

Provedor: Receita Federal

<https://ec2-54-226-68-80.compute-1.amazonaws.com/simplesaml/module.php/casp1/main.php>

Autenticar Avançar

**BRASIL**  
UM PAÍS DE TODOS  
GOVERNO FEDERAL

Figura 39. Tela de autenticação e agregação do CPF

Cliente Ativo

Indique qual Provedor de Identidade você deseja usar para obter o atributo:

**rg**

Para obter este atributo, você precisa se autenticar no provedor selecionado.

Autenticação Realizada com Sucesso.

Usuário: user2

Senha: \*\*\*\*\*

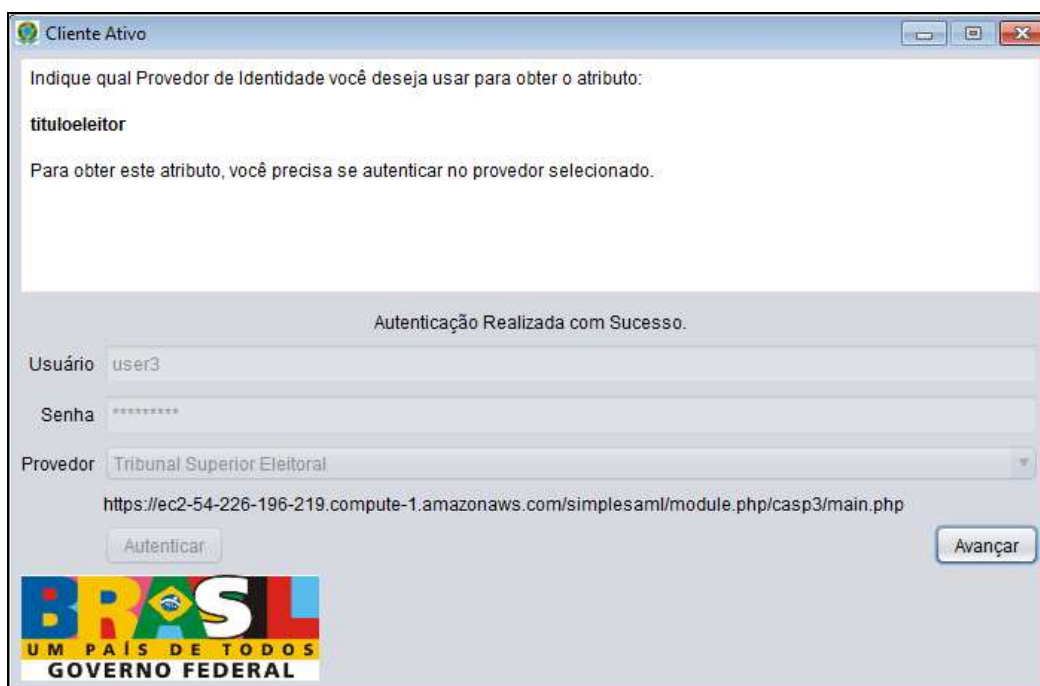
Provedor: Secretaria de Segurança Pública

<https://ec2-54-226-232-34.compute-1.amazonaws.com/simplesaml/module.php/casp2/main.php>

Autenticar Avançar

**BRASIL**  
UM PAÍS DE TODOS  
GOVERNO FEDERAL

Figura 40. Tela de autenticação e agregação do RG



Indique qual Provedor de Identidade você deseja usar para obter o atributo:

**titulo eleit**

Para obter este atributo, você precisa se autenticar no provedor selecionado.

Autenticação Realizada com Sucesso.

Usuário: user3

Senha: \*\*\*\*\*

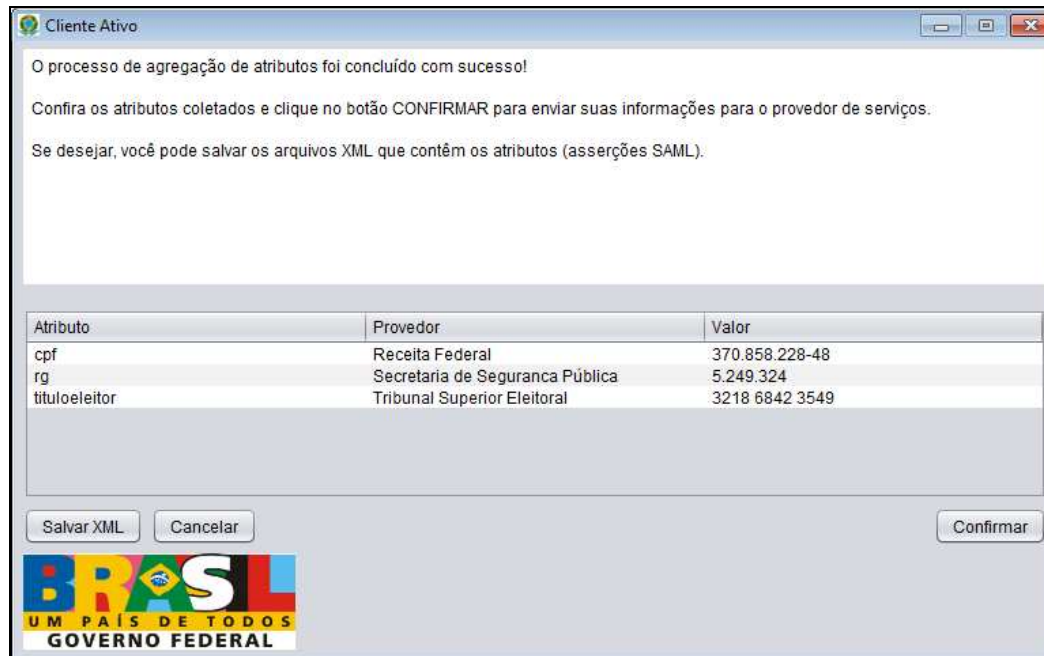
Provedor: Tribunal Superior Eleitoral

<https://ec2-54-226-196-219.compute-1.amazonaws.com/simplesaml/module.php/casp3/main.php>

Autenticar Avançar

**BRASIL**  
UM PAÍS DE TODOS  
GOVERNO FEDERAL

Figura 41. Tela de autenticação para agregação do Título de Eleitor



O processo de agregação de atributos foi concluído com sucesso!

Confira os atributos coletados e clique no botão CONFIRMAR para enviar suas informações para o provedor de serviços.

Se desejar, você pode salvar os arquivos XML que contêm os atributos (asserções SAML).

Atributo	Provedor	Valor
cpf	Receita Federal	370.858.228-48
rg	Secretaria de Segurança Pública	5.249.324
titulo eleit	Tribunal Superior Eleitoral	3218 6842 3549

Salvar XML Cancelar Confirmar

**BRASIL**  
UM PAÍS DE TODOS  
GOVERNO FEDERAL

Figura 42. Tela de resumo dos atributos agregados no Cliente Ativo





Figura 43. Tela final da Polícia Federal após receber os atributos do Cliente Ativo

#### Quadro 8. Detalhamentos do caso de teste CT 04

Tipo de teste	Funcional
Descrição (passos)	O objetivo deste caso de teste é verificar o correto salvamento das asserções SAML.
Contexto/pré-requisitos	Mesmos do CT 01, CT 02 e CT 03.
Dados do teste (entrada)	Mesmos do CT 01, CT 02 e CT 03.
Resultados Esperados	Espera-se verificar que os arquivos SAML, agregados pelo Cliente Ativo nos Provedores de Identidade, sejam salvos corretamente no computador do usuário.

**Execução do teste:** Executaram-se os casos de teste 01, 02 e 03, até o momento que o resumo da agregação de atributos (ver Figura 42) foi apresentada. Neste momento, o usuário clicou em salvar XML em um diretório da máquina do usuário o resultado da agregação de atributos.

#### Resultado do teste:

Quatro arquivos XML foram salvos no computador. Um foi o XML Response (resultado da agregação) e mais as três asserções SAML, uma para cada um dos provedores de identidade que foram utilizados no processo de agregação dos atributos.

Quadro 9. Detalhamentos do caso de teste CT 05

Tipo de teste	Segurança
Descrição (passos)	Executar todo o processo de solicitação de agregação de atributos descrito no CT 03 e monitorar com um <i>sniffer</i> de rede ( <i>wireshark</i> ) as trocas de mensagens entre o cliente ativo, os IdPs e os SPs, a fim de monitorar o vazamento de informações na rede.
Contexto/pré-requisitos	<i>Sniffer</i> de rede ( <i>wireshark</i> ) instalado e em execução na máquina do usuário, dos IdPs e dos SPs
Dados do teste (entrada)	Mesmos do CT 03.  Monitorar todas as requisições ( <i>Request</i> ) e respostas ( <i>Response</i> ) HTTP.
Resultados Esperados	Constatar no log de monitoramento da ferramenta que todas as requisições estão criptografadas.

**Execução do teste:** Após iniciar a captura de pacotes no *wireshark* tcp na porta 443 (ssl). Executaram-se todos os procedimentos descritos no Caso de Teste 03 para realizar o monitoramento com a ferramenta *wireshark*. A Figura 44 demonstra o filtro aplicado aos pacotes coletados (*tcp.port==443*), ou seja filtraram-se os pacotes enviados e recebidos na porta padrão HTTPs. Os resultados apresentados foram o log das trocas de mensagens entre o computador de teste e os servidores utilizados no protótipo do mecanismo agregador de atributos. Percebeu-se, então, que não é possível detectar quais foram as mensagens trocadas entre a aplicação e os provedores, demonstrando que todas as trocas foram criptografadas corretamente.

**Resultado do teste:** Constatou-se no log de monitoramento da ferramenta que todas as requisições estão criptografadas.

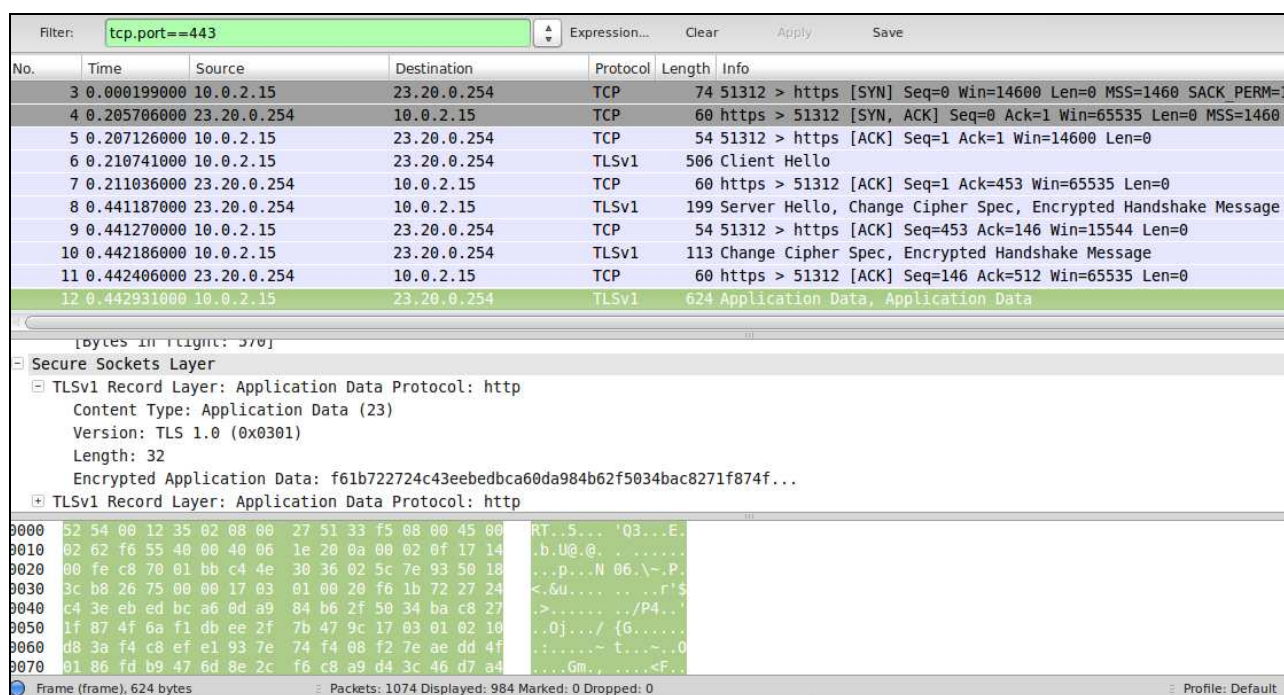


Figura 44. Log de requisições na porta 443 (ssl)

Quadro 10. Detalhamentos do caso de teste CT 06

Tipo de teste	Portabilidade
Descrição (passos)	O objetivo deste caso de teste é verificar o correto funcionamento do ambiente de testes implementado em plataformas operacionais diferentes, bem como a utilização dos principais navegadores de internet.
Contexto/pré-requisitos	Mesmos do CT 03.
Dados do teste (entrada)	Mesmos do CT 03.
Resultados Esperados	Espera-se verificar o correto funcionamento do experimento nas principais plataformas operacionais e navegadores de Internet.

**Execução do teste:** Os testes foram realizados em vários computadores e navegadores *Web*, conforme a listagem abaixo:

- Windows 7 e Internet Explorer 10;
- Windows 7 e Firefox 23;
- Windows 7 e Google Chrome 26;
- Windows 8 e Google Chrome 26;
- Windows 8 e Firefox 23;

- Windows 8 e Internet Explorer 10;
- Linux e Firefox 23;
- Linux e Google Chrome 26;
- Mac OS X e Firefox 22;
- Mac OS X e Safari 6.0.5; e
- Mac OS X e Google Chrome 30;

**Resultado do teste:**

Em todos os experimentos, a aplicação foi executada com sucesso. Em alguns casos, o cliente ativo não foi executado automaticamente e necessitou-se executá-lo, mas da mesma forma foi possível utilizar a aplicação.

**5.2.1 Análise da Execução dos Casos de Testes**

Todos os casos de testes executados obtiveram resultados positivos, logo é possível afirmar que as funcionalidades desenvolvidas estão de acordo com seus casos. Quanto aos testes de portabilidade, os resultados apontam que, quando são usados navegadores Web nas suas versões mais recentes e atualizadas e quando a versão da máquina virtual Java suportada está corretamente instalada, o mecanismo agregador executa suas funcionalidades corretamente.

**5.2.2 Resultados e Análise da Pesquisa de Satisfação**

Esta seção apresenta os resultados e análise da pesquisa de satisfação que foi elaborada para avaliação do mecanismo agregador de atributos e que foi realizada em um período de dez (10) dias.

A pesquisa 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 para o governo, somando trinta e nove (39) avaliadores.

## 5.3 AVALIAÇÃO DOS RESULTADOS

### 5.3.1 Avaliação da pesquisa de satisfação

A seguir, são apresentadas as análises feitas em cima de cada objetivo traçado no projeto do experimento:

1. Identificar o conhecimento do avaliador em relação a alguns conceitos sobre gestão de identidades (autenticação *SSO*, provedores de identidades, autenticação federada, *SAML*, *OpenID*, *OAuth*).

A respeito dos conceitos e tecnologias disponíveis no mercado que têm alguma ligação com gestão de identidades federadas, avalia-se que, exceto em relação ao *SAML*, os avaliadores têm, em sua maioria, o conhecimento sobre o assunto, já que 76.9% dos avaliadores que participaram da pesquisa têm o conhecimento sobre *SSO* (*Single Sign-on*); outros 56.4% sabem o significado de autenticação federada e 66.7% responderam ter conhecimento sobre o que é um provedor de identidades (*IdP – Identity Provider*).

A respeito do *SAML*, apenas 35.5% dos avaliadores responderam conhecer a tecnologia, o que demonstra que a maioria possui pouco conhecimento para utilização desse padrão. Apesar do pequeno grupo avaliado, esta falta de conhecimento é um ponto negativo, visto que para a ampla adoção desta especificação como uma solução de gestão de identidades federadas, o conhecimento sobre *SAML* é muito importante, pois é a tecnologia utilizada para a criação de federações. Logo, a falta desse conhecimento pode dificultar uma possível implantação de uma federação governamental como estratégia nacional de gestão de identidades.

Já em relação aos protocolos *OAuth* e *OpenID*, os avaliadores responderam ter mais conhecimento: 53.8% e 64.1%, respectivamente evidenciaram, o que se considera bom, pois essas tecnologias também podem ser utilizadas para implantação de outros sistemas que promovem o compartilhamento de identidades entre provedores e favorece a migração para outros modelos de gestão de identidade, que não os tradicionais.

2. Identificar se os avaliadores trabalharam direta ou indiretamente no desenvolvimento de *software* de governo eletrônico.

Os resultados da pesquisa demonstram que a maioria (56.4%) das pessoas que responderam ao questionário não têm relação com o desenvolvimento de *softwares* para o governo eletrônico e que apenas (26.3%) trabalham de forma direta com desenvolvimento. Acredita-se que a visão de desenvolvedores que implantam SPs, baseados no modelo tradicional, poderia ser favorável para a compreensão dos benefícios do mecanismo agregador.

3. Identificar qual sistema operacional e navegador os avaliadores usaram nos testes.

As questões sobre sistemas operacionais e navegadores Web serviram para comprovar a aplicabilidade do protótipo que faz uso do mecanismo agregador desenvolvido para diferentes ambientes operacionais e navegadores mais utilizados. Com isso, comprova-se a portabilidade do mecanismo implementado, possibilitando que o mesmo seja independente de plataforma operacional e de navegador, bastando apenas que o usuário tenha um computador com os *softwares* atualizados.

4. Identificar se os avaliadores conseguiram executar todo o experimento, conforme descrito no roteiro e quais os problema que ocorreram.

Conforme as respostas obtidas, tem-se que 82.1% dos avaliadores conseguiram executar o experimento por completo, e apenas 17.9% tiveram algum tipo de problema com o experimento.

Diante dessas respostas, observa-se que os problemas aconteceram em virtude da não utilização de navegadores e sistemas operacionais, conforme indicado nos procedimentos do experimento (utilizar os navegadores padrão configurado na máquina do usuário). Em outra resposta de um dos avaliadores que teve problemas, este indicou que estava usando um iPad. Possivelmente, outros avaliadores também devem ter utilizado um *tablet* ou *smartphone*, porém não informaram. Outro fator que pode ter contribuído para os problemas é a versão do Java instalado no computador do usuário. No roteiro, estava indicada qual a versão do Java deveria ter sido utilizada. Para impedir este tipo de problema, seria interessante implementar algumas funcionalidades no protótipo, para detectar os requisitos mínimos requeridos no computador do usuário de forma a impedir que o usuário continue a execução da aplicação.

5. Identificar se o que estava sendo executado no protótipo partiu de uma ação do avaliador e se as mensagens de erros (caso tenham ocorrido) o ajudaram a resolver o problema.

Os resultados demonstram que, conforme a maioria (89,7%) dos avaliadores, sempre foi necessário uma ação do avaliador para realizar as ações requisitadas pelo sistema. Isto é positivo uma vez que o usuário precisa ter consciência de suas ações sobre o sistema (modelo centrado no usuário). Em relação as mensagens de erro do sistema, 53,8% dos avaliadores responderam que “não se aplica”, ou seja, não obtiveram erros durante a realização do experimento e, portanto, não os reportaram. Ainda referente aos erros ocorridos no sistema, apenas 7,7% responderam que as mensagens de erro não foram suficientes para resolver o problema e 10,3% assinalaram como parcialmente. Logo, diante da ocorrência de erros, o sistema contribui para a resolução destes.

6. Identificar se os avaliadores se sentiram confortáveis (satisfação do usuário) quanto ao uso do protótipo e em quais situações eles não tiveram a sensação de conforto.

Os resultados apontam que 76,9% dos avaliadores se sentiram confortáveis durante a utilização do experimento. Isso demonstra uma boa satisfação dos usuários no uso do mecanismo agregado de atributos. Alguns 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 provedores. Em relação ao consentimento dos usuários para realizar algumas ações, isto foi definido como um requisito do sistema (modelo centrado no usuário). Em relação ao provimento da autenticação SSO, através do cliente ativo, já era previsto que os avaliadores sentiriam a falta deste modo de funcionamento do mecanismo. Pretende-se prover o suporte a este modo na próxima versão do mecanismo. Outro motivo reportado pelos avaliadores se refere ao uso de certificados auto assinados, o que no caso de um protótipo experimental acredita-se ser tolerável. Por fim, um avaliador apontou que o uso do aplicativo executado na máquina do usuário não lhe agradara e 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.

7. Verificar se os avaliadores ficaram satisfeitos em relação à apresentação das informações.

Do ponto de vista de 76,9% dos avaliadores, as informações apresentadas pelo protótipo do mecanismo agregador de atributos estão claras e compreensíveis. Pode ser que a insatisfação dos avaliadores seja em relação aos serviços (Serviço de Emissão de Passaportes, PCA e SDPCA), que

não era o foco da avaliação. De qualquer forma, pretende-se estudar como é possível melhorar este item no cliente ativo.

8. Verificar se o grau de experiência dos avaliadores em relação ao protótipo foi satisfatório.

Os resultados demonstram que 69,2% dos avaliadores indicaram que seu grau de experiência foi satisfatório e ninguém se declarou insatisfeito. Cruzando as respostas dos avaliadores parcialmente satisfeitos, observa-se que a maioria destes são os que gostariam que a autenticação SSO, através do cliente ativo, fosse suportada.

9. Verificar se os avaliadores ficaram satisfeitos em relação ao tempo de resposta.

O tempo de resposta foi positivamente avaliado durante a realização do experimento. 87.2% dos avaliadores responderam que ficaram satisfeitos com o tempo de resposta do sistema. É importante destacar que o uso do protocolo SSL compromete o tempo de resposta, porém, conclui-se que muitos avaliadores aceitam esta degradação em detrimento ao uso de um canal seguro.

10. Verificar se os avaliadores se sentiram mais seguros ao utilizar os serviços do protótipo, em relação aos serviços que estes utilizam.

Apenas 15.4% das pessoas responderam não se sentirem seguras durante a utilização do experimento. As demais pessoas, 41%, responderam que se sentiram seguras, utilizando-se do mecanismo agregador de atributos, e 43.6% das pessoas avaliaram que se sentiram parcialmente seguras na utilização do sistema. Foram seis avaliadores que não se sentiram seguros, alguns destes não conseguiram completar a execução dos experimentos, porém, os demais não apontaram seus motivos. Acredita-se que estes consideram os atuais serviços de e.gov seguros e por isso a solução proposta não pôde ser considerada mais segura.

11. Verificar se os avaliadores, em algum momento, não souberam o que fazer e se estes tiveram dificuldades para entender as funções dos serviços.

A maioria dos avaliadores, 87.2%, responderam que não para esta pergunta, ou seja, sempre souberam que ação tomar com o sistema para executar a tarefa solicitada. Apenas 10.3% dos avaliadores responderam não saber o que fazer em algum momento. Alguns dos avaliadores, (10.3%), que responderam não saber o que fazer em algum momento da utilização do protótipo, não



souberam o que fazer ou não conseguiram completar o experimento por estarem usando um dispositivo móvel, ou por não estarem com a máquina virtual Java instalada em seu equipamento, ou por utilizarem um navegador *Web* desatualizado.

12. Verificar se os avaliadores gostariam de utilizar o mecanismo agregador de atributos em aplicações de governo eletrônico.

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.

13. Verificar se os avaliadores consideram que o uso do mecanismo agregador de atributos pode agilizar o processo de obtenção e apresentação dos atributos do usuário em aplicações de e.gov.

Para a grande maioria, 97.4% das pessoas que participaram da pesquisa, a utilização de um mecanismo agregador para obter de forma segura os atributos dos usuários pode ser realizada com mais rapidez e agilidade. Observa-se nesta questão que a maioria dos avaliadores consideram o processo de agregação de atributos seguro. Uma pessoa afirmou que os serviços (aplicações *web*) possuem fragilidades, porém não as apontou.

14. Verificar se os avaliadores apontaram que o uso do mecanismo agregador de atributos pode trazer mais flexibilidade para os serviços de e.gov.

A maioria das pessoas 74.4%, que responderam ao questionário, afirmaram que a maioria dos serviços do governo seria possível apresentar mais flexibilidade com o uso do mecanismo. Alguns dos avaliadores, que não acharam que o mecanismo agregador traria mais flexibilidade, não conseguiram executar todos os passos do experimento por usarem dispositivos móveis ou por não estarem com JVM e navegador com versões atualizadas ou porque gostariam que o mecanismo suportasse autenticação SSO.

15. Verificar se os avaliadores afirmaram que o mecanismo agregador de atributos pode garantir a privacidade dos usuários.

A maioria dos avaliadores, 89.7%, responderam sim, que o mecanismo agregador de atributos pode garantir a privacidade dos usuários no processo de coleta de seus atributos em diferentes provedores de identidade. Alguns dos que não avaliaram como possível, tiveram problemas na execução de todos os passos do experimento. Uma pessoa afirmou que os serviços (aplicações *web*) possuem fragilidades, porém não as apontou.

16. Identificar quais os impactos negativos que o uso do mecanismo proposto pôde trazer para os desenvolvedores de aplicações e.gov.

Segundo os avaliadores, existem alguns impactos negativos para os desenvolvedores de aplicação de e.gov na utilização do mecanismo agregador de atributos proposto, a saber:

- “redesenvolvimento” dos mecanismos de autenticação: na realidade com a autenticação federada concentrar-se-a em poucos provedores a tarefa de autenticação (IdPs);
- a necessidade de aprender uma nova tecnologia: sim, isto será necessário para que a autenticação federada e a agregação de atributos sejam providas; e
- cultura dos desenvolvedores, em aceitar que atributos de outros IdPs possam ser utilizados: identifica-se uma falta de conhecimento dos benefícios da autenticação SSO federada.

Outro impacto negativo está no vazamento de informações pessoais, em ataques e problemas de segurança por considerar que a solução não garante a segurança dos dados. Porém, foram poucos avaliadores que apontaram este impacto como negativo.

Outros pesquisadores apontaram que o problema pode estar nos próprios usuários do mecanismo por oferecerem resistência ao uso de um mecanismo como o proposto nesse trabalho.

Outro pesquisador respondeu que poderia ser mais complexo para o usuário utilizar o mecanismo agregador de atributos ou poderia dar a impressão de que os serviços não estão interligados.

17. Se os avaliadores recomendariam o mecanismo agregador de atributos para ser usado em serviços de e.gov.

No que tange a questões de recomendação do mecanismo, foi possível verificar com os experimentos que o objetivo foi alcançado, pois 97,4% das pessoas que responderam aos questionários afirmaram que gostariam de utilizar um mecanismo como o proposto por esse trabalho nas aplicações governamentais.

#### 18. Identificar o que os avaliadores avaliaram como melhor no experimento executado.

Os avaliadores utilizaram vários termos para avaliar positivamente a aplicação. A maioria dos avaliadores destacaram a agilidade e simplicidade no uso do mecanismo agregador de atributos. Isso mostra que a utilização de um aplicativo mediado pelo cliente pode perfeitamente ser utilizado em um ambiente de e.gov, sem comprometer demasiadamente a usabilidade das aplicações de governo.

Outros dois pontos positivos que receberam destaque nas avaliações dos usuários foram o compartilhamento de informações e a segurança. Como, por exemplo, a vantagem de poderem compartilhar identidades de múltiplos provedores de identidade apontado por um dos avaliadores. Apesar de o mecanismo ter sido desenvolvido, utilizando-se certificados auto assinados, este cumpriu seu papel em demonstrar para os usuários que a aplicação tem por objetivo prover canais seguros entre o cliente ativo, IdPs e SPs.

#### 19. Identificar o que poderia ser melhorado no mecanismo agregador de atributos.

Quanto a esta questão aberta, as opiniões apresentadas na íntegra no Apêndice F foram agrupadas nas seguintes sugestões:

- prover autenticação SSO através do cliente ativo;
- implementar a funcionalidade de política de liberação de atributos;
- fazer uso de certificados SSL emitidos por autoridades certificadoras confiáveis;
- trazer ajustes na interface do cliente ativo para facilitar o seu uso e para apresentar melhor algumas informações;
- prover a criação de uma API e documentação para integração e uso do mecanismo agregador de atributos em aplicações de e-Gov; e

- explicitar para os usuários quando os mecanismos de segurança estão sendo utilizados na solução.

### 5.3.2 Comparação com os trabalhos relacionados

Conforme descrito no Capítulo 2, existem seis abordagens para implantação de agregação de atributos em sistemas de gerenciamento de identidades. Dentre os trabalhos mais recentes, analisados no Capítulo 3, a maioria segue abordagem de *proxy* que faz uso de uma terceira parte confiável para agregar os atributos. A abordagem baseada em *proxy* possui vantagens tais como a facilidade de implementação e, em especial, o suporte a autenticação SSO (*Single Sing-On*). Porém, a privacidade pode não ser garantida nesta abordagem diante da facilidade desta terceira parte em poder rastrear as interações entre o usuário e os provedores de identidade e de serviço, já que esta mantém o controle das informações do usuário (CHADWICK; INMAN, 2009).

Os trabalhos de Hoellrigl *et al.* (2010) e Vossaert *et al.* (2010) seguem a abordagem mediada pelo cliente. Apesar de pouco adotada, a abordagem mediada pelo cliente é a mais adequada quando se pretende priorizar a privacidade dos dados (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.

No trabalho de Hoellrigl *et al.* (2010), que faz uso de uma abordagem mediada pelo cliente, o ambiente operacional que executa o cliente ativo é restrito a uma solução proprietária da *Microsoft*. O mecanismo proposto neste trabalho provê portabilidade, garantindo assim que o cliente ativo possa ser executado em diferentes plataformas operacionais.

No estudo apresentado por Vossaert *et al.* (2010), os autores apresentam um mecanismo agregador de atributos no formato de um módulo de confiança (*trusted module*) que fica de posse dos usuários, no formato de um cartão inteligente (*smart card*). O mecanismo agregador de atributos proposto neste trabalho pode também ser implementado em um módulo de confiança (*smart card*) com o intuito de oferecer um mecanismo de autenticação mais forte baseado em certificados digitais, por exemplo. Pode-se inclusive utilizar os cartões inteligentes que já estão disponíveis em algumas áreas do governo federal ou que estão sendo gerados no novo Registro de Identidade Civil (RIC).

Vossaert *et al.* (2010) apontam ainda que os atributos dos usuários podem ser salvos localmente no cartão inteligente, e isso também pode ser realizado no mecanismo agregador de atributos, podendo assim disponibilizar serviços para os usuários sem que estes precisem se autenticar novamente em provedores de identidades, como descrito pelos autores.

## 6 CONCLUSÕES

Um sistema de gerenciamento de identidades federadas pode fornecer a base para a gestão dos atributos dos usuários em aplicações de Governo Eletrônico. Os sistemas que seguem o modelo de identidades federadas são sólidos e garantem o acesso federado de seus usuários, porém, muitas vezes, questões referentes à privacidade dos usuários não são devidamente consideradas.

Na tentativa de evitar o comprometimento das informações do usuário, alguns trabalhos descritos na literatura buscam resolver o problema referente à privacidade dos usuários. Estes trabalhos descrevem soluções de IdM federados centrados no usuário, que visam atribuir o controle das informações aos próprios usuários. Uma característica importante sobre os sistemas de gerenciamento de identidades centrados nos usuários é a capacidade do usuário de poder escolher o provedor de identidades que deseja utilizar. O usuário pode optar por utilizar um determinado provedor e, a qualquer momento, trocá-lo, sem a preocupação de perder acesso aos serviços que costuma utilizar, com a possibilidade, ainda, de utilizar múltiplos provedores de identidade.

Uma limitação de alguns sistemas de gerenciamento de identidades federadas atuais empregados em estratégias nacionais de gestão de identidades está em limitar que os usuários possam selecionar apenas um de seus IdPs em qualquer sessão criada com um provedor de serviços (SP). A agregação de atributos é um mecanismo que pode ser utilizado em conjunto com os sistemas de gerenciamento de identidades federadas centrados no usuário para promover o compartilhamento dos atributos dos usuários coletados de múltiplos provedores de identidades.

O objetivo deste trabalho foi prover a agregação de atributos dos usuários, que estão distribuídos em múltiplos provedores de identidades, garantindo a privacidade dos usuários, 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. Os métodos de pesquisa utilizados foram distribuídos em quatro fases.

Na primeira fase, foi executado um procedimento técnico de pesquisa bibliográfica de modo a realizar a fundamentação teórica, que abordou a área de governo eletrônico, sistemas de gerenciamento de identidade, a especificação SAML, agregação de atributos e as abordagens para implementação da agregação de atributos. Ainda nessa fase, foi executado um protocolo de busca,

visando identificar os trabalhos relacionados ao tema desta dissertação. Os trabalhos relacionados foram analisados de forma a identificar suas características e limitações.

Na segunda fase, definiu-se o mecanismo agregador de atributos mediado no cliente, bem como seus modos de funcionamento. Na terceira fase, foi realizada a implementação do mecanismo agregador de atributos (prova de conceito) e de um protótipo de um cenário de uso que faz uso mecanismo agregador de atributos. Por fim, na quarta fase, foi realizada a avaliação do mecanismo agregador de atributos, a partir do protótipo implementado, de modo a comprovar as hipóteses de pesquisa em relação à privacidade, flexibilidade e usabilidade da solução proposta através de testes de software, de uma pesquisa de satisfação de usuários e da comparação com trabalhos relacionados.

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

O sistema agregador de atributos definido nesta dissertação inova em relação aos trabalhos relacionados, ao prover uma solução que evita a rastreabilidade dos atributos do usuário, através de uma abordagem mediada pelo cliente e alinhada à arquitetura E-PING, com o objetivo de trazer mais flexibilidade para uma estratégia nacional de gestão de identidades federadas e centrada no usuário. Todas as escolhas tecnológicas visam garantir a interoperabilidade e a portabilidade da solução proposta.

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

Na avaliação do mecanismo agregador de atributos, procurou-se analisar o atendimento aos requisitos funcionais e não funcionais do mecanismo agregador de atributos e as hipóteses de

pesquisa. A avaliação foi dividida em três etapas. A primeira refere-se aos testes de *software* executados pelos desenvolvedores do protótipo; a segunda refere-se a um experimento que envolveu o uso do protótipo implementado por especialistas que trabalham ou prestam serviços para o Governo e a aplicação de um questionário com uma pesquisa de satisfação de usuários (teste de usabilidade), e a terceira etapa foi a comparação do mecanismo proposto com os trabalhos relacionados. Com a pesquisa de satisfação dos usuários, foi possível avaliar os impactos decorrentes do uso do mecanismo agregador, bem como comprovar o seu funcionamento em diferentes ambientes operacionais e navegadores *Web*.

Por fim, com os resultados obtidos foi possível comprovar as hipóteses de pesquisa, afirmando, então, que foi possível desenvolver um mecanismo agregador de atributos mediado pelo cliente que traz mais flexibilidade para uma estratégia nacional de gestão de identidades federadas, sem prejudicar sua interoperabilidade. Comprovou-se também que o mecanismo agregador garante a privacidade dos usuários, porém com alguns prejuízos em relação à usabilidade das aplicações de governo eletrônico.

## 6.1 CONTRIBUIÇÃO DA DISSERTAÇÃO

A principal contribuição dessa dissertação está no desenvolvimento de um mecanismo agregador de atributos alinhado ao programa de Governo Eletrônico Brasil que: (i) é executado como um cliente ativo na máquina do usuário de forma a evitar a rastreabilidade dos usuários por parte de SPs e IdPs; (ii) exige o consentimento dos usuários para o compartilhamento de seus atributos; (iii) interage com os IdPs e SPs por canais seguros; e (iv) adota padrões e tecnologias que contribuem para a garantia da interoperabilidade e portabilidade.

## 6.2 TRABALHOS FUTUROS

Como trabalhos futuros, propõem-se:

- concluir a implementação do modo permanente estático (autenticação SSO através do cliente ativo) e implementar o permanente dinâmico (definição de uma política de liberação de atributos), de forma a promover melhor integração com a federação de identidades;



- avaliar o perfil ECP (*Enhanced Client or Proxy Profile* V2.0) do SAML para ser aplicado no desenvolvimento do Cliente Ativo;
- integrar o Cliente Ativo em um cartão inteligente para avaliar a viabilidade do mesmo ser integrado ao Novo Registro de Identidade Civil (RIC); e
- adaptar o mecanismo agregador de atributos para que o mesmo possa ser integrado ao *Shibboleth* para aprimorar as funcionalidades das federações acadêmicas.

## REFERÊNCIAS

AARTS, R. MADSEN, P. 2006. **Liberty ID-WSF interaction service specification v.2. Liberty Alliance Project**. Disponível em: <<http://www.projectliberty.org>>. Acesso em: 11 outubro 2012.

BALDONI, Roberto. Federated Identity Management System in e-Government: the Case of Italy. **Electronic Government, an International Journal**. Roma, v. 9, n. 1, p. 64-84, 01/2012

BARBOSA, Alexandre Fernandes. **Governo Eletrônico: Dimensões da Avaliação de Desempenho na Perspectiva do Cidadão**. 2008. 248. Tese. Tese (doutorado) - Escola de Administração de Empresas de São Paulo. Fundação Getúlio Vargas VARGAS, São Paulo, 2008.

BARROS, Aidil Jesus Paes; LEHFELD, Neide Aparecida de Souza. **Fundamentos de metodologia científica: um guia para iniciação científica**. São Paulo: Makron Books, 2000.

BARTON, Tom; BASNEY, Jim; FREEMAN, Tim; SCAVO, Tom; SIEBENLIST, Frank; WELCH, Von; ANANTHAKRISHNAN, Rachana; BAKER, Bill; GOODE, Monte; KAEHEY, Kate Keahey. Identity Federation and Attribute-based Authorization through the Globus Toolkit, Shibboleth, GridShib, and MyProxy. In: ANNUAL PKI R&D WORKSHOP, 5., 2005, Gaithersburg. **Proceedings...** Gaithersburg: NIST Technical Publication, 2006. p. 54-68.

BHARGAV-SPANTZEL, Abhilasha; CAMENISH, Jan; GROSS, Thomas; SOMMER, Dieter. User centricity: a taxonomy and open issues. **Journal of Computer Security**, v. 15, n. 5, p. 493-527, Jan. 2007.

BLOGOSLAWSKI, Ilson Paulo Ramos; FACHINI, Olímpio; FAVERI, Helena Justen de. **Educar para a pesquisa: normas para produção de textos científicos**. 3. ed. Rio do Sul: NOVA LETRA, 2008.

BRASIL, Comitê Executivo de Governo Eletrônico. **e-PING – Padrões de Interoperabilidade de Governo Eletrônico**. Disponível em: <<http://www.governoeletronico.gov.br/acoes-e-projetos/e-ping-padroes-de-interoperabilidade>>. Acesso em: 10 Set. 2011.

BRASIL, Polícia Federal. **Documentação para Passaporte Comum**. 2013 Disponível em: <<http://www.dpf.gov.br/servicos/passaporte/documentacao-necessaria/documentacao-para-passaporte-comum/documentacao-para-passaporte-comum>> Acesso em: 15 março 2013.

BURR, William E.; DODSON, Donna F.; POLK, W. Timothy. Electronic authentication guideline. **NIST Special Publication 800-63**, p. 63. 2004.

CAMENISCH, J; PFITZMANN, B. Security. Federated Identity Management. In: PETKOVIC, Milan; JONKER, Willem. **Security, Privacy, and Trust in Modern Data Management**. Berlin: Springer Berlin Heidelberg, 2007. p. 213-238.

BRASIL, Caixa Econômica Federal. **Conheça a lista de documentos necessária para seu financiamento**. 2013 Disponível em: <<http://www1.caixa.gov.br/habitacao/documentoshabitacaocaixa/>> Acesso em: 20 março 2013.

CGI.br (Comitê Gestor de Internet no Brasil). **Pesquisa sobre o Uso das Tecnologias da Informação e da Comunicação no Brasil: TIC Governo Eletrônico**. 2010. São Paulo, 2010. 50p.

CHADWICK, David. Federated identity management. in: ALDINI, Alessandro; BARTHE, Gilles; GORRIERI, Roberto. **Foundations of Security Analysis and Design V**. Berlin: Springer Berlin Heidelberg, 2009, p. 96-120.

CHADWICK, David W. Authorisation using attributes from multiple authorities. *In: IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)*. 20., 2006, Manchester. **Proceedings...** [S.l.: s.n.], 2006. p. 326-331.

CHADWICK, David. Inman. G. SIU, K. W. S. FERDOUS, M. S. Leveraging Social Networks to Gain Access to Organisational Resources. **DIM '11 Proceedings of the 7th ACM workshop on Digital identity management**. Chicago, p. 43-52. Outubro de 2011.

CHADWICK, David; INNMAN, George. KLINGENSTEIN, Nate. A Conceptual model for Attribute Aggregation. **Future Generation Computer Systems**. v. 26, n 7, p. 1043 -1052, Junho de 2010.

CHADWICK, David; INMAN, George. A Privacy Preserving Attribute Aggregation Model for Federated Identity Managements Systems. **European Journal for the Informatics professional**, v. 6, n. 1, p. 21-26, Fevereiro de 2010.

CHADWICK, David; INMAN, George. Attribute aggregation in federated identity Management. **IEEE Computer Society**, v. 42, n. 5, p 44-53. Junho de 2009.

DAWES, S. S.; PARDO, T. A. Building Collaborative Digital Government Systems Systemic: constraints and effective practices. In: McIVER JR., W.; ELMAGARMID, A. (eds.). **Advances in Digital Government Technology, Human Factors, and Policy**. Boston: Kluwer Academic, 2002. p. 259–273.

DE MELLO, Emerson Ribeiro. **Um modelo para confiança dinâmica em ambientes orientados a serviço**. 2009. 126, Tese. Programa de Pós-Graduação em Engenharia Elétrica, Universidade Federal de Santa Catarina, Florianópolis, 2009.

DE MELLO, Emerson Ribeiro; WANGHAM, Michelle Silva; FRAGA, Joni da Silva; CAMARGO, Edson T. de; BÖGER, da Silva. A model for authentication credentials translation in service oriented architecture. In: GAVRILOVA, Marina L.; TAN, C. J. Kenneth; MORENO, Edward David. **Transactions on Computational Sciences IV: special issue on security in computing**. Berlin: Springer Berlin Heidelberg, 2009. p. 68-86.

DENCKER, A. **Métodos e técnicas de pesquisa**. 2. ed. São Paulo: Futura, 1998.

GEMMILL, Jill; ROBINSON, John-Paul; SCAVO, Tom; BANGALORE, Purushotham. Cross-domain authorization for federated virtual organizations using the myVocs collaboration environment. **Concurrency and computation: practice & experience**, Chichester, v. 21, n. 4, p. 509-532, March. 2009.

GIL, Antonio Carlos. **Métodos e técnicas de pesquisa social**. 6. ed. São Paulo: Atlas, 2008.

GROEPER, Ralf; GRIMM, Christian; MAKEDANZ, Siegfried; PFEIFFENBERGER, Hans; ZIEGLER, Wolfgang; GIETZ, Peter; SCHIERS, Michael. A concept for attribute-based authorization on D-Grid resources. **Future Generation Computer Systems**. Alemanha: Elsevier, v.25, n.3, p.275-280, mar. 2009.

HATAKEYMA, Makoto. SHIMA, Shigeyoshi. Privilege Federation between Different User Profiles for Service Federation. In: **ACM Conference on Computer and Communications Security**, 15, New York, 2008. Proceedings... New York: ACM Press, 2008. p. 41-50.

HOELLRIGL, Thorsten. KÜHNER, Holger. DINGER, Jochen. HARTENSTEIN, Hannes. User-Controlled Automated Identity Delegation. In: **Network and Service Management**, 1, Niagara Falls, 2010. Proceedings... Niagara Falls: IEEE Computer Society, 2010. p. 230 - 233.

HULSEBOSCH, Bob; WEGDAM, Maarten; ZOETEKOUW, Bas; DIJK, Niels Van; POORTINGA, Remco. **Virtual collaboration attribute management**. 2011. Disponível em: <<http://www.surfnet.nl/nl/Innovatieprogramma's/gigaport3/Documents/EDS%2011-06%20Attribute%20Management%20v1.0.pdf>> Acesso em: 21 setembro de 2011.

IBGE. **Censo Demográfico 2010**. 2011. Disponível em: <<http://www.ibge.gov.br/home/estatistica/populacao/censo201/default.shtm>>. Acessado em 05 de agosto de 2011.

JOSANG, A. POPE, S. User centric identity management. In: AusCERT Asia Pacific Information Technology Security Conference, 4, Gold Coast, 2005. **Proceedings...** Queensland: University of Queensland, 2005. p. 1 - 13.

KLINGENSTEIN, Nate. Attribute Aggregation and Federated Identity. In: International Symposium on Applications and the Internet Workshops (SAINTW'07), 1, 2007, Hiroshima. Proceedings... Hiroshima: IEEE Computer Society, 2007. p. 26.

LAKATOS, Eva Maria; MARCONI, Maria de Andrade. **Metodologia Científica**. 2. ed. São Paulo: Atlas, 1999.

LANDAU, Susan. GONG, Hubert Le Van. WILTON, Robin. Achieving Privacy in a Federated Identity Management System. In: International Conference, FC 2009, 13, Accra Beach, 2009. **Proceedings...** Berlin: Springer Berlin Heidelberg, 2009. p. 51-70.

LEE, JaeWon; KIM, Heeyoul; HONG, Joon Sung; SAMSUNG Co Ltd. KIM, Heeyoul; HONG, Joon Sung. An Attribute Aggregation Architecture with Trust-Based Evaluation for Access Control. In: **Network Operations and Management Symposium**. 2008, Salvador. Proceedings... Salvador: IEEE, 2008, p. 1011 - 1014.

LEWIS, James Andrew. **Authentication 2.0: New Opportunities for Online Identification**. 2008 Disponível em: <<http://csis.org/publication/authentication-20>>. Acesso em 12 abril de 2012.

LIPS, Marian. PANG, Chiky. **Identity management in information age government: exploring concepts, definitions, approaches and solutions**. 2008. Disponível em: <<http://www.egov.vic.gov.au/focus-on-countries/pacific-region/new-zealand/trends-and-issues-new-zealand/identity-management-new-zealand/identity-management-in-information-age>>

government-exploring-concets-definitions-approaches-and-solutions-in-pdf-format-558kb.html>. Acesso em: 15 de junho de 2012.

MALIKI, T. E.; Seigneur, J.M. A survey of user-centric identity management technologies. In The International Conference on Emerging Security Information, Systems, and Technologies, 2007. 1, Valencia, 2007. **Proceedings...** Valencia: SecureWare, 2007. p. 12–17.

OASIS. **SAML V2.0 Executive Overview**. 2005a. Disponível em: < <https://www.oasis-open.org/committees/download.php/13525/sstc-saml-exec-overview-2.0-cd-01-2col.pdf> >. Acesso em: 05 julho de 2012.

OASIS. **Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0**. 2005b. Disponível em: < <http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf> >. Acesso em: 23 de março. de 2013.

OASIS. **SAML V2.0 Technical Overview**. 2008. Disponível em: < <http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.pdf> >. Acesso em maio de 2013.

OBAMA, B. **Memorandum for the heads of executive departments and agencies. The Administration of WHITE HOUSE**, 2011. Disponível em: <[http://www.whitehouse.gov/the\\_press\\_office/Transparency\\_and\\_Open\\_Government](http://www.whitehouse.gov/the_press_office/Transparency_and_Open_Government)>. Acesso em: 26 de agosto de 2011.

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

GEMMILL, Jill; LYNN, Jason; ROBINSON, John-Paul. **MyVOCS - My Virtual Organization Collaboration Suite**. 2005. Disponível em: <<http://events.internet2.edu/2005/spring-mm/sessionDetails.cfm?session=1948&event=229>>. Acesso em: 24 de novembro de 2011.

GOV.BR. **Programa de Governo Eletrônico brasileiro**. 2013. Disponível em: <<http://www.governoeletronico.gov.br>>. Acessado em: 13 Jun. de 2013.

SILVA, E; MENEZES, E. **Metodologia da Pesquisa e Elaboração de Dissertação**. 2001. Disponível em: <<http://projetos.inf.ufsc.br/arquivos/Metodologia%20da%20Pesquisa%203a%20edicao.pdf>>. Acesso em: 19 Junho 2011.

STEVENS, Toby; ELLIOTT, John; HOIKKANEN, Anssi; MAGHIROS, Ioannis; LUSOLI, Wainer. **The State of the Electronic Identity Market: Technologies, Infrastructure, Services and Policies**. JRC Scientific and Technical Reports, p. 1.84, Outubro de 2010.

SIMPLESAMLPHP. **SimpleSAMLphp Documentation**. 2013. Disponível em: <<http://simplesamlphp.org/docs/stable/>>. Acesso em: 12 maio de 2013.

THIBEAU, Don; DRUMMOND, R. **Open trust frameworks for open government: Enabling citizen involvement through open identity technologies**. 2009. Disponível em: <[http://openid.net/docs/Open\\_Trust\\_Frameworks\\_for\\_Govts.pdf](http://openid.net/docs/Open_Trust_Frameworks_for_Govts.pdf)>. Acesso em 23 de setembro 2011.

UNDP. **United Nations E-Government Survey 2010: Leveraging E-Government at a Time of Financial and Economic Crisis**. Nova York: Un Publishing Section, 2010.

VOSSAERT, Jan. LAPON, Jorn. DECKER, Bart De. NAESSENS, Vincent. User-Centric Identity Management Using Trusted Modules. In: European Workshop, 7, Atenas, 2010. **Proceedings...** Berlin: Springer Berlin Heidelberg, 2010. p. 155-170.

WANGHAM, Michelle S. MELLO, Emerson Ribeiro de. BÖGER, Davi da Silva. GUERIOS, Marlon. FRAGA, Joni da Silva. Gerenciamento de Identidades Federadas. In: **X Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais**, 10, 2010, Fortaleza. Anais do X Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais. Porto Alegre: Sociedade Brasileira e Computação, 2010. p. 447-460.

WATT, John. SINNOTT, Richard O. Supporting Federated Multi-Authority Security Models. In: ACM International Symposium on Cluster, 11, Newport Beach, 2011. **Proceedings...** New York: ACM Press, 2011. p. 620-621.

White House. **Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure**. 2012 Disponível em:  
<[http://www.whitehouse.gov/assets/documents/Cyberspace\\_Policy\\_Review\\_final.pdf](http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf)> Acesso em 12 de maio de 2012.

## **APÊNDICE A – REVISÃO SISTEMÁTICA**

Uma revisão sistemática de literatura é um meio para identificar, interpretar e avaliar todos os resultados relevantes de uma pesquisa acerca de uma questão, área ou fenômeno em particular. Utilizando uma metodologia rigorosa e que possa ser reproduzida posteriormente. A revisão sistemática tem por objetivo apresentar uma avaliação concisa a respeito de um tópico (KITCHENHAN, 2009).

A primeira atividade desta revisão sistemática foi de definir um protocolo, a fim de encontrar na literatura, trabalhos relevantes acerca do tema sobre agregação de atributos. O escopo da pesquisa foi voltado para a identificação de técnicas utilizadas para agregação de atributos, com a tentativa de identificar se as implementações que focam em sistemas de identidades federadas, e quais abordagens são comumente estudadas e utilizadas, bem como da existência de implementações de mecanismos de agregação de atributos disponíveis ou em desenvolvimento.

### **OBJETIVO**

Executar uma revisão sistemática cujo objetivo é identificar, analisar e avaliar as técnicas e soluções de agregação disponíveis e utilizadas no gerenciamento de identidades e possivelmente sendo aplicadas em ferramentas de e-Gov de outros países.

Fez-se necessário uma revisão sistemática da literatura para que se ter conhecimento dos trabalhos que estavam sendo realizados na área de agregação de atributos e agregação de atributos para identidades federadas.

### **PERGUNTA**

Quais são as principais soluções de agregação de atributos?

Nas soluções de agregação de atributos, qual o modelo de gestão de identidades (tradicional, centralizado, federado, centrado no usuário)?

Quais modelos de agregação de atributos são utilizados em soluções privadas e governamentais de que possam ser utilizadas como base de estudos para a agregação de atributos

nas implementações de gerenciamento de identidades governamentais que seja flexível e heterogêneo;

Para os modelos de agregação de atributos disponíveis qual ou quais os modelos de gestão de identidade foram utilizados.

## **ESTRATÉGIA UTILIZADA PARA PESQUISA DOS ESTUDOS PRIMÁRIOS**

O método de escopo de busca nas fontes de pesquisa deu-se em bases de dados eletrônicas on-line, incluindo *journals* e anais de conferências.

O escopo da pesquisa deu-se em bases de dados eletrônicas, incluindo *journal* e anais de conferências.

### **TERMOS DE BUSCA:**

- Em Inglês: “Attribute Aggregation” AND (“Electronic Identity” OR “Centric User Attribute Aggregation”)
- Em Português: “Agregação de Atributos” AND (“Identidade Eletrônica” OR “Agregação de Atributos Centrada no Usuário”)

### **FONTES:**

- Google acadêmico: <http://scholar.google.com.br>
- IEEEExplore: <http://ieeexplore.ieee.org>
- CAPES: <http://www.periodicos.capes.gov.br>
- ACM Digital Library: <http://portal.acm.org>

## **CRITÉRIOS E PROCEDIMENTOS PARA A SELEÇÃO DE ESTUDOS**

Os trabalhos foram filtrados a partir dos seguintes critérios:

- pela análise do título do trabalho;
- Pela análise do resumo e das conclusões do trabalho;
  - pela data de publicação do trabalho;



- critérios para inclusão de estudo:
  - para a questão primária: foram incluídos no estudo trabalhos cujos títulos e resumos contenham informações referentes à agregação de atributos. A conclusão foi analisada para verificar a contribuição do trabalho. A data de publicação do trabalho deveria ser superior ou igual ao ano 2002.
  - para a questão secundária: os mesmos critérios da questão primária, porém título e resumo deveriam conter também a informação sobre ataques, vulnerabilidades ou técnicas de segurança.
- critérios para exclusão de estudo:
  - para a questão primária: foram excluídos do estudo trabalhos cujos títulos e resumos sejam conflitantes, ou seja, o título remete a um assunto enquanto o resumo remete a outro assunto. Os trabalhos publicados antes do ano 2002 não foram analisados.
  - para a questão secundária: os mesmos critérios da questão primária além de que o título e resumo informados não falam de agregação de atributos.
- processo de seleção preliminar: as estratégias de pesquisa foram aplicadas para identificar os estudos primários potenciais. Os trabalhos selecionados que não atenderam aos critérios de inclusão e também não atenderam aos critérios de exclusão, o mesmo será incluído.
- processo de seleção final: cópias dos trabalhos que foram incluídos como resultados da pesquisa inicial foram revisados. Esta revisão concluiu a seleção de trabalhos que foram inclusos no processo de extração de dados.

## **LISTA DE VERIFICAÇÃO E PROCEDIMENTOS PARA AVALIAÇÃO DA QUALIDADE DOS ESTUDOS**

Os estudos foram avaliados em sua qualidade abordando os seguintes aspectos:

- objetivos: os objetivos do trabalho deveriam ser no sentido de estabelecer ou aplicar uma técnica de agregação de atributos. Os mesmos deveriam estar bem definidos e delimitados, sem a pretensão de resolver problemas de grande abrangência.

- condução: o projeto deveria estar bem referenciado e possuir, preferencialmente uma etapa experimental, com a validação das hipóteses. Eventos negativos ocorridos durante o estudo, como por exemplo, dificuldades quanto à população e os equipamentos, tornando o trabalho elegível a ter uma atribuição de menor qualidade.
- experimentos: a população deveria ser escolhida de forma aleatória evitando vieses na amostra e com o tamanho considerável (acima de 30) de indivíduos.

### **OS RESULTADOS FORAM TABULADOS DA SEGUINTE FORMA**

- N° de artigos por ano e por fonte;
- N° de artigos candidatos (selecionados) por ano e por fonte;
- N° de artigos selecionados por ano e por fonte;

### **ESTRATÉGIA DE EXTRAÇÃO DE INFORMAÇÃO**

Para cada estudo selecionado, mediante a execução do processo de avaliação da qualidade dos estudos primários, foram extraídos os seguintes dados de cada artigo:

- local de execução do estudo;
- ano de publicação;
- classificação do artigo;
- resumo do artigo;
- resultados do estudo;
- lições aprendidas; e
- perspectivas futuras.

### **SÍNTESE DOS DADOS EXTRAÍDOS**

Os resultados foram organizados em tabelas. A partir da tabulação dos dados, foram extraídos os dados de maior incidência, identificando qual é o item mais comentado pelos trabalhos relacionados.

## APÊNDICE B – CONFIGURAÇÃO DO FRAMEWORK SIMPLESAMLPHP

A seguir serão descritos os principais detalhes referentes ao desenvolvimento dos Módulos do SimpleSAMLPHP. Todas as informações para estudo foram obtidas na documentação oficial do *framework* na internet SIMPLESAMLPHP (2013).

A primeira configuração importante que foi realizada para facilitar o desenvolvimento está na criação de variáveis globais que contém os endereços dos sete servidores que fazem parte do experimento implementado.

Conforme pode ser observado na Figura que segue definiu-se sete variáveis globais no framework SimpleSAML. Essas variáveis são utilizadas no desenvolvimento dos módulos específicos do protótipo e facilitam a manutenção do mesmo. As três primeiras linhas (20, 21 e 22) contém os endereços dos provedores de serviço da Polícia Federal, do Serviço de Descoberta de Provedor de Cliente Ativo e do Cliente Ativo respectivamente. A linha vinte e quatro (24) contém a configuração do endereço do IdP de autenticação para o SP da Polícia Federal. Este IdP contém a configuração dos três provedores de serviço apresentados inicialmente, logo para essas aplicações o SSO é garantido e foi implementado.

As três últimas linhas (26, 27 e 28) contém a configuração do IdPs utilizados para a agregação de atributos, e são respectivamente os provedores dos atributos CPF, RG e Título de Eleitor.

20	<code>\$pfhost</code>	<code>= 'ec2-23-20-0-254.compute-1.amazonaws.com';</code>
21	<code>\$sdpcahost</code>	<code>= 'ec2-54-226-102-13.compute-1.amazonaws.com';</code>
22	<code>\$pcahost</code>	<code>= 'ec2-54-226-126-153.compute-1.amazonaws.com';</code>
23		
24	<code>\$idphost</code>	<code>= 'ec2-54-242-236-246.compute-1.amazonaws.com';</code>
25		
26	<code>\$caidp1</code>	<code>= 'ec2-54-226-68-80.compute-1.amazonaws.com';</code>
27	<code>\$caidp2</code>	<code>= 'ec2-54-226-232-34.compute-1.amazonaws.com';</code>
28	<code>\$caidp3</code>	<code>= 'ec2-54-226-196-219.compute-1.amazonaws.com';</code>

Após a configuração das variáveis globais que são utilizadas em todos os módulos que foram desenvolvidos para o protótipo necessita configurar os metadados para o correto funcionamento do SSO. A primeira configura é no arquivo *metadata/saml20-sp-remote.php*.

A figura que segue demonstra a configuração dos metadados para o SP da Polícia Federal. Esta mesma configuração deve ser realizada nos demais módulos, como os que foram implementados (SDPCA e PCA). Conforme se observa nas linhas dez (10) e onze (11) da figura as duas configurações mais importantes são: O endereço a URL do IdP responsável pelo controle e autenticação SSO e a URL do servidor IdP responsável pelo *logout* da sessão do usuário respectivamente. Ou seja, a primeira URL será utilizada para que o sistema saiba redirecionar o navegador *Web* do usuário para o formulário de autenticação no provedor de identidade. A segunda URL é responsável por destruir todas as sessões criadas para um determinado usuário, ou seja, se em qualquer aplicação dos provedores de serviço, o usuário efetuar o *logout* as demais aplicações também serão desconectadas necessitando novo *login* do usuário.

```

3  require_once SimpleSAML_Module::getModuleDir('mvc').'/lib/functions.php';
4
5  $conf = SimpleSAML_Configuration::getInstance();
6
7  $metadata[prepend_protocol($conf->getValue('idphost').'/simplesaml/saml2/idp/metadata.php')] =
8  array(
9      'name' => 'Padrão',
10     'certFingerprint' => 'afe71c28ef740bc87425be13a2263d37971dalf9',
11     'SingleSignOnService' => prepend_protocol($conf->getValue('idphost').'/simplesaml/
saml2/idp/SSOService.php'),
12     'SingleLogoutService' => prepend_protocol($conf->getValue('idphost').'/simplesaml/
saml2/idp/SingleLogoutService.php')
13 );

```

A configuração demonstrada na Figura abaixo representa a configuração que foi realizada no provedor de identidade. Ou seja, para que o mecanismo de autenticação SSO funcione corretamente o IdP deve conhecer as configuração de URL para consumo das asserções bem como a URL para realização do logout do sistema, respectivamente representadas na linha 8 e 9 da figura.

```

3  require_once SimpleSAML_Module::getModuleDir('mvc').'/lib/functions.php';
4
5  $conf = SimpleSAML_Configuration::getInstance();
6
7  $metadata[prepend_protocol($conf->getValue('pghost').'/simplesaml/module.php/saml/sp/
metadata.php/default-sp')] = array(
8      'AssertionConsumerService' => prepend_protocol($conf->getValue('pghost').'/
simplesaml/module.php/saml/sp/saml2-acs.php/default-sp'),
9      'SingleLogoutService' => prepend_protocol($conf->getValue('pghost').'/simplesaml/
module.php/saml/sp/saml2-logout.php/default-sp'),
10 );

```

Ainda nas configurações do IdP *simpleSAML* foi necessário configurar os metadados referente ao mecanismo de autenticação. No caso do protótipo aqui apresentado, as autenticações foram realizadas de maneira estática. Mas o framework possibilita que sejam utilizados diversos tipos de conexões, como por exemplo: Diretórios LDAP, Banco de Dados, arquivos de

configuração, etc. Na linha seis (6) tem-se a representação do mecanismo de autenticação que foi utilizado e que pode ser observado em detalhes na segunda figura abaixo. Outras configurações importantes estão na chave de acesso e no certificado utilizados pelo framework, respectivamente representados nas linhas 7 e 8 da figura.

```

3  /* Configuração mecanismo de Autenticação */
4  $metadata['__DYNAMIC:1__'] = array(
5      'host' => '__DEFAULT__',
6      'auth' => 'example-userpass',
7      'privatekey' => 'server.pem',
8      'certificate' => 'server.crt'
9  );

```

Como o objetivo do trabalho aqui descrito era desenvolver um mecanismo de agregação de atributos, foi utilizado no protótipo o modelo estático de usuário e senha. Como exemplo tem-se a seguir onde especificamente na linha dezoito (18) pode-se observar o usuário (*user*) e a senha de autenticação (*userpass*).

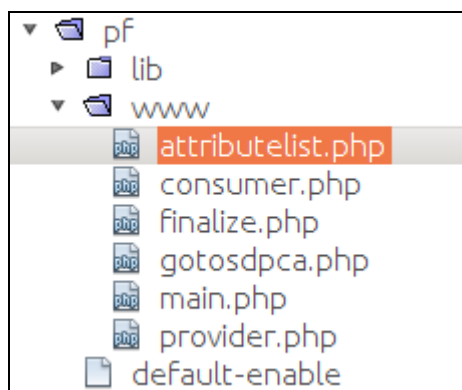
```

15      'example-userpass' => [
16          'exampleauth:UserPass',
17
18          'user:userpass' => [
19              'name' => 'Username'
20          ]

```

Após a configuração no framework, conforme descrito anteriormente, e que precisa ser realizada em todos os provedores de serviço e provedores de identidade que fazem parte da federação, foi desenvolvido o módulo, que nada mais é a interface gráfica da aplicação.

A primeira figura da próxima página representa a estrutura de criação do módulo do provedor de serviço da Polícia Federal. Cada arquivo contido no diretório *www* faz parte do serviço de emissão de passaporte e pode ser acessado a partir do navegador Web.



A figura abaixo representa parte do código do arquivo *attributelist.php*. A parte mais importante está em como informar ao framework *simpleSAML* que este arquivo ou página deve ser protegido. A linha oito (8) representa esta configuração, no caso ao adicionar esta marcação em qualquer arquivo do módulo desenvolvido, automaticamente o framework irá verificar que esta página precisa de autenticação e irá redirecionar o navegador Web do usuário para o provedor de identidade. Para que o usuário autentique-se e tenha acesso garantido a esta página. O framework leva em consideração para o redirecionamento as configurações de metadados que foram apresentadas anteriormente, para redirecionar o usuário ao provedor de identidade adequado.

```

3  require_once SimpleSAML_Module::getModuleDir('mvc').'/lib/functions.php';
4
5  require_once SimpleSAML_Module::getModuleDir('mvc').'/include/header.php';↵
6
7  call_user_func(function() {
8      $controller = new sspmod_pf_controller_MainController();
9      //continua ...

```

## **APÊNDICE C – MENSAGEM CONVITE PARA PARTICIPAÇÃO DA AVALIAÇÃO**

A seguir apresenta-se a mensagem de texto enviada para todos os participantes da pesquisa de satisfação referente a implementação do protótipo do Mecanismo Agregador de Atributos.

Caro Profissional,

Gostaríamos de contar com sua colaboração para avaliar um Mecanismo Agregador de Atributos voltado para Aplicações de Governo Eletrônico. Este trabalho foi desenvolvido no contexto de um projeto de mestrado e no momento está em fase de avaliação.

O experimento deve tomar cerca de quinze (15) minutos do seu tempo.

Você deverá acessar um Serviço que fará uso do Mecanismo Agregador de Atributos e em seguida, responder a uma pesquisa de satisfação. O questionário abrange a avaliação do mecanismo agregador de atributos, bem como um breve levantamento técnico sobre seu conhecimento nos assuntos que norteiam essa pesquisa.

Para ler as instruções de acesso e iniciar o processo de avaliação acesse o link a seguir:

<https://docs.google.com/forms/d/1BJylTjwi8lB4owXzYeCtn6KNc0pMyJaKom-kWlA4qtw/viewform>

Acesse também: Vídeo de apresentação (<http://www.youtube.com/watch?v=kdjixPmXjn8>)

Sua colaboração é muito importante.

Marcondes Maçaneiro

Michelle S. Wingham (orientadora)

---

UNIVALI - Universidade do Vale do Itajaí  
Mestrado em Computação Aplicada



## APÊNDICE D – QUESTIONÁRIO DE PESQUISA – GOVERNO

### Pesquisa de Satisfação: Uso do Mecanismo Agregador de Atributos

Caro(a) Avaliador(a),

Primeiramente, agradecemos por ter aceito participar deste processo de avaliação do protótipo do mecanismo agregador de atributos.

Este trabalho está sendo desenvolvido pelo aluno de mestrado Marcondes Maçaneiro sob orientação da Prof. Michelle Wingham (UNIVALI- Mestrado de Computação Aplicada).

\* Importante: Lembramos que o experimento a ser executado é de caráter científico e não tem ligação com o governo federal, ou com suas aplicações. Todos os dados neste contidos são fictícios, utilizados apenas para comprovação das funcionalidades do mecanismo agregador de atributos.

\*\* Utilize um computador Desktop ou um Notebook para realizar o experimento, e que tenha instalado Sistema Operacional e Navegador de Web nas suas versões mais recentes.

\*\*\* É importante que você tenha a Máquina Virtual Java (JRE) instalada no computador que irá utilizar para executar o experimento. Se necessário, você pode obter a JVM neste endereço, [http://java.com/pt\\_BR/](http://java.com/pt_BR/). Se você já utiliza aplicações Java através de um navegador Web provavelmente você já tem instalado o JRE, nesse caso, apenas verifique a versão instalada. Recomenda-se a utilização da Versão 7.

Os objetivos do mecanismo agregador de atributos são:

- 1 - Permitir que o compartilhamento dos atributos dos usuários entre Provedores de Serviços e Provedores de Identidades Governamentais;
- 2 - Fornecer informações confiáveis aos Provedores de Serviços por meio de trocas de atributos em asserções SAML assinadas digitalmente;
- 3 - Agregar atributos dos usuários que estão distribuídos em diferentes Provedores de Identidade para que estes atributos possam ser apresentados a um Provedor de Serviços que esteja requisitando este conjunto de atributos; e
- 4 - Disponibilizar um canal seguro para a agregação de atributos dos usuário, de forma que suas informações não sejam rastreadas.

Os objetivos do serviço (Solicitação de Emissão de Passaportes) que faz uso do mecanismo agregador de atributos são:

- 1 - Agilizar o processo de solicitação de passaporte disponibilizando a Polícia Federal os atributos de identidade dos solicitantes atestados por seus provedores de identidades;
- 2 - Permitir a agregação de atributos dos usuários (CPF, RG e Título de Eleitor) que estão em diferentes Provedores de Identidades (Receita Federal, Tribunal Superior Eleitoral e Polícia Federal/RIC).

O tempo total para realização do experimento e da avaliação deve ser em torno de 15 minutos.

Antes de iniciar o experimento gostaríamos de fazer algumas perguntas em relação ao seu perfil de avaliador, clique em "Continuar" para responder a estas questões.

\*Obrigatório

### Perfil do Avaliador

1. **1) Em que esfera governamental você atua? \***

*Marcar apenas uma oval.*

- ☐ Municipal
- ☐ Estadual
- ☐ Federal

2. **2) Se você quiser indique qual instituição ou órgão do governo você trabalha?**

.....

3. **3) A quantos anos você atua na área de TI em instituições do Governo? \***

*Marcar apenas uma oval.*

- ☐ Menos de 1 ano
- ☐ Entre 1 e 5 anos
- ☐ Entre 5 e 10 anos
- ☐ Mais de 10 anos

4. **4) Em que área da TI governamental você atua? \***

*Marcar apenas uma oval.*

- ☐ Suporte de Serviços de TI
- ☐ Desenvolvimento de Sistemas (programador, analista, testador)
- ☐ Redes de computadores ou Segurança Computacional
- ☐ Gerência de Projetos
- ☐ Outro: .....

5. **5) Você conhece o conceito de autenticação SSO? \***

SSO significa Single Sing On e também é conhecida como autenticação única.

*Marcar apenas uma oval.*

- ☐ Sim
- ☐ Não

6. **6) Você conhece o conceito de Autenticação Federada ? \***

Autenticar no provedor de identidade de sua instituição e poder acessar serviços de outras instituições

*Marcar apenas uma oval.*

- ☐ Sim
- ☐ Não

7. **7) Você sabe o que são provedores de identidade (IdP - Identity Provider)? \***

Provedores de Identidade são responsáveis pelo processo de autenticação dos usuários (validar as credenciais dos usuários) e por gerenciar os atributos de identidade dos usuários ligados a este provedor.

Marcar apenas uma oval.

- ☐ Sim
- ☐ Não

8. **8) Você já teve alguma experiência com o desenvolvimento de aplicações de governo eletrônico (G2C, G2G, G2B)? \***

Trabalhou como gerente, analista, programador ou testador?

Marcar apenas uma oval.

- ☐ Sim, diretamente.
- ☐ Sim, indiretamente.
- ☐ Não

9. **9) Você conhece as tecnologias listadas abaixo? \***

Marcar apenas uma oval por linha.

	Sim	Não
SAML	<input type="radio"/>	<input type="radio"/>
oAuth	<input type="radio"/>	<input type="radio"/>
OpenID	<input type="radio"/>	<input type="radio"/>

10. **10) Qual sistema operacional você está utilizando para executar esse experimento? \***

.....

11. **11) Qual navegador Web você está utilizando para executar esse experimento? \***

Marcar apenas uma oval.

- ☐ Google Chrome
- ☐ Mozilla Firefox
- ☐ Safari
- ☐ Internet Explorer
- ☐ Opera
- ☐ Outro: .....

## Utilização do Serviço de Solicitação de Emissão de Passaportes que faz uso do Mecanismo Agregador de Atributos

Para iniciar a avaliação você precisa seguir os passos a seguir:

- 1 - Acesse o Serviço de Solicitação de Emissão de Passaportes e siga as instruções do próprio



serviço.

\* Endereço do portal: <https://ec2-23-20-0-254.compute-1.amazonaws.com/simplesaml/module.php/pf/main.php>

1.1 - Como o certificado deste servidor é um certificado autoassinado, você precisa aceitar como confiável o certificado para estabelecer a conexão segura com o serviço. Observe que o protocolo HTTPS está sendo utilizado em todos os serviços, logo, você precisará repetir este passo a cada novo serviço que acessar.

2. Ao tentar acessar o serviço, você será redirecionado para o Provedor de Identidades (IdP) da Polícia Federal. Identifique-se com o usuário e senha abaixo.

\* Usuário: user

\* Senha: userpass

3 - Após efetuar a autenticação no IdP, o serviço de Solicitação de Emissão de Passaportes da Polícia Federal apresentará uma lista indicando os atributos necessários para realizar o pedido de passaporte. Você deverá avançar conforme solicitado pela aplicação para ir até o SDPCA (Serviço de Descoberta de Provedor de Cliente Ativo).

4 - Neste momento, você será direcionado para o SDPCA para indicar de qual provedor do Governo você fará o download do mecanismo agregador de atributos (chamado de aplicativo de cliente ativo) que será executado em sua máquina e que é o responsável por recolher dos diferentes provedores de identidade os seus atributos.

4.1 Note pela URL (<https://ec2-54-226-102-13.compute-1.amazonaws.com/simplesaml/module.php/sdpca/main.php>) de acesso a este serviço que você não está mais acessando o serviço inicial da Polícia Federal, o que indica que sua autenticação inicial foi compartilhada e aceita por este serviço (SSO), pois o mesmo também necessita de identificação do usuário para acesso as suas informações.

4.2 Você deve clicar em avançar para em seguida indicar o provedor do aplicativo cliente ativo.

5 - Neste momento, você foi redirecionado para o Provedor de Cliente Ativo (PCA) conforme pode notar na URL (<https://ec2-54-226-126-153.compute-1.amazonaws.com/simplesaml/module.php/pca/main.php>). Novamente, este serviço aceitou a sua autenticação feita no IdP da Polícia Federal.

5.1. - Este provedor permite que você faça o download do aplicativo (cliente ativo) que será executado na sua máquina e que irá recolher os atributos que estão nos diferentes provedores de identidades, agregá-los e entregá-los ao Serviço de Solicitação de Emissão de Passaportes. Este aplicativo é uma Java Web Start (JWS) e está assinado para que você tenha certeza que este foi criado por uma entidade confiável do Governo. Clique em download para obter o aplicativo de cliente ativo.

6. Caso esse aplicativo não seja executado automaticamente, execute-o. Toda vez que o aplicativo é iniciado, o software Java Web Start acessa o serviço de provedor de cliente ativo para verificar se há uma nova versão disponível. Como esta conexão é segura (SSL), o navegador informa que o certificado do servidor não é confiável, logo você precisa aceitar este certificado como confiável. Além disso, por motivos de segurança, o aplicativo está assinado com o certificado do servidor, logo você precisará também confiar nesta assinatura.

7 - A primeira tela do aplicativo indicará que você precisa acessar o Provedor de Serviços para obter a lista dos atributos que este deseja.

8 - Você será redirecionado para o provedor de identidades, pois este acesso ao provedor de serviços exige autenticação.

\* Usuário: user

\* Senha: userpass

9. Após realizar a autenticação, o aplicativo irá solicitar que você selecione um Provedor de Identidade para cada um dos atributos, selecione o provedor na lista de provedores e utilize as informações abaixo para autenticar em cada um deles.

Provedor da Receita Federal (para obter o CPF)

\* Usuário: user1

\* Senha: userpass1

Lembre-se que após se autenticar, você precisa clicar em Avançar para continuar o processo de agregação.

Provedor da Polícia Federal/RIC (para obter o RG)

\* Usuário: user2

\* Senha: userpass2

Lembre-se que após se autenticar, você precisa clicar em Avançar para continuar o processo de agregação.

Provedor do Tribunal Superior Eleitoral (para obter o Título de Eleitor)

\* Usuário: user3

\* Senha: userpass3

Lembre-se que após se autenticar, você precisa clicar em Avançar para continuar o processo de agregação.

9 - Após acessar os provedores de identidade e obter todos os atributos, será exibida uma tela contendo todos os atributos e seus respectivos valores. Você pode ainda salvar as asserções SAML que contém os atributos emitidos pelos Provedores de identidades (arquivos XML). Nesta tela, você deverá Concordar com a liberação dos atributos ao Provedor da Polícia Federal.

10 - Por fim, após realizar todos os procedimentos para agregação de atributos e liberar o envio dos mesmo para o Provedor da Polícia Federal, o aplicativo de cliente ativo abrirá automaticamente uma aba do navegador Web , no qual será exibido novamente o resumo de seus atributos e valores e um código de protocolo gerado pelo Provedor de Serviço, no recebimento e aceite das asserções SAML recebidas com seus atributos.

Após a execução dos passos descritos acima, por favor, preencha o formulário de avaliação.

## Avaliação de Usabilidade - Pesquisa de Satisfação do Usuário

Lembre-se que o foco desta avaliação é o uso do Mecanismo Agregador de Atributos (aplicativo de cliente ativo).

12. **12) Você conseguiu executar com sucesso todos os passos descritos no roteiro do experimento? \***

*Marcas apenas uma oval.*

☐ Sim

☐ Não

13. **13) Caso você não tenha executado com sucesso todos os passos, identifique o(s) passo(s) e descreva o problema.**

---



---



---



---



---

14. **14) Foi necessário cancelar a execução de algum serviço e iniciar novamente? \***

*Marcar apenas uma oval.*

- ☐ Sim  
☐ Não

15. **15) No experimento, os serviços utilizados sempre exigiram uma ação sua? \***

*Clicar em um botão, avançar, aceitar!*

*Marcar apenas uma oval.*

- ☐ Sim  
☐ Parcialmente  
☐ Não

16. **16) Você se sentiu confortável ao utilizar os serviços? \***

*Marcar apenas uma oval.*

- ☐ Sim  
☐ Não

17. **17) Caso contrário, o que não te trouxe a sensação de conforto?**

---

---

---

---

---

18. **18) As mensagens de erros, caso tenham ocorridos, foram suficientes para apontar e contornar o problema? \***

*Marcar apenas uma oval.*

- ☐ Sim  
☐ Parcialmente  
☐ Não  
☐ Não se aplica

19. **19) No seu ponto de vista, a apresentação das informações está legível (claras e compreensíveis)? \***

*Marcar apenas uma oval.*

- ☐ Sim  
☐ Parcialmente  
☐ Não

20. **20) Mesmo durante o pouco período de tempo que você utilizou os serviços, foi possível ter um grau de experiência satisfatório? \***

*Marcar apenas uma oval.*

- ☐ Sim  
☐ Parcialmente  
☐ Não

21. **21) Os serviços reagiram rapidamente as suas ações? \***

*Marcar apenas uma oval.*

- ☐ Sim  
☐ Parcialmente  
☐ Não

22. **22) Você se sentiu mais seguro ao utilizar os serviços, comparando com serviços de Governo Eletrônico que você utiliza? \***

*Marcar apenas uma oval.*

- ☐ Sim  
☐ Parcialmente  
☐ Não

23. **23) Você em algum momento não soube o que fazer ao acessar os serviços? \***

*Marcar apenas uma oval.*

- ☐ Sim  
☐ Parcialmente  
☐ Não

24. **24) Levou muito tempo para você compreender as funções dos serviços acessados no experimento? \***

*Marcar apenas uma oval.*

- ☐ Sim  
☐ Não

25. **25) Você gostaria de utilizar o mecanismo agregador de atributos em aplicações governamentais? \***

O mecanismo agregador de atributo é o aplicativo de cliente ativo que você fez o download e executou na sua máquina.

*Marcar apenas uma oval.*

- ☐ Sim  
☐ Não



26. **26) Na sua opinião, o processo de obter de forma segura os atributos dos usuários podem ser realizadas com mais rapidez utilizando o mecanismo agregador de atributos? \***

*Marcar apenas uma oval.*

- ☐ Sim  
☐ Não

27. **27) Na sua opinião, o mecanismo agregador pode trazer mais flexibilidade para os Serviços de Governo Eletrônico? \***

*Poder coletar de forma segura de diferentes provedores de identidade os atributos dos usuários e apresentá-los para um Serviço de Governo Eletrônico.*

*Marcar apenas uma oval.*

- ☐ Sim, pode trazer mais flexibilidade para a maioria dos serviços  
☐ Sim pode trazer mais flexibilidade, mas para poucos serviços  
☐ Não da forma como está, precisa de ajustes  
☐ Definitivamente não.

28. **28) Na sua opinião, o mecanismo agregador de atributos pode garantir a privacidade do usuário no processo de coleta de seus atributos em diferentes provedores de identidades? \***

*Marcar apenas uma oval.*

- ☐ Sim  
☐ Não

29. **29) Na sua opinião, para os desenvolvedores de aplicações de Governo Eletrônico, o uso do mecanismo agregador de atributos pode trazer algum impacto negativo? \***

*Marcar apenas uma oval.*

- ☐ Sim  
☐ Não

30. **30) Se sim, qual impacto negativo?**

---

---

---

---

---

31. **31) Você recomendaria essa aplicação para ser utilizada em serviços a serem oferecidos pelo governo? \***

*Marcar apenas uma oval.*

- ☐ Sim  
☐ Não



32. **32) O que você achou de melhor no experimento que você executou? Por quê?**  
Lembre-se que o foco desta avaliação é o mecanismo agregador de atributos.

.....

.....

.....

.....

.....

33. **33) O que você acha que pode ser melhorado no mecanismo agregador de atributos e por que?**

.....

.....

.....

.....

.....

34. **34) Você tem algum comentário adicional sobre o mecanismo agregador de atributos para a equipe de desenvolvimento?**

.....

.....

.....

.....

.....

---

## **APÊNDICE E – QUESTIONÁRIO DE PESQUISA – EMPRESAS**

O formulário de pesquisa para os funcionários de empresas externa segue o mesmo padrão do utilizado para os funcionários públicos, contendo apenas algumas diferenças. Basicamente o que difere são as 4 perguntas referentes ao perfil do avaliador, que são:

1. Para que esfera governamental você presta serviço?
2. Se você quiser, indique qual(is) instituição(ões) do governo você presta serviços?
3. Há quantos anos você atua na área de TI?
4. Para qual área da TI governamental sua empresa (ou você) presta serviços?

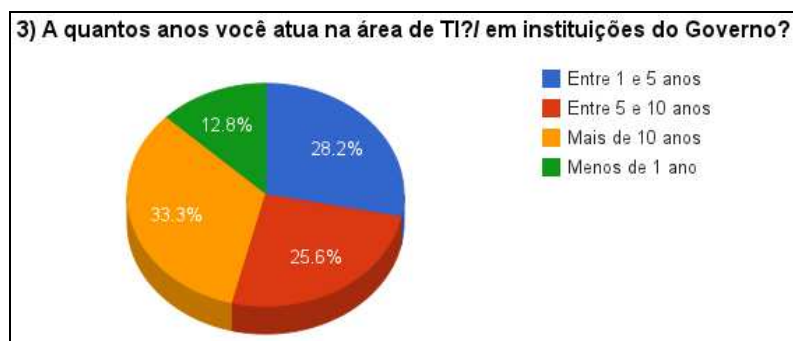
## APÊNDICE F – OPINIÃO DOS USUÁRIOS NOS FORMULÁRIO DE PESQUISA

Após o término da pesquisa de satisfação, os resultados foram agregados em única tabela, logo os resultados apresentados a seguir são de todos os avaliadores. O gráfico da Figura abaixo refere-se à atuação dos profissionais nas esferas governamentais, onde 38,5% atuam na esfera municipal, 23,1% atuam na esfera estadual e 25,6% atuam na esfera federal. Os demais 12,8% atuam em mais de uma esfera governamental.



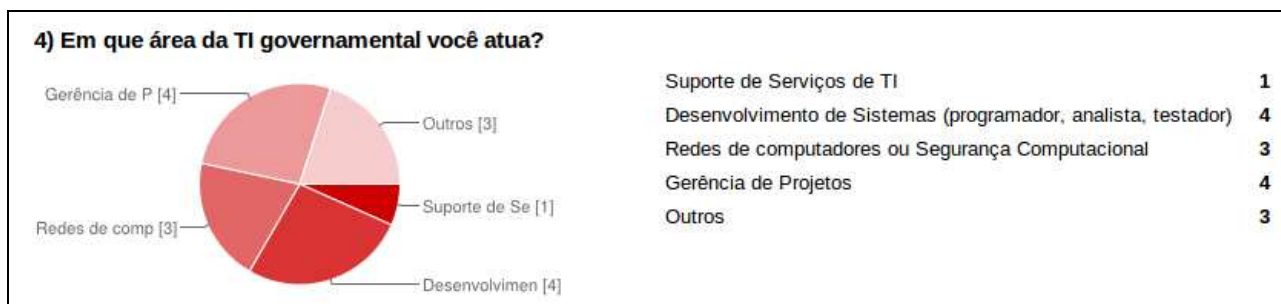
Gráfico referente a atuação ou prestação de serviços governamentais

O gráfico apresentado na Figura abaixo refere-se ao tempo de atuação dos profissionais na área de TI das empresas e do governo. Esse gráfico demonstra que a pesquisa foi aplicada em um grupo bem diversificado. Sendo que 41% atua a menos de 5 anos, 25,6% atua entre 5 e 10 anos e 33,3 % atuam a mais de 10 anos.



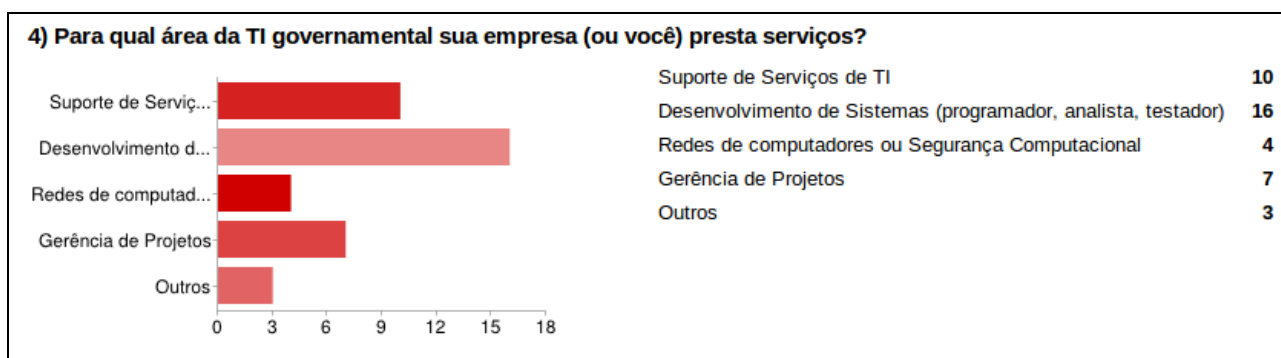
Tempo de atuação com tecnologia da informação

Os gráficos das duas próximas Figuras referem-se a quarta pergunta dos questionários de pesquisa. A Figura abaixo refere-se especificamente ao questionário para profissionais que trabalham para o governo.



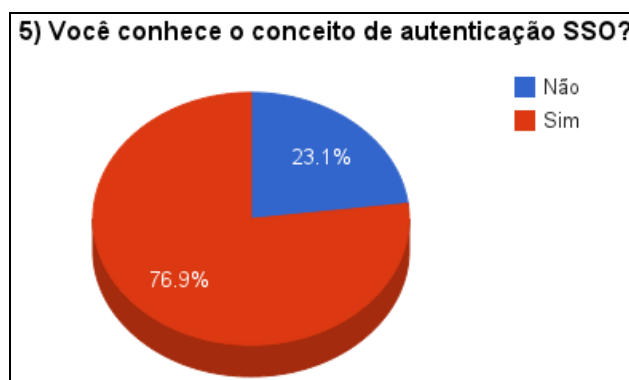
Área de atuação no governo

Já o gráfico apresentado na próxima Figura representa o número de respostas obtidas sobre a atuação dos pesquisados que trabalham em empresas externas ao governo. Esse grupo de avaliadores tinha a opção de poder selecionar mais de uma resposta para esta pergunta. Os totais demonstram que a grande maioria dos avaliadores que responderam a pesquisa atua com desenvolvimento de sistemas e com suporte a serviços de tecnologia da informação.



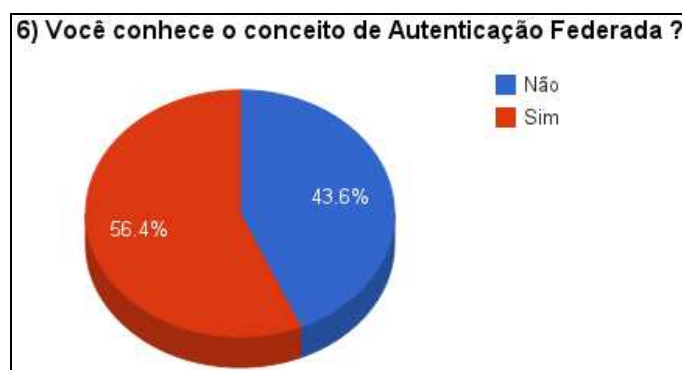
Área de atuação em empresas externas ao governo

A Figura abaixo ilustra o conhecimento dos entrevistados sobre o conceito de SSO. Este mostra que a grande maioria, 76,9%, conhece o significado de SSO.



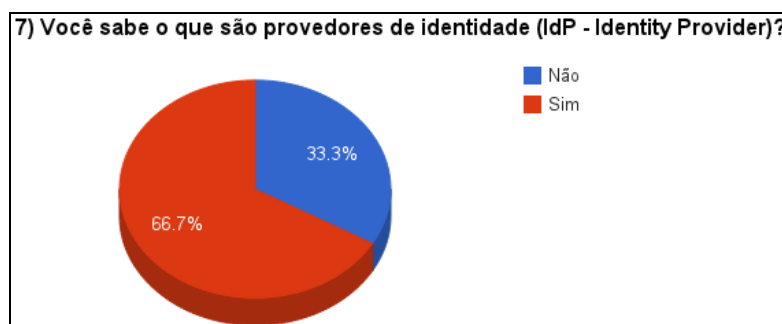
Conhecimento de SSO

O gráfico apresentado na Figura abaixo indica o conhecimento sobre autenticação federada. Esse gráfico demonstra que a maioria dos entrevistados, 56,4% conhece este conceito.



Conhecimento sobre autenticação Federada

O gráfico apresentado na Figura abaixo demonstra que a maioria, 66,7%, dos entrevistados sabe o que são os provedores de identidades.



Conhecimento sobre provedores de identidade

A Figura abaixo apresenta um gráfico classificando a experiência dos entrevistados no desenvolvimento de aplicações de governo eletrônico. Para esse caso a maioria, 56,4%, não trabalha com esse tipo de desenvolvimento e apenas 25,6% dos entrevistados atua diretamente com o desenvolvimento de soluções de governo eletrônico.



Experiência com o desenvolvimento de aplicações de governo eletrônico

A Tabela abaixo representa a porcentagem de conhecimento dos entrevistados referente aos protocolos SAML, OAuth e OpenID. Resultado em 38,5% dos avaliadores responderam que conhecem SAML, 53,8% dos avaliadores conhecem o protocolo OAuth e 64,1% dos avaliadores tem conhecimento sobre o protocolo OpenID.

Porcentagem de conhecimentos dos protocolos referente a pergunta de pesquisa 9

Protocolo	Porcentagem de Avaliadores que conhecem
SAML	38,5 %
oAuth	53,8 %
OpenID	64,1 %

O gráfico da Figura abaixo representa os sistemas operacionais utilizados pelos pesquisados durante o experimento.



Sistemas operacionais utilizados

A Figura abaixo apresenta a porcentagem de utilização dos navegadores Web durante o experimento. Como resultado tem-se que a maioria, 66,7% dos avaliadores utilizaram o navegador

*Google Chrome* durante o experimento. Em segundo lugar, tem-se o navegador Firefox, e em terceiro lugar o navegador Internet Explorer da Microsoft.



Navegadores Web utilizados

O gráfico apresentado na Figura abaixo representa a quantidade de avaliadores que executaram com sucesso o experimento, sendo que 82,1% conseguiram executar e 17,9% tiveram algum tipo de problema conforme relatados a seguir.



Execução do experimento

A seguir algumas respostas obtidas dos usuários quando não foi possível executar o experimento, ou ocorreu algum erro:

1. *“Inicialmente eu estava utilizando o chrome para executar o experimento, mas como o Firefox é meu navegador padrão, após utilizar o aplicativo Java, eu fui enviado para uma nova aba no Firefox, a qual não mantinha a mesma sessão do experimento inicial. Tive que reiniciar o processo no novo navegador.”;*



2. “No Serviço de descoberta de Provedor de Cliente Ativo a seguinte mensagem foi apresentada: “Parâmetros esperados”.”;
3. “No Safari (que eu havia começado o experimento), ele parou após o primeiro login, depois de continuar aparecia na parte de baixo da tela aparece em vermelho com um fundo vermelho: Parâmetros esperados.”;
4. “Na tela: <https://ec2-54-226-126-153.compute-1.amazonaws.com/simplesaml/module.php/pca/main.php>, Quando clicado no botão: clique aqui para iniciar o download da aplicação, uma mensagem de erro era apresentada, e o download não foi iniciado.”;
5. “Depois de escolher o provedor de cliente ativo, ficou com a mensagem “redirecionando...” e não saiu daí.”;
6. “No último passo, o cliente não abriu uma nova aba/janela do navegador com o protocolo de recebimento dos atributos.”; e
7. “Não consegui salvar o arquivo XML. Obtinha erro de negação de gravação em disco para todos os locais que tentei gravar (área de trabalho, unidade c, meus documentos). Talvez seja algo com meu sistema operacional.”.

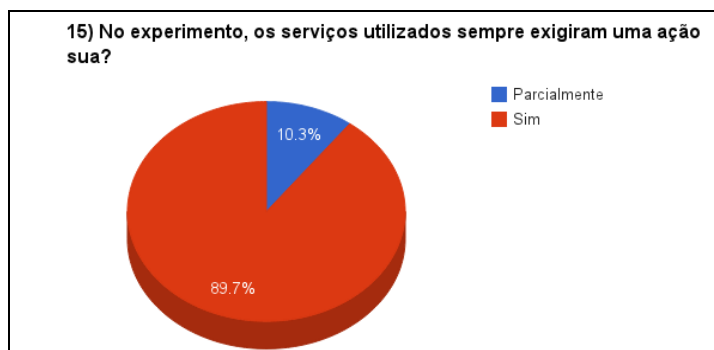
O gráfico apresentado na Figura abaixo representa a porcentagem de avaliadores que precisaram reiniciar o experimento por algum tipo de problema, alguns desses problemas relacionados as respostas já apresentadas anteriormente na descrição da Figura abaixo.



Necessidade de reinício do experimento

A Figura abaixo representa as respostas referente a necessidade de ação do usuário questionada na pergunta quinze do formulário de pesquisa. A maioria, 89,7% responderam que Sim,

considerando que foi sempre necessária uma ação, e 10,3% consideram que foi parcialmente necessária uma ação ao utilizarem o experimento.



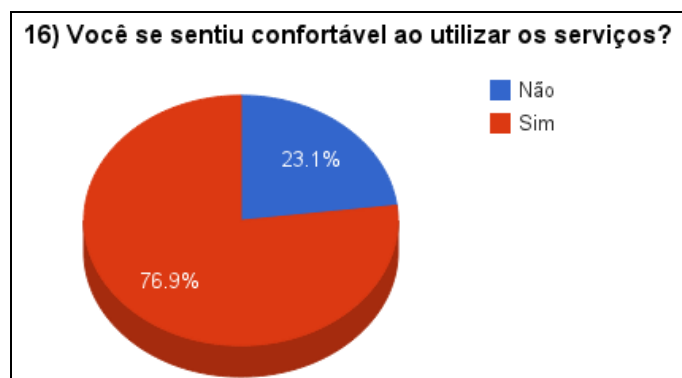
Exigência de ação o usuário

A Figura abaixo apresenta as porcentagens de avaliadores que consideram o sistema confortável para uso ou não. Sendo que 76,9% responderam que sim e 23,1% responderam que não. A questão seguinte questionava os avaliadores sobre o porquê não foi confortável utilizar o sistema (opcional). Com isso obteve-se as seguintes respostas:

1. *“O processo pareceu extremamente burocrático, e eu como usuário senti que estava fazendo trabalho que o computador poderia ter feito, ao ter que escolher os provedores e me logar separadamente em cada um deles.”;*
2. *"O fato de ser necessário autenticar e posteriormente avançar para cada IdP informado. Quando é clicado em avançar e troca o ""documento"" exigido poderia ser informado de forma mais clara que a tela mudou, por duas vezes achei que tivesse somente limpado a tela anterior.";*
3. *“O navegador sempre informava que a url que estava tentando acessar não era uma url segura”;*
4. *“A aplicação é interessante e atingiu os objetivos no que tange aos conceitos envolvidos, entretanto integrar dados não precisa ser uma tarefa manual como a descrita. Entendo que todos os conceitos podem ser adotados por ferramentas próprias de integração de dados, utilizando SSO, de forma automatizada.”;*
5. *"1. Ter que ficar aceitando os certificados o tempo todo. 2. Ter que informar, em cada serviço, o usuário e senha.";*

6. *"No endereço da página, não vi nada que identificasse que fosse da polícia federal. Achei pouco explicado para um leigo, o que estava acontecendo."*;
7. *"Prefiro que este serviço fosse oferecido em algum site ou portal em vez de aplicação cliente Java para ser baixada, pois, desta forma o site funcionaria independente de software instalado no lado cliente, como a máquina virtual java."*;
8. *"Ter que rodar uma aplicação java com certificados auto assinados não é confortável já que as mensagens de aviso são intimidadoras por parte do próprio java."*; e

*"Fato de ter de autenticar os usuários e então avançar deixa fluência da aplicação prejudicada. Talvez se a autenticação fosse feita no mesmo momento do avançar o processo seria mais fluido."*.



Uso confortável do sistema

A Figura abaixo representa se as mensagens de ajuda foram suficientes para auxiliar os avaliadores no caso de terem recebido algum erro durante a utilização do protótipo. Para esta questão 53.8% dos avaliadores responderam não terem obtido erros durante a utilização do experimento. Outros 28.2% dos avaliadores responderam que sim, e apenas 7,7% dos avaliadores responderam que as mensagens de erro não foram suficientes.

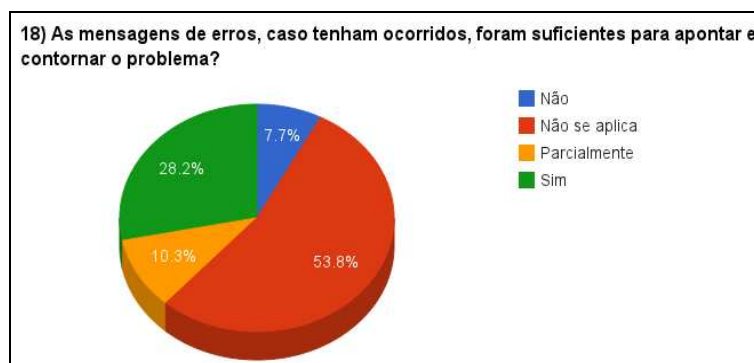


Gráfico referente a pergunta 18 dos formulários de pesquisa

A Figura abaixo representa o ponto de vista dos avaliadores quanto à apresentação das informações do protótipo. Foram 76,9% dos avaliadores que consideraram a aplicação clara e compreensível.



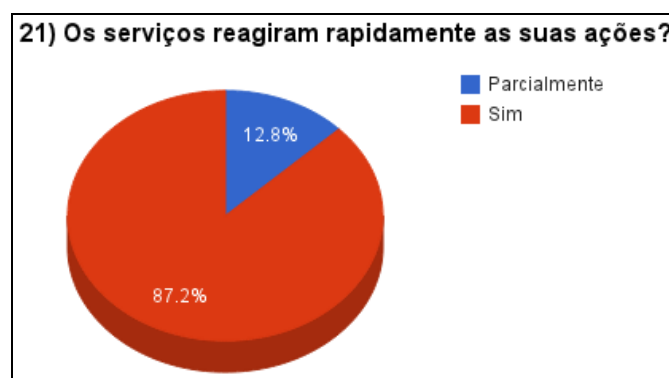
Apresentação legível das informações

Sobre o grau de experiência (ver Figura abaixo) observa-se que 69,2% dos avaliadores que responderam o questionário de pesquisa se consideram satisfeitos quando da utilização do protótipo do mecanismo agregador de atributos no cenário de emissão de passaportes.



Grau de experiência

Quanto à rapidez na execução dos serviços desenvolvidos para o protótipo de mecanismo agregador de atributos (ver Figura abaixo) conclui-se que a maioria, 87,2% dos avaliadores que responderam o questionário consideram que a aplicação respondeu rapidamente as suas ações.



Rapidez dos serviços

A questão vinte e dois (ver Figura abaixo) foi criada para detectar se os participantes da pesquisa se sentiram seguros ao utilizar os serviços oferecidos no protótipo de mecanismo agregador de atributos em comparação aos serviços de governo eletrônico que estes utilizam atualmente.

Como resposta a esta questão obteve-se 43,6% dos avaliadores consideram parcialmente seguros, 41% consideram-se mais seguros que os serviços de governo que atualmente utilizam e apenas 15,4% dos avaliadores responderam não se sentirem mais seguros.



Segurança na utilização dos serviços

A Figura abaixo apresenta os resultados sobre a questão em que o usuário deveria responder se algum momento ele não soube o que fazer durante a utilização do experimento. Como resposta obteve-se a maioria, 87,2% dos avaliadores responderam que não ficaram sem saber o que fazer. Isso comprova que as mensagens explicativas que foram introduzidas no protótipo guiam o usuário nas ações necessárias.



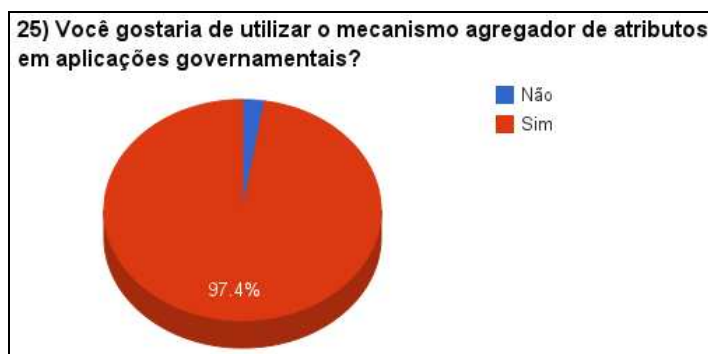
Não saber utilizar o experimento

O gráfico apresentado na Figura abaixo representa as respostas obtidas sobre a compreensão das funções dos serviços acessados no experimento. A grande maioria, 94,9% dos avaliadores, respondeu que não levou muito tempo para compreender as funções.



Tempo para compreender as funções do serviço

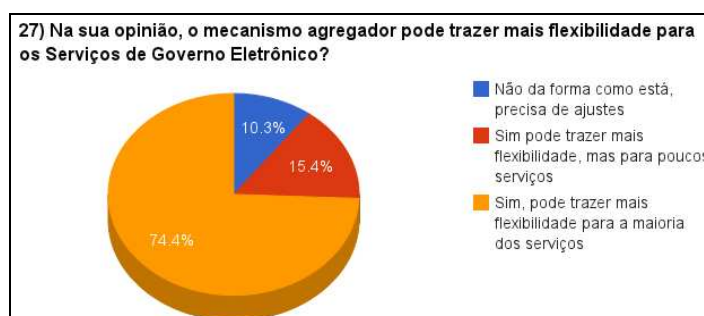
A Figura abaixo ilustra que 97,4% dos avaliadores gostariam de utilizar o mecanismo em aplicações de e-GOV, mais especificamente, dos trinta e nove avaliadores que responderam à pesquisa, apenas um respondeu que não gostaria de utilizar o mecanismo proposto por este trabalho.



Desejo de utilizar o mecanismo em aplicações de e-GOV

A questão 26 que questiona a opinião dos avaliadores com relação o processo de obter de forma segura os atributos dos usuários. Questionando se esse pode ser realizado com mais rapidez utilizando o mecanismo agregador de atributos, obteve o mesmo resultado apresentado para a questão 25, onde, 97.4% dos avaliadores responderam que sim.

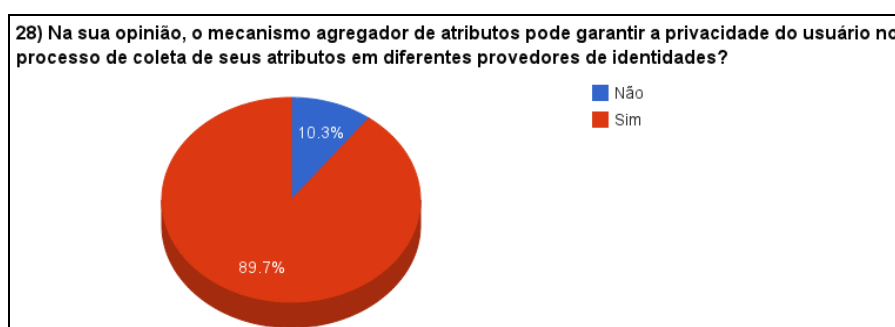
O gráfico apresentado na Figura abaixo refere-se as respostas obtidas referentes à flexibilidade que o mecanismo agregador de atributos pode trazer para os serviços de governo eletrônico. A maioria, 74,4% dos usuários responderam que sim, pode trazer mais flexibilidade para a maioria dos serviços de governo eletrônico.



Flexibilidade do mecanismo agregador de atributos

A Figura abaixo ilustra os resultados sobre a opinião dos usuários referente as garantias de privacidade no processo de coleta de seus atributos em diferentes provedores durante a utilização do mecanismo agregador.

A maioria, 89,7% dos avaliadores respondeu que sim, é possível garantir a privacidade dos usuários durante o procedimento de agregação de atributos de múltiplos provedores.



Privacidade do mecanismo agregador de atributos

A Figura abaixo ilustra os resultados sobre a opinião dos avaliadores referente aos impactos negativos no uso do mecanismo agregador de atributos pelos desenvolvedores de aplicações de governo eletrônico. Como resposta obteve-se 69,2% dos avaliadores que responderam não ter impactos negativos para os programadores no uso do mecanismo agregador de atributos, e 30,8% dos avaliadores responderam que sim, que terá impacto negativo para os desenvolvedores de aplicações de governo eletrônico.





Impacto negativo

A questão trinta do questionário de pesquisa era opcional e foi criada para complementar as respostas dos avaliadores que indicaram haver impactos negativos para os desenvolvedores no uso do mecanismo agregador de atributos.

Como resposta a esta pergunta obtiveram-se as seguintes opiniões:

1. *“A cultura dos desenvolvedores ainda não está aberta a ponto de aceitar atributos de outros IdPs, é um desafio conseguir aplicar um projeto deste porte em qualquer das esferas governamentais”;*
2. *“Vazamento de informações pessoais, ataques e outros problemas relacionados à segurança.”;*
3. *“A resistência na utilização por alguns usuários, que se tratando da área pública existe bastante.”;*
4. *“Não tenho como opinar de forma incisiva, para definir se existe a possibilidade da existência de impactos negativos, acredito que existam riscos, porém o mecanismo se mostra promissor na área.”;*
5. *“Pode parecer mais complexo para o usuário, ou pode dar a impressão de que os serviços não estão integrados, e é por isso que você precisa ficar acessando vários serviços.”;*
6. *“A necessidade de adequação das aplicações existentes para poderem utilizar o protocolo SAML poderia ser vista como um impacto negativo por parte dos desenvolvedores.”;*
7. *“Reimplementação de mecanismos de autenticação.”;* e

8. *“Curva de aprendizagem de novas tecnologias, talvez problemas com escalabilidade devido à alta demanda de requisições.”.*

As respostas obtidas na pergunta trinta e um do formulário de pesquisa que questionou os avaliadores se eles recomendariam o protótipo que acabaram de testar para ser utilizado em serviços a serem oferecidos pelo governo federal teve o mesmo padrão de respostas obtidas na questão 25 e 26 apresentadas anteriormente. Para essa questão 97,5% dos avaliadores responderam que recomendariam a aplicação para ser utilizada em serviços que forem oferecidos pelo governo.

Ao final do formulário de pesquisa foram feitas três perguntas opcionais para os usuários, com objetivo de receber opiniões dos usuários que não foram possíveis de serem contempladas com as perguntas de resposta padrão que foram apresentadas.

As perguntas e respectivas opiniões dos usuários serão apresentadas a seguir:

- O que você achou de melhor no experimento que você executou? Por quê?
  - *“A possibilidade de utilizar atributos já consolidados e confirmados em um IdP”;*
  - *“A facilidade em utilizar o serviço em função das telas dinâmicas passo à passo.”;*
  - *“A sua interface é clara, intuitiva e objetiva. Em nenhum momento fiquei com dúvida de como proceder para utilizar a mesma.”;*
  - *“Ágil e simples.”;*
  - *“Com certeza a possibilidade de agregação dos atributos de identidade é o maior benefício deste experimento. A aplicação desta ideia pode ajudar muito a simplificação na forma com as aplicações de governo necessitam a entrada de informações de cada usuário.”;*
  - *“O processo de autenticação é interessante e pode ser utilizado em ampla escala, principalmente com a evolução do projeto. Como desenvolvedor de aplicações para integração de dados com código aberto, em java, percebi que o potencial é grande e pode ser utilizado, principalmente nesta época em que o combate à espionagem na internet vem sendo amplamente discutida. A solução pode estar mais perto, e fácil, do que se imagina!”;*

- *“Infelizmente não foi possível concluir o experimento, por conta disso não posso opinar.”;*
- *“A integração de vários portais”;*
- *“Muito rápido, de fácil uso, uma aplicação como essa oferecendo segurança a processos comuns à pessoas comuns teria muito valor, muito mais acessibilidade ao cidadão.”;*
- *“achei muito boa a ideia de que o serviço possa buscar minhas informações em vários lugares diferentes, facilitando a minha vida para agregar as minhas informações, sem que seja necessário que todas as informações sejam compartilhadas com todos os órgãos o tempo todo.”;*
- *“Poucos passos para que fosse executado.”;*
- *“Agilidade na busca de diversas informações.”;*
- *“A ideia é muito boa, pois se tem uma maior agilidade e segurança nos serviços.”;*
- *“Normalmente quando acessamos serviços de e-Gov são solicitadas informações que de alguma forma existem em alguma base de dados. Nada melhor do que acessá-las diretamente e ir agregando os atributos necessários e solicitados em um cadastro/formulário que está sendo preenchido para acessar algum serviço de e-Gov.”;*
- *“Compartilhamento de atributos de usuários por aplicativos de diferentes órgãos governamentais.”;*
- *“Praticidade e rapidez”;*
- *“A facilidade de captura das informações.”;*
- *“Durante o experimento foram utilizados vários usuários e senhas. Não ficou claro como o usuário poderia obter estes dados em uma aplicação real.”;*
- *“Em geral o experimento em si ficou bom.”;*
- *“O fato de o cliente listar somente os IdPs relevantes para cada atributo sendo coletado (demonstrando o uso dos metadados dos IdPs).”;*
- *“O mecanismo é simples e fácil de usar, com botões intuitivos e mensagens claras.”*

- *“A não necessidade de logar em múltiplos sistemas.”; e*
- *“Por tudo ocorrer em ambiente seguro HTTPS, por não ser necessário informar dados pessoais diretamente no navegador, mas sim serem requisitados.”;*
- O que você acha que pode ser melhorado no mecanismo agregador de atributos e por que?
  - *“A melhoria está no repasse de confiança deste serviço ao usuário.”*
  - *“Toda a parte de segurança precisaria ser aprimorada e totalmente segura para o usuário final.”*
  - *“Inicialmente não tenho nenhuma sugestão, até mesmo por que a mesma cumpriu com seus objetivos de forma pratica.”*
  - *“Eu acho que o mecanismo automaticamente deveria buscar agregar automaticamente todas as informações do usuário no momento da criação de uma conta universal, e a partir daí sempre logar com a conta universal em qualquer um dos serviços.”*
  - *“O fato de ser necessário autenticar e posteriormente avançar para cada IdP informado.”*
  - *“Quando é clicado em avançar e troca o ""documento"" exigido poderia ser informado de forma mais clara que a tela mudou, por duas vezes achei que tivesse somente limpado a tela anterior.”*
  - *“Infelizmente o mecanismo de validação dos certificados digitais realizados pelos browsers atualmente é bastante crítico. Desta forma, realizar a emissão de certificados digitais confiáveis (através de uma entidade certificadora confiável) poderiam ajudar bastante no processo de navegação da consolidação dos atributos pelo browser. No meu caso, utilizando o Mozilla Firefox, foi necessário adicionar as exceções de certificados digitais em praticamente todas as etapas.”*
  - *“Talvez a criação de uma api bem documentada que englobe todas as funcionalidades e que possa ser utilizada de forma padrão por todos os desenvolvedores em seus diversos softwares.”*
  - *“As mensagens trocadas deve ser mais explicativas para o usuário.”*

- *“necessidade de autenticação constante em cada serviço.”*
- *“Para o público em geral, a aceitação das identidades por parte do usuário pode causar estranheza e desconfiança. Isso pode ser um empecilho ou até mesmo confundir o usuário.”*
- *“achei que tinham muitos "passos": logar, continuar, etc. Talvez no futuro fosse possível eu configurar meus provedores de informação, e daí, eu simplesmente escolho que provedor vai fornecer o que e o sistema pode ter uma senha única para eu autorizar que ele vá em todos os serviços e pegue as informações que eu aceitei.”*
- *“Acredito que todos os dados pudessem ser solicitados em uma só janela, ao invés de vários passos (usuário e senha de cada órgão)”*
- *“Deve-se deixar claro ao usuário que os dados estão sendo trafegados de forma segura e que estes dados somente serão utilizados para a finalidade específica do serviço que está sendo utilizado/solicitado. Deixar claro também ao usuário que as questões de privacidade dos serviços que estão sendo utilizados e dos dados que estão sendo utilizados será garantida. Estas questões deixarão os usuários mais a vontade e seguros para a utilização do mecanismo. A nível de confiança dos usuários para o uso da solução irá aumentar.”*
- *“Mais notas explicativas do que está acontecendo...”*
- *“Clareza nas informações e segurança”*
- *“Por que precisei fazer uso de 4 usuários? O usuário deveria ser único.”*
- *“Faltou uma explicação mais objetiva, do ponto de vista de um leigo, quais os reais benefícios do uso do mecanismo agregador de atributos.”*
- *“A realização de um download de um cliente para poder fazer a agregação. Embora isso permita que os atributos sejam todos salvos na máquina do usuário, não existe nenhuma garantia de que esses atributos não estão sendo salvos em nenhum outro lugar (nem foi explicitamente mencionado em nenhum momento).”*
- *“Melhor seria se fosse executado em um portal pelo browser.”*
- *“Checkbox para salvar usuários e senhas dos diversos serviços.”*

- *“Tela integrada com o resultado dos serviços já executados em uma lista que irão buscar os dados automaticamente caso os campos de usuário e senha já estejam salvos e com um status (verde, amarelo, vermelho) informando o status do serviço.”*
- *“Fato de ter de autenticar os usuários e então avançar deixa fluência da aplicação prejudicada. Talvez se a autenticação fosse feita no mesmo momento do avançar o processo seria mais fluido.”*
- Você tem algum comentário adicional sobre o mecanismo agregador de atributos para a equipe de desenvolvimento?
  - *“Parabéns pelo trabalho.”*
  - *“Acredito que para a adoção desta tecnologia pelo governo, a simplificação do uso deste mecanismo é primordial. Desta forma, a criação de uma API (framework) para utilização deste mecanismo pode ser interessante para facilitar seu uso e posteriormente sua adoção.”*
  - *“Sugiro a criação de plugin para o Pentaho Data Integration (kettle), que contemple o SSO com toda a autenticação necessária. Com isso a adoção da solução por diversas áreas seria muito facilitada e, eu diria, difundida, visto que o Brasil é um dos maiores utilizadores da suíte open source de BI Pentaho Data Analytics.”*
  - *“Interessante, acredito que está no caminho certo, porém acredito que deve-se minimizar as ações dos usuários, a questão do aceite de identidades das url's fornecidas é algo que pode atrapalhar o entendimento do usuário.”*
  - *“O passo 10 do roteiro diz que após a conclusão, o aplicativo de cliente ativo abrirá automaticamente uma aba do navegador Web, no qual será exibido novamente o resumo de seus atributos e valores e um código de protocolo gerado pelo Provedor de Serviço, no recebimento e aceite das asserções SAML recebidas com seus atributos. Não ocorreu desta forma comigo. Uma nova janela foi aberta e foi necessário informar o usuário e senha novamente para visualizar as informações. Acredito que isso não seja importante para o processo principal, mas achei que deveria comentar. Também no formulário principal da pesquisa, as perguntas são direcionadas para pessoas que provavelmente trabalham para órgãos*

*governamentais. Não é o meu caso, e em algumas perguntas tive que escolher uma opção para conseguir prosseguir.”*

- *“Excelente iniciativa.”*
- *“Talvez testar a aplicação no iOS. Acho que no meu caso não funcionou por eu estar acessando do iPad.”*
- *“Durante o preenchimento inicial dos dados preliminares, informei que utilizaria o Google Chrome. No entanto, após a captura das informações e apresentação dos registros Cpf, Rg e Título, cliquei em avançar e ele tentou abrir uma aba no IE e não no Chrome. Isso gerou um erro e não consegui visualizar o final do processo. Não revi as informações nem tão pouco o número de protocolo gerado. Fiz duas vezes o processo e o erro persistiu.”*
- *“Trabalho bastante interessante, mas precisaria saber mais sobre o mecanismo e suas decisões de design/implementação para poder fazer uma avaliação mais substanciada.”*
- *“Não ficou claro porque acontece os redirecionamentos da aplicação web onde deve-se aceitar múltiplos certificados continuamente.”*

## APÊNDICE G – DETALHES DE DESENVOLVIMENTO DO PROTÓTIPO

O diagrama de classes que pode ser observado na apresentado a seguir. Representa as classes que foram concebidas durante o desenvolvimento do cliente ativo e também algumas classes de bibliotecas externas.

A principal biblioteca externa utilizada no desenvolvimento do Cliente Ativo faz parte da fundação Apache<sup>17</sup>, representada pelo pacote de classes *org.apache.http*. No modelo essas classes estão nominadas como: *HttpClient*, *SSLConnectionFactory*, *HttpResponse*, *DefaultHttpClient*, *NameValuePair* e *HttpRequestBase*.

Especificamente para o desenvolvimento do Cliente Ativo foram utilizadas as demais classes, as principais classes são: *Connection*, *MainView*, *AuthView*, *ProviderView* e *FinishView*.

A classe *Connection* é responsável por realizar a autenticação nos provedores de identidade utilizados durante o processo de agregação dos atributos e receber destes as asserções SAML. A classe *MainView* é responsável pela tela inicial do Cliente Ativo, onde é exibido para o usuário as informações iniciais sobre a utilização deste.

A classe *AuthView* é responsável pelo controle da autenticação iniciar realizada no provedor de identidade da Polícia Federal. É durante essa autenticação que o Cliente Ativo tem terá acesso ao XMLRequest (ver Figura abaixo) contendo a lista de atributos requeridos pelo Provedor de Serviço de solicitação de Passaporte.

Para a agregação das asserções SAML de cada um dos provedores de identidade utiliza-se a classe de controle *ProviderView*. Essa classe realiza a autenticação no provedor de identidade e executa a agregação da asserção SAML no provedor.

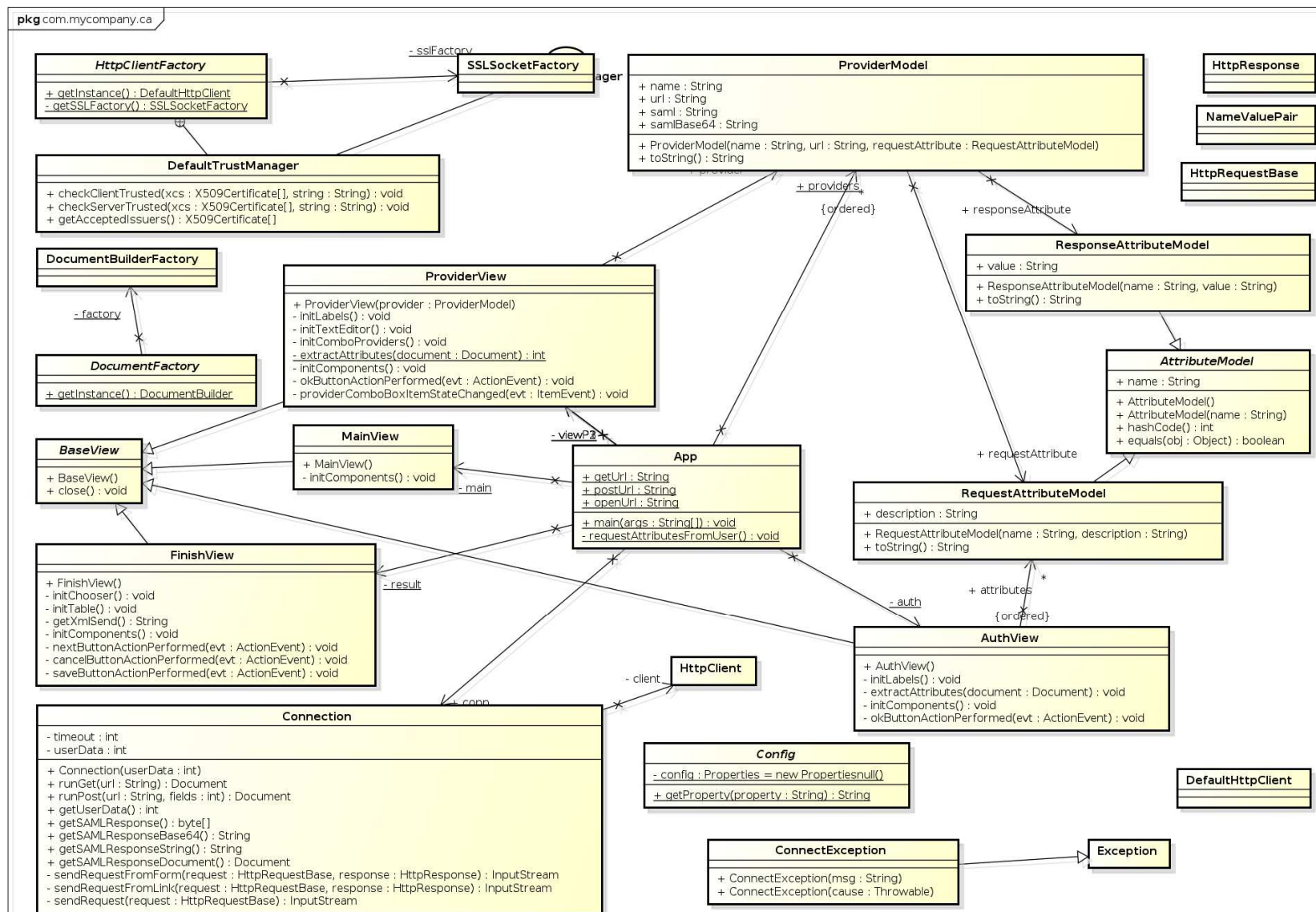
Por fim, a classe *FinishView* é responsável por exibir o resumo dos atributos e valores agregados. Essa classe também implementa a funcionalidade que permite o usuário salvar os arquivos SAML e o XML de resposta (ver Figura abaixo) que será enviado ao provedor de serviço. Esta classe também implementa a comunicação com o provedor de serviço para realizar a entrega

---

<sup>17</sup> A Fundação Apache (*Apache Foundation*) é uma organização, sem fins lucrativos, formada por um grupo de empresas que é responsável por uma grande quantidade de projetos de código aberto (*open-source*).



do XML de resposta com as asserções SAML agregadas. Essa funcionalidade só é executada quando o usuário confirmar que deseja realizar o compartilhamento.



Modelo de Classes

## **APÊNDICE H – RESULTADOS DA PESQUISA DE SATISFAÇÃO**

### **Atores**

No cenário implementado, tem-se um ator primário e seis atores secundários conforme listados a seguir:

- Usuário (ator primário);
- SDPCA (Serviço de Descoberta de Provedor de Cliente Ativo);
- PCA (Provedor de Cliente Ativo);
- SP do Serviço de Emissão de Passaporte;
- Provedor de Identidade (IdP) da Polícia Federal;
- Provedor de Identidade (IdP) da Receita federal; e
- Provedor de Identidade (IdP) do Tribunal Superior Eleitoral.

### **Casos de Uso do Cenário de Solicitação de Emissão de Passaportes**

A figura a seguir ilustra o diagrama de casos de uso para o cenário de solicitação de emissão de passaporte. Em seguida os quadros apresentam os casos de usos expandidos.

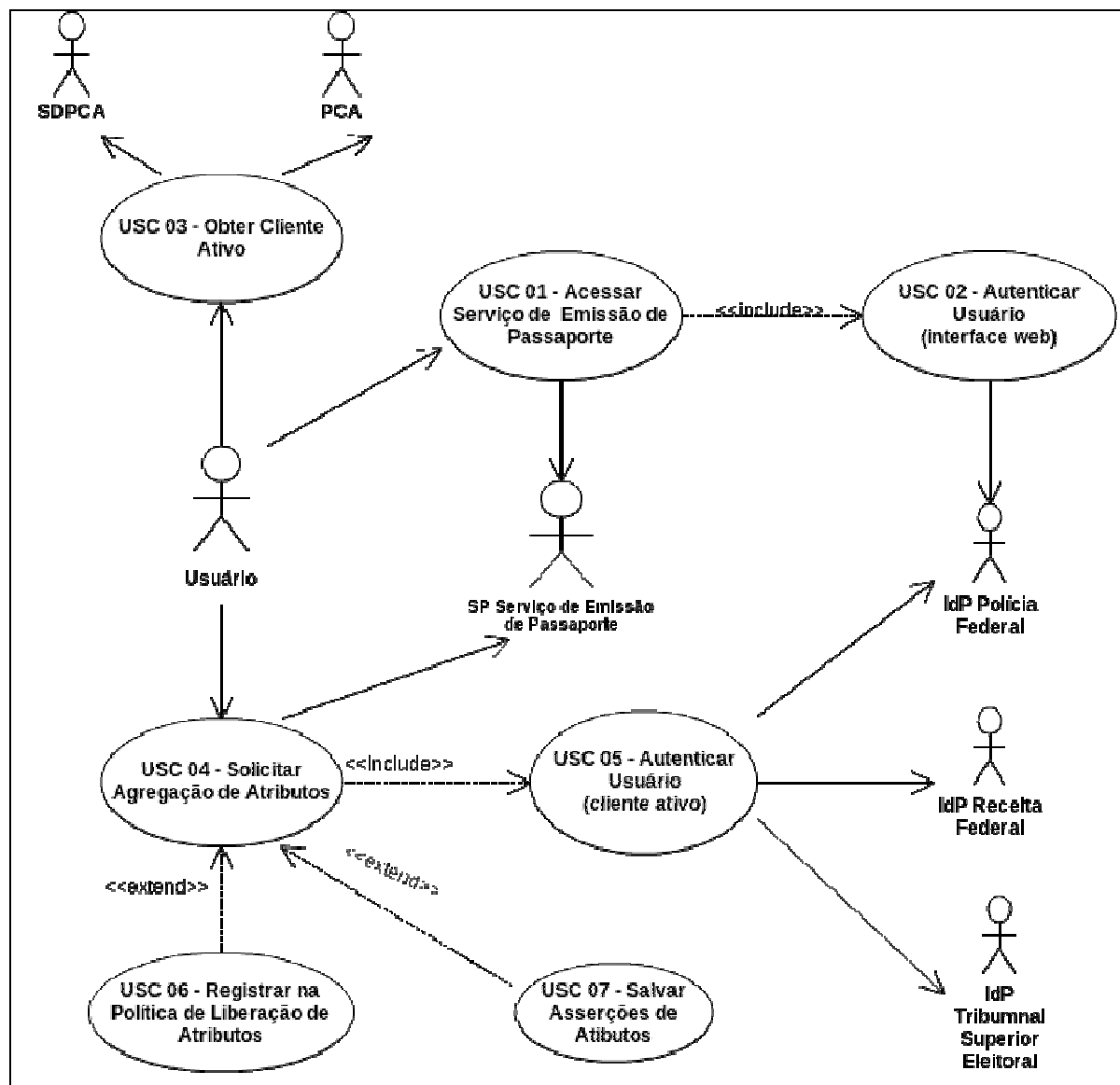


Figura: Diagrama de Casos de uso do Protótipo

## USC 01 – Acessar o Serviço de Emissão de Passaporte

<b>Breve descrição</b>	O usuário deve acessar a página do serviço para solicitar um passaporte
<b>Ator(es) Primário(s)</b>	Usuário, SP do Serviço de Emissão de Passaporte
<b>Pré-condições</b>	O usuário acessar a o portal do provedor de serviços.
<b>Fluxo principal</b>	<ol style="list-style-type: none"> <li>1. O usuário acessa o serviço do SP.</li> <li>2. O serviço apresenta as informações sobre como proceder para solicitação de passaporte.</li> <li>3. O usuário confirma que deseja solicitar um passaporte.</li> <li>4. O sistema redireciona o navegador do usuário para o provedor de identidades da polícia federal para que este se autentique (USC 02)</li> <li>5. Após a autenticação bem sucedida, o serviço apresenta a lista de atributos necessários.</li> <li>6. O usuário confirma que deseja executar o processo de agregação de atributos.</li> </ol>
<b>Fluxos alternativos e exceções</b>	Fluxo alternativo (5): Se a autenticação não for bem sucedida. <ol style="list-style-type: none"> <li>1. O sistema de solicita uma nova autenticação;</li> <li>2. Volta passo 3.</li> </ol>
<b>Pós-condições</b>	Redireciona o navegador do usuário para o SDPCA

## USC 02 – Autenticar usuário (interface web)

<b>Breve descrição</b>	O usuário deve se autenticar no IdP da Polícia Federal
<b>Ator(es) Primário(s)</b>	Usuário, IdP da Polícia Federal
<b>Pré-condições</b>	1. O usuário deve executar o USC 01;
<b>Fluxo principal</b>	<ol style="list-style-type: none"> <li>1. O usuário deve informar seu usuário e senha de acesso;</li> <li>2. O IdP da Polícia Federal deve validar as credenciais de acesso do usuário; e</li> <li>3. O IdP da Polícia Federal deve redirecionar o navegador do usuário para o Serviço de Emissão de Passaporte.</li> <li>4. O SP deve apresentar para o usuário a lista de atributos necessários.</li> </ol>
<b>Fluxos alternativos e exceções</b>	Fluxo alternativo (2): Caso o usuário tenha informado as credencias de acesso inválidas; <ol style="list-style-type: none"> <li>1. O sistema apresenta uma mensagem de erro.</li> <li>2. Volta ao passo 1.</li> </ol>
<b>Pós-condições</b>	O IdP da Polícia Federal redireciona o navegador do usuário para o SP do Serviço de Emissão de passaporte que apresenta a lista de atributos necessários.

## USC 03 – Obter o Cliente Ativo

<b>Breve descrição</b>	O usuário deve acessar o SDPCA selecionar um PCA para então obter o Cliente Ativo.
<b>Ator(es) Primário(s)</b>	Usuário, SDPCA, PCA
<b>Pré-condições</b>	<ol style="list-style-type: none"> <li>1. O usuário deve estar autenticado em um IdP confiável do SDPCA;</li> <li>2. Ao ser redirecionado para o SDPCA, o <i>token</i> de autenticação deve ser transportando junto com a requisição de acesso.</li> </ol>
<b>Fluxo principal</b>	<ol style="list-style-type: none"> <li>1. O SDPCA aceita a autenticação do usuário realizada do IdP da Polícia Federal (<i>token</i> de autenticação) e define uma sessão para este usuário.</li> <li>2. O SDPCA apresenta uma lista de provedores de Cliente Ativo (PCA);</li> <li>3. O usuário seleciona um provedor de sua preferência;</li> <li>4. O usuário confirma que deseja acessar o PCA;</li> <li>5. O sistema redireciona o navegador do usuário para o PCA;</li> <li>6. O PCA informa as instruções de acesso ao Cliente Ativo (CA) para o usuário;</li> <li>7. O usuário confirma que deseja baixar e executar o Cliente Ativo.</li> <li>8. O SDPCA envia o código do cliente ativo para o usuário.</li> </ol>
<b>Fluxos alternativos e exceções</b>	<p>Fluxo alternativo (1): SDPCA não aceita o token de autenticação</p> <ol style="list-style-type: none"> <li>1. O SDPCA redireciona o navegador do usuário para o IdP (USC 02)</li> <li>2. Se autenticação bem sucedida, voltar para o passo 2.</li> </ol> <p>Fluxo alternativo (6): O usuário cancela o <i>download</i> do CA</p> <ol style="list-style-type: none"> <li>1. O PCA apresenta uma mensagem que o <i>download</i> foi interrompido e volta ao passo 2.</li> </ol>
<b>Pós-condições</b>	O Cliente Ativo é executado no computador do usuário

## USC 04 – Solicitar Agregação de Atributos

<b>Breve descrição</b>	O usuário, no uso do Cliente Ativo, deve se autenticar nos IdPs, obter as asserções SAML, realizar a agregação de atributos e apresentar o resultado da agregação para o SP.
<b>Ator(es) Primário(s)</b>	Usuário, SP do Serviço de Emissão de Passaporte, IdP da Polícia Federal, IdP da Receita Federal, IdP do Tribunal Superior Eleitoral
<b>Pré-condições</b>	1. O Cliente Ativo deve estar sendo executado no computador do usuário.
<b>Fluxo principal</b>	<ol style="list-style-type: none"> <li>1. O usuário confirma que deseja realizar a agregação de atributos;</li> <li>2. O cliente ativo tenta acessar o Serviço de Emissão de Passaporte do SP da Polícia Federal;</li> <li>3. O SP redireciona o cliente ativo para o IdP para que o usuário se autentique.</li> <li>4. O usuário informa as suas credenciais de acesso;</li> <li>5. O IdP da Polícia Federal verifica as credenciais de acesso do usuário, e caso a autenticação seja bem sucedida, o cliente ativo é redirecionado para o SP</li> <li>6. O SP do Serviço de Emissão de Passaporte envia para o cliente ativo a lista de atributos necessários;</li> <li>7. O cliente ativo solicita que o usuário indique o IdP para obter o atributo CPF;</li> <li>8. O usuário informa suas credencias de acesso e seleciona o provedor de identidade que contém o atributo requisitado (USC 05);</li> <li>9. O cliente ativo solicita para que o usuário indique o IdP para obter o segundo atributo;</li> <li>10. O usuário informa suas credencias de acesso e seleciona o provedor de identidade que contém o atributo requisitado (USC 05).</li> <li>11. O cliente ativo solicita para que o usuário indique o IdP para obter o terceiro atributo;</li> <li>12. O usuário informa suas credencias de acesso e seleciona o provedor de identidade que contém o atributo requisitado (USC 05).</li> <li>13. O cliente ativo exibe a lista de atributos e valores agregados e pede ao usuário que confirme o desejo de enviar o resultado da agregação para o SP;</li> <li>14. O usuário confirma que deseja enviar seus atributos para o SP;</li> <li>15. O cliente ativo executa automaticamente o navegador Web padrão do usuário, redireciona o navegador do usuário para o SP e envia o resultado da agregação;</li> <li>16. O SP exibe a tela de resumo da agregação, confirmando o resultado do recebimento dos atributos solicitados, gera um número do protocolo e apresenta ao usuário.</li> </ol>
<b>Fluxos alternativos e exceções</b>	<p>Fluxo de exceção (4): Caso o usuário tenha informado as credências de acesso inválidas;</p> <ol style="list-style-type: none"> <li>1. O IdP apresenta uma mensagem de erro.</li> </ol> <p>Volta ao passo 1.</p>
<b>Pós-condições</b>	O SP do Serviço de Emissão de Passaporte gera o protocolo virtual da solicitação do usuário.

## USC 05 – Autenticar Usuário (cliente ativo)

<b>Breve descrição</b>	O usuário deve se autenticar no IdP da Polícia Federal.
<b>Ator(es) Primário(s)</b>	Usuário, IdP da Polícia Federal
<b>Pré-condições</b>	1. O Cliente Ativo deve estar sendo executado no computador do usuário e é redirecionado para o IdP.
<b>Fluxo principal</b>	1. O cliente ativo deve informar o usuário e senha do usuário para o IdP; 2. O IdP deve validar as credenciais de acesso do usuário; e 3. Se autenticação bem sucedida, o IdP envia para o cliente ativo a asserção SAML com o atributo requisitado.
<b>Fluxos alternativos e exceções</b>	Fluxo de exceção (2): Caso o usuário tenha informado as credências de acesso inválidas; 2. O IdP apresenta uma mensagem de erro. 3. Volta ao passo 1.
<b>Pós-condições</b>	O IdP envia asserção SAML para o cliente ativo.

## USC 06 – Registrar na Política de Liberação de Atributos

<b>Breve descrição</b>	Quando o usuário selecionar a opção para registrar a Política de Liberação de Atributos, o cliente deve persistir as asserções agregadas em arquivo.
<b>Ator(es) Primário(s)</b>	Usuário, Cliente Ativo
<b>Pré-condições</b>	1. O cliente ativo deve ter finalizado com sucesso a agregação de atributos.
<b>Fluxo principal</b>	1. O usuário informa ao cliente ativo que deseja realizar o registro das asserções agregadas em sua Política de Liberação de Atributos. 2. O cliente ativo solicita a senha do usuário para te acesso ao seu arquivo de política 3. O usuário informa a senha. 4. O cliente ativo registra o resultado da agregação no arquivo da política de agregação de atributos
<b>Fluxos alternativos e exceções</b>	Fluxo alternativo (3): Caso o usuário tenha informado as credências de acesso inválidas; 1. O IdP apresenta uma mensagem de erro. 2. Volta ao passo 2. Fluxo de exceção (4): O cliente ativo registra o resultado da agregação 1. O usuário indica ao sistema que deseja salvar suas asserções na política de liberação de atributos 2. O sistema salva as asserções do usuário na política de liberação de atributos Se salvamento das asserções na política de liberação de atributos for mal sucedida, voltar para o passo 1
<b>Pós-condições</b>	Após realizar a agregação de atributos com sucesso o cliente ativo armazenará as asserções em um arquivo.



## USC 07 – Salvar Asserções de Atributos

<b>Breve descrição</b>	Quando o usuário selecionar a opção para salvar as asserções SAML retornadas e o resultado da agregação de atributos, o cliente ativo deverá persistir as asserções SAML em arquivos.
<b>Ator(es) Primário(s)</b>	Cliente Ativo
<b>Pré-condições</b>	1. O cliente ativo de estar em execução
<b>Fluxo principal</b>	<ol style="list-style-type: none"> <li>1. O usuário informa ao cliente ativo que deseja salvar as asserções SAML.</li> <li>2. O usuário escolhe o local em seu computador que gostaria de salvar as asserções SAML.</li> <li>3. O cliente ativo grava os arquivos das asserções SAML agregadas dos provedores de identidade.</li> </ol>
<b>Fluxos alternativos e exceções</b>	<p>Fluxo de exceção (3): O cliente ativo grava as asserções SAML recebidas</p> <ol style="list-style-type: none"> <li>1. O usuário seleciona que deseja salvar suas asserções de identidade</li> <li>2. O usuário escolhe um local em seu computador para salvar o documento XML e as asserções SAML</li> <li>3. O sistema salva o documento XAML e as asserções SAML no local escolhido pelo usuário</li> </ol> <p>Se salvamento dos arquivos for mal sucedida, voltar para o passo 1.</p>
<b>Pós-condições</b>	As asserções SAML são armazenada em arquivos na máquina do usuário.