UNIVALI

FORMULÁRIO DE PROJETO DE TRABALHO - PIBIT

1. TÍTULO DO PROJETO DE TRABALHO:

Um Sistema de Gestão de Identidades Federadas e Centrado no Usuário alinhado ao Programa de Governo Eletrônico Brasileiro

2. ÁREA DE CONHECIMENTO: Ciência da Computação (1.03.00.00-7)

2.1 Sub-área de conhecimento: Sistemas de Computação (1.03.04.00-2)
2.2 Grupo de Pesquisa: Grupo de Sistemas Embarcados e Distribuídos (GSED)
2.2.1 Linha de Pesquisa ou Área: Sistemas Distribuídos

3. RESUMO

Um programa de Governo Eletrônico tem como princípio democratizar o acesso à informação, ampliar discussões e dinamizar a prestação de serviços públicos. Um ponto chave para os sistemas ou aplicações de governo eletrônico é a criação de um sistema de identificação, de autenticação e de autorização de usuários. Esses sistemas são conhecidos como sistemas de gestão de identidades, do inglês, *Identity Management (IdM) systems*. No Brasil, o programa GOV.BR, até o momento, não definiu qual será a estratégia nacional de gestão de identidades. Este projeto tem como objetivo prover a gestão de identidades adequada ao programa GOV.BR, por meio do desenvolvimento de um sistema de gestão identidades federadas e centrado no usuário, baseado no padrão SAML. O projeto envolverá (1) a análise das estratégias nacionais de gestão de identidades federadas adotadas em outros países visando identificar as soluções tecnológicas amplamente aceitas nestes países, (2) a modelagem do sistema de gestão de identidades federadas e centrado no usuário, (3) a implementação de um protótipo do sistema e a sua integração em um estudo de caso (aplicação de eGov) para verificação da sua aplicabilidade e (4) a realização de testes de software, que contribuirão para aferir a conformidade com o padrão SAML e os impactos da solução na usabilidade e funcionalidades da aplicação. Por fim, (5) a divulgação dos resultados desta pesquisa, na forma de artigos e relatórios técnicos.

Palavras-chaves: Gestão de Identidades. Governo Eletrônico. Gestão de Identidades Federadas.

4. INTRODUÇÃO

Inúmeros países estão adotando políticas relacionadas à abertura e à transparência de seus governos. Segundo Thibeau e Reed (2009), um governo aberto é a doutrina política que defende que os negócios da administração pública devem ser abertos a todos os níveis, ao escrutínio público. O objetivo real de um governo aberto (*Open Government*) é o aumento da participação do cidadão e o envolvimento destes no governo (THIBEAU e REED, 2009).

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

funções governamentais. Os programas de Governo Eletrônico (e-Gov) bem sucedidos dependem do uso adequado das TICs empregadas nas organizações para promover os trabalhos colaborativos em prol de objetivos comuns (DAWES e PARDO, 2008).

Segundo Thibeau e Reed (2009), o crescente aumento das redes sociais, blogs, mensagens e tecnologias conhecidas como Web 2.0 têm o potencial de aumentar o fluxo de informações entre governos e cidadãos em ambos os sentidos, criando assim um cenário de colaboração.

Muitos países, tais como: Estados Unidos, Nova Zelândia, Itália, Reino Unido e Dinamarca, estão expandindo os seus programas de e-Gov aprimorando as suas infraestruturas de colaboração, sendo que o grande desafio está em garantir a interoperabilidade entre estas infraestruturas devido a heterogeneidade dos procedimentos e dos dados existentes entre a administração pública central e as locais (BALDONI, 2010). Esta diversidade pode tornar difícil a implantação destes programas (OECD, 2011).

No relatório das Nações Unidas sobre governos eletrônicos (UNITED NATIONS, 2014), o Brasil ocupa a 57º posição do ranking mundial de desenvolvimento de aplicações de eGov. Este relatório apresenta ainda um ranking que trata da utilização das aplicações por parte dos cidadãos, chamado E-Participação. Neste ranking, o Brasil ocupa a 24º posição (UNITED NATIONS, 2014).

Um ponto chave para os sistemas ou aplicações de governo eletrônico é a criação de um sistema de identificação, de autenticação e de autorização de usuários. Esses sistemas são conhecidos como sistemas de gestão de identidades (*Identity Management (IdM) systems*) (BALDONI, 2010). A gestão de identidades pode ser entendida como o conjunto de processos e tecnologias usados para garantir a identidade de uma entidade ou de um veículo, garantir a qualidade das informações de uma identidade (identificadores, credenciais e atributos) e para prover procedimentos de autenticação, autorização, contabilização e auditoria (ITU-T, 2009).

Um dos problemas, no caso das aplicações e-Gov, é possibilitar que as aplicações (provedores de serviços) suportem a autenticação única (*Single Sign On*) de usuários. Comumente, as instituições do governo acabam duplicando o cadastro de pessoas já registradas. Outro problema que deve ser tratado no gerenciamento de identidades é a privacidade das informações (HANSEN et al. 2008). Em um cenário ideal, os usuários devem exercer o direito de determinar como suas informações serão manipuladas, informando quais informações poderão ser compartilhadas com terceiros, como esse compartilhamento deve ser feito e também indicando o período de tempo no qual essas informações poderão ficar disponíveis nos sistemas.

Sistemas de gestão de identidades federadas permitem o compartilhamento dos atributos do usuário e a autenticação única através de múltiplos domínios, tornando-se facilitadores para os sistemas governamentais [BALDONI 2012]. Nos últimos anos, alguns governos aprovaram estratégias nacionais de gestão de identidades baseadas no modelo federado buscando melhorar seus serviços de governo eletrônico, dentre estes, destacam-se: Nova Zelândia, Austrália, Canadá e Estados Unidos [OECD 2011].

Neste contexto, este projeto visa contribuir na área de gestão de identidades federadas, mas especificamente para aplicações do Programa de Governo Eletrônico Brasileiro.

5. PROBLEMA

De acordo com Dhamija e Dusseault (2008), os sistemas de gestão de identidades são sistemas complexos, com características poderosas e muitas vulnerabilidades potenciais. Combinados com os requisitos de privacidade e segurança exigidos nestes, criam desafios íngremes de usabilidade e desempenho. Garantir a segurança e a privacidade sem comprometer os requisitos de usabilidade e desempenho torna-se um problema a ser resolvido (DHAMIJA e DUSSEAULT, 2008).

Segundo Dhamija e Dusseault (2008), a gestão da confiança entre as organizações participantes de um cenário de colaboração e seus usuários torna-se um problema crítico, sendo que os sistemas de gerenciamento de identidades devem então prover relações de confiança com seus usuários e demais partes confiáveis envolvidas.

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 afirma ainda que durante as trocas de informações que ocorrem nestes sistemas, os provedores podem rastrear a identidade do usuário e seus acessos. Esta prática pode comprometer a privacidade dos usuários.

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

De acordo com a Organização de Cooperação e Desenvolvimento Econômico – OECD (Organisation for Economic Cooperation and Development), vários países já iniciaram alguma ação em relação à gestão de identidades digitais (OECD, 2011). O governo brasileiro ainda não definiu a estratégia nacional de gestão de identidades a ser adotada nas aplicações de Governo Eletrônico. Visando atender ao requisito de interoperabilidade, o programa de e-Gov do Brasil definiu a arquitetura e-PING (Padrões de Interoperabilidade de Governo Eletrônico), que traz algumas diretrizes para definição de estratégias de interoperabilidade entre sistemas (BRASIL, 2014). Dentre estas, destacam-se o uso do SAML como padrão para a troca de informação sobre autenticação e autorização entre domínios, da especificação WS-Security 1.1 para o fornecimento de segurança às mensagens trocadas e WS-Trust 1.4 para a gestão de relacionamentos confiáveis entre os envolvidos na troca de mensagens seguras (intermediação).

A partir do problema apresentado, tem-se as seguintes questões de pesquisa:

- Dentre as estratégias nacionais de gestão de identidades federadas de outros países, baseadas no padrão SAML, quais soluções tecnológicas atendem as necessidades de um modelo centrado no usuário e estão alinhadas ao Programa de eGov Brasileiro?
- Como conceber um sistema de gestão de identidades federadas centrado no usuário, baseado no padrão SAML, e como prover a gestão da confiança das entidades envolvida?
- Quais são os impactos decorrentes do uso da solução proposta em uma aplicação de eGov, em relação a usabilidade e as funcionalidades da aplicação?

5.1 – Solução Proposta

Este trabalho caracteriza-se como uma pesquisa aplicada e experimental que objetiva desenvolver e avaliar o uso de um sistema de gestão de identidades federadas e centrado no usuário para o programa GOV.BR, adequado as características e diversidades do país. O sistema a ser desenvolvido neste trabalho deverá prover autenticação única em ambientes heterogêneos, atravessando domínios administrativos de segurança mesmo que usem tecnologias de autenticação distintas, tendo como base o padrão SAML (OASIS, 2008).

O uso do modelo centrado no usuário em programas de governo participativo é interessante devido a possibilidade de o usuário selecionar quais informações deseja liberar aos provedores de serviços, respeitando assim a privacidade dos usuários. Na solução proposta, por meio do modelo centrado no usuário, os cidadãos terão a possibilidade ainda de interagir com as aplicações e-Gov a partir de serviços de autenticação comumente utilizados, como por exemplo, o *framework* OpenID Connect ou o *Facebook Connect*.

Na solução proposta, o padrão SAML será usado para representar informações de segurança (credenciais de autenticação) na forma de asserções e na troca dinâmica de informações de segurança entre parceiros da federação governamental. Para que os processos de colaboração G2B, G2G e G2C se concretizem, o sistema proposto deve ainda contemplar um modelo de gestão de confiança (*Trust Framework*) que definirá como as relações de confiança entre os domínios administrativos deverão ser estabelecidas, como os níveis de garantia (*Level of Assurance - LoA*) podem ser definidos e avaliados e quais regras comuns são necessárias para operação da federação de serviços governamentais.

6. OBJETIVOS

6.1. Objetivo geral

Prover a gestão de identidades federadas adequada ao programa de governo eletrônico brasileiro, por meio do desenvolvimento de um sistema de gestão de identidades federadas centrado no usuário.

6.2. Objetivos específicos

- Analisar as estratégias nacionais de gestão de identidades federadas de outros países visando identificar quais soluções tecnológicas atendem as necessidades de um modelo centrado no usuário e estão alinhadas ao programa eGov.BR;
- Conceber um sistema de gestão de identidades federadas centrado no usuário para as redes colaborativas governamentais brasileiras que atenda os requisitos impostos pelo e-PING;
- Verificar a aplicabilidade do sistema proposto por meio da implementação de um protótipo e da sua integração a um estudo de caso – aplicação web de eGov;
- Verificar os impactos do uso do protótipo na usabilidade e funcionalidades da aplicação e Gov.

7. JUSTIFICATIVA

Nos programas de e-Gov, a gestão de identidades pode levar a prestação de serviços on-line eficientes (BALDONI, 2010). Como consequência, nos últimos anos, vários governos têm aprovado diretrizes para melhorar os serviços de e-Gov e as medidas de identificação para acesso a informação individual do cidadão e de registros do governo disponíveis na Web. Segundo Baldoni (2010), a representação da identidade digital e o formato para a troca de informações entre recursos tornam-se problemas críticos, especialmente porque neste cenário cada organização possui sua arquitetura e requisitos.

Para Maler e Reed (2008), a interoperabilidade é um desafio contínuo para prover identidades federadas. No entanto, muitos desenvolvedores estão começando a combinar diferentes soluções, de acordo como estas crescem em popularidade. A possibilidade de combinar diferentes soluções em um ambiente federado voltado para o programa de e-Gov brasileiro é também o foco deste projeto.

Uma das funções básicas oferecidas pelo gerenciamento de identidade federado é a autenticação única (Single Sign-On - SSO) (MALER e REED, 2008). Esta autenticação traz facilidades para os usuários, pois permite que esses passem pelo processo de autenticação uma única vez e usufruam das credenciais obtidas por todos os serviços que desejarem acessar. Garantir tal conceito dentro de um único domínio administrativo e de segurança não é algo complexo, porém garantir o SSO em uma federação com diferentes tecnologias de segurança (credenciais de autenticação) é algo desafiador.

Segundo Gottschalk e Solli-Saether (2008), a gestão de identidades federadas é um mecanismo necessário para implementar políticas eGov interoperáveis em nível nacional. Esse tipo de sistema possibilita a integração de instituições parceiras que fazem parte de uma federação. Por estas características, o sistema a ser desenvolvido neste trabalho seguirá este modelo. As principais soluções de gestão de identidades federadas adotadas em redes acadêmicas e redes colaborativas organizacionais são baseadas na especificação SAML (Shibboleth, WS-Federation e CardSpace). Este padrão também tem sido utilizado nos sistemas de gestão de identidades adotados nas redes colaborativas governamentais de diversos países e por isto foi escolhido como padrão base para a solução proposta.

Enquanto no mundo real uma pessoa escolhe quais informações revelar de si a outras pessoas, levando em consideração o contexto e a sensibilidade da informação, no mundo digital essa tarefa é desempenhada pelo sistema de gestão de identidades. Com objetivo de garantir a privacidade, é

importante que este sistema de gestão possibilite que o usuário controle a liberação de seus atributos para os provedores de serviços (CHADWICK e INMAN, 2013). Tendo como foco a privacidade, a solução proposta também seguirá o modelo centrado no usuário.

7.1. Viabilidade do Projeto

O projeto de pesquisa proposto é viável, pois as bibliotecas e as ferramentas necessárias para o desenvolvimento do protótipo do sistema de gestão de identidades federadas centrado no usuário são de código aberto e bem documentadas. Além disso, algumas destas ferramentas já foram e estão sendo utilizadas em outras pesquisas do grupo de pesquisa. Além disso, o projeto proposto está inserido um projeto maior, já em andamento, que envolve o Ministério da Justiça e a UnB. Este projeto maior envolve a análise das estratégias nacionais de gestão de identidades dos principais países que já possuem soluções implantadas e a definição de uma estratégia nacional a ser empregada no Registro de Identidade Civil (RIC) do Brasil. Alguns estudos bibliográficos já foram desenvolvidos no contexto deste projeto, porém, vale ressaltar, que a concepção de um sistema de gestão de identidades centrado no usuário será realizada na pesquisa aqui proposta. Pretende-se ainda utilizar o ambiente virtual de experimentação em gestão de identidades da RNP (GIdLab) que já oferece uma federação SAML e um ambiente OpenID Connect disponível para realização de experimentos. Por fim, é importante destacar que o candidato a bolsista possui um bom conhecimento no desenvolvimento de aplicações Web em Java, incluindo Serviços Web.

8. REVISÃO BIBLIOGRÁFICA/FUNDAMENTAÇÃO TEÓRICA

Segundo Clauß e Köhntopp (2001), a identidade de uma pessoa é composta por uma grande quantidade de informações pessoais que caracteriza essa pessoa em diferentes contextos dos quais esta faz parte. A identidade é composta pela combinação de subconjuntos, chamados de identidades parciais, sendo que alguns identificam unicamente uma pessoa (p.ex. cpf) e outros não (p.ex. sexo). No contexto de um órgão do governo, a identidade pode estar associada com funções, privilégios, direitos e responsabilidades. Cabe salientar que uma mesma informação pessoal pode estar presente em diferentes identidades parciais.

Um sistema de gestão de identidades provê ferramentas para o gerenciamento dessas identidades parciais em um mundo digital. Segundo Chadwick (2009), a gestão de identidades consiste em um conjunto de funções e habilidades, como administração, descoberta e troca de informações, usadas para garantir a identidade de uma entidade e as informações contidas nessa identidade, permitindo assim que relações comerciais possam ocorrer de forma segura. Assim, um sistema de gerenciamento de identidades consiste na integração de políticas e processos de negócios, resultando em um sistema de autenticação de usuários aliado a um sistema de gestão de atributos.

De acordo com Bhargav-Spantzel et al. (2007), o sistema de gerenciamento de identidades é caracterizado pelos seguintes elementos:

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

Segundo Jøsang e Pope (2005), os sistemas de gestão de identidades seguem modelos classificados como tradicional, centralizado, federado e centrado no usuário. O modelo tradicional ainda é amplamente utilizado nos sistemas atuais. Neste modelo, a autenticação é tratada de forma isolada por cada provedor de serviços. O usuário deve se autenticar em cada serviço que deseja utilizar, pois não existe compartilhamento de identidades entre os provedores de serviços. O modelo tradicional é amplamente utilizado nos atuais sistemas presentes na Internet. Neste modelo, a identificação do usuário é tratada de forma isolada por cada provedor de serviços (SP), o qual também atua como provedor de identidades (IdP). Cabe ao usuário criar uma identidade digital para cada SP que deseje interagir, não havendo assim o compartilhamento das identidades desses usuários entre diferentes SPs.

Apesar de amplamente adotado, o modelo tradicional (isolado) é custoso tanto para usuários quanto para SPs. Cada SP pode exigir um conjunto próprio de atributos para compor a identidade digital do usuário. Por outro lado, um conjunto comum de atributos pode ser exigido por diversos SPs, como nome da conta, senha, endereço, data de nascimento. Para os usuários, gerenciar inúmeras identidades é algo custoso. Primeiro, por ter que fornecer as mesmas informações diversas vezes, segundo, por ter que se preocupar em criar um nome de usuário e senha diferente para cada SP, uma vez que usar a mesma senha por diversos provedores não é aconselhado (WANGHAM *et al.*, 2010).

O modelo centralizado surgiu como uma solução para a inflexibilidade do modelo tradicional e está fundamentado no compartilhamento das identidades dos usuários entre SPs e no conceito de autenticação única (Single Sign-on - SSO) (BHARGAV-SPANTZEL et al, 2007). Neste modelo, só existe um único IdP o qual é responsável por autenticar os usuários, sendo que todos os provedores de serviços devem confiar plenamente nas informações fornecidas por este IdP.

Visando contornar as dificuldades apresentadas pelo modelo centralizado, o modelo de identidades federadas está fundamentado sobre a distribuição da tarefa de autenticação dos usuários por múltiplos IdPs, estando estes dispostos em diferentes domínios administrativos. Um domínio administrativo pode representar um órgão do governo e é composto por usuários, SPs e um único IdP (CAMENISCH E PFITZMANN 2007).

A gestão de identidades federadas é uma abordagem para otimizar a troca de informações relacionadas a identidade através de relações de confiança construídas nas federações. Acordos estabelecidos entre IdPs garantem que identidades emitidas em um domínio sejam reconhecidas por SPs de outros domínios e o conceito de autenticação única é garantido mesmo diante de diferentes domínios. Dessa forma, o modelo de identidades federadas consegue oferecer facilidades para os usuários, pois evita que estes tenham que lidar com diversas identidades e passar diversas vezes pelo processo de autenticação. Para os SPs, o benefício é que estes poderão lidar com um número menor de usuários temporários (CAMENISCH E PFITZMANN 2007).

Jøsang e Pope (2005) consideram a gestão de identidades federadas como um modelo centrado nos Ids. Apesar de haver a distribuição das identidades por diversos provedores, informações desses usuários, uma vez liberadas para esses provedores, podem ser disponibilizadas a terceiros. O modelo centrado no usuário objetiva dar ao usuário o total controle sobre suas identidades digitais, contudo as principais propostas e implementações deste modelo fazem uso de um dos modelos apresentados anteriormente, sendo o modelo de identidades federadas o mais usado.

9. METODOLOGIA

Em relação a metodologia, este projeto se enquadra como uma pesquisa aplicada que visa gerar um protótipo de uma solução tecnológica (sistema de gestão de identidades). Quanto aos objetivos de pesquisa, este projeto se caracteriza como uma pesquisa exploratória uma vez que realizará um levantamento sistemático de soluções similares e/ou que possam contribuir para a composição da solução proposta por este projeto. Nos procedimentos técnicos, será feita uma pesquisa bibliográfica, a qual visa identificar materiais já publicados acerca do assunto, bem como analisar soluções já desenvolvidos. Será utilizada uma abordagem quantitativa no processo de avaliação dos impactos na usabilidade da solução proposta integrada a um estudo de caso. Porém, uma abordagem qualitativa será seguida para avaliação dos impactos em relação à privacidade e as funcionalidades da aplicação. A gestão desse projeto se dará através de reuniões periódicas entre orientador, bolsista e demais colaboradores envolvidos e seguirá uma abordagem ágil. A seguir, tem-se o plano de trabalho e a indicação de alguns procedimentos metodológicos.

9.1 Plano de Trabalho

Ativ.1. Estudo bibliográfico

Esta primeira atividade é destinada à formação do acadêmico-pesquisador, através do estudo sobre gestão de identidade e o seu uso em programas de E-gov. Textos de apoio serão indicados pela orientadora e reuniões periódicas serão realizadas para auxiliar a consolidação da base teórica da pesquisa. Faz parte desta etapa, analisar os sistemas adotados em outros países com o objetivo de selecionar soluções tecnológicas adequadas aos requisitos de programa de E-Gov brasileiro. Como resultado desta etapa, o bolsista deverá redigir um texto sobre os assuntos estudados.

Ativ. 2- Levantamento do estado da arte de trabalhos relacionados a partir da execução de um protocolo de busca.

Ativ.3. Definição e Modelagem do Sistema de Gestão de Identidades Federadas Centrado no usuário

Definir os requisitos funcionais e não funcionais do sistema de gestão de identidades centrado no usuário alinhado aos Programa eGov.BR. A modelagem do sistema será realizada utilizando a linguagem UML e outras técnicas de análise de requisitos.

Ativ. 4- Implementação do Protótipo do Sistema Proposto

Primeiramente, o bolsista investirá um tempo para fazer pequenos experimentos com as bibliotecas que implementam a especificação SAML 2 e com os *frameworks* gestão de identidades federadas abertos tais como o OpenID, OpenAM, SimpleSAMLPHP e Shibboleth. Em seguida, um protótipo do sistema será desenvolvida de acordo com os requisitos elicitados na Ativ. 3.

Ativ. 5 – Avaliar a confirmada com os padrões e especificações recomendados na arquitetura ePING.

O protótipo do sistema de gestão de identidades passará por testes de software (tanto de unidade quanto de integração) visando melhorar sua qualidade e sua conformidade com as especificações utilizadas (p.ex. SAML).

Ativ. 6. Avaliar a Aplicabilidade do Protótipo do Sistema Proposto

O protótipo será integrado a um estudo de caso – uma aplicação de eGov visando avaliar a aplicabilidade e interoperabilidade do protótipo.

Ativ 7 - Avaliar os impactos do uso do protótipo na usabilidade e na privacidade dos usuários, por meio de testes de usabilidade com usuários da aplicação de eGov, testes de segurança automatizados e por meio de uma análise qualitativa de riscos.

Ativ. 8. Documentação e Divulgação de Resultados

Esta etapa compreenderá a produção dos relatórios parcial e final, bem como de um artigo discutindo os resultados alcançados com este projeto de pesquisa, a ser submetido para um evento de iniciação científica.

10. CRONOGRAMA DE ATIVIDADES DE PESQUISA

Ativid.	Ago/14	Set/14	Out/14	Nov/14	Dez/14	Jan/15	Fev/15	Mar/15	Abr/15	Mai/15	Jun/15	Jul/15
Ativ. 1												
Ativ. 2												
Ativ. 3												
Ativ. 4												
Ativ. 5												
Ativ. 6												
Ativ. 7												
Ativ. 8												

11. REFERÊNCIAS

BALDONI, R. Federated Identity Management Systems in e-Government: the Case of Italy. **Electronic Government**: An International Journal. v. 8, n. 1, 2010.

BHARGAV-SPANTZEL, A., CAMENISCH, J., GROSS, T., e SOMMER, D. User centricity: a taxonomy and open issues. **Journal of Computer Security**, v. 15, n. 5, p. 493–527, 2007.

CAMENISCH, J; PFITZMANN, B. Federated Identity Management. In: PETKOVIĆ, M; JONKER, W (eds.). **Security, Privacy, and Trust in Modern Data Management**. Berlin; Heidelberg: Springer Verlag, 2007. p. 213-238, cap. 5.

CHADWICK, D. Federated identity management. In: ALDINI, A.; BARTHE, G.; GORRIERI, R (eds). **Foundations of Security Analysis and Design V**. Berlin; Heidelberg: Springer-Verlag, 2009. p. 96–120.

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

CLAUß, S. e KÖHNTOPP, M. Identity management and its support of multilateral security. **Computer Networks**, v. 37, n. 2, p. 205–219, 2001.

DAWES, S. S. e PARDO, T. A. Advances in Digital Government Technology, Human Factors, and Policy, chapter Building Collaborative Digital Government Systems Systemic: constraints and effective practices, pages 259-273. Springer, US, 2008.

GOTTSCHALK, P.; SOLLI-SAETHER, H. Stages of e-government interoperability. **Electronic Government**: An International Journal, v. 5, n. 3, p. 310–320, 2008.

HANSEN, M.; SCHWARTZ, A.; COOPER, A. Privacy and identity management. **Security Privacy**, IEEE, v. 6, n. 2, p. 38 –45, 2008.

JOSANG, A; POPE, S. User centric identity management. *In*: **AusCERT Asia Pacific Information Technology Security Conference**, 2005, Gold Coast, Australia. 2005. p. 1-13.

ITU. NGN identity management framework. [S.l.]: International Telecommunication Union (ITU), 2009. Recommendation Y.2720.

LEWIS, J. A. **Authentication 2.0** - new opportunities for online identification. Center for Strategic and International Studies: Technical report, 2008. Disponível em: <http://csis.org/files/media/csis/pubs/080115_authentication.pdf>. Acesso em: 10 jun. 2014.

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

ONU. United Nations. **E-Government Survey**. 2014, Disponível em: <http http://unpan3.un.org/egovkb/Reports/UN-E-Government-Survey-2014 >. Acesso em: 10 jun. 2014.

MALER, E.; REED, D. The venn of identity: Options and issues in federated identity management. **Security Privacy**, IEEE, v. 6, n. 2, p. 16–23, 2008.

THIBEAU, D. e REED, D. Open trust frameworks for open government: Enabling citizen involvement through open identity technologies. White paper, OpenID Foundation and Information Card Foundation. 2009.

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.