Um Mecanismo de Agregação de Atributos para um Sistema de Gerenciamento de Identidades Federado Alinhado ao Programa de Governo Eletrônico Brasileiro

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

[1]Centro Universitário para o Desenvolvimento do Alto Vale do Itajaí (UNIDAVI), SC

[2]Universidade do Vale do Itajaí (UNIVALI) – Itajaí, SC - Brasil

marcondes@unidavi.edu.br.br, wangham@univali.br

Resumo. *Este trabalho descreve um mecanismo para agregação de atributos que pode ser integrado a um sistema de gerenciamento de identidades federado e centrado no usuário. O mecanismo proposto segue o modelo de agregação baseado em clientes ativos e está alinhado ao programa de governo eletrônico brasileiro, tendo como norte as regas impostas pela arquitetura E-Ping. O mecanismo visa ainda garantir a privacidade dos usuários (de seus atributos).*

1. Introdução

No modelo tradicional de gerenciamento de identidades, amplamente utilizado nos atuais sistemas computacionais presentes na Internet, a identificação do usuário é tratada de forma isolada por cada provedor de serviços, o qual também atua como provedor de identidades. Cabe ao usuário criar uma identidade digital para cada provedor de serviços que deseje interagir, não havendo assim o compartilhamento das identidades desses usuários entre diferentes provedores de serviço (Wangham et al, 2010).

Comumente, as organizações acabam criando duplicidades em seus sistemas de autenticação, isso pode se tornar um caos, duplicando informações em várias bases de dados separadas, e criando para o usuário um grande complicador, que é o gerenciamento de várias contas em várias aplicações diferentes. Segundo Baldoni (2010), uma solução para o problema descrito acima é o modelo de gerenciamento de identidades federadas (FIDM, do inglês *Federated Identity Management*).

A maioria dos sistemas de gerenciamento de identidades que seguem o modelo de identidade federada restringe a fonte de identidade e de atributos a um único provedor de identidades (IdP) em qualquer sessão criada com um provedor de serviços (SP) (Klingenstein, 2007). Com isto, as autorizações são limitadas a um subconjunto de atributos da identidade do usuário. Para muitos serviços baseados na Web, isto não é o suficiente. O que é necessário é um mecanismo que permite agregar os atributos de um usuário a partir de múltiplos IdPs em uma sessão única, processo conhecido como **agregação de atributos**. Em alguns mecanismos, a união dos atributos, pode ser processada por uma terceira parte confiável. (Chadwick e Inman, 2009). Essa terceira parte confiável mantem um controle melhor das informações do usuário como é o caso do Sistema CardSpace da Microsoft (Chadwick e Inman, 2009).

O objetivo deste trabalho é desenvolver um mecanismo de agregação de atributos para um sistema de gerenciamento de identidades federado que seja centrado

no usuário, alinhado ao programa de Governo Eletrônico Brasileiro (E-GOV.BR), e que garanta a privacidade dos usuários.

2. Solução Proposta

O mecanismo de agregação de atributos proposto segue uma arquitetura orientada a serviço (AOS) e oferece um controle centrado no usuário, ou seja, todo o processo para agregação de atributos deve ser controlado pelo cidadão e não por uma terceira parte confiável. Para garantir isto, o mecanismo segue o modelo de agregação mediada pelo cliente, no qual um cliente ativo é responsável por associar identidades parciais dos usuários (conjunto de atributos) distribuídas em diferentes IdPs a fim de coletar as múltiplas identidades dos usuários. A solução visa garantir a privacidade dos usuários minimizando o conhecimento dos IdPs sobre as associações de identidades e garantindo o total controle do usuário sobre a criação, manutenção e privacidade das informações.

Este mecanismo está ainda alinhado às recomendações da arquitetura E-Ping do Brasil (BRASIL, 2011). Para tal os provedores de identidade podem ser implementados com padrões SAML ou com tecnologias que seguem a especificação WS-Trust. Os atributos coletados serão consolidados em asserções SAML e serão repassados pelo cliente ativo ao provedor de serviço. Para garantir a heterogeneidade no uso de múltiplas identidades parciais, o mecanismo de agregação de atributos será ainda integrado com mecanismos de transposição e tradução de credenciais (de Mello, 2009). Com o mecanismo, pretende-se garantir o controle do usuário, sem impedir seu acesso a serviços e sem prejudicar sua experiência de uso da ferramenta. O cidadão poderá ainda utilizar como credencial (fonte de atributos) o novo Registro de Identidade Civil (RIC) Brasileiro.

O presente trabalho encontra-se em andamento e em fase de analise e modelagem do mecanismo de agregação.

Referências

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

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

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

DE MELLO, E. R., WANGHAM, M. S., da S. FRAGA, J., CAMARGO, E., e da S BÖGER, D. (2009). Model for authentication credentials translation in service oriented architecture. Transactions on Computational Sciences Journal, 5430:68–86.

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

WANGHAM, Michelle S. MELLO, Emerson Ribeiro de. BÖGER, Davi da Silva. GUERIOS, Marlon. FRAGA, Joni da Silva. (2010) “Gerenciamento de Identidades Federadas**”**. In: Minicurso SBSEG 2010, Capítulo 1.