Gestão de Identidades na Web das Coisas: Um Estudo de Caso em Saúde Eletrônica

Marciel de Liz Santos[1,2], Marlon Domenech[1*], Michelle S. Wangham[1]

Universidade do Vale do Itajaí (UNIVALI) – Itajaí, SC – Brasil

Centro Universitário par o Desenvolvimento do Alto Vale do Itajaí - UNIDAVI

marciel.dls@gmail.com, marloncdomenech@gmail.com, wangham@univali.br

Abstract. *Providing identity management (IdM) in the scene of Web of Things (WoT) is an important requirement to ensure protection of information made available or consumed by the devices in WoT. This work aims to assess impacts caused in an application of electronic health (e-health) arising from the use of an IdM system user-centered that is based on OpenID Connect standard and that attends the requirements for this WoT application. Security, performance, functionality and usability tests will be performed to assess the impacts of the use of the proposed IdM system in an e-health Web application.*

Resumo. *Prover a gestão de identidades (IdM) no cenário da Web das Coisas (WoT) é um requisito importante para garantir a proteção de dados disponibilizados ou consumidas por dispositivos na WoT. Este trabalho visa avaliar os impactos causados em uma aplicação de saúde eletrônica (e-health) decorrentes do uso de um sistema de IdM centrado no usuário que faz uso do OpenID Connect e que está alinhado aos requisitos exigidos por esta aplicação. Testes não funcionais, incluindo os de segurança, serão executados para avaliar os impactos decorrentes do uso do sistema de IdM proposto por uma aplicação Web de assistência médica remota.*

1. Introdução

O conceito de Internet das Coisas (*Internet of Things*, IoT) abrange uma infraestrutura de hardware, software e serviços que conectam objetos físicos à rede de computadores. Estes objetos são participantes ativos nos processos de negócios e nas trocas de dados, que incluem suas identidades e informações de seu ambiente [CTEC 2008].

Outro conceito importante no cenário de IoT é o de Web das Coisas (*Web of Things* – WoT). A WoT objetiva a interação entre dispositivos da IoT através do uso de protocolos Web difundidos na Internet, o que facilita a interação entre os próprios dispositivos e também entre dispositivos e outras aplicações da Internet [GUINARD e TRIFA, 2009]. Uma maneira para permitir este tipo de interação se dá através do uso da arquitetura REST (*Representational State Transfer*), a qual funciona com base no protocolo HTTP (*Hypertext Transfer Protocol).*

Com a ascensão da Internet das Coisas, os serviços médicos estão sofrendo grandes modificações, constituindo *cyber-physical systems* (CPSs) específicos para a assistência

* Bolsista CAPES.

médica (monitoramento e controle) via Internet [Aramudhan e Mohan 2010]. Os serviços de saúde eletrônica (*e-health*) requerem a garantia de diversos requisitos de segurança, uma vez que a informação é altamente sensível e que os dispositivos, muitas vezes móveis e sem fio, estão expostos na Internet contendo diversas informações do ambiente em que estão inseridos e dos pacientes [Peyton et al. 2007, Mirkovick et al 2011]. Nestes serviços, é necessário prover a autenticação dos dispositivos e dos usuários e prover o controle de acesso às informações que os dispositivos e usuários irão oferecer ou consumir [Aramudhan e Mohan 2010]. Uma forma de prover estes mecanismos é através de uma Infraestrutura de Autenticação e de Autorização (IAA).

Com uma IAA, é possível implantar a gestão de identidades (*Identity Management* – IdM) [Liu et al. 2012]. IdM pode ser entendida como o conjunto de processos e tecnologias usados para garantir a identidade de uma entidade ou de um dispositivo, 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]. As entidades envolvidas em um sistema de IdM são: (i) usuário ou dispositivo, entidade que utiliza um serviço fornecido por um provedor de serviços; (ii) provedor de identidades (*Identity Provider* – IdP), responsável por manter a base de dados de usuários do domínio e validar suas credenciais (autenticar usuários); e (iii) provedor de serviços (*Service Provider* – SP), que oferece recursos ou serviços aos usuários. Os sistemas de IdM seguem modelos classificados como tradicional, centralizado, federado e centrado no usuário [Jøsang e Pope 2005].

Este trabalho tem por objetivo avaliar os impactos causados pelo uso de um sistema de IdM centrado no usuário por um sistema de assistência médica remota no cenário da WoT. No sistema de IdM proposto, a autenticação de usuários e de dispositivos e o estabelecimento das relações de confiança entre usuários, IdPs e SPs são providos pela IAA *OpenID Connect*[1]. De forma a avaliar a aplicabilidade do sistema de IdM e os impactos decorrentes do seu uso em um CPS de assistência médica remota, um protótipo do sistema está sendo desenvolvido fazendo uso de hardwares abertos, de dispositivos de monitoramento de sinais vitais e de serviços web *restful*. Experimentos serão realizados para quantificar os impactos no desempenho da rede e no uso dos recursos computacionais dos dispositivos, quando o sistema de IdM é empregado.

2. Solução Proposta

Diante das características dos sistemas (CPSs) de Assistência Médica Remota e da Web das Coisas, a escolha pelo modelo de IdM centrado no usuário se justifica por permitir (1) que usuários tenham controle sobre o fluxo de liberação de seus atributos para os SPs[2], (2) que usuários possam escolher o IdP, (3) que usuários possam trocar de IdP sem a preocupação de perder acesso aos serviços e, por, (4) dificultar o rastreamento das informações do usuário. Estas características contribuem para a garantia da privacidade dos usuários, requisito importante em aplicações de *e-health*.

Dentre as IAA que implementam o modelo de IdM centrado no usuário, o *OpenID Connect* possui diversas características que justificam sua adoção no cenário proposto. É uma solução formada pela integração do *OpenID*[3] com o *OAuth 2.0*[4], e é gratuita, aberta e

[1] http://openid.net/connect/

[2] No OpenID Connect, estes são conhecidos como Partes Confiantes (*Rely Parties*).

[3] http://openid.net/

descentralizada (nenhuma autoridade central aprova ou registra as partes confiantes ou provedores de serviços). Este padrão utiliza apenas pedidos e respostas HTTP, por isso não exige nenhuma capacidade especial do software cliente e não está vinculada à utilização de *cookies* ou à utilização de qualquer outro mecanismo específico de gerenciamento de sessão do SP. Esta integração provê uma solução mais segura quando comparada ao OpenID e ao próprio OAuth, contornando os ataques de *phishing*, *cross-site scripting (CSR)*, *cross-site request forgery* (CSRF), dentre outros.

Outra característica muito importante no contexto deste trabalho é que, devido ao uso do *OAuth 2.0*, no *OpenID Connect*, é possível que clientes sejam não apenas navegadores web, mas também scripts ou outros dispositivos (devido ao uso de uma API REST), o que possibilita que este provedor seja usado para autenticação não apenas de usuários, mas de dispositivos inteligentes que enviam dados para a aplicação de assistência médica remota. Vale destacar ainda que não foi encontrado na literatura nenhum trabalho no cenário de saúde eletrônica que faça uso do *OpenID Connect*.

A Figura 1 ilustra os passos necessários (1 a 6) para que um usuário acesse os dados (sinais vitais de um paciente) dos dispositivos médicos disponibilizados como recursos via *smart gateway* (serviços *restful*). Quando um usuário tenta acessar um recurso protegido, o navegador é redirecionado para um *OpenID Connect Provider (OAuth Server)* para que o usuário proceda com a autenticação. Outro fluxo ilustrado (A a D), refere-se aos passos para que um dispositivo médico envie para uma aplicação web de assistência médica os dados monitorados do paciente. Neste fluxo, ocorre o processo de autenticação do dispositivo (no caso do *smart gateway*) para que este possa publicar dados na aplicação web que também exige autenticação.

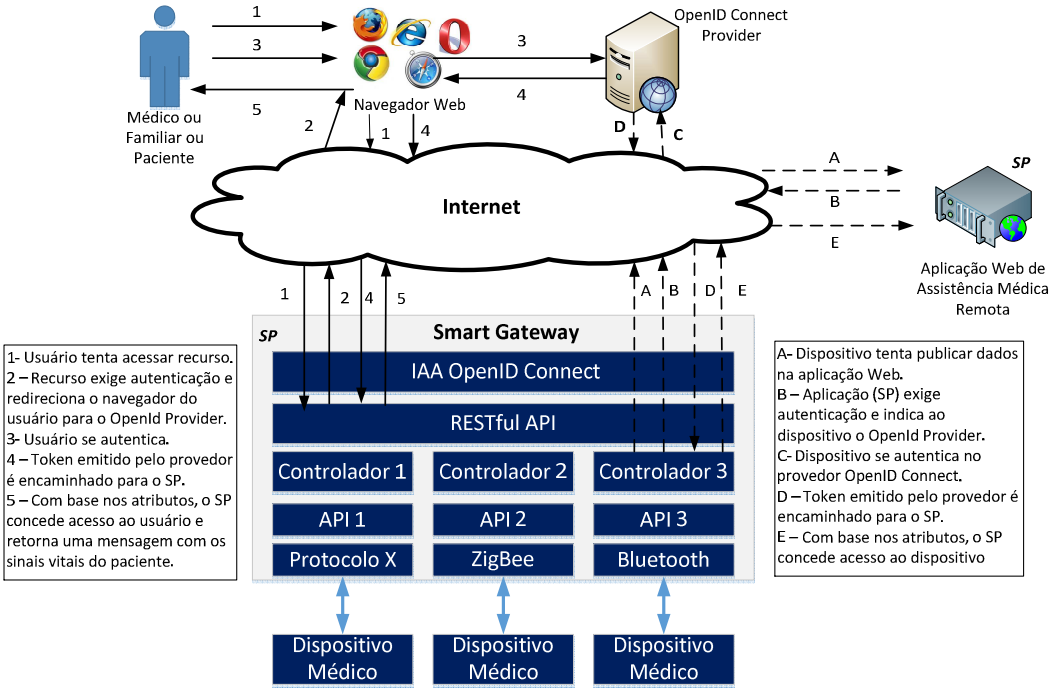

Figura 1- Uso do OpenID Connect por um CPS de Assistência Médica Remota

[4] http://oauth.net/

4. Considerações Finais

A análise e projeto do sistema de assistência médica via WoT e da IAA que faz uso do OpenID Connect já foi concluída. Atualmente, um protótipo está sendo implementado e estão sendo utilizados o RaspeberyPi, como *smart gateway*, a implementação OpenIDConnect do MITRE e a linguagem Java, para implementar os serviços web *restful* e a aplicação Web de assistência médica. Nos experimentos de avaliação, serão consideradas as seguintes métricas: latência e *throughput* (desempenho da rede) e o uso dos recursos computacionais dos dispositivos (consumo de memória, consumo de CPU, espaço de armazenamento utilizado e consumo de energia), quando o OpenID Connect é empregado.

Referências

Aramudhan, M. e Mohan, K. (2010). "New Secure Communication Protocols for Mobile E-Health System", In: Communications in Computer and Information Science, Networked Digital Technologies, 1, Volume 88, Prague. Proceedings…, Springer Berlim Heidelberg, Prague, p. 639-647.

CTEC (2008). "Future networks and the internet: Early Challenges regarding the "Internet of Things"", Commission Staff Working Document, European Union.

Guinard, D. e Trifa, V. (2009), "Towards the Web of Things: Web Mashups for Embedded Devices", In: International World Wide Web conferences, Proceedings of Workshop on Mashups, Enterprise Mashups and Lightweight Composition on the Web, 9, 2009, Piscataway. Proceedings…, IEEE Press, Piscataway, p. 196-199.

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

ITU-T (2009), "NGN identity management framework. Recommendation Y.2720", http://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Y.2720-200901-I!!PDF-E&type=items, Maio 2013.

Liu, Jing, Xiao, Yang e Chen, C.L.P. (2012), "Authentication And Access Control in the Internet of Things", In: 32nd International Conference, Distributed Computing Systems Workshops, 32, 2012, Macau, Proceedings…, IEEE Computer Society, Macau, p. 588-592.

Mahalle, Parikshit et al. (2010), "Identity Management Framework towards Internet of Things (IoT) Roadmap and Key Challenges", In: Recent Trends in Network Security and Applications. 1, Volume 89, 2010, Aalborg. Proceedings…, Springer Berlin Heidelberg, Aalborg, p. 430 – 439.

Mirkovic, J., Bryhni, H. e Ruland, C.M. (2011), "Secure solution for mobile access to patient's health care record", In: 13th IEEE International Conference, E-health Network Applications and Services, 13, 2011, Columbia. Proceedings…, IEEE Computer Society, Columbia, p. 196-303.

Peyton, L. et al. (2007), "Addressing Privacy in a Federated Identity Management Network for E-health", In: Eight World Congress WCMeB 2007, 8, Toronto. Proceedings..., IEEE Computer Society, Toronto, p. 12.

