Identity Management in E-Health: A Case Study of Web of Things application using OpenID Connect

Marlon Cordeiro Domenech, Eros Comunello and Michelle Silva Wangham
Laboratory of Embedded and Distributed Systems and 4Vision Lab
University of Vale do Itajaí – Florianópolis, Brazil
{marloncdomenech, eros.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 user data made available or consumed by the medical devices in WoT. This work aims to purpose the use of a user-centric IdM system in an ambient assisted living (AAL) environment in the WoT scenario. The IdM system is based on OpenID Connect that attends some of the main security requirements of an AAL environment.**

I. Introduction

Population growth have required a more broad and efficient health system [1]. It should be noted the need of new technological solutions to take care the increasing number of people with chronic illness or elderly with frail health [2]. In this sense, the concept of *ambient assisted living* (AAL) became interesting because it covers whole medical assistance to patients in their houses, trying to keep them independent of the health infrastructures, like hospitals [2], [3].

Enabling technologies for AAL communications include ubiquitous computing, wireless communication, and intelligent user interfaces. These technologies can be specially adapted to the different health conditions of the patients [2]. AAL has a strong relationship to "Ambient Intelligence", which is one technology leading to the Internet of Things (IoT)[3]. The IoT concept covers a hardware, software and services infrastructure that connect physical objects to the Internet [4]. The IoT is supposed to being capable of providing all characteristics necessary for an AAL environment. The possibility of having low-cost devices monitoring patient's health condition in real time contributes for making possible AAL. The integration with cloud services is facilitated, due to the full connectivity of these devices with the Internet [4].

An important concept in the IoT scenario is the Web of Things (WoT). The WoT aims the interaction among IoT devices using Web protocols. It facilitates the communication among devices and other Internet applications [5]. A way to permit this interaction is through the use of RESTful web services. Such web services follow the REST (REpresentational State Transfer) architectural principles. The characteristics of the web make it a good choice for sharing health information in an interoperable and friendly way with the patient and professionals involved in his/her treatment.

The technological development of AAL solutions has raised questions about the patient's right to privacy. In the cases that the distribution of health information is necessary, the patients must be consulted beforehand [6]. Due to the sensitive nature of medical data, it must be accessed just by the patient and those people who are directly involved in his/her treatment. Consequently, appropriate security mechanisms must be provided. Such mechanisms must provide privacy while they allow data access just for authorized people [7].

In an AAL environment, services embedded in medical devices (cyber-physical systems - CPSs) need to ensure several security requirements, due to the high sensitivity of the information and due to the exposure of the devices on the Internet [8], [9]. In these environments, it is necessary to provide device and user authentication. It is also necessary to provide access control to the information that is going to be consumed or offered by the devices [10]. A way to provide such mechanisms is through the use of an Authentication and Authorization Infrastructure (AAI).

An AAI makes it possible to provide Identity Management (IdM) [11] in an AAL environment. IdM is the set of processes and technologies used to guarantee (i) the identity of an entity or a device, (ii) the quality of identity information (identifiers, credentials and attributes) and (iii) for providing authentication, authorization and audit services [12].

In this paper, we describe the use of user centric IdM system in an AAL environment in the WoT scenario. In the proposed solution, the OpenID Connect framework is used to authenticate users and devices and to establish the trust relationships among users and other entities. The remainder of this paper is structured as follows. The Section II reviews some concepts relating to IdM and IoT. The Section III presents some related works. The use of OpenID Connect with the e-health application is presented in the Section IV. The Section V presents a case study and Section VI concludes the paper.

II. Background

This section presents the main concepts and technologies related to the research problem and to the proposed solution.

A. Identity Management in E-Health systems

An IdM system has three main entities [13]: (i) Identity Provider (IdP), responsible for generating identities, for maintaining user information and for authenticating users; (ii) Service Provider (SP), which offers resources and services to users; and (iii) the user or device, the entity that uses a service and needs to be authenticated.

IdM systems follow models classified as traditional, centralized, federated and user-centric [13]. In the traditional model, the SP operates as both SP and IdP. In this model

978-1-4799-6644-8/14/$31.00 ©2014 IEEE

there is no identity sharing among SPs. Thus, for each SP, the user has different identifiers and credentials [13].

In the centralized model, there is only one IdP trusted by users and SPs. Sharing of user's identity information among SPs and Single Sign-On (SSO) are possible. SSO enables user to authenticate once and to use the authentication with all the SPs. However, the IdP is a single point of failure. Also, as the IdP has control over user's identity information, it may do whatever it wants with such information [13].

In the federated model, IdP's functions are shared among several IdPs, localized in different security domains. A federation is composed by IdPs and SPs of different domains. SPs accept the authentication token issued by an IdP, due to trust relationships established among IdPs and SPs in the federation. Federated model solves the single point of failure problem of the centralized model and offers facilities to the users, because they do not have to authenticate many times, as well they do not have to cope with many identities [13].

Nevertheless, in the centralized and federated models there is a lack of user control over identity information stored on the IdP, because the IdP controls such information and can disclose it to third parties (e.g. SP). User-centric model solves this problem. This model aims to give more control to the user over transactions that involve his identity data [13]. For example, in some IdM systems the disclosure of identity attributes is conditioned to user consent. Implementations of this model are made in the basis of one of the presented models, where the federated model is the most used.

User-centric IdM model is more appropriate to e-health applications, because it allows users to have control over identity information (e.g. user attributes) and over the release of such information. Thereby, user's privacy requirements can be met, a need highlighted by [6], [7]. In some circumstances, different users (e.g. patient, health professionals) localized in different security domains may need access to patient's health data. In such situations, users may not use the same IdP for authentication, what makes the federated model more adequate.

OpenID is an open framework focused on user's digital identity that adopts both the user-centric IdM model and the federated IdM model [14]. OpenID allows Internet users to access different sites with a single digital identity, what eliminates the need of different user names and passwords for each SP, thus providing SSO. OpenID is decentralized, what means no central authority approves or registers relying parties. With OpenID, a user can choose the OpenID Provider (IdP) he wants to use (e.g. Yahoo or Google). **OpenID Connect 1.0** is a simple identity layer on top of the OAuth 2.0 protocol. It allows Clients (SPs) to verify the identity of the user based on the authentication performed by an Authorization Server (OpenID Provider), as well as to obtain basic profile information about the user in an interoperable and REST-like manner [15].

The inclusion of OAuth 2.0 in OpenID architecture made possible to have non web browser clients, such as web applications or devices. Thus, an OpenID Connect Provider can be used not just for user authentication, but also for authenticating smart devices and applications. In the scenario of e-health applications, especially those included in the AAL concept, it is an important feature.

B. Internet of Things

According to [16], the basic idea of IoT consists on the presence of a plurality of objects that interact and cooperate to achieve a common goal. In IoT, things share information using unique addressing schemes and standardized communication protocols. In smart environments contexts, like AAL environments, information generated by an object can be shared among several platforms and applications.

Main characteristics of IoT are (i) resource restrictions as memory (RAM or ROM), processing power and energy; (ii) restrictions of communication mechanisms, which are mostly wireless, have low transmission power and low data rate; (iii) heterogeneity of technologies and devices; (iv) the large number of invisible computers or devices in an environment that collaborate with the user, forming a ubiquitous and pervasive environment; and (v) the possibility of interactions among users and things in the physical and virtual world [14], [16].

Concretization of the IoT is possible through the use and integration of several enabling technologies (e.g. RFID, Wireless Sensor Network, and NFC) [16]. This integration leads to the creation of a variety of smart environments, composed of heterogeneous devices. Due to this heterogeneity, there is a trend in current research to treat IoT as Web of Things (WoT), where Web's open standards are used to provide sharing of information and interoperability among devices [17].

For integrating things to the Web there are two methods: direct and indirect integration. Direct integration requires all things to have an IP and an embedded web server. However, not all devices can afford the computational cost of embedding a web server, and it is not always necessary to integrate directly to the Web. For these cases, the solution is the indirect integration, on which a smart gateway may be used [17].

Smart gateway is a component that allows web interaction with different types of embedded devices. *Smart gateway's* function is to integrate proprietary APIs of embedded devices and to expose features of such devices as resources identified by a URI, directly accessible in the Web and manipulable through the use of HTTP protocol [14].

In the WoT context, a widespread software architectural style is the REST (REpresentational State Transfer) [18]. Due to the simplicity, flexibility, lightness, loose coupling, uniform interfaces and stateless interactions promoted by REST, RESTful web services paradigm is preferred for *ad-hoc* integration in the Web. RESTful web services enable more seamless integration of devices of WoT with global networks, such as the Internet [17].

Security is one of the obstacles to overcome to the effective use of WoT in e-health scenario. Some security properties need to be ensured, as (i) confidentiality, (ii) integrity, (iii) services availability, (iv) authenticity of both consumer and data provider and (v) privacy, which refers to the need of mechanisms to control exposure of user's data [19].

Based on these security properties, some security requirements exist for the WoT applications. In [20] some security requirements are pointed out: (i) identity management (IdM), especially identification, authentication and authorization of users and devices; (ii) secure data communication, including

authentication of communicating peers, assuring data confidentiality and integrity; (iii) secure network access, assuring access to the network or services just for authorized devices; and (iv) tamper resistance, keeping the device secure even when facing a physical attack.

III. Related Works

A solution for secure access to Electronic Health Records (EHR) using mobile device is proposed in [8]. Four entities compose the solution: (i) user, who wants to access the EHR; (ii) SP, which provides the EHR service; and (iii) two different authentication services, which together authenticate the user to the SP. This solution enables secure communication and authentication between a user (using a mobile application) and an SP. HTTPS protocol and two factor authentication (PIN code and One Time Password) are used as security mechanisms. However, the proposed solution does not address the publication of user's health data in an SP. The authentication services are centralized and are not a widely known solution, what affects the interoperability. Use of medical devices as SPs or as publishers of user's health data in SPs (Machine-to-Machine - M2M communication) is not addressed.

A scenario of a Health Service Provider (HSP) that wants to access patient's data stored in another HSP is addressed in [21]. An approach of federated IdM is proposed, where an IdP in the same domain of an HSP has a trust relationship with IdPs of other domains. For protecting patient's privacy, each HSP uses a local identifier for a patient. An algorithm proposed by the authors is used for converting the patient's local ID into a global ID, used to refer to the patient within the federation. An IdP that receives a data request referring to the global ID can discover the user's local ID. A trusted third party, called mediator, is proposed for helping in this conversion. Mediator does not store patient's local IDs, ensuring that there is no user tracking in HSPs. In this work, the protocol for the exchange of messages is proprietary what affects interoperability and M2M communication is not addressed.

In [22] is proposed an IdM system for e-health based on Service Oriented Architecture (SOA), in which systems expose their functionalities as services. A user-centric approach is used, enabling the patient to control the release of identity attributes to SPs, as well as the choice of the most appropriate identity for each access. User's identity is registered in a central IdP, which is responsible for the creation of national e-IDs for each user. In this work, the use of SAML guarantees interoperability of attributes and SSO authentication. Nevertheless, M2M communication is not addressed.

A federated IdM approach for e-health using Liberty Alliance framework is presented in [9]. Liberty Alliance framework leverages the privacy of patient identity using pseudonyms. Such message exchange happens among federation entities only after user consent. However, Liberty Alliance framework has some breaches of privacy and does not comply with some aspects of the legislation related to privacy. So, the authors' proposal is to include an audit service in the framework, which serves to log operations made with sensitive data. Audit trails aim at giving traceability to operations made with user data. Thus, the solution can not prevent privacy of being compromised. To augment systems privacy, logs are recorded so as to avoid correlation with patient's identity data. Access control happens on user's health data in an SP, as well as on applications publishing in user's behalf. However, the paper does not focus in M2M communication.

Proposal described in [7] aims to increase user privacy by using identity pseudonymization[1], metadata obfuscation and anonymous authentication. In the proposed mechanism, the user may divide his identity into several sub-identities, which have data chosen by the user. For each sub-identity, a pseudonym is created and the user can choose the sub-identity he wants to use in each situation. However, the proposal provides a proprietary mechanism, what affects interoperability with other systems. The work focuses just on user IdM and does not address medical devices publishing user's health data.

A federated IdM framework for distributed e-health systems, with privacy preserving features, is proposed in [6]. In the proposal, the user can use different pseudonyms in each HSP. Aggregation of data from different HSPs is possible after user consent. Aggregation is made without breaking the secrecy of the user's real identity. However, a trusted authority can break user's anonymity if needed. Thus, privacy is provided to the user about his identity (that can be violated, in case of need) and about his data (that can be correlated after user consent). A weakness of the framework is that it trusts in the integrity of the entity responsible for revoking user's anonymity, which has total control over the link between user's real identity and his pseudonyms. Also, the proposal does not focus in interoperability and M2M is not addressed.

A framework for authentication and access control of mobile users that access health information systems is proposed in [23]. The proposal focus in an AAL context, trying to assess the compliance of patients in administration of medicine dosages. Patients, physicians and medicaments are identified by RFID tags, and the process from drug prescription to drug administration is monitored using an information system based on IoT concept. Access to sensitive data is made by patients and physicians using mobile device. Authentication and access control tasks can be based on (i) username, password and RFID identification (ii) and also in a digital certificate (stored in a smartcard). Authentication happens from the mobile application to the server and vice-versa, and can only happen with user participation. However, the authentication protocol is not interoperability-driven. IdM model is centralized, but it is not user-centric. Finally, RFID tags are used, but the use of medical devices, such as sensors, is not addressed.

Table I compares related works and the proposed solution. A clear focus of related works on federated IdM is possible to notice. However, IoT concept integrated with federated IdM and e-health applications was not addressed. Similarly, no work addressed the application of IdM frameworks as OpenID, OAuth or OpenID Connect in the context of e-health.

Provide authentication of both users and devices in a scenario involving an e-health application and WoT devices is the main contribution of this work. Compared to the described related works, this is the first to address the device (in this case the Smart Gateway) as a SP, which provides patient's health data. To the authors knowledge, this is the first work to use OpenID Connect as the IdM solution in an e-health scenario.

[1]Permits detaching user identity from user data.

Table I. COMPARISON AMONG RELATED WORKS

Work	IdM Model	Authentication	IdM Technology	Device as SP
[8]	Centralized	User with a mobile phone application	Proprietary	No
[21]	Federated	Practitioner	Proprietary	No
[22]	Centralized and User-Centric	Users in general	SAML	No
[9]	Federated and User-Centric	Users in general	Liberty Alliance	No
[7]	User-Centric	Users in general	Proprietary	No
[6]	Federated and User-Centric	Users in general	Proprietary	No
[23]	Centralized	Users and applications	Digital Certificate	No
This work	Federated and User-Centric	Users in general and devices	OpenID Connect	Yes

IV. PROPOSED SOLUTION

Facing the characteristics of cyber-physical systems (CPSs) of remote medical assistance (AAL) and the needs of users of e-health systems, the choice of the user-centric IdM model is the most suitable, by the following reasons:

- Empower the user: users may have control over the attribute liberation flow to SPs;
- Give options to the user: beyond enabling the user to choose the IdP more appropriate for a transaction, users can change IdP without the worry about losing access to e-health services;
- Privacy: tracking of user information is made more difficult.

OpenID Connect has several characteristics that justify its adoption in the proposed scenario. OpenID Connect is free, open and decentralized (no central authority approves or registers relying parties or service providers). This standard uses just HTTP requests and responses. Thus, OpenID Connect does not require any special ability of the client software and it is not tied to using cookies or any other specific mechanism for the management of SP's session. Such integration provides a more secure solution when compared to OpenID and OAuth, because it is not vulnerable to attacks like phishing, cross-site scripting and cross-site request forgery.

Due to the use of OAuth 2.0 and a REST API on OpenID Connect, clients can be not just web browsers, but also scripts or devices. OAuth 2.0 and the REST API enable the IdP (OpenID Connect Provider) to be used for authenticating users and smart devices, which send data to a remote medical assistance application.

As shown in Figure 1, the proposed architecture involves the use of medical devices by the patient (e.g. wearable devices), which continuously monitor patient's health condition. Devices can use different communication protocols (e.g. IEEE 802.15.4, Wi-Fi and Bluetooth). Devices unable to make user's information available on the web due to resources restrictions are connected to a Smart Gateway, that acts as a bridge among devices and the Internet, as described in the Section II.

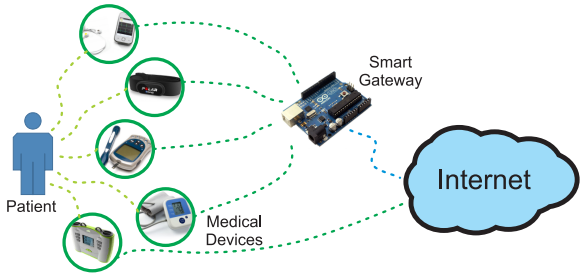

Figure 1. Use of medical devices as SP or connected to the Smart Gateway

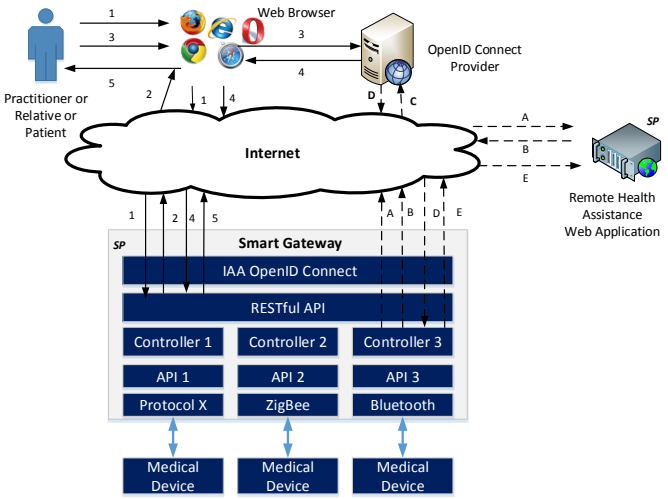

Figure 2. Use of OpenID Connect by a Remote Medical Assistance CPS

In the proposed architecture, the Smart Gateway, beyond acting as an aggregator of devices' resources and making such resources available through RESTful web services, has a primordial role in the implementation of the IdM solution, as shown in the Figure 2.

Figure 2 shows steps (1 to 5) needed for a user to access data (patient's vital signs) of medical devices made available as RESTful web services by the Smart Gateway. This flow shows that when a user tries to access a protected resource on the Smart Gateway, the web browser is redirected to an OpenID Connect Provider (OAuth Server) for user authentication. Based on this authentication, the authorization process happens, which guarantees that just authorized users (in conformance to security policy defined beforehand) access sensitive data on the Smart Gateway.

Steps needed for the user to access data on the Smart Gateway follows:

1) A user tries to access a resource on the Smart Gateway;
2) As the resource requires authentication, user's web browser is redirected to the OpenID Connect Provider;
3) User authenticates on the OpenID Connect Provider;
4) After authentication, a token is generated by the OpenID Connect Provider and sent to the SP (Smart Gateway);
5) Based on user's attributes, the SP grants access to

the required resource and answers with a message containing data about the patient's vital signs.

Proposed architecture also considers the integration of the Smart Gateway with remote medical assistance web applications, in which the Smart Gateway feeds such applications with patient's health data. For instance, an application could analyse the evolution of patient's health condition after the beginning of a treatment, based on data sent by devices. Such data may be provided in short time intervals.

However, for this integration among the Smart Gateway and web applications to be secure, the identification of the Smart Gateway as an authorized provider of specific user's health data is needed. Thus, in the Figure 2 is shown another flow (A to D), which refers to steps needed for medical device to send patient's monitored data to medical assistance web application. In this flow, the device's authentication process (e.g. Smart Gateway) happens, which enables the device to publish data to the web application.

A) Device tries to publish data to the web application;
B) Web application, which is the SP in this case, requires authentication and indicates the OpenID Connect Provider to the device;
C) Device authenticates to the OpenID Connect Provider;
D) OpenID Connect Provider issues a token, which is forwarded to the SP (web application);
E) Based on the device's attributes, SP grants the required access.

Thus, identity management is provided for users and devices in the e-health scenario.

V. Case Study

This Section describes a scenario of ambient assisted living (AAL), where an e-health application is used for monitoring the health condition of a person. Integration of the e-health application with OpenID Connect, for providing authentication and authorization of users and devices, is also presented.

Figure 3 depicts the scenario of the e-health application. Person is wearing a heartbeat sensor and a temperature sensor. Both can communicate using Bluetooth and IEEE 802.15.4. House has a humidity sensor that communicates using Wi-Fi. Person has also a smartphone with an application for getting measurements of the accelerometer, in order to know if the person falls. Smartphone can communicate using both Bluetooth and Wi-Fi.

An open hardware[2] is acting as a Smart Gateway, aggregating information of sensors in a RESTful web service. Despite of the many connectivity options, the range of the wireless signal is limited in the Smart Gateway and sensor device. As shown in Figure 3, a situation where another device is used to intermediate communication between sensor and Smart Gateway is considered, due to distance concerns.

[2]BeagleBone Black is an open hardware low cost platform (portable computer) that has a 1GHz AM335x ARM® Cortex-A8 processor, 512MB DDR3 RAM and 2GB 8-bit eMMC on-board flash storage. It also has many connectivity options, like Ethernet, Wi-Fi, IEEE 802.15.4 and Bluetooth.

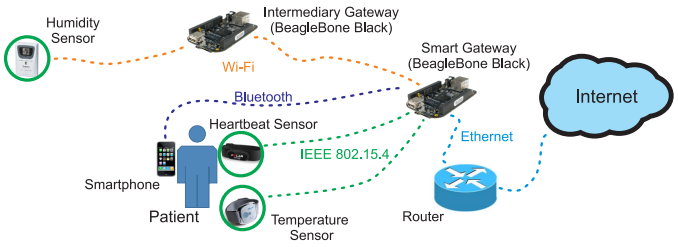

Figure 3. Scenario of E-health Application

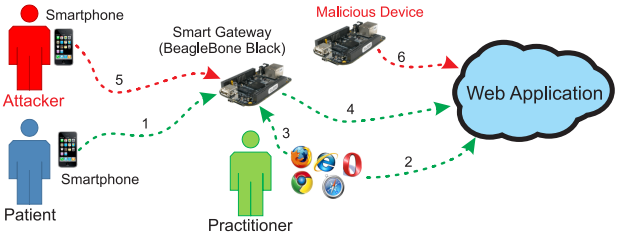

Figure 4. Access to E-health Data

Web service in the Smart Gateway can provide real time data about patient's health condition. Also, at short intervals, the Smart Gateway sends information aggregated about patient's health condition to a web application hosted in a Cloud Computing platform.

As shown in the Figure 4, many kinds of access may happen in this application. Patient can access his health data from his smartphone in the Smart Gateway (step 1). Practitioner, using a web browser, can access patient's health data in the web application (for historical data) (step 2) or in the Smart Gateway (for real time data) (step 3). Smart Gateway can periodically send health data to the web application (step 4).

All accesses described above are legitimate. Although, it is also possible that unauthorized people try to access patient's health data (step 5), as well as unauthorized devices can try to update the web application with false data (step 6). OpenID Connect can provide identity management for this scenario, enabling the provision of authentication and access control of users, devices and applications. As a consequence, these attempts at illegitimate access will not be successful.

When a user, using his smartphone, tries to access his health data directly on the Smart Gateway, the Smart Gateway redirects the application to an OpenID Connect IdP indicated by the user. After authentication, Smart Gateway makes an access control decision based on user's attributes provided by the IdP (released with user's consent).

If patient's practitioner wants to access patient's health data on the Smart Gateway using a web browser, the process is similar. When practitioner tries to access the web application, his web browser is redirected to the OpenID Connect Provider (IdP) chosen. After authentication, web application makes access control decision, based on practitioner's attributes provided by the IdP, and may provide access to the required resource. In the same way, the attacker shown in the Figure 4, who is a valid user to the provider but unauthorized to access patient's data, tries to access such data. Based on attributes of the attacker, provided by the IdP where he authenticated, the

web application denies access to required resources.

Another possible situation is when the Smart Gateway tries to send patient's health data to the web application, to update its database with new data. Given this update attempt, web application sends the Smart Gateway to the OpenID Connect Provider for authentication. After Smart Gateway authentication, web application receives, from the IdP, device's attributes with which it will make an authorization decision. Based on this decision, data provided by the Smart Gateway will be accepted or rejected. Similarly, when an attacking device (shown in Figure 4) acting as a Smart Gateway tries to update the web application with false data about the patient, the update may be reject in two moments: (i) in the authentication phase, because the device does not have a valid identity on a trusted IdP; (ii) or in the attribute evaluation process (authorization held on Smart Gateway).

As shown above, adding the OpenID Connect framework to the e-health application leverages the security of it, enabling authentication and authorization tasks based on identities of users, devices and applications. Also, due to OpenID Connect's features, provide a user-centric IdM solution is possible, meeting user's privacy requirements.

VI. Conclusion

This paper described the use of the user-centric IdM framework - OpenID Connect 1.0, in an ambient assisted living environment in the WoT scenario. OpenID Connect is used for authentication and authorization of users and devices and to establish trust relationships among entities in different security domains, in a federated approach. This work is the first approach using OpenID Connect in an application of e-health that uses IoT devices. This approach made possible to leverage the use of e-health applications that use IoT devices, providing an interoperable solution that can deal with security requirements of patients and applications that involve users and devices, especially those related to authentication and authorization. Also, the solution meets user's privacy requirements and empowers the patient, that may control the disclosure of sensitive identity information to third parties.

Continuation of this work includes evaluating the implementation of the AAL scenario integrated to a user centric IdM system. In the evaluation phase, the following metrics will be considered: latency and throughput of the network and the use of computational resources of the devices (memory and energy consumption and CPU and storage usage). Use of the solution in different scenarios and the evaluation of user's acceptance in a larger experiment involving many users are envisioned as future works.

Acknowledgment

The first author is supported by CAPES (Brazil).

References

[1] M. Layouni, K. Verslype, M. T. Sandıkkaya, B. De Decker, and H. Vangheluwe, "Privacy-preserving telemonitoring for ehealth," in *Data and Applications Security XXIII*. Springer, 2009, pp. 95–110.

[2] W. Wilkowska and M. Ziefle, "Privacy and data security in e-health: Requirements from the user's perspective," *Health informatics journal*, vol. 18, no. 3, pp. 191–201, 2012.

[3] A. Dohr, R. Modre-Opsrian, M. Drobics, D. Hayn, and G. Schreier, "The internet of things for ambient assisted living," in *Information Technology: New Generations (ITNG), 2010 Seventh International Conference on*, April 2010, pp. 804–809.

[4] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[5] D. Guinard, V. Trifa, F. Mattern, and E. Wilde, "From the internet of things to the web of things: Resource-oriented architecture and best practices," in *Architecting the Internet of Things*. Springer Berlin Heidelberg, 2011, pp. 97–129.

[6] R. Au and P. Croll, "Consumer-centric and privacy-preserving identity management for distributed e-health systems," in *Hawaii International Conference on System Sciences, Proceedings of the 41st Annual*. IEEE, 2008, p. 234.

[7] D. Slamanig and C. Stingl, "Privacy aspects of ehealth," in *Availability, Reliability and Security, 2008. ARES 08. Third International Conference on*. IEEE, 2008, pp. 1226–1233.

[8] J. Mirkovic, H. Bryhni, and C. M. Ruland, "Secure solution for mobile access to patient's health care record," in *e-Health Networking Applications and Services (Healthcom), 2011 13th IEEE International Conference on*. IEEE, 2011, pp. 296–303.

[9] L. Peyton, J. Hu, C. Doshi, and P. Seguin, "Addressing privacy in a federated identity management network for ehealth," in *Management of eBusiness, 2007. WCMeB 2007. Eighth World Congress on the*. IEEE, 2007, p. 12.

[10] M. Aramudhan and K. Mohan, "New secure communication protocols for mobile e-health system," in *Networked Digital Technologies*. Springer, 2010, pp. 639–647.

[11] J. Liu, Y. Xiao, and C. P. Chen, "Authentication and access control in the internet of things," in *Distributed Computing Systems Workshops, 2012 32nd International Conference on*. IEEE, 2012, pp. 588–592.

[12] ITU, "Ngn identity management framework," Recommendation Y.2720, 2009.

[13] A. Bhargav-Spantzel, J. Camenisch, T. Gross, and D. Sommer, "User centricity: a taxonomy and open issues," *Journal of Computer Security*, vol. 15, no. 5, pp. 493–527, 2007.

[14] P. Mahalle, S. Babar, N. R. Prasad, and R. Prasad, "Identity management framework towards internet of things (iot): Roadmap and key challenges," in *Recent Trends in Network Security and Applications*. Springer, 2010, pp. 430–439.

[15] T. O. Foundation, "Openid connect core 1.0," January 2014, http://openid.net/specs/openid-connect-core-1_0.html.

[16] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[17] D. Zeng, S. Guo, and Z. Cheng, "The web of things: A survey (invited paper)," *Journal of Communications*, vol. 6, no. 6, 2011.

[18] R. T. Fielding and R. N. Taylor, "Principled design of the modern web architecture," *ACM Trans. Internet Technol.*, vol. 2, no. 2, pp. 115–150, May 2002.

[19] R. Roman, P. Najera, and J. Lopez, "Securing the internet of things," *Computer*, vol. 44, no. 9, pp. 51–58, 2011.

[20] S. Babar, P. Mahalle, A. Stango, N. R. Prasad, and R. Prasad, "Proposed security model and threat taxonomy for the internet of things (iot)." in *CNSA*, ser. Communications in Computer and Information Science, N. Meghanathan, S. Boumerdassi, N. Chaki, and D. Nagamalai, Eds., vol. 89. Springer, 2010, pp. 420–429.

[21] M. Deng, R. Scandariato, D. de Cock, B. Preneel, and W. Joosen, "Identity in federated electronic healthcare," in *Wireless Days, 2008. WD '08. 1st IFIP*, Nov 2008, pp. 1–5.

[22] M. Campos, M. Correia, and L. Antunes, "Leveraging identity management interoperability in ehealth," in *Security Technology (ICCST), 2011 IEEE International Carnahan Conference on*, Oct 2011, pp. 1–8.

[23] F. Goncalves, J. Macedo, M. Nicolau, and A. Santos, "Security architecture for mobile e-health applications in medication control," in *Software, Telecommunications and Computer Networks (SoftCOM), 2013 21st International Conference on*, Sept 2013, pp. 1–8.