Consolidate the Identity Management Systems to Identify the Effective Actor Based on the Actors Relationship for the Internet of Things

Ausama Majeed and Adil Al-Yasiri

School of Computing, Science, and Engineering, University of Salford
Manchester, UK

a.a.majeed@edu.salford.ac.uk, a.al-yasiri@salford.ac.uk

Abstract. Service providers in the Internet of Things need to truly establish the identity of the user(s) as the effective actor(s) (EA) identity rather than the communicating objects to offer the right services. Objects are seamlessly interconnected by anyone, anywhere, and anytime on behalf of the EA. An actor in the IoT is any identified entity, which interacts with other entities over the Internet. It could have different identities that are managed by different Identity Management systems ($IdMs$) in every domain they interact with which are not always interoperable with each other. Moreover, the communicated objects identities can also be used to identify their EAs identities based on their relationship. The actor relationships are not always fixed; they can be changed or even revoked. Therefore, a global identity management system ($GIdM$) is proposed to consolidate the $IdMs$ in order to establish the identity of a requester across-domain. A $GIdM$ facilitates the establishment of dynamic trust relationships and the validation of the EA identity based on the relationship type and a set of identity attributes. Comparisons between the proposed solution ($GIdM$) with the state-of-the-art works show that the $GIdM$ system can overcome the current limitations for establishing the EA identity globally in the IoT.

Keywords: Global Identity Management, Consolidate $IdMs$, IoT, Identity, Effective Actor, Identity Establishment Requirements.

1 Introduction

Establishing the identity of an actual user, denoted as the effective actor (EA) hereafter, behind any communicated object/device (Co) is an important, yet challenging task for the service providers (SPs) in the Internet of things (IoT). The IoT is the environment of interconnecting various object types, which are denoted as things. To manage and control dealings with these things, every SP has a permanent trust relationship with an identity provider (IdP) to form a so-called Identity Management system (IdM) [1]. The IdM aims to ensure that the SP offers services to a trusted user (client) to increase the enterprise's security and efficiency. Traditionally, every enterprise deploys an IdM system to manage the identity of its users (clients) within the enterprise domain or within a group of domains called a Circle of Trust (CoT) [2]. An actor in the IoT is any identified entity, which needs to interact with other entities over the Internet such as people, places, devices, services or more. Actors can own diverse identity data within several $IdMs$ domains, which are valid and used within that domain [3, 4]. Moreover, these $IdMs$ are not always interoperable/compatible with each other. This is because they often use varying types of identity data and different identity verification methods. Therefore, improving the $SP's$ ability to identify the EAs behind the communicated objects across their IdM domains is crucial to the success of the IoT.

The IoT implies of a sheer number of interconnected objects Co that are communicating over the Internet. The Cos range from tiny sensors with limited computing and communication capabilities to high computing and communication capabilities. The Cos, at any time, could be owned by one or more owners and used by a single or multiple EAs [5]. This will change the current ways of actor interaction from "owner" and "subscriber" into much broader ways such as interact with free devices as discussed in [6 – 8]. In other words, these Cos could be interconnected on behalf of actors other than their legal owners. The actors' interactions are establish based on an actor relationship (AR) between an EA and one Co or more. These ARs may not always be static in nature; it could be dynamically established and after a period will be changed or even vanished. Three types of AR are defined in our previous work in [9] that are permanent, semi-permanent, and open-access relationships. Moreover, domain interaction is another interaction method which needs to be considered by the $IdMs$ in the IoT because actors can interact locally within a domain or externally across domains. The cross-domain interaction requires an existing trust relationship between the $IdMs$ that manage the Co.

Therefore, we do believe that to establish the EA identity behind the $Co(s)$, we need an interoperable IdM system that is able to consolidate the existed $IdMs$ to facilitate establishing the identity by SPs in the IoT. Thus, we propose a global identity management system $GIdM$ to solve these limitations.

The rest of the paper is organised as follows: Section 2 reviews the state-of-the-art about $IdMs$ in the IoT; Section 3 discusses the requirements for establishing the effective actor identity. These requirements are used to develop a new system called Global Identity Management ($GIdM$) used to verify the identity, which is discussed in Section 4. In Section 5 we evaluate the $GIdM$ by comparing it with those from the state-of-the-art. Section 6 concludes the paper with references at the end.

2 State-of-the-Art Related to $IdMs$ in the IoT

There are several IdM systems for use in the IoT, which follow different architectures and standards as summarized below.

The Liberty Alliance [10] is a collaboration of companies and organisations that aim to establish IdM standards, recognizable identity federation, cross-domain authentication, and session management. The process is mainly supported by SAML [11] to promote the identity federation framework and the identity web service framework. In this approach, the user uses a single federated identity issued by an IdP to access services from any SP within the circle of trust (CoT) [12], and supports user privacy and network identity security by using pseudonyms. However, it does not consider the actor relationship between the user and the communication device. Shibboleth [13] is a federated IdM used for sharing resources between research and academic institutions based on SAML2 and web redirection. It presents a common interface between the academic institutes in terms of authentication systems using a proof-of-rightful-possession. Again, the actor relationship is missing. OpenID [14] is a decentralized framework for user-centric IdM. OpenID facilitates accessing services from different SPs by the users using a single digital identity, which is issued by an OpenID IdP. However, this framework does not consider the actor relationship and could suffer from a cross-domain $IdMs$ interoperability problem in an open environment such as the IoT. The Eclipse Higgins [15] is a user-centric IdM that improves the interoperability across $IdMs$ by defining a new layer (context) to link the identities. However, the actor relationship is also missing. OAuth 2.0 framework focuses on defining a user authorisation protocol to allow the "resource owner" to permit a third-party client, on behalf of the owner, to access/perform an action on the resource in a "resource server" [16 - 17] without sharing his credentials with the third-party. Again, the actor relationship is missing. PICOS is a user-centric model aims to develop and evaluate existing $IdMs$s to supply the community service with mobile communication SPs [18]. It allows users to create a restricted area where the user can share his/her partial identity with selected users to offer services or share resources [19]. However, it does not consider the device identity or its relationships with the user to identify and authenticate the user in these social roams. STORK is a user-centric IdM framework co-funded by the European Union to authenticate citizens and employees by any State of the EU using the eID [20]. Again, the device identity and its relationship with the user are missing.

Mahalle proposed an identity management layer with a set of processes for IoT in [8]. The author relies on context to define a separate context identity (CID) and a namespace dependent identifier to the communicated device identifer. However, the proposed solution ignores the user identity and their relationship with the device. Chibelushi et al. [21], proposed a user-centric IdM framework for healthcare in IoT. Because all the healthcare devices use ad-hoc network in their communications, they claim that they need to bind the devices and users identification when sharing devices and create a seamless interaction in IoT domains. Still, the proposed IdM system does not address device-to-device communication issues nor across-domains identification. Van Thuan & Butkus [22], proposed a user-centric IdM within the IoT's gateway architecture that supports a federated model. In spite of binding the identities of the user and the device, they do not describe the relationships clearly in their solution. Zdravkova [23], proposed a user-centric IdM within a cloud-based IoT architecture by using an identity agent in the computing devices. The work uses the identification of a single thing (device) with a SP to identify the other things belonging to the user (called Single-Thing-Sign-On). The proposed IdM uses the relationships between a human user and the things without clearly defining those relationships. Abreu et al. [24] proposed a user-centric IdM within the "Advanced Metering Infrastructure" in the ICT to maintain the identity privacy of the operator/engineer in remotely accessing the smart meters. A RTU ("Remote Terminal Unit") is used as a broker between the smart meter and the requester which is in charge of validating the requester identity within the authorization server. Again, they did not consider the device identity, its relationship with the requester, nor dynamically establish a trust relationship within the communicated parties. Bernabe et al. [25] proposed a privacy-preservation IdM to authenticate the users in the claim-based machine to machine environment. The identities of both user and device will be used to get the Identity Mixer (Idemix) credential to maintain the privacy. The federated identity environment is achieved by using SCIM ("System for Cross-domain Identity Management") standard [26]. However, the impact of the relationship between the user and the communication object on the identification is missing again.

To sum up, the above IdM solutions are designed to work in the IoT environment. However, despite their advantages, none of them supports a dynamic establishment of a trust relationship across $IdMs$ domains or a relationship-based identity establishment. Therefore, a new IdM system to support attribute sharing is required to overcome the limitations in the current IdM solutions.

3 The Effective Actor's Identity Establishment Requirements

The IoT provides an environment for different actor types, such as people, sensors, devices and objects, to interact. They are registered with one or more service domain IdP, each supplies the actors with an identifier based on their roles. In other words, an actor could have as many identifiers as its roles in the domain. Establishing an EA identity in a large-scale environment, such as the IoT, needs to fully encompass the role of each actor and the relationship nature between the IoT actors. By analysing typical IoT's scenarios, we believe that the following requirements are sufficient to establish the EA identity.

Req 1. Decoupling identities of related actors. The SP should be able to differentiate between the EA identifier and the communication object/device identifier. As these entities are related actors, this requires representing them in a semantic format.

Req 2. Identifying the home IdP for the actor. Each actor's identifier should be paired with its native IdM registration domain identifier. This is due to two IoT's facts: (1) services in the IoT could be requested within one domain (intra-domain) or across multiple domains (inter-domain); (2) the entities' nomadic nature with the aim of consuming services offered by any SP anywhere. Thus, the SP (or the visited domain IdP) must be aware of the domain that manages the identifier to be involved in the EA identity establishment process.

Req 3. Identifying actor's attributes. The SP should establish the EA identity before provisioning the request. Generally, it is important for the SP to recognise the following:

- How does the EA interact with the communication object(s) to transmit the data/request? The SP should recognise the relationship type between the EA and the communication object that transmits the data/request.
- What is the EA type (i.e. Person, Device, System or Application) that maps each actor to its permitted role in the domain?

– What is the Internet connectivity type (i.e. passive or active) of the communication device that permits the actor to take its specified role in the domain?

Req 4. Actors' identity delegation. The interacting actors, i.e. the EA and the communication object, should delegate their identities to form an actor relationship representation

Req 5. The IdP awareness of actor relationships. The communication object(s)/device(s) should be aware of their relationship with the EA actor, on whose behalf they communicate. This relationship should be registered within the actor domain $IdP(s)$. It should also be identifiable, recognisable and provable by the SP.

Req 6. The establishment of a dynamic trust relationship. The SP should be able to establish a dynamic trust relationship with the IdP of unrelated domains in order to involve it in the identity verification.

Req 7. Relationship-based identity establishment. The SP should establish the EA identity based on its identifier and the actor relationship instead of the physical identity, such as the IP address. This is because physical identities like the IP address refer to the communication object location on the network rather than its end user.

Req 8. Efficient protocol to share the actor's attributes. A new authentication protocol is required which should allow SPs to establish the EA identity based on its relationship(s) with the communication device(s) and the actor's characteristics..

4 A Global Identity Management System ($GIdM$)

We propose the IdM , which is a general framework to establish the effective actor identity of nomadic objects that might belong to different $IdMs$ in the IoT. $GIdM$ consolidates the existing $IdMs$ to allow the SP to interoperate with different $IdPs$ dynamically in order to meet the above requirements. The first three requirements (Req.1 – Req.3) are considered in the design of a new identifier to represent the EA identity, the Co identity, and their relationsip attributes in a semantic format called *Global Actors' Relationship Identifier* ($GARI$). More details of the $GARI$ is found in our previous work in [9].

4.1 $GIdM$ architecture

The $GIdM$ architecture contains four main layers, as depicted in figure 1. The first (lower) layer is the *$GARI$ Composer layer* that is used to represent the actor relationship with SPs in the IoT environment. The next layer is the *service* providers *layer*, which contains SPs from different $IdMs$. Each SP could have a trust relationship with one IdP (or even more) to control the access of their services by trusted requesters within the IdM boarder. The SPs are responsible for establishing the requester's identity by using an identity verification method. Once the requester identity is successfully established, the requested services will be offered. The third layer is the *identity providers layer* which contains all the $IdPs$. Each IdP can have a trust relationship with one SP or more. Each trust relationship between the SP and IdP represents a subset of the IdM domain that managed the user identities. Entities within a domain are allowed to use identifiers issued by the IdP responsible for that domain to request a service from SPs within that domain. However, in the IoT, such a trust relationship between an independent SP and the actors' home $IdPs$ might not exist in advance as they can belong to unrelated domains. Thus, an additional layer called Trusted Domains Registry (TDR) is added on top of these layers.

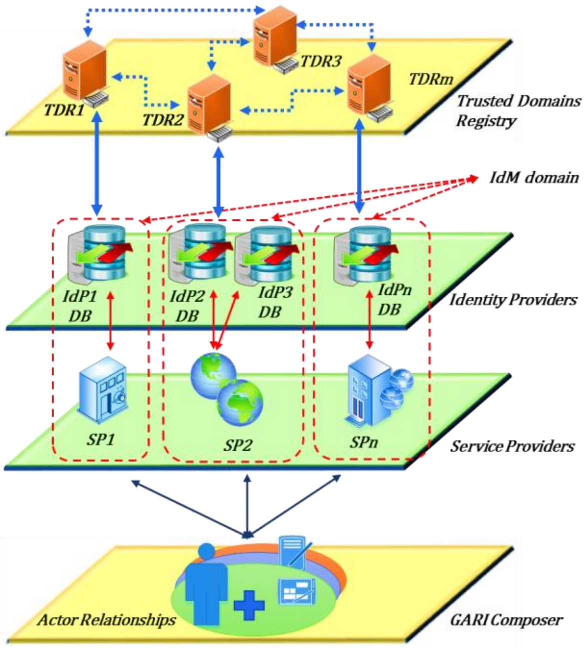

Fig. 1. The $GIdM$ Architecture

The idea behind using the TDR layer is for the purpose of maintaining trust relationships between the IdM entities. Each TDR implies a list of trusted SPs and $IdPs$; hence, the SPs can dynamically establish the required trust relationship with foreign $IdPs$ relying on the information maintained in these $TDRs$.

4.2 An Identity Establishment Framework

In the proposed $GIdM$, SP plays an important role in controlling and dispatching the requested service. This is because it could be of different capabilities such as a standalone entity like smart devices or gateway that operates on behalf of other tiny objects like sensors. Thus, it has to manage the process of identity establishment of an EA in order to offer the right service by using the following steps:

- ***GARI* Analysis**: To establish the requester's identity, the SP decomposes the received $GARI$ to extract the actor relationship(s) attributes in addition to the actors' identities information.

- ***Verify the Actors Domain(s)***: Checking whether an SP already has a trust relationship with the IdP that manages the actor's identity is a prerequisite to verify the actor's identity. Therefore, every IdP supplying an actor identity will be checked to verify whether it is trusted by the SP or not. If it is not, a trust relationship has to be established based on the TDR prior to performing the identity verification. In the case where the IdP is not trusted, it will not be involved in the identity verification process.
- ***Verify the EA identity based on $\boldsymbol{AR(s)}$***: All the actors' relationship(s) are used to verify the EA identity by their domains $IdPs$. This will be done by a direct connection between the SP and the involved $IdPs$ to verify the identity using the ARs attributes.
- ***Reasoning the identity establishment***: Finally, the SP checks the replies of all the identity verification requests that were sent to the involved $IdP(s)$ in previous step within a period of time. If they are verified by those $IdP(s)$, then the identity will be established successfully, otherwise, it is failed.

Applying these steps require two main phases. Firstly, establishing a dynamic trust relationship between the SP and the IdP of each actor in the relationship. Secondly, verifying the AE identity based on its relationship(s) with the communicated object(s). It is worth to note that the first phase is required only in the case where the trust relationship(s) with the IdP are not pre-established; otherwise both should be followed in sequence.

5 The $GIdM$ Evaluation

This section evaluates the proposed $GIdM$ by comparing it with the IdMs solutions that were presented in section 2 using the requirements in section 3 as evaluation factors as described in Table 1.

Decoupling identities of related actors (Req.1) is fulfilled by precisely declaring both actor's identities. In addition to $GARI$, three other solutions ([21], [8], and [23]) have fully implemented this requirement. The others have either considered the user or object/application identity. Identifying the IdP that manages the actor identity (Req.2) is required by the SP to establish the identity of mobile and remote requesters that might be managed by different $IdP(s)$, i.e. "Where Are You From" $WAYF$ bases. From the table, five of the proposed solutions did not support this requirement that are ([14], [16], [18], [21], and [24]). Identifying actor's attributes in Req. 3 is fulfilled only by $GARI$. The other solutions have not fulfilled the requirement except ([8], [21], [23], [24], and [25]) that partially fulfilled the EA by considering the Person type only. Delegation of the actors' identities requirement, (Req.4), supports the hybrid IdM model where the user and object (actors) control their identities when they interact with each other. Req.4 is fully fulfilled only by the $IdMs$ in ([15], [21], [8], [23], and the $GIdM$), while the others considered either the user or object identity. Similarly, Req.5 which is the $IdPs$ awareness of the actor relationship, by considering a fixed relationship between actors, is partially fulfilled in ([15], [21], [23], and [24]). $GIdM$ is the only IdM that considers different types of the actor relationship. The other solutions neither model the actor's relationship concept in a general form nor consider the alternate and vanish possibilities of these relationships. The table also shows that the state-of-the-art IdM solutions fail to support Req.6, Req.7, and Req.8. They rely on a static pre-established trust relationship between the communicated $SP(s)$ and $IdP(s)$ within a domain or CoT. In other words, the $SP(s)$ do not dynamically establish a trust relationship with foreign $IdP(s)$ to verify the actor identity; hence the static form is not suitable for a large number of $SP(s)$ and $IdP(s)$ such as in IoT [26]. Moreover, the EA identity establishment based on the actor's relationship is missing from the state-of-the-art $IdMs$. They are built based on amodel of fixed relationships between the actors, i.e. user and device, without considering the other types of actor interaction. Finally, an efficient protocol to exchange the attributes of actor relationship is missing as well in these $IdMs$. This is because the attributes themselves have never been introduced by current solutions. All these limitations have been addressed in $GIdM$, where the actors identities are represented explicitly in the $GARI$; it supports establishing mutual trust relationships between unknown entities relying on a set of $TDRs$.

To summarise, the comparison between $GIdM$ and the state-of-the-art $IdMs$ shows that the $GIdM$ with the $GARI$ is the only solution that satisfies the whole requirements to establish the EA identity. Therefore, the $GIdM$ is the most suitable IdM to be used in the IoT for it allows SPs to identify the Effective Actors based on relationship(s) globally.

Table 1. A comparison of $IdMs$ solutions for the IoT

***IdM* projects**	**Requirements to establish the *EA* identity**							
	Req.1	**Req.2**	**Req.3**	**Req.4**	**Req.5**	**Req.6**	**Req.7**	**Req.8**
Liberty Alliance [10]	U	✓	-	U	-	-	-	-
Shibboleth [13]	U	✓	-	U	-	-	-	-
OpenID [14]	U	-	-	U	-	-	-	-
Higgins [15]	U	✓	-	✓	✓	-	-	-
OAuth2.0 [16]	U	-	-	U	-	-	-	-
PICOS [18]	U	-	-	U	-	-	-	-
STROK [20]	U	✓	-	U	-	-	-	-
Mahalle [8]	O/A	✓	P	U/O	-	-	-	-
Chibelushi, et al. [21]	✓	-	P	✓	✓	-	-	-
Van Thuan & Butkus [22]	✓	✓	-	✓	-	-	-	-
Zdravkova [23]	✓	✓	P	✓	✓	-	-	-
Abreu et al. [24]	U	-	P	U	✓	-	-	-
Bernabe et. al. [25]	O/A	✓	P	U/O	-	-	-	-
GIdM	✓	✓	✓	✓	✓	✓	✓	✓
U: user, O: object, A: application, P: person, ✓: fulfilled, - : unfulfilled.								

6 Conclusion

There are several $IdMs$ proposed to be used in the IoT environment. However, they are not always interoperable with each other, which may hamper the realization of the IoT benefits. Moreover, users as effective actors could have different relationships with communication objects that are interconnected with others to offer services or data on behalf of their actual user. Thus, Identifying the user(s) in the IoT is a difficult task facing the SPs. In this research, we proposed a new IdM architecture to consolidate these $IdMs$ to interoperate with each other in order to facilitate the establishment of a dynamic trust relationship and the validation of the EA identity based on the relationship type and a set of identity attributes. $GIdM$ has been evaluated based on its perceived benefits in comparison to other solutions to establish the effective actor's identity by SPs that may be managed by different $IdMs$ in the IoT. However, further research to manage the trust and reputation measurements of these SPs and $IdPs$ by the $TDRs$ nodes is required.

Acknowledgment. The first author would like to thank the Ministry of Higher Education and Scientific Research of Iraq – University of Thi-Qar for funding him during this research.

References

1. Fongen, A.: Identity Management and Integrity Protection in the Internet of Things. In: 3rd International Conference on Emerging Security Technologies, pp. 111-114, IEEE Press, (2012)
2. Yeluri R, Castro-Leon E.: Identity Management and Control for Clouds. In: Building the Infrastructure for Cloud Security, pp. 141-159, Apress, (2014)
3. Angin, A., Bhargava, B., Ranchal, R., Singh, N., Linderman, M.: An Entity-Centric Approach for Privacy and Identity Management in Cloud Computing. In 29th Symposium on Reliable Distributed Systems, pp. 177–183, IEEE (2010).
4. Lampropoulos, K., Denazis, S.: Identity Management Directions in Future Internet. IEEE Communcation Magazine, 49(12), pp. 74–83 (2011).
5. Lam KY., Chi CH.: Identity in the Internet-of-Things (IoT): New Challenges and Opportunities. In: Lam KY., Chi CH., Qing S. (eds) Information and Communications Security. ICICS 2016. LNCS, vol. 9977. Springer, Cham (2016).
6. Gartner: The Identity of Things for the Internet of Things - (G00270277), (2015).
7. Forgerock, Whitepaper: The Identity of Things (IDoT): Access Management (IAM) Reference Architecture for The Internet of Things (IoT). (2015).
8. Mahalle, PN., Railkar, PN.: Identity Management for Internet of Things. River Publishers, Denmark (2015).
9. Majeed A., Al-Yasiri A.: Formulating A Global Identifier Based on Actor Relationship for the Internet of Things. In: Mitton N., Chaouchi H., Noel T., Watteyne T., Gabillon A., Capolsini P. (eds) Interoperability, Safety and Security in IoT. InterIoT

2016, SaSeIoT 2016. LNICS, Social Informatics and Telecommunications Engineering, vol. 190, pp. 79-91. Springer, Cham (2017)

10. The Liberty Alliance project homepage. http://projectliberty.org/. last accessed: 15/01/2016.
11. SAML: Advancing open standards for the information society Homepage. http://www.oasis-open.org/committees/tc_home.php?wg_a. last accessed: 15/01/2016.
12. Torres J., Nogueira M., Pujolle G.: A Survey on Identity Management for the Future Network. Communication Survey Tutor, IEEE 15(2), pp. 787–802 (2013).
13. Shibboleth project Homepage, http://shibboleth.net/about/. Last accesses 15/01/2016.
14. OpenID project Homepage, http://openid.net/. Last accesses 15/01/2016.
15. Higgins Homepage, http://pde.cc/tags/higgins/. Last accesses 10/01/2018.
16. Open Authorization Hompage, https://oauth.net. Last accesses 10/01/2018.
17. API Crazy: Comparison of OpenID Connect with OAuth2.0 & SAML2.0, 2014. https://apicrazy.com/2014/07/23/comparison-of-openid-connect-with-oauth2-0-saml2-0/. Last accesses 10/10/2017.
18. PICOS Homepage: Privacy and Identity Management for Community Services. http://www.picos-project.eu. Last accesses 10/10/2017.
19. G´ orniak, S., Elliott, J., Ford, M., Birch, D., Tirtea, R., Ikonomou, D.: Managing Multiple Electronic Identities. European Network and Information Security Agency, ENISA (2011).
20. STORK- Secure idenTity acrOss boRders linKed Homepage. http://www.eid-stork.eu. Last accesses 10/07/2017.
21. Chibelushi, C., Eardley, A., Arabo, A.: Identity management in the Internet of Things: the role of MANETs for healthcare applications. Computer Science and Information Technology 1(2), pp. 73–81 (2013).
22. Thuan D. V., Butkus P.: A User Centric Identity Management for Internet of things. In: International Conference on IT Convergence and Security (ICITCS), pp. 1-4, IEEE Publisher, Beijing (2014).
23. Zdravkova V.: Identity Management Approach in Internet of Things. Aalborg University (2015).
24. Abreu A., Santin,A., Lando, A., Witkovski, A., Ribeiro, A., Stihler, M., Zambenedetti, V., Chueiri, I.: A Smart Meter and Smart House Integrated to an IdM and Key-based Scheme for Providing Integral Security for a Smart Grid ICT. Mobile Networks and Applications, Springer US (2017).
25. Bernal Bernabe, J., Hernandez-Ramos, J., Skarmeta Gomez, A.: Holistic Privacy-Preserving Identity Management System for the Internet of Things. Mobile Information System, Hindawi, pp. 1–20 (2017).
26. Hunt, P., Grizzle, K., Wahlstroem, E., Mortimore, C.: System for Cross-domain Identity Management: Core Schema. No. RFC 7643 (2015).