FI-WARE authorization in a Smart Grid scenario

George Suciu, Cristiana Istrate,
Mari-Anais Sachian
R&D Department
BEIA Consult International
Bucharest, Romania
george@beia.ro,
cristiana.istrate@beia.ro,
anais.sachian@beia.ro

Alexandru Vulpe, Marius Vochin
Telecommunications Department
University POLITEHNICA of
Bucharest
Bucharest, Romania
alex.vulpe@radio.pub.ro,
marius.vochin@upb.ro

Aristeidis Farao, Christos Xenakis
Department of Digital Systems
University of Piraeus
Piraeus, Greece
arisfarao@unipi.gr,
xenakis@unipi.gr

***Abstract* — The traditional models of electric grid, based on centralized systems for the production and distribution of energy, have changed dramatically over the recent years. The integration of top-notch technologies that are not usual in critical infrastructures, such as Internet of Things (IoT) or Big Data, have favored the evolution towards a more dynamic and interconnected power network model, which is currently known as Smart Grid (SG). In this paper it is presented the architecture of a global authorization component is proposed for any Smart Grid scenario, related to the SealedGRID project. This component is modeled following a hierarchical architecture composed by different authorization entities, which effectively manage the access to the different resources within the grid infrastructure based on well-defined policy rules, while also taking into consideration the security state of such resources (per domains or substations) by means of a context-awareness module. The overall aim of SealedGRID is to design, analyze and implement a scalable, highly trusted and interoperable Smart Grid (SG) security platform.**

***Keywords* — smart energy, Smart Grid, IoT, AuthZ, FI-WARE, policy, security.**

I. INTRODUCTION

The traditional electric grid models are based on centralized systems for the production and distribution of energy, and have changed dramatically over the recent years. The integration of latest generation technologies that are unusual in critical infrastructures, such as the Internet of Things (IoT) or Big Data, have facilitated the evolution towards a more dynamic and interconnected power network model, currently known as the Smart Grid (SG).

The contributions of the SG appear as a consequence of the introduction of a two-way flow of information between producers and customers, from which both of them can benefit. This flow enables a fine-grain consumption metering, which is reported back in near real time to the:

1) respective energy service providers to provide updated pricing data to the consumers; or
2) control utilities to manage in real time the energy load in the grid according to the real demand.

This way, the utility company can carry out accurate procedures of Demand Response, by anticipating high peaks of demand, avoiding and mitigating power outages and accommodating the load of the available generators. On the other hand, the consumers can participate in programs to reduce electricity use when the price of energy rises, while they can be able to sell the (renewable) electricity generated at home (by means of solar panels, for instance), thereby becoming the so-called microgrids.

The aforementioned model of metering is referred to as Advanced Metering Infrastructure (AMI). From a technical point of view, this infrastructure embodies a plethora of interconnected elements that collect the consumption data measured in the households to later be transferred to utilities through aggregation points and where part of this information is analyzed by means of Meter Data Management Systems (MDMS). Consequently, the process of data acquisition and processing to conduct further control procedures entails industrial and information technology equipment (which is integrated across the entire infrastructure) as well as the correct usage of devices and resources by all the stakeholders involved. At the same time, the increasing complexity of this architecture for the retrieval of metering information and the consequent control of the electricity generation has favored the appearance of cyber-security attacks that may jeopardize the availability of resources and hence put the stability of the grid at risk.

In this complex environment, access control is essential to manage the permissions of all users, processes and heterogeneous devices that continuously interact within the infrastructure. Therefore, it becomes mandatory to study the full range of requirements of this scenario to accurately apply the available solutions and propose a hybrid access control mechanism. This issue is addressed in this paper, which defines fine-grained policies by means of an authorization component that flexibly accommodates all these requirements in a modular way. More specifically, this component will be an integrated part of a hierarchical authorization framework over different devices. This authorization framework complies with robust policy rules following consolidated standards in the industry and considering the health state of the context at all times, using for this case a context-awareness manager. This authorization component also leverages the authentication module to validate the identity of the elements that request access to resources and sign the tokens that are received by the corresponding authorization entities.

The joining of all these components can certainly help issuing access control decisions in a timely manner without interfering in the throughput of the network assets, and ensuring a minimum level of security at all times.

Section II of the paper presents the Related Work, where the security implementations referring to the software developments have been presented. Afterwards, section III presents the system architecture of the SealedGRID project. Section IV presents the implementation of the authorization component, while section V describes the integration of FI-

978-1-7281-6728-2/20/$31.00 ©2020 IEEE

WARE AuthZ server and SealedGRID agent. Finally, in section VI, the results are concluded, and the future work is stated.

II. Related Work

Security interoperability is recognised as one of the most challenging research areas within the field of critical infrastructures by International Organizations such as the NIST, and IEEE. In this context, diverse technologies (sensors, meters, actuators, etc.) and various communication systems (WiMax, WiFi, ZigBee, 3G cellular, etc.) as well as different domains have to live together in a unified ecosystem to lead critical actions. These actions, related to the control of user's sensitive information (e.g., electrical consumption) running across the various components of the SG may be: i) corrupted by malicious actors if data are not correctly protected, or ii) disrupted due to the lack of standardization and interoperability mechanisms. The design of secure authorization and interoperability mechanisms is a complex task as specified in [1, 2]. They state that the interconnection between systems that were not originally envisioned to interoperate may present unanticipated problems, not just in operation, but in data availability, resolution, and format; it may also cause significant delays in the primitive operations.

A method for subdividing SG areas into microgrid domains is also considered by [3] to propose a Role-Based Access Control (RBAC) mechanism dependent on the area of responsibility. [4] proposes a scheme that provides a dynamic authorization for each user-role by computing the attribute-based hash value. The authorization is maintained so that each user can perform only those actions that are allowed under the access permissions granted to it. Regarding policy enforcement in SG environments, [5] proposes the use of smart energy gateways to establish trust relationships between parties using asymmetric key cryptography and cryptographic hash functions. [6] provides a middleware architecture based on RBAC, Policy Enforcement Points (PEPs) and Policy Decision Points (PDPs) to collect data streams from multiple sources connected to the Advanced Metering Infrastructure (AMI) in a standardised format. In [7], a solution based on the usage of PEPs and PDPs has been proposed to interconnect large distributions, containing technologies belonging to different infrastructures, manufacturers and vendors. In [8], a data-centric access control framework for smart grids that follow the publish/subscribe model has been proposed, adopting an Attribute-Based Authorization Policy. In [9], an authorization mechanism for monitoring and reduction of resource consumption by resource trading contribution, based on blockchain technology, has been designed. The proposed environment provides secure data access and storage along with controller functions transfers among householders.

The main limitation of the related work has to do with the fact that these solutions are not able to cope with the dynamic environment of SG, since they are based mainly on RBAC. Moreover, the above solutions do not provide any implementation details, nor performance evaluations through simulations.

Itron's OpenWay Riva [10] is a commercial communication platform that provides well-defined points of interoperability between customer and utility systems, greatly simplifying and reducing integration costs and issues.

III. SealedGRID Architecture

This section presents the SealedGRID architecture and its main components, as seen in Fig. 1. The Smart Meter (SM) is placed within a house or building, its purpose being to collect the readings of the electricity consumption. The Aggregator represents the binder between the collector and the smart meters. It has the role to sum all the readings received by the meters and transmit the results to the Utility. In this way, data becomes available without putting too much load on the Utility.

The role of the Utility device is to accumulate high-frequency aggregated values, and to use them later as it is a demand for a response, or to sum these values, in the end resulting in the total grid consumption. It can also be used for billing by computing the total consumption of a customer at the end of a billing period. The functions of the Utility are Federated Login, Access Control/Policy Maker, Key Management, TEE.

The SealedGRID architecture is especially based on the following requirements: End-to-End Security, Data-Driven Systems (Monitor→Analyse→Act), Platforms and Support Devices, Cross-Cutting Functionality, Tiered Approach, configurability, and Programmability. The Cross-Cutting functionality is necessary for the protection and the security of all layers of a smart grid. End-to-End Security provides security across all different layers and all devices. The Tiered Approach will collect and process information both close to IoT devices and at a cloud level. Data-Driven Systems will be used for the SealedGRID project and will support the development of smart grid blockchain based monitoring platform. These types of systems are based on the collection and the processing of security-related data to assess risks, identify and visualize threats and produce alerts. The SealedGRID architecture should be the support for the protection of different Smart Grid platforms and devices. The last requirement, configurability, and programmability are necessary to make the architecture of SealedGRID project more flexible in accommodating different security mechanisms in a configurable and programmable fashion.

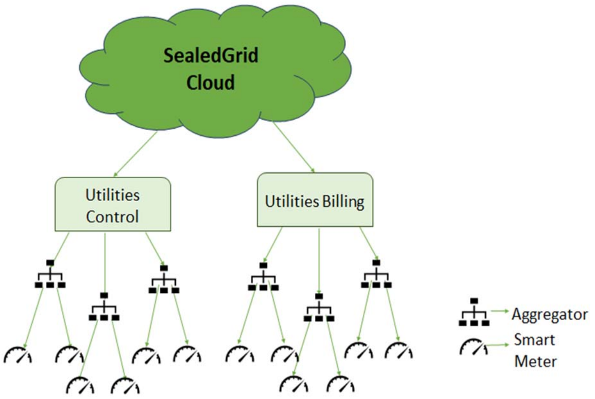


Fig. 1. SealedGRID Architecture Overview

Referring on the architecture of the authorization components, in the SealedGRID scenario, when different domains are interconnected to each other and collaborate, it is common to apply authorization frameworks based on the presence of Policy Information Points (PIPs), Policy Enforcement Points (PEPs) and Policy Decision Points (PDPs). These are entities that uptake different responsibilities on the authorization procedure (i.e., the decision of whether granting access to a resource that has been requested). SealedGRID will use a hierarchical architecture for the design and implementation of the authorization components (namely, the PIPs, PEPs and PDPs). Fig. 2 shows this architecture from a global perspective, portraying multiple roles spread over the topology, which will be further addressed when designing the actual control access policy.

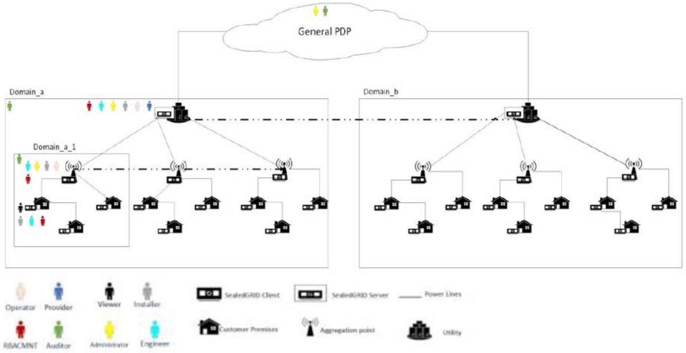


Fig. 2. Global architecture of the authorization components

For the moment, the figure specifically focusses on the assignation of PIPs, PEPs and PDPs to the infrastructure components. On the one hand, all elements of this infrastructure can be considered as a PIP and PEP, since all the SealedGRID devices embody a context-awareness module that provides information at all times to ease the access control decision. At the same time, all the devices can potentially submit an access request to the rest of elements within the same domain or others. For instance, a SealedGRID SM could potentially access its local aggregator and then this device could access its associated utility or other aggregators.

As for the decision points, different issues must be addressed. On the one hand, it is established the way to enable a multi-domain scenario where multiple utilities actively collaborate in a certain region for the management of the power supply, which results in a federated network that involves several partners (i.e., assuming the existence of more than one utility interconnected, as well as providers and customers). From the authorization perspective, this leads to the necessity of creating a common framework to define a global access control policy that applies rules for the secure and interoperable access between resources that belong to different domains.

Arrived at this point, all these initial assumptions are the subject of study to implement the global PDP using a Cloud Computing infrastructure. The reason is that the definition and readjustment of a global access control policy to the whole set of utilities underneath, needs to be centralised. This way, by placing PDPs on the individual utilities in a local way, the overhead introduced in the decision computation is reduced, since all requests that involve the local access to resources within a domain can be effectively resolved by the delegated utility. The use of utilities as intermediate PDPs with the global one thereby allows them to periodically update their policy rules by fetching the new changes from the cloud. In addition, this procedure can be also carried out at a domain level, by placing low-level PDPs in the precise aggregators when the requests concern devices in a localized area. For this purpose, some computation nodes in the edge of the network or the Fog Computation technology can be leveraged.

Fig. 3 represents the hierarchical architecture of these PDP entities at all levels, showing how remote stakeholders can gain access to resources by using PEP instances through the PDPs places in the domain or leveraging the PDP-cloud. Altogether, this design simplifies the centralized actions in the cloud and any occurrence of bottlenecks between domains.

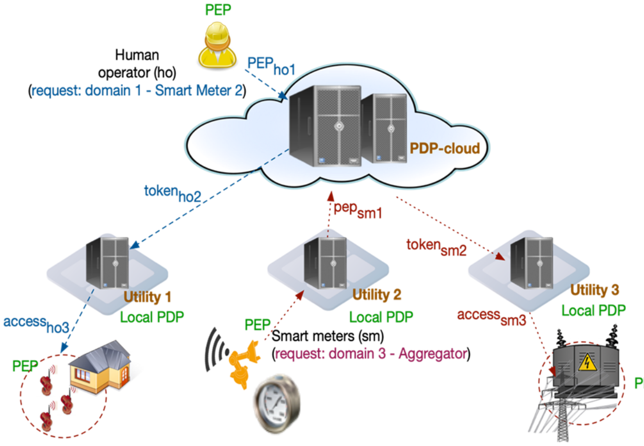


Fig. 3. Hierarchical architecture of the PEP and PDP entities

IV. IMPLEMENTATION OF THE AUTHORIZATION COMPONENT

This section describes an example implementation of SealedGRID eXtended Access Control Markup Language (XACML)-based PDPs as well as Policy Administration Points (PAP). In this case, both the PDP and PAP implementations rely on the open source AuthzForce Server [11], which is part of a FI-WARE system. AuthZForce provides a multi-tenant RESTful Application Programming Interface (API) to PAP and PDP which support Attribute-Based Access Control (ABAC) and is fully compliant with OASIS XACML 3.0 standard.

XACML policies are divided into a hierarchy of three levels, <PolicySet>, <Policy>, <Rule>:

- <PolicySet> represents a collection of <Policy> entities each containing one or more <Rule> elements;
- Every <Rule> from a <Policy> is evaluated as to whether it should provide access to a resource or not;
- The entire <Policy> result is defined by the whole result of all <Rule> entities processed in turn;
- Different <Policy> results are then evaluated against each other through combining algorithms that define which <Policy> wins in case of conflict.

AuthzForce is a FI-WARE Generic Enabler (GE), that provides open interfaces to application developers (APIs) as well as supporting interoperability with other GEs. AuthzForce Server is applied to comply with the SealedGRID purposes. While it is possible to use the core (community edition) [12] or just the RESTful PDP [13], it is only sufficient to provide further developments of the SealedGRID ecosystem and interoperate with other potential FI-WARE GEs.

Both for security and resource limitation reasons, the SealedGRID server exposes to the outer world (on the public Internet) only a selected set of endpoints, namely the endpoints which are invoked for the provisioning of the SealedGRID services, over the HyperText Transfer Protocol Secure HTTP(S) protocol. In addition to such endpoints, the platform also provides means to the project team members (for developers and system administrators in the future) to access the resources for performing deployment of new components, configurations, maintenance activities, etc. Therefore, the SealedGRID server can be accessed at three different levels:

1. HTTP access to the dashboard provided by Keyrock;
2. Direct access via SSH (Secure Shell) protocol;
3. Direct HTTP(S) access to service endpoints.

Access at levels 1 and 2 requires an active connection via SSH tunneling towards the authorization server. To get this access working, it is necessary to have a valid user account on the physical server. Access at level 3 is publicly available at URLs (Uniform Resource Locators) directly reachable from the Internet. This type of access is used by the SealedGRID components for inter-communication and from the SealedGRID devices for accessing the SealedGRID services.

As for visualisation, Keyrock provides a web-based dashboard for managing roles and applications, which allows users to monitor the environments and perform actions based on their role. The dashboard allows a series of RBAC operations on the users and applications. Some examples are shown in the following images. Fig. 4 represents the overview of the Keyrock Identity management that has been set up for SealedGRID along with a few example roles and a SealedGRID application.

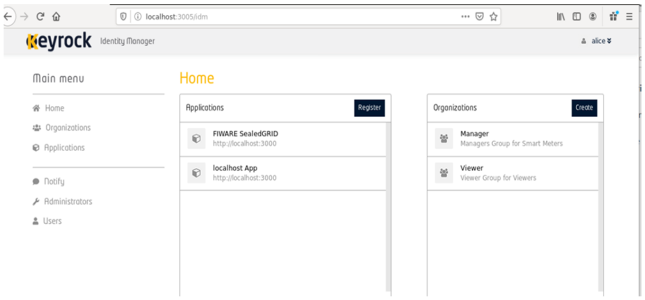
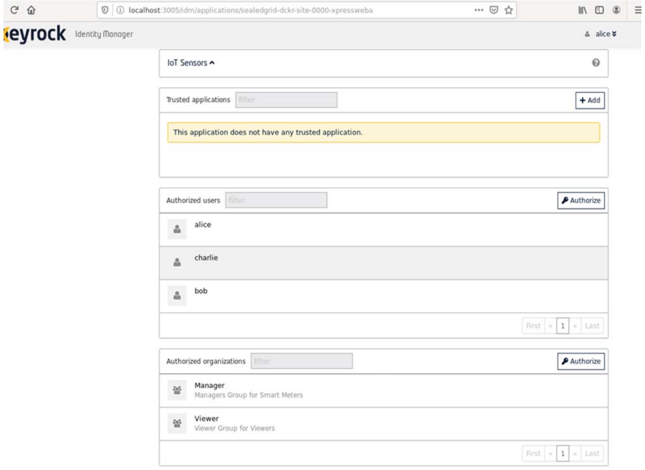


Fig. 4. Access to SealedGRID identity management dashboard

Fig. 5 shows the application view, listing the authorized users and the authorized organizations, etc.



This application does not have any trusted application.

Fig. 5. SealedGRID identity management dashboard - application view

Fig. 6 shows the user view, listing the authorized users belonging to a specific group within an organization, and the applications that they are authorized to use.

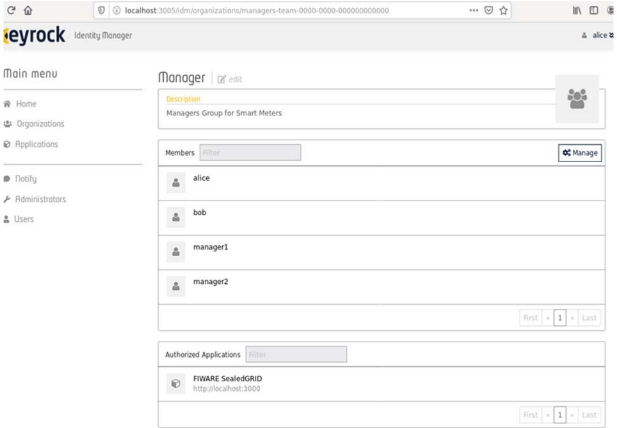


Fig. 6. SealedGRID identity management dashboard - user (role) view

Every SW application, secured by the Keyrock generic enabler, can define a set of permissions - i.e., a set of things that can be done within the application. For example, within the application, the ability to view SM readings could be secured behind a View permission. Similarly, the ability to send a command to operate a SM could be secured behind an Operate permission. These permissions are grouped together in a series of roles - for example: View and Operate could both be assigned to the Security role, meaning that Users who are subsequently given that role would gain both permissions. Permissions can overlap and be assigned to multiple roles - maybe Operate is also assigned to the management role. In turn, users or organizations will be assigned to one of more roles - each user will gain the sum of all the permissions for each role they have. For example, if Alice is assigned to both management and security roles, she will gain all permissions View and Operate. The concept of a role is unknown to a user - they only know the list of permissions they have been granted, not how the permissions are split up within the application. In summary, permissions are all the possible actions that can be done to resources within an application, whereas roles are groups of actions which can be done by a type of user of that application.

Referring to direct access via SSH protocol, Keyrock provides a web-based dashboard for managing roles and applications, which allows users monitoring capabilities. This type of access is used by SealedGRID developers and administrators for installing software, handling configurations, managing updates, etc. Due to resource limitations, the whole infrastructure was set up leveraging only one server.

Considering the direct HTTP(S) access to service endpoints, the HTTP services deployed are made available to the outer world via a dedicated SealedGRID server. The services allow administering XACML policies (PAP) and requesting decisions from the AuthzForce server (PDP).

V. Integration of authentication and authorization components

The token provided by SOMA, the key management and authentication solution that has been implemented in an isolated simulation environment, has to be validated by the authentication component. To do this, the authentication component proceeds to send a request to the AuthZ server containing the value of the Environment Category corresponding to the value of the SOMA certificate validity (whether it is true or false).

The policy can be added or updated by making the necessary request to the AuthZ server. Each request can (optionally) present an environment value (i.e. a value of the context). The environment attribute is called is-soma-present and, if present, has to be True, for the request to be validated.

Referring to the authentication module, it is required to validate the identity of the entities that submit the access request. It involves not only SealedGRID devices (which may perform a local authentication using SOMA), but also human operators, engineers or customers using mobile devices, for which the use of OpenID protocol might be required. In general, this module accepts any token that has previously been signed with the appropriate certificates of authority. Once they have been validated, the token is processed with the access manager.

In this module we utilize the key pair of an Introducer node, and the public key of a normal node. The attributes of the normal node, along with its public key are hashed before being signed with the introducer's private key. At this point, the essence of a SOMA certificate has been created. Any node with access to the introducer's public key will be able to verify that the hashed public key and attributes of this specific node are endorsed by an empowered entity in the network. For certificate verification, the introducer's public key is utilized. Depending on the verification outcome, the corresponding JavaScript Object Notation (JSON) request will be performed.

VI. Conclusion and Future Work

To conclude, the paper presented one of the key modules of SealedGRID, namely the authorization module which is composed from PIP/PEP/PDP, RBAC/ABAC and related standards. The implementation of the authorization component based on FI-WARE has been presented, describing mainly Keyrock integration. Also, the integration of FI-WARE AuthZ server and SealedGRID agent has been introduced. As future work, all of these components will be integrated to provide a dynamic and complex authorization engine and the security policy manager will be specified.

Ackwoledgment

This work has been supported by "European Union's Horizon 2020 research and innovation program under grant agreement No. 777996 (SealedGRID project). This work has been partially funded by the Operational Programme Human Capital of the Ministry of European Funds through the Financial Agreement 51675/09.07.2019, SMIS code 125125.

References

[1] T. Magee, "Secure Interoperable Open Smart Grid Demonstration Project," 2014.

[2] C. Alcaraz and J. Lopez, "Secure Interoperability in Cyber-Physical Systems," Cyber Warfare and Terrorism, pp. 521–542, 2020.

[3] D. Rosic, U. Novak, and S. Vukmirovic, "Role-Based Access Control Model Supporting Regional Division in Smart Grid System," 2013 Fifth International Conference on Computational Intelligence, Communication Systems and Networks, 2013.

[4] N. Saxena, B. J. Choi, and R. Lu, "Authentication and Authorization Scheme for Various User Roles and Devices in Smart Grid," IEEE Transactions on Information Forensics and Security, vol. 11, no. 5, pp. 907–921, 2016.

[5] N. Kuntze, C. Rudolph, I. Bente, J. Vieweg, and J. V. Helden, "Interoperable device identification in Smart-Grid environments," 2011 IEEE Power and Energy Society General Meeting, 2011.

[6] A. Veichtlbauer A, D. Engel, J. Ressel, F. Knirsch, O. Langthaler and F. Moser, "Advanced metering and data access infrastructures in smart grid environments," 2013 seventh international conference on sensor technologies and applications (SENSORCOMM), pp. 63–8, 2013.

[7] C. Alcaraz, J. Lopez, and S. Wolthusen, "Policy enforcement system for secure interoperable control in distributed Smart Grid systems," Journal of Network and Computer Applications, vol. 59, pp. 301–314, 2016.

[8] L. Duan, D. Liu, Y. Zhang, S. Chen, R. P. Liu, B. Cheng, and J. Chen, "Secure Data-Centric Access Control for Smart Grid Services Based on Publish/Subscribe Systems," ACM Transactions on Internet Technology, vol. 16, no. 4, pp. 1–17, Jul. 2016.

[9] R. Alcarria, B. Bordel, T. Robles, D. Martín, and M.-Á. Manso-Callejo, "A Blockchain-Based Authorization System for Trustworthy Resource Monitoring and Trading in Smart Communities," Sensors, vol. 18, no. 10, p. 3561, 2018.

[10] "OpenWay Riva," Itron. [Online]. Available: https://blogs.itron.com/tag/openway-riva/. [Accessed: 20-Feb-2020].

[11] Authzforce, "authzforce/server," GitHub, 25-Jul-2019. [Online]. Available: https://github.com/authzforce/server. [Accessed: 08-Dec-2019].

[12] Authzforce, "authzforce/core," GitHub. [Online]. Available: https://github.com/authzforce/core. [Accessed: 08-Dec-2020].

[13] Authzforce, "authzforce/restful-pdp," GitHub. [Online]. Available: https://github.com/authzforce/restful-pdp. [Accessed: 08-Dec-2019].