Attribute-based Access Control for Secure and Resilient Smart Grids

George Suciu
BEIA Consult International
Bucharest, Romania
george@beia.ro

Cristiana-Ioana Istrate
BEIA Consult International
Bucharest, Romania
cristiana.istrate@beia.ro

Alexandru Vulpe
University Politehnica of Bucharest
Bucharest, Romania
alex.vulpe@radio.pub.ro

Mari-Anais Sachian
BEIA Consult International
Bucharest, Romania
anais.sachian@beia.ro

Marius Vochin
University Politehnica of Bucharest
Bucharest, Romania
mvochin@elcom.pub.ro

Aristeidis Farao
Neurosoft S.A, Greece
Piraeus, Greece
a.farao@neurosoft.gr

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

Recent advancements of Information and Communication Technologies (ICT) have made it a part of almost every domain of everyday life, including the power grid, leading to what is known as the Smart Grid. But the power grid, a critical economic and social infrastructure, is vulnerable to security threats stemming from the use of ICT and to new emerging vulnerabilities and privacy issues. Access control is a fundamental element of the security infrastructure, as, ideally, the principle of less privilege, zero-trust, segregation of duties, and other best practices should be applied without disrupting the functioning of the power grid while also properly maintaining the security of the Smart Grid. The paper presents the work undertaken in the SealedGRID project and the steps taken for implementing Attribute-based Access Control policies specifically tailored to the Smart Grid.

Keywords: Smart Grid, Attribute-based Access Control, eXtensible Access Control Markup Language, Abbreviated Language For Authorization

1. INTRODUCTION

There has been rapid evolution in the field of Information and Communication Technologies (ICT) and this evolution has also found its way into the electrical grid. Thus, the term Smart Grid [1] has been devised as representing a more intelligent, responsive, and efficient electrical system, using ICT for centrally monitoring, controlling, and optimising the power grid.

However, with the arrival of ICT, the power grid [2], which is a vital economic and social infrastructure, also inherits the security threats from the ICT world. These include privacy issues and vulnerabilities that are related to the characteristics of the Smart Grid infrastructure. Since a potential attack to the Smart Grid [3] may lead to disastrous failures, ranging from destruction of other interconnected critical infrastructures (e.g. gas, water, and transportation) to loss of human lives, the problem is deemed as critical. Moreover, one cannot simply migrate ICT security solutions to the Smart Grid, therefore new approaches are necessary.

Blockchain [4] is a novel driving technology behind the decentralized web. It is a shared, immutable ledger that enables recording of transactions and tracking assets in a business network. An asset can be anything from tangible ones (a house, a car, currency, land) to intangible ones (energy consumption, intellectual property, branding). Anything that is quantifiable can be tracked and stored in a blockchain network, reducing risk and cutting costs for all involved.

This paper presents a new architecture for secure and resilient smart grids. The main contribution of this paper is the specific combination of Blockchain

solutions and Web of Trust for the optimization of key management and authentication for the Smart Grid nodes.

The paper is organized as follows: Section 2 briefly describes the SealedGRID project and its envisioned achievements, while Sec 3 introduces the challenges and opportunities of blockchain in Smart Grids. Sec 4 describes the proposed SealedGRID architecture, introducing the main components while Sec 5 preliminary evaluates a reference implementation of the SealedGRID authorization and policy enforcement framework.

2. About SealedGRID Project

The electrical network [5] is one of the most important economic and social infrastructures that can be exposed to security threats in the ICT sector, introducing new confidentiality issues and vulnerabilities related to the specific features of the smart network infrastructure. The SealedGRID effectively and jointly cope with three significant challenges:

- **Scalability**: Smart Grid Utilities will manage a plethora of Smart Meters, making the Utility side of the Smart Grid a highly vulnerable target, since a potential attack may destruct the entire energy distribution system.
- **Trust**: Smart Grid nodes will be accessible by customers creating a fertile field for malicious users that may physically modify hardware or software to intercept personal information or alter energy measurements and costs.
- **Interoperability**: Smart Grid protection will cope with inter-domain security issues between nodes that implement different security policies and services.

SealedGRID aims at designing, analyzing, and implementing a scalable, highly trusted and interoperable Smart Grid security platform. Towards this direction, SealedGRID is committed to creating a fully integrated and multi-disciplinary programme, while all efforts and funding will be focused on this purpose. This platform will offer enhanced features that enable strong authentication, attribute-based access control, role-based access control, anonymous attestation mechanism, trusted execution environment, digital certificates, web of trust and blockchain.

3. Blockchain and Smart Grids

Blockchain [6] represents a decentralized digital repository managed by a network of equally assigned computers where each one of them executes tasks for independent authenticating. It is a reliable architecture for data transaction which might be suspicious, by offering features such as immutability and tampering detection. Advances in this field made possible the management of larger data transactions.

Going forth with the upcoming changes and development in Smart Grid [7], this technology can be applied to a power energy system or the energy produced may be converted to cryptocurrency. Specifically, for this operation, blockchain [8] serves as a strong security measure that will limit the possibility of intrusion by finding the exact key.

A Smart Grid system though, can face various challenges [9], like if it is secure enough, if someone can breach into the system, what is to be done in situations where the system faces outages, what can be done to save more energy? Facing such issues must be solved for optimization and security.

The SealedGRID project aims at including the aforementioned features, therefore its conceptual architecture will be further described.

4. Architecture description

The participant entities in the proposed functional architecture behind smart grids, presented in Figure 1, include the SG device (Smart Meter), the SG aggregator, the SG utility, the external adversary and the insider adversary. The Smart Meter [10] is responsible for collecting electricity consumption readings. The number of Smart Meters in each building varies, depending on the size of the building.

The Aggregators are intermediate nodes between the collector and the Smart Meters, which sum the individual readings received by the meters and transmit the result to the collector. This way, processing is distributed among the Aggregators and data for demand response become available without putting too much load on the Utility. In some cases, the architecture might not include explicit entities that perform intermediate aggregation and Smart Meters can play this role as well.

The Utilities accumulate high-frequency aggregated values. They can either use these values as is for demand response (e.g., control the electricity

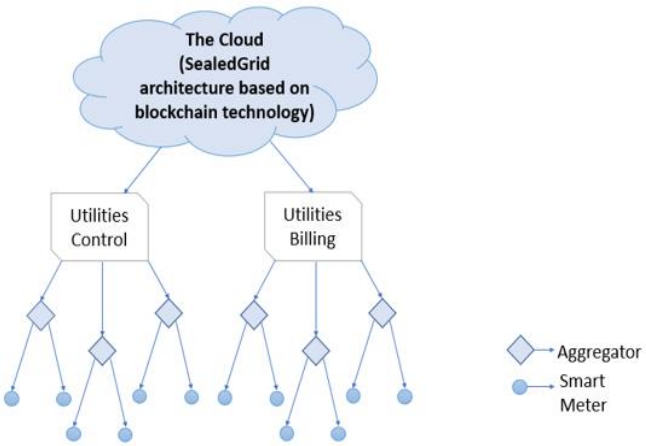

Figure 1: *SealedGRID conceptual architecture*

consumption in a specific area) or sum them to come up with the total grid consumption. The collector is also responsible for billing by computing the total consumption of a customer at the end of a billing period (e.g., one month) using low-frequency metering data.

The external adversary is not part of a SealedGRID domain. It aims at destroying the domain, violating customer's privacy or endangering the accountability, the availability, the integrity or the confidentiality of the system.

The insider adversary is part of a SealedGRID domain. The device can successfully complete the authentication and the authorization process with the platform. It aims at violating customer's privacy or endangering the accountability, the availability, the integrity or the confidentiality of the system.

4.1 Security policy considerations

Within SealedGRID, strict security policies are being considered. When different domains are connected to each other and collaborate, it is common to apply authorization frameworks based on:

Policy Enforcement Points (PEP) [11]: These are used by devices or processes to request different resources of the system and intercept and forward an authorization request to a Policy Decision Point (PDP).

Policy Decision Points (PDP): Once the decision is taken, the PEP permit or denies the access. Therefore, the PDP is in charge of designing the control-access policy and managing authorization between domains.

All SealedGRID devices are considered as **Policy Information Points (PIPs)**: they associate the set of attribute values to resources (e.g., Smart Meters) based on the context information.

In SealedGRID we transition from Role-Based Access Control (RBAC) to Attribute-Based Access Control (ABAC). Thus, we consider, within SealedGRID, the use of eXtensible Access Control Markup Language (XACML) for devising RBAC policies. XACML [12] is an XML-based language for access control that is standardized by the OASIS consortium. It provides a fine-grained authorization method as it specifies the requirements and variables in an access control policy that are used to authorize access to a resource.

The challenge in SealedGRID is represented by mapping the entities of the SealedGRID system to the usual components that are used to specify XACML policies. In XACML [13] four categories are defined:

Subject: Defines who or what is demanding access to an information asset

Resource: Represents the information asset or object impacted by the action

Action: Represents the action the subject wants to perform

Environment: Defines the context in which access is requested.

Table 1: *Defined entities*

Short name	Namespace	Category	Data type	Value range
role	eu.sealedgrid.user	Subject	String	Operator, Auditor, Provider, Customer, Administrator, Installer, Engineer
actionId	eu.sealedgrid.action	Action	String	View, Read, Dataset, Reporting,FileRead,FileWrite ,FileManagement,Control, Config, SettingGroup, Security
objectType	eu.sealedgrid.object	Resource	String	SmartMeter, Aggregator, Utility
criticality	eu.sealedgrid.context	Environment	String	Low, Medium, High
anomalyLevel	eu.sealedgrid.context	Environment	Double	0...0.01...1
communicationProtocol	eu.sealedgrid.context	Environment	String	Modbus, OPC UA, Ethernet/IP
domainId	eu.sealedgrid.domain	Subject	String	A, B, C, D…

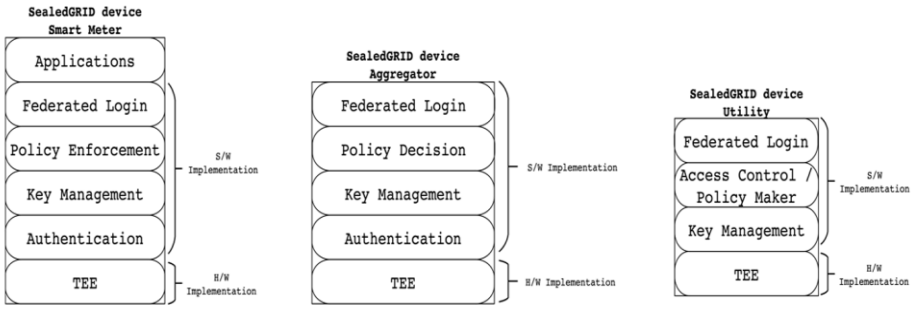

Figure 2*: Components and their functions*

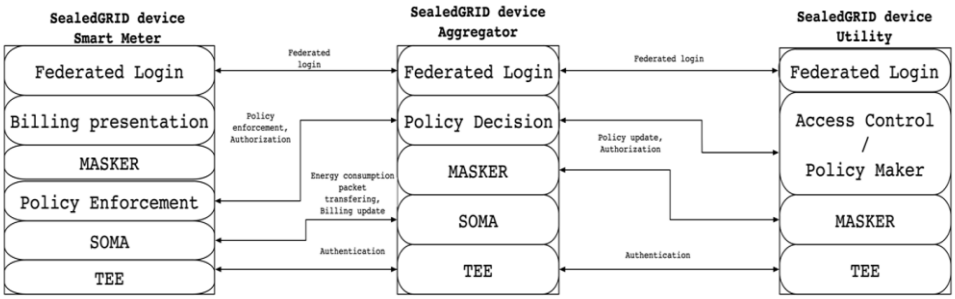

Figure 3: *The main architectural components with the modules that comprise each component*

An example sentence like:

```
Jane Doe wants to view a confidential document at work during regular business hours
```

can be translated into an XACML policy but before that, authorization requirements have to be gathered.

In SealedGRID we performed this exercise and defined a series of subjects, resources, actions and environments that are used to define XACML

policies. Table 1 illustrates a part of the entities defined. The values for roles and actions have been identified according to roles and rights belonging to IEC-62351-8. This is a reference in the sector to address the security of industrial network, since it provides useful guidelines for introducing authenticity, confidentiality and integrity in the communication and control protocols of the Smart Grid. It is composed of eleven parts, part 8 being especially applied to control access mechanisms based on RBAC.

In Figure 2, a detailed description with the required functionalities of each component is provided.

In Figure 3, a detailed description for each component, its modules, and how they interact with other components, is provided.

5. IMPLEMENTATION AND DISCUSSION

As an example of Attribute-based Access Control for Smart Grids, the following simple authorization requirement:

```
Any customer can read or report a problem with a smart meter
```

was translated into the following attribute-based rule

```
A user with role=="viewer" can actionId=="view" AND actionId=="Reporting" on objectType=="smartMeter"
```

To create an XACML policy [14], and demonstrate the example above, we used the Abbreviated Language For Authorization (ALFA) programming language which is widely used in the formulation of access-control policies. We used the entities that were previously defined in Table 1 to implement XACML policies for our SealedGRID system.

The first step was to define the attributes that we were going to define for implementing the access rules for our SealedGRID system. As previously mentioned in Section 2, we had to define a Subject, a Resource and an Action. As previously stated, the Subject performs an Action which has an impact on the Resource.

Therefore, we defined the Attributes as in the following code:

```
namespace Attributes {
      import System.*

      attribute role {
        id = "eu.sealedgrid.user.role"
        type = string
        category = subjectCat
      }

      attribute objectType {
            id                          =
"eu.sealedgrid.object.objectType"
            type = string
            category = resourceCat
      }

    attribute actionId {
        id                              =
"eu.sealedgrid.action.actionId"
        type = string
        category = actionCat
    }
}
```

The following code snippet illustrated the formulation of the simple Access Control policy defined previously:

```
namespace eu.sealedgrid.object{
      policy userReporting{
            target              clause
Attributes.objectType == "SmartMeter"
            apply permitOverrides
            rule {
                  permit
                  condition
Attributes.role    ==    "viewer"    &&
Attributes.actionId == "Reporting"
            }
      }
}
```

The resulted XACML policy is retrieved after running our defined Access Control policy and is displayed below:

```
<?xml version="1.0" encoding="UTF-8"?>
[...]
PolicyId="eu.sealedgrid.object.userReporting"
    [...]
       <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
           <xacml3:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">SmartMeter</xacml3:AttributeVal
ue>
           <xacml3:AttributeDesignator
```

```
                AttributeId="eu.sealedgrid.object.objectType"
                DataType="http://www.w3.org/2001/XMLSchema#string"
                Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
                MustBePresent="false"
            />
        </xacml3:Match>
    [...]
    <xacml3:Rule
             Effect="Permit" RuleId="eu.sealedgrid.object.userReporting.Id_62">
    [...]
          <xacml3:Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of">
                <xacml3:Function
FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-equal"/>
                    <xacml3:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">viewer</xacml3:AttributeValue>
                    <xacml3:AttributeDesignator
                        AttributeId="eu.sealedgrid.user.role"
                        DataType="http://www.w3.org/2001/XMLSchema#string"
                        Category="urn:oasis:names:tc:xacml:1.0:subject-
category:access-subject"
    [...]
DataType="http://www.w3.org/2001/XMLSchema#string">Reporting</xacml3:AttributeValu
e>
                    <xacml3:AttributeDesignator
                        AttributeId="eu.sealedgrid.action.actionId"
                        DataType="http://www.w3.org/2001/XMLSchema#string"
                        Category="urn:oasis:names:tc:xacml:3.0:attribute-
category:action"
    [...]
```

This previous example serves two purposes:

1. It shows how an XACML policy is written for smart grids. Using XACML policies will be one of the cornerstones of smart grids access control.
2. It also shows an example of how a generated XACML policy looks compared to the simplicity of using the ALFA language and highlights the more human-readable way of formulating an Attribute-based Access Control policy

This generated XACML policy will be the pillar of smart grids access control. These rules will be processed by an authorization engine that can be accessed by external entities to submit a request and obtain the corresponding authorization token. At the same time, this authorization engine can be coupled with a context awareness mechanism to assess the security for the requested action according to the context it is in.

6. Conclusion and Future Work

The paper presented steps taken to implement XACML policies tailored for smart grids. Proper XACML entities were defined according to the scope and purpose of the SealedGRID project. Also, a reference implementation of a simple policy using ALFA was described.

Future work will lead to the implementation of the aforementioned policies into the overall SealedGRID system

Acknowledgment

This research has received funding from the EU as part of the SealedGRID project (H2020-MSCA-RISE-2017 under grant agreement No 777996)

References

[1] Abbasi, S., Barati, M., & Lim, G. J. (2019). A Parallel Sectionalized Restoration Scheme for Resilient Smart Grid Systems. IEEE Transactions on Smart Grid, 10(2), 1660–1670. http://doi.org/10.1109/tsg.2017.2775523

[2] Electric Network Analysis in Energy Processing and Smart Grid. (2018). Energy Processing and Smart Grid, 5–29. http://doi.org/10.1002/9781119521129.ch2

[3] The Smart Grid: Status and Outlook - fas.org. Retrieved May 2, 2019, from https://fas.org/sgp/crs/misc/R45156.pdf

[4] Blockchain: A Technical Introduction. (2018). Inclusive FinTech, 207–258. http://doi.org/10.1142/9789813238640_0006

[5] Analysis of Information Security Protection Strategy for Network Electronic Engineering Archives. (2018). 2018

5th International Conference on Electrical & Electronics Engineering and Computer Science (ICEEECS 2018). http://doi.org/10.25236/iceeecs.2018.084

[6] Rahman, M. A., Rashid, M. M., Hossain, M. S., Hassanain, E., Alhamid, M. F., & Guizani, M. (2019). Blockchain and IoT-Based Cognitive Edge Framework for Sharing Economy Services in a Smart City. IEEE Access, 7, 18611–18621. http://doi.org/10.1109/access.2019.2896065

[7] Passerini, F., & Tonello, A. M. (2019). Smart Grid Monitoring Using Power Line Modems: Anomaly Detection and Localization. IEEE Transactions on Smart Grid, 1–1. http://doi.org/10.1109/tsg.2019.2899264

[8] Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., … Peacock, A. (2019). Blockchain technology in the energy sector: A systematic review of challenges and opportunities. Renewable and Sustainable Energy Reviews, 100, 143–174. http://doi.org/10.1016/j.rser.2018.10.014

[9] Khoussi, S., & Mattas, A. (2017). A Brief Introduction to Smart Grid Safety and Security. Handbook of System Safety and Security, 225–252. http://doi.org/10.1016/b978-0-12-803773-7.00011-5

[10] Smart Meter Data and Privacy. (2015). Data Privacy for the Smart Grid, 55–74. http://doi.org/10.1201/b18005-5

[11] Retrieved May 2, 2019, from https://www.jerichosystems.com/technology/glossaryterms/policy_enforcement_point.html

[12] Pereira, Ó. M., Semenski, V., Regateiro, D. D., & Aguiar, R. L. (2017). The XACML Standard - Addressing Architectural and Security Aspects. Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security. http://doi.org/10.5220/0006224901890197

[13] Oh, Y., & Lee, S. U.-J. (2018). Case Study for Collecting Policy Evaluation Factors upon Request when Creating XACML Policy. Journal of KIISE, 45(9), 975–979. http://doi.org/10.5626/jok.2018.45.9.975

[14] Ayed, D., Lepareux, M.-N., & Martins, C. (2015). Analysis of XACML policies with ASP. 2015 7th International Conference on New Technologies, Mobility and Security (NTMS). http://doi.org/10.1109/ntms.2015.7266473