FI-WARE based authorization for a smart grid's scalable, trusted, and interoperable platform - Practical Experience Report

George Suciu[1][0000−0001−8455−6177], Alexandru Vulpe[1,2][0000−0003−1970−1117], Cristiana Istrate[1], Mari-Anais Sachian[1], and Marius Vochin[2][0000−0003−1962−035X]

[1] Beia Consult International SRL, Bucharest, Romania
{george,cristiana.istrate,anais.sachian}@beia.ro
[2] University Politehnica of Bucharest, Bucharest, Romania
alex.vulpe@radio.pub.ro, marius.vochin@upb.ro

Abstract. The traditional models of the electric grid, based on centralized systems for the production and distribution of energy, have greatly changed over the recent years, with the Smart Grid having an increased vulnerability to external attacks. This report presents the architecture of a global authorization component that is proposed for a Smart Grid scalable, trusted, and interoperable platform, related to the SealedGRID project. This component is modeled by using a hierarchical architecture consisting of different authorization entities, that effectively manage the access to the various resources within the grid infrastructure based on defined policy rules, while also taking into account the security state of these resources (per domains or substations).

Keywords: Smart Grid · Security · Access Control.

1 Introduction

We report here on fine-grained access control policies for crticial infrastructure (Smart Grid) by means of an authorization component that will be an integrated part of a hierarchical authorization framework over different devices. This authorization framework complies with robust policy rules following industry standards and considering the health state of the context at all times.

2 System Model

The SealedGRID hierarchical architecture and its main components are presented in Fig. 1. 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 and also communicate with a blockchain component [1].

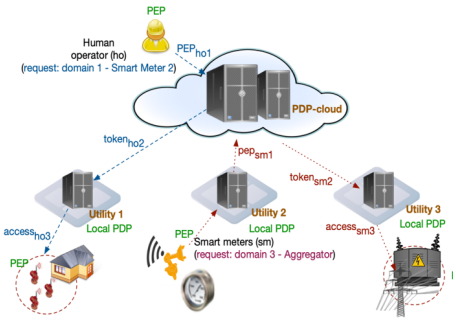

Fig. 1: Hierarchical architecture of the PEP and PDP entities

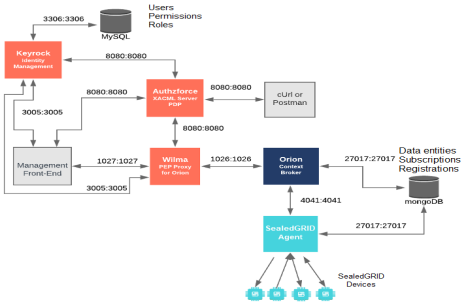

Fig. 2: Envisioned interaction between SealedGRID authorization components

3 Integration of FI-WARE and SealedGRID

Management and SealedGRID device application will be based on those created in FIWARE and will secure access to the context broker behind a PEP proxy.

All access control decisions will be delegated to an AuthZForce server which will read the ruleset from a previously uploaded policy domain. At the moment, interaction with other Generic Elements (GEs) is only facilitated (they are included in the service creation scripts) and will be for further implementation. Fig. 2 illustrates the interaction between the GEs adapted for SealedGRID purposes.

The token provided by SOMA[2], the key management and authentication solution , has to be validated by the authentication component. For this, it sends a request to AuthZForce containing the value of the Environment Category corresponding to the value of the SOMA certificate validity (true or false). The policy can be added or updated by making the necessary request to AuthZForce. The environment attribute has to be True, for the request to be validated.

4 Conclusions

One of the key modules of SealedGRID, namely the authorization module which is composed from PIP/PEP/PDP, RBAC/ABAC and related standards, has been presented. The implementation of the authorization component based on FI-WARE has been presented as well as its integration with SealedGRID agent.

References

1. Suciu, G., Sachian, M.A., Dobrea, M., Istrate, C.I., Petrache, A.L., Vulpe, A., Vochin, M.. Securing the smart grid: A blockchain-based secure smart energy system. In 2019 54th International Universities Power Engineering Conference (UPEC), pp. 1-5. IEEE, 2019
2. Demertzis, F. F. & Xenakis, C. SOMA-E: Self-organized mesh authentication-Extended. Mathematical and Computer Modelling, 2013, 57, 1606-1616