SealedGRID: Scalable, trustEd, and interoperAble pLatform for sEcureD smart GRID

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

Christoforos Ntantogian
Department of Digital Systems, University of Piraeus, Greece
dadoyan@unipi.gr

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

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

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

Currently, much effort is being made on a European and global level, to push towards realizing a sustainable development of the Smart Grid, with the minimum vulnerability to external attacks or to malicious Smart Grid nodes. Utility companies globally invest in an efficient, controlled and flexible distribution of the energy to optimize the services they provide to the end customers. On the other hand, individual clients call for more efficient Smart Grid solutions with guaranteed highly secure Demand Response services that could reduce their electricity bill without sacrificing their privacy or their energy-consuming habits. In this paper, we present the SealedGRID that provides an innovative platform that abides by the existing standardization work and is directly utilized by the shareholders to provide new tools towards a scalable, highly trusted, and interoperable Smart Grid security platform.

Smart Grid, SealedGRID, Scalability, Trust, Interoperability, Privacy, Secure, Demand Response

1. INTRODUCTION

The advantages of the Smart Grid (SG) in a general scale are energy independence, emissions control and global warming combat. Each Utility is able to design better pricing policies, capacity and usage planning and to increase resilience and protection against cyber and physical attacks. On the other hand, there are the households, that represent the customers. They are the entity who consumes the produced energy. The SG enables them to manage in real-time their energy consumption, billing and even let them be involved as energy producers. However, the SG which is a vital economic and social infrastructure is exposed to security threats inherited from the Information and Communications Technology sector. The problem is assessed as crucial, considering that a potential attack to the SG may lead to cascading failures, ranging from destruction of other interconnected critical infrastructures (e.g., gas, water, and transportation) to loss of human lives.

SealedGRID aims to design, analyze, and implement a scalable, highly trusted and interoperable SG security platform. The SealedGRID architecture should support security as a cross-cutting functionality that protects and secures all layers of a SG. Also, SealedGRID supports security end-to-end e.g., across all different layers of a SG system and across all the components that it comprises. Moreover, it provides security functions of various latencies that operate in various timescales. Furthermore, the SealedGRID architecture supports security monitoring and behavioral analysis functionalities. In particular, SealedGRID supports the development of data driven systems that are based on the collection and processing of security-related data in order to assess risks, identify and visualize threats and produce alerts, among other security services. Finally, the architecture is flexible in accommodating different security mechanisms in a configurable and programmable fashion e.g., without essential changes in the structure and implementation of the SG compliant systems.

The rest of the paper is organized as follows: Section 2 presents the reference architecture of SealedGRID and its goals. Section 3 presents the related work; while Section 4 describes how SealedGRID outweighs the other state-of-the-art research activities and presents the different utilized technologies by SealedGRID and describes how these are integrated in the architecture. Section 5 provides the SealedGRID impact on the SG ecosystem . Finally, Section 6 concludes the paper and envisions future work.

2. SEALEDGRID

Figure 1 depicts a simplified representation of the SealedGRID platform. In this architecture, we assume that that there is a mix of SealedGRID-equipped devices and legacy devices that implement different or deprecated security mechanisms. Moreover, each Operator or Utility defines its own security policy. Devices residing in a domain where SealedGRID has already been deployed need only SealedGRID Client in order to communicate securely with the rest of SealedGRID enabled devices. SealedGRID Client comprises the following modules: i) key management; ii) authentication; iii) trusted computing; iv) privacy protection components which can securely communicate with other SealedGRID Clients. In places where interoperability with legacy devices and diverse policies should be preserved (e.g., inter-connections) the SealedGRID Server will be installed. SealedGRID Server comprises a SealedGRID Client to communicate with other Clients, as well as the following modules: i) authorization and ii) security interoperability component. SealedGRID Server acts as a gateway and ensures secure and reliable communication with other SG entities that are not equiped with one. Furthermore, it assists in the gradual deployment of the proposed platform, preserves compatibility with older devices, and ensures that diverse security policies among utilities are not broken while SG operations are successfully fulfilled. The SealedGRID Client is part of a Smart Meter that has been installed in households or other buildings; while the SealedGRID Server is installed in an Aggregator or a Utility.

3. RELATED WORK

In this section, we present, the state-of-the-art technologies and the current research activity of the SealedGRID modules. Starting with the Key management of the SG; state-of-the-art findings show that each category of solutions presents its own weaknesses. There are key management schemes based on shared secret keys e.g, [1] uses symmetric keys and every node has to maintain one key for each secure connection to another node; this, however, hinders scalability. Also, there are schemes that utilize ID-based cryptography, like [2]; however, their main drawback is that the Private Key Generator should always be online and available, and can be a single point of failure. Furthermore, there are schemes based on hierarchical Public Key Infrastructure (PKI) architecture e.g., [3]. Nevertheless, this architecture does not suit the SG, as stated in [4], since it does not meet the high availability requirement, with the root Certification Authority (CA) being a single point of failure. In [5] group key management is used, producing a solution that is robust against replay and node capture attacks. As for commercial products, Sensus utilizes the Security Key Lifecycle Manager [6] from IBM in its smart meters, while Elster implements its own key management system in its EnergyAxis solutions [7]; however, both key management systems are centralized. SYPRIS Electronics [8] provides its Cryptographic Key Management System, which is based on compartmentalization (e.g., use different

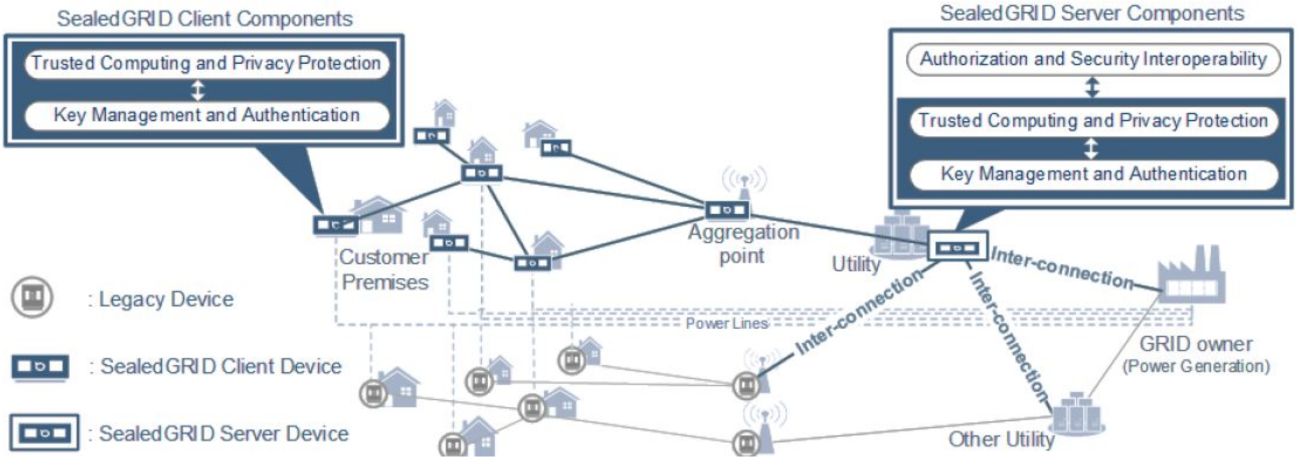
SealedGRID Client Components
Trusted Computing and Privacy Protection
Key Management and Authentication
SealedGRID Server Components
Authorization and Security Interoperability
Trusted Computing and Privacy Protection
Key Management and Authentication
Customer Premises
Aggregation point
Utility
Inter-connection
Inter-connection
Inter-connection
Power Lines
GRID owner (Power Generation)
Other Utility
: Legacy Device
: SealedGRID Client Device
: SealedGRID Server Device

Figure 1: *Abstract representation of the SealedGRID platform as it will be applied to the Smart Grid*

keys for different locations or types of devices) and centralized key generation.

[9] proposed a lightweight, mutual authentication and key agreement protocol based on hash message authentication codes. DNP3 Authentication [10] and IEC 62351-5 [11] are some of the primary cyber security standards identified by NIST as pertinent to their ongoing interoperability effort. In the commercial domain, Maxim provides an integrated authentication protocol based on AES encryption in products like its MAX36025 smart meter [12]. Gemalto provides security solutions to smart meter manufacturer; for authentication, the recommended solution is an identity-based model utilizing a PKI [13]. Finally, regarding Blockchain technology, there are no systematic approaches yet that attempt to investigate how Blockchain [14] technology can be employed in SG to achieve non-trusting members of SG to interact to each other without the need of a trusted intermediary.

According to standardization organizations CEN/CENELEC/ETSI [15], the efficiency and privacy requirements of a privacy preserving mechanism for the SG can be met using masking. Such methods [16], [17], [18] lack protection against non-repudiation and adaptability in case a node joins or leaves. Commercially, the well-known privacy compliance and risk management company TRUSTe provides the TRUSTed Smart Grid Privacy Program [19] that assesses and certifies the privacy practices of third-party companies that require access to consumers' energy usage data. Energy Smart Florida, which has deployed over three million advanced smart meters, protects privacy by not storing customer identifying information and usage history in the meters, while all information is encrypted [20].

International Organizations such as the NIST, and IEEE recognize security interoperability as one of the most challenging research areas within the field of critical infrastructures. 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 coexist in a unified ecosystem to lead critical actions. These actions, related to the control or 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 [21], [22]. They state that the inter-connection 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 [23] to propose a Role Based Access Control (RBAC) mechanism dependent on the area of responsibility. In [24], a data-centric access control framework for smart grids that follow the publish/subscribe model is proposed, adopting an Attribute-Based Authorization Policy. The main limitation of the related works has to do with the fact that these solutions are not able to cope with 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 [25] 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. UL offers certification, assessment and compliance services in several commercial sectors; in the smart grid domain [26] they test and certify systems and products, as well as verifying performance, security and interoperability between them prior to installation.

The idea of hardware security modules in the SG is not new, but very limited work related to the SG exists currently [27]. Recently, there have been efforts to anonymise trusted computing operations, like bi-directional communications [28] and remote attestation [29]. Generally, two prevalent specifications for trusted computing exist: the Trusted Platform Module (TPM) [30] and the Trusted Execution Environment (TEE) [31]. The most significant limitations of the TPM platform include: i) increased cost of a device, ii) no protection against runtime attacks, iii) the assumption that a TPM cannot be tampered, and iv) no suitability for mobile and embedded devices. Also, TPM is not designed to provide runtime attestation of executable programs, thus, reducing its effectiveness.

4. SEALEDGRID APPROACH

In this section, we clarify, how the proposed SealedGRID research activities go a step further, towards the accomplishment of the project research and technological objectives.

4.1. Authorization and security interoperability

SealedGRID designs and implements an innovative authorization mechanism based on a hybrid RBAC and Attribute Based Access Control (ABAC) mechanism that exploits the best of both methods providing simplicity of policies, and at the same time flexibility and ability to cope with the dynamic environments. Access control is employed to all identified data instances in SG including “data-in-use” at endpoints, “data-in-motion” on network, and “data-in-rest” in storage systems. The proposed access control achieves identity federation through Single-Sign-On mechanisms based on contemporary protocols e.g., OpenID Connect and oAuth2.0 and deploys appropriate policy enforcement and deployment entities to achieve interoperability between different SG domains. To further support interoperability, a context–aware manager in SealedGRID discovers, translates and verifies security policies enforced by different SG domains. Authorization and security interoperability procedures run in the protected environment offered by the trusted computing component, while they support the operation of the privacy protection protocol.

The SealedGRID deploys OpenID Connect and OAtuth2.0 to achieve interoperability and ensure communication among its components. However, we do not analyze these technologies, since they precede the SealedGRID and are borrowed from the field of online services further, [32]. Since, different domains and devices need to be interconnected with each other, the authorization is applied based on Policy Information Points (PIP), Policy Enforcement Points (PEP) and Policy Decision Points (PDP). The PIPs associate the set of attribute values to resources (e.g., SM) based on the context information. The PDP (e.g, Utility) issues the policy for a specific domain and the PEP enforces the policy to its domain.

Also, SealedGRID integrates the Opinion Dynamics [33] as the context-awareness mechanism to retrieve data of the current state of the system in real time. This is an algorithm to detect and trace Advanced Persistent Threats during their entire lifecycle, from a holistic perspective. It analyzes information from external sources (e.g., Intrusion Detection System) together with Machine Learning techniques and correlates them with the anomalies measured by their neighbors.

Further, SealedGRID adopts the Blockchain technology tor tracking the actions and policy decisions of SG nodes. SealedGRID readjusts the policy in the best and the most rapid way. This can be achieved through Dynamic context-awareness policy readjustment using the Blockchain. Also, when a device leaves the SealedGRID domain, the information must be propagated to the database promptly, thus Blockchain constitutes an effective solution. Authorization in the Blockchain is implemented using public key cryptography [34].

4.2. Key Management and Authentication

SealedGRID proposes a novel, hybrid key management mechanism for the SG based on the Web-of-Trust (WoT) [35] and Blockchain concept, a combination that has not been considered by other state-of-the-art solutions. It uses digital certificates, in order to capitalize on its advantages related to key management, when compared to symmetric key cryptography and secret keys, like [36], [1], [37]. Due to WoT, this solution is decentralized, resilient to failures and network segmentation, provides certificate revocation, and supports efficient look-ups of the established trust relationships, using Distributed Hash Tables (DHT). In contrast to PKI only based solutions, like [3], all participated nodes are used for introducing new nodes to the system. Moreover, the proposed solution is robust against certificate compromise; that is, if the certificate of a central node (e.g Utility company) is revoked, this does not lead to the re-issuing of all certificates signed by it. This holds because, following WoT, certificates are signed by multiple endorsers. Regarding authentication, the projected solution supports device-to-device, device-to-network, and user-to-device/network mutual authentication thanks to digital certificates (available from key management), and trusted computing which provides a secure environment for such critical operations. In contrast to centralized authentication systems, like RADIUS and Diameter, our proposal is distributed, in order to operate over intermittent communications or temporary offline servers. Based on the WoT, SG nodes perform mutual authentication by creating chains of trust among them; the efficiency of the authentication procedure is improved by using DHTs.

As mentioned previously, a PKI approach relies on Trusted Third Party (TTP) introducing a single point of failure like in [38]. On the other hand, WoT has a high barrier to entry, but the SealedGRID can overcome this drawback, since for a node joining the participation of the CA (e.g., a Utility company) is mandatory. However, in order to be able to use SealedGRID in fully decentralized SG environments, the adoption of the Blockchain technology in conjunction with WoT is investigated. A Blockchain is represented by a distributed ledger, completely transparent, so that an interested member can review all entries. The unique property of this technology is that once some data has been recorded inside a Blockchain, it becomes tough to change it. The hash of the block can be compared to a fingerprint because it is a unique key and it identifies a block and its contents. The hash is a one-way function, therefore it is easy to generate code but starting from a hash code, it is impossible to get the original data without the private key. Another element inside each block is the hash of the previous block which effectively creates a chain of blocks, making a Blockchain secure [39]. By being distributed, the Blockchain can store certificates [34].

SealedGRID investigates the technology of Certcoin [40], that is a public and decentralized authentication scheme which incorporates the best aspects of transparent CA and WoT. Certcoin provides the ability to publish a public key corresponding to a given node in a reliable, permanent way facilitating authentication. Certcoin maintains a public ledger of nodes and their associated public keys. The public ledger can be easily stored in the proposed DHT solution, where the latter facilitates public key look-up. Certcoin can be applied to devices with limited processing and memory capabilities like SMs and embedded devices. When a node is initially registered in SealedGRID, the transaction contains signed information about two public keys that are associated with the node. The first public key belongs to the online key pair, while the second belongs to the offline key pair. The online secret key is used to authenticate messages to the rest of the nodes and the Utility, while the offline is stored in a safe place and used for revoking keys and signing new ones in case of security breach or key compromise.

SealedGRID utilizes SOMA [41], this is a certificate-based authentication infrastructure that creates a large-scale secure authentication system for mesh-networks without the need of a TTP. The participated nodes decide by themselves with whom to interact and why to trust each of the nodes, independently. Moreover, SOMA is based on a Pretty Good Privacy (PGP) architecture, where the nodes create the public and private keys themselves. The SOMA certificates are securely stored within the Trust Execution Environment (TEE) and exchanged between the nodes based on PGP WoT. Each participated node uses its keyring independently, placing their trust depending on the identification credentials gathered. A node, after assessing the certificates on its keyring and evaluating the identity of the communicating parties, uses these credentials to establish a secure communication channel.

4.3. Trusted computing and privacy protection

SealedGRID proposes an alternative trusted computing platform, designed for devices with limited capabilities, such as SG devices. Related work on trusted computing for the SG is limited, leaving plenty of space for novelty; our main aim is to utilize on-processor technologies like TEE [31] as a secure runtime environment in order to avoid Trusted Platform Module's (TPM) [30] drawbacks, and complement it with mature TPM services (like remote attestation and sealing/secure storage). Also, the proposed solution offers creation, secure storage and handling of cryptographic keys for the key management component. For privacy protection, SealedGRID proposes a privacy-preserving metering data aggregation mechanism based on masking, in order to fulfill the requirements of private data protection, efficiency, low resource complexity, economic feasibility and scalability; moreover, it protects against non-repudiation, which is a common weakness of such methods. Consumption related data is protected with established trust relationships by the key management component, while all operations are executed in the protected environment of the trusted computing component.

SealedGRID uses the TEE, as it is proposed in [42], to: a) protect components private keys and its sensitive data through secure storage; b) endorse remote attestation, and c) secure critical procedures like key management, aggregation and protection of energy consumption, securely storage of digital certificates and to perform the cryptographic functions.

Moreover, MASKER [43] is integrated to provide a privacy-preserving aggregation solution. SMs share masked values with the Utility and obfuscate their real consumption readings. This way, an Aggregator provides Utility with an aggregated consumption by several SMs without knowing the real energy consumption. The Utility subtracts the used masks from the total sum, resulting the real combined consumption of all relevant SMs. Only the relevant SMs are able to know their real energy consumption. MASKER requires TEE to protect the performed sensitive computations, to store data and execute crucial operations. Furthermore, it provides confidentiality and authenticity to the executed code and stored data, integrity to CPU registers, memory and sensitive input/output, while it is able to prove the trustworthiness of SealedGRID nodes, components and modules. Finally, by utilizing MASKER in SealedGRID, we achieve a privacy preserving aggregation solution of energy consumption that facilitates DR, which is highly trusted and scalable, imposing low computation overhead.

5. IMPACT ON SMART GRID ECOSYSTEM

In this section we present SealedGRID impact on SG ecosystem.

5.1. Impact on Utility Companies

One of the major concerns of Utility companies in order actively proceed to the adoption of innovative and state of the art solutions, is the interoperability with old-fashioned/traditional equipment, as well as the high integration costs. Conversely, SealedGRID builds on a realistic architectural image of industrial installations comprising legacy (like Supervisory Control and Data Acquisition - SCADA) and emerging (e.g., automated and interconnected) types of energy infrastructures. Subsequently, SealedGRID takes into account the special characteristics of energy infrastructures, their cyber and physical requirements, and proposes solutions that promote systemic prevention with the minimum possible additional cost. Special consideration is given to the fact that this additional cost should be much less than the benefit gained by the adoption of SealedGRID solutions. Moreover, SealedGRID endorses interoperability to allow companies to promote better offers and to create a competitive energy infrastructure market. Consequently, SealedGRID is expected to contribute to the fulfillment of the objective of efficient operation of critical infrastructure, while preserving quality of service, for the ultimate benefit of customers.

5.2. Impact on Energy Distribution Operators

The establishment of high information security models is among the top of energy distribution operators business priorities. The SealedGRID platform along with its security methodology and mitigation techniques for cyber, physical and potential cyber-physical threats provides an integrated solution that is applicable to existing systems as well. It also provides advanced security features in legacy equipment upgrading their capabilities for operation in modern computing environment. The SealedGRID concept is expected to limit the security risks for the expansion of remote energy distribution network management, towards the evolution of SGs. This offers more trouble free management to energy distribution operators and contribute towards an extensive deployment of SGs. Furthermore, the adoption of SealedGRID provides an efficient mechanism for the mitigation of security risks related to the infusion of Information and Communications Technology in the energy distribution operators.

6. CONCLUSIONS

To this end, in this paper we have proposed a complete architecture for SG ecosystem elaborating on the technologies the SealedGRID utilizes. This architecture is able to provide privacy energy consumption, access to critical areas as well as secure interoperability. Since, European Union regulations require that member nations ensure that 80% of residential households will have been fitted with SG nodes by 2020. Following these regulations, Utility companies have allocated a lot of effort to install smart meters into millions of homes across Europe. SealedGRID takes advantage this moment to establish a DR energy consumption strategy that does not only provide customers with lower bills, but also contributes towards building a wiser energy consumption mentality for the new generations. As future work, we intend to implement the proposed architecture in order to show the feasibility of the security components for practical use cases based on federated, complex and heterogeneous SG environments.

ACKNOWLEDGEMENT

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

REFERENCES

[1] X. Long, D. Tipper, and Y. Qian. An advanced key management scheme for secure smart grid communications. In *2013 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pages 504–509, Oct 2013.

[2] A. Mohammadali, M. Sayad Haghighi, M. H. Tadayon, and A. Mohammadi-Nodooshan. A novel identity-based key establishment method for advanced metering infrastructure in smart grid. *IEEE Transactions on Smart Grid*, 9(4):2834–2842, July 2018.

[3] Y. W. Law, M. Palaniswami, G. Kounga, and A. Lo. Wake: Key management scheme for wide-area measurement systems in smart grid. *IEEE Communications Magazine*, 51(1):34–41, January 2013.

[4] T. Baumeister. Adapting pki for the smart grid. In *2011 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pages 249–254, Oct 2011.

[5] Nian Liu, Jinshan Chen, Lin Zhu, Jianhua Zhang, and Yanling He. A key management scheme for secure communications of advanced metering infrastructure in smart grid. *Industrial Electronics, IEEE Transactions on*, 60:4746–4756, 10 2013.

[6] Ibm encrypting data with confidence, across the enterprise and beyond. 2015.

[7] Elster energyaxis system, release 8.0. 2012. `https://www.elstersolutions.com/en/product-details-all-regions/338/en/EnergyAxis`.

[8] Sypris electronics cryptographic key management system. https://www.sypriselectronics.com/information-security/cyber-security-solutions/smart-grid-security/.

[9] Lili Yan, Yan Chang, and Shibin Zhang. A lightweight authentication and key agreement scheme for smart grid. *International Journal of Distributed Sensor Networks*, 13(2):1550147717694173, 2017.

[10] *DNP3 Users Group Technical Committee. DNP3 Secure Authentication Specification Version 2.0, DNP Users Group Documentation as a supplement to Volume 2 of DNP3. Technical report, DNP Users Group, 2008.*

[11] Iec ts 62351 series, power systems management and associated information exchange – data and communications security, tech specification, 2007. http://www.iec.ch/smartgrid/standards/.

[12] Max36025 smart meter. https://www.maximintegrated.com/en/products/power/supervisors-voltage-monitors-sequencers/MAX36025.html.

[13] Gemalto identity-based model utilizing a pki https://safenet.gemalto.com/data-protection/advanced-metering-infrastructure-smart-grid-security.

[14] Bitcoin blockchain. http://blockchain.info/.

[15] *CEN/CENELEC/ETSI, "Smart Grid Information Security", December 2014.*

[16] Sören Finster and Ingmar Baumgart. Elderberry: A peer-to-peer, privacy-aware smart metering protocol. In *2013 Proceedings IEEE INFOCOM Workshops, Turin, Italy, April 14-19, 2013*, pages 37–42, 2013.

[17] R. Vijayanand, D. Devaraj, B. Kannapiran, and Kamatchi Kartheeban. Bit masking based secure data aggregation technique for advanced metering infrastructure in smart grid system. *2016 International Conference on Computer Communication and Informatics (ICCCI)*, pages 1–5, 2016.

[18] F. Knirsch, G. Eibl, and D. Engel. Error-resilient masking approaches for privacy preserving data aggregation. *IEEE Transactions on Smart Grid*, 9(4):3351–3361, July 2018.

[19] Trusted smart grid privacy program. https://www.truste.com/privacy-certification-standards/trusted-smart-grid/.

[20] Energy smart florida. https://www.fpl.com/smart-meters/pdf/ensuring-privacy.pdf.

[21] *Magee, T. Secure Interoperable Open Smart Grid Demonstration Project Consolidated Edison Company Of New York, Inc., 2014.*

[22] *Alcaraz, C. Lopez, J. Secure Interoperability in Cyber-Physical Systems Security Solutions and Applied Cryptography in Smart Grid Communications, IGI Global, 2016, 137.*

[23] Daniela Rosic, Ugljesa Novak, and Srdjan Vukmirovic. Role-based access control model supporting regional division in smart grid system. *2013 Fifth International Conference on Computational Intelligence, Communication Systems and Networks*, pages 197–201, 2013.

[24] Li Duan, Dongxi Liu, Yang Zhang, Shiping Chen, Ren Ping Liu, Bo Cheng, and Junliang Chen. Secure data-centric access control for smart grid services based on publish/subscribe systems. *ACM Trans. Internet Technol.*, 16(4):23:1–23:17, December 2016.

[25] Itron's openway riva. https://www.itron.com/na/industries/electricity/openway-riva.

[26] Ul. http://industries.ul.com/energy/smart-grid.

[27] Andrew J. Paverd and Andrew P. Martin. Hardware security for device authentication in the smart grid. In Jorge Cuellar, editor, *Smart Grid Security*, pages 72–84, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg.

[28] Andrew J. Paverd, Andrew P. Martin, and Ian Brown. Privacy-enhanced bi-directional communication in the smart grid using trusted computing. *2014 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pages 872–877, 2014.

[29] J. Zhao, J. Liu, Z. Qin, and K. Ren. Privacy protection scheme based on remote anonymous attestation for trusted smart meters. *IEEE Transactions on Smart Grid*, 9(4):3313–3320, July 2018.

[30] *Trusted Computing Group, TPM Mobile with Trusted Execution Environment for Comprehensive Mobile Device Security, Whitepaper, June 2012.*

[31] *GlobalPlatform: Trusted Execution Environment System Architecture, 2011.*

[32] *Killing the Password and Preserving Privacy with Device-Centric and Attribute-based Authentication*. Zenodo, February 2019. https://arxiv.org/abs/1811.08360.

[33] Rubio et. al. Tracking advanced persistent threats in critical infrastructures through opinion dynamics. In Javier Lopez, Jianying Zhou, and Miguel Soriano, editors, *Computer Security*, pages 555–574, Cham, 2018. Springer International Publishing.

[34] T. Robles D. Martín R. Alcarria, B. Bordel and M.-Á. Manso-Callejo. A blockchain-based authorization system for trustworthy resource monitoring and trading in smart communities. *Sensors*, 18:3561 – 3569, 2018.

[35] *Callas, J., Donnerhacke, L., Finney, H., Shaw, D., Thayer, R.: OpenPGP Message Format. RFC 4880 (Proposed Standard) (Nov 2007)*.

[36] J. Kim and H. Choi. An efficient and versatile key management protocol for secure smart grid communications. In *2012 IEEE Wireless Communications and Networking Conference (WCNC)*, pages 1823–1828, April 2012.

[37] Sheng Xiao, Weibo Gong, and Don Towsley. *Dynamic Key Management in a Smart Grid*, pages 55–68. Springer New York, New York, NY, 2014.

[38] Parvez et. al. Securing metering infrastructure of smart grid: A machine learning and localization based key management approach. *Energies*, 9(9), 2016.

[39] G. Suciu, C. Nădrag, C. Istrate, A. Vulpe, M. Ditu, and O. Subea. Comparative analysis of distributed ledger technologies. pages 370–373, Nov 2018.

[40] *Conner Fromknecht, Dragos Velicanu, and Sophia Yakoubov. A decentralized public key infrastructure with identity retention. Technical report, Cryptology ePrint Archive, Report 2014/803, 2014. http://eprint. iacr. org, 2014.*

[41] Demertzis et. al. Self-organised key management for the smart grid. In Symeon Papavassiliou and Stefan Ruehrup, editors, *Ad-hoc, Mobile, and Wireless Networks*, pages 303–316, Cham, 2015. Springer International Publishing.

[42] Karopoulos et. al. Towards trusted metering in the smart grid. In *2017 IEEE 22nd International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, pages 1–5, June 2017.

[43] Georgios Karopoulos, Christoforos Ntantogian, and Christos Xenakis. Masker: Masking for privacy-preserving aggregation in the smart grid ecosystem. *Computers Security*, 73:307 – 325, 2018.