MSCA-RISE-2017 - Research and Innovation
Staff Exchange

European Commission
Horizon 2020
European Union funding
for Research & Innovation

Scalable, trustEd, and interoperAble pLatform for sEcureD smart GRID

Sealed GRID

WP1 Project Management and Coordination

Deliverable D1.3 “Progress Report 2”

Editor(s):	Christos Xenakis (UPRC), Nikos Passas (UPRC)
Author(s):	Christos Xenakis (UPRC), Nikos Passas (UPRC)
Dissemination Level:	**PU**
Nature:	**R**
Version:	0.4

SealedGRID Project Profile

Contract Number	777996
Acronym	SealedGRID
Title	Scalable, trustEd, and interoperAble pLatform for sEcureD smart GRID
Start Date	January 1st, 2018
Duration	48 Months

Partners

	University of Piraeus Research Center	Greece
	Universidad de Malaga	Spain
	BEIA consult International SRL	Romania
	NEUROSOFT Software Productions SA	Greece
	National Inter-University Consortium for Telecommunications	Italy
	Fogus Innovations & Services P.C.	Greece

Document History

Version	Date	Author	Remarks
0.1	24/12/2020	UPRC	Initial table of contents
0.1	20/1/2021	UPRC	Revised Table of contents
0.2	22/01/2021	UPRC	Secondee Contribution
0.2	22/01/2021	NEURO	Farao, Bolgouras, Tsolkas Contribution
0.4	28/01/2021	UPRC, UMA	WP5 status
0.5	02/02/2021	UPRC	Draft version

Executive Summary

This document is part of the WP1 – Project Management and Coordination. The purpose of this report is to summarize all the administrative and technical activities performed during the third year of the project. The main administrative activities include setting up and coordinating the management bodies of the project, guiding the coordinating the consortium towards management requirements. The main technical activities of the third year include the implementation of key management, authentication component and the design of the authorization and security interoperability component, as well as the assignment of tasks and responsibilities to the beneficiaries, the effective communication of the outcomes to the consortium via the preparation of documents, conference calls, emails, and the specification of tasks in the project management tool, the specification of software engineering practices for the development of the modules and their integration, the monitoring of the implementation efforts, and the editing supervision of the technical deliverables.

This document is organized as follows. Section 1 describes the main achievements in terms of technical and administrative management, while Section 2 provides information for technical impact of each secondee during the third year of the project. Section 3 describes any kind of deviations from the agreed workplan, Section 4 concludes the report and set main targets for the third year.

Table of Contents

List of Figures

List of Tables

Abbreviations

Abbreviation	Meaning

Table 1 Abbreviations

1 Explanation of the work carried out per WP

1.1 WP1 - Project management and Coordination (UPRC, 1PM-48PM)

1.1.1 Objectives

The purpose of this work package is to provide the overall project coordination as well as the administrative and technical management of the SealedGRID project.

1.1.2 Description of work conducted during the first half of the project

During the third year (2020) of the project this WP carried out activities related to:

- Close monitoring of project tasks and milestones as described in the EU Grant Agreement and Consortium Agreement.
- Interaction with ECAS participants.
- Organization of project tasks/events and training activities.
- Management of available resources and funding, as well as delivery of documents.

1.1.3 Website, Communication and File Repository

The website that was set up during the first period of the project is still up and running which contains news about the SealedGRID project and its progress. The website is updated very frequently with news about the SealedGRID project. Moreover, its backups are frequently created and securely stored on-line in cloud and in a protected off-line environment.

Also, the social media accounts of the SealedGRID project are carefully maintained:

- Twitter [Account](https://twitter.com/sealedgridh2020?lang=en)
- Facebook [Page](https://www.facebook.com/SealedGRIDH2020/)
- LinkedIn[Account](https://www.linkedin.com/in/sealedgrid-project-98246b187)
- LinkedIn [Group] (https://www.linkedin.com/groups/13607573/)
- YouTube[Channel](https://www.youtube.com/channel/UC7k6Lz_RgV9GDPYyTi8qtTA).

The mail list (**sealedgrid-list@ssl-unipi.gr**), that was set up to facilitate rapid e-mailing and ensure the correct inclusion of those involved in the project is still used. The mailing list was set up and is still maintained by the UPRC.

Except for Skype [1], GoToMeeting [2] (Skype and GoToMeeting introduced in previous deliverable), Teams [3] and Google Meet [4] are tools that are used widely by the consortium in order to schedule and carry out conference calls. These offer several useful features such as screen sharing and recording of the conference call.

Furthermore, the SealedGRID consortium maintains the GitLab (www.sealedgridgit.ds.unipi.gr) to store and exchange documents. During this year (2020), it has been equipped with the well-known and available for free COMODO antivirus [5]. In addition, accounts in DropBox [6] and in Google Drive [7] are used for online multi-editing and storage.

Zenodo [6] is still used as the project data and publication repository and is linked to the SealedGRID project-site at OpenAIRE [7] [8]. Zenodo is still used since it remains a simple and innovative service that enables researchers, scientists, EU projects and institutions to share and showcase

multidisciplinary research results (Data and publications) that are not part of existing institutional or subject-based repositories.

1.1.4 Milestones

In the following table the status of the milestones of the project are presented.

Table 2 List of Milestones

Milestone number	Milestone title	Lead beneficiary	Due Date (in months)	Means of verification	General Status
MS1	Requirements definition and initial dissemination networking activities	UPRC	12	D1.1 (**Done**), D1.2 (**Done**), D2.1 (**Done**), D7.1 (**Done**), Social media and project website up and running (**Done**), 4 public talks delivered (**Done**), 2 newsletter issued (**Done**), 25% of the secondments started. (**Done**)	**Completed**
MS2	Development started, and planned actions completed	UMA	22	D3.1 (**Done**), 1 brochure (**Done**), 4 newsletters (**Done**), 1 video clip delivered (**Done**), 50% of the secondments started (**In Progress**)	**In Progress**
MS3	Half of the technical components completed	UPRC	30	D3.2 (**Done**), D4.1 (**Done**), D5.1 (**Done**), 1st workshop (**Done**), 1st brochure delivered (**Done**), 90% of the secondments started (**In Progress**)	**In Progress**
MS4	SealedGRID components individually implemented and tested	UMA	36	D4.2 (**In Progress**), D5.2 (**Done**), D1.4 (**In Progress**), 2nd workshop organized (**In Progress**), 60% of the secondments completed (**In Progress**)	**In Progress**
MS5	SealedGRID testbed ready	BEIA	42	D6.1 (**In Progress**), 3rd workshop organized (**In Progress**), No remaining secondments to start (**In Progress**)	**In Progress**

1.2 WP3 – Key Management and Authentication (UPRC, 7PM-28PM)

1.2.1 Objectives

The objectives of this WP were to:

- Design and develop a scalable and de-centralized key management mechanism for the SG,
- Design and implement an authentication protocol among users, SG devices and the SG, and
- Evaluate the proposed mechanisms through simulation.

1.2.2 Description of work conducted during the third year of the project

- **Task 3.2: Authentication for the SG (Completed):** The SealedGRID researchers during this task defined the authentication component that will be utilized within the SealedGRID platform. Moreover, the security model is provided. The authentication component is composed of a certificate-based approach to authenticate entities in the network, a lookup mechanism for the certificates and the integration of blockchain technology. Moreover, they included the evaluation of this component that is performed through simulations to test how the solution behaves mainly in terms of speed and reliability. The SealedGRID authentication mechanism is based on the combination of a certificate and a blockchain infrastructure, while at the same time its functionality is Credential Authority - independent. A self-organized ecosystem that is efficient and scalable is created, without making any compromises regarding the self-governing characteristics defined in each network node. The participating nodes create the keys needed to use on the certificates, much like on a PGP architecture. The certificates and the signatures they have accumulated, indicating the corresponding trust relationships that have been built, are stored on the ledger. Every node of the network has a copy of the ledger, which is not stored on a central server or a TTP. The communication between the nodes is based on the signatures that can be found in the certificates that have been published on the blockchain. The TEE will still be utilized for the storage of the secret keys and the secure signing of the certificates, an action that requires the use of secret keys. Remote attestation to ensure that the software running on the nodes is not malicious will also be performed utilizing the TEE.

1.2.3 Contributions per beneficiary

- **UPRC:** contributed with the design and development of the authentication and key management component, as well as assisted with their implementation and evaluation.
- **UMA:** contributed, during the design phases of both the components, by defining the requirements of these components to be compatible with WP5.
- **NEURO:** contributed during the implementation and evaluation phases, and defined requirements for the smooth integration of the components to the SealedGRID platform.
- **BEIA:** was responsible for the validation of the evaluation results, while it defining together with NEURO the hardware and software components that was needed for the evaluation of the two components. Additionally, made contributions in blockchain related work.

1.2.4 Deliverables

Table 3 List of WP3 Deliverables

No.	Deliverable Title	Lead	Planned Delivery	Actual Delivery
D3.2	Authentication Component	UPRC	M28	M32

1.3 Work Package 4 – Trusted Computing and Privacy Protection (UPRC 21PM-36PM)

1.3.1 Objectives

The objectives of WP4 are to:

- Design and implement an alternative trusted computing component for SG devices,
- Design and implement a privacy solution for the protection of sensitive data, and
- Evaluate the proposed mechanisms through simulation and emulation.

1.3.2 Description of work conducted during the third year of the project

- **Task 4.1: Trusted computing for the SG (Completed)**: In this the researchers presented the entire process that followed while choosing a trusted computing technology, designing a functional trusted computing component that fulfils the requirements of the SealedGRID project (defined in D2.1), implementing it and measuring its performance. The chosen technology is the TrustZone trusted execution environment technology which is abundantly available in devices with ARM processors which are common in small devices that cover the needs of the smart meters of SealedGRID. With this in place, we selected the OP-TEE platform, a complete TEE environment that provides a secure and a normal world with the usage of the TrustZone technology and can be used to develop both physical devices based or emulation-based TEE applications. After the selection process, the researcher created a trusted computing component architecture that aims at providing versatility in its functionality by giving commonly used primitive functions to the user (cryptography, signatures, hashing and storage). Moreover, its overall performance and correctness of the SealedGRID trusted computing component showed above the acceptable limits for the targeted functionality and it is expected to cover any of the SealedGRID use case scenarios.
- **Task 4.2: Privacy protection for the SG (In progress):** This task includes the design and implementation of a component that will preserve the privacy of sensitive data exchanged among SG entities. It will be based on WP3 and Task 4.1 for trust establishment and secure operation, and WP5 for compatibility in inter-connection points. This component will comprise: i) a trust establishment mechanism, that will provide secure exchange of secret values, and ii) a data protection mechanism, that will provide lightweight masking of consumption data. The proposed component will be evaluated through simulation.

1.3.3 Contributions per beneficiary

- **UPRC:** UPRC researchers design the trusted computing and privacy protection components.
- **BEIA:** BEIA researchers are responsible for the validation of the evaluation results, while they will contribute to the define of the hardware and software components that will be needed for the evaluation of the two components.
- **UMA:** UMA researchers contribute, during the design phases of both the components, by defining the requirements of these components in order to be compatible with WP3 and WP5.
- **NEURO** will collaborate during the implementation and evaluation, the definition of the hardware and software components that will be needed for the evaluation of the two components and also define requirements for the smooth integration of the components to the SealedGRID platform.

1.3.4 Deliverables

Table 4 List of WP4 Deliverables

No.	Deliverable Title	Lead	Planned Delivery	Actual Delivery
D4.1	Trusted computing component	UPRC	M30	M36
D4.2	Privacy protection component	BEIA	M36	-

1.4 Work Package 5 – Authorization and Security Interoperability (UMA 10PM-36PM)

1.4.1 Objectives

Based on the components built in WP3 and WP4, this WP further enhances and extends the security features of SealedGRID. In particular, the objectives of this WP are to:

- Design and implement an authorization framework for SG.
- Design and implement SSO solutions.
- Design and implement context-aware mechanisms to enhance interoperability.
- Evaluate the proposed mechanisms based on well-defined scenarios and experiments.

1.4.2 Description of work conducted during the first half of the project

- **Task 5.1: Design and implementation of an authorization mechanism (BEIA-Completed)**: concluded with the implementation of a prototype of this authorization component, through a server that implements an access control policy based on RBAC and ABAC by using the XACML language (eXtensible Access Control Markup Language). A subset of rules defined according to the IEC-62351 were thereby processed by an authorization engine that can be accessed by external entities through a public API to submit a request and obtain the corresponding authorization token.
- **Task 5.2: Design and implementation of security interoperability (UMA-Completed)**: addressed the design of the components for achieving security interoperability in this context and conducted the implementation of the context awareness manager. More specifically, it firstly describes the integration of policy translation mechanisms across SealedGRID domains, based on the authorization architecture introduced in Task 5.1. Secondly, we also focus on the deployment of single-sign on protocols based on the emerging OpenID Connect protocol, which is intended to operate with the existing authentication model in the SealedGRID infrastructure. Then, the precise integration of the context-awareness manager in the authorization workflow is explained by means of practical experimentations.
  In addition to these contributions, in D5.2 we also analysed the integration of distributed ledger technologies (DLTs) such as the Blockchain in the SealedGRID architecture for auditing procedures and look further into policy readjustment mechanisms that authorization entities may put into practice to ensure a long-term support for existing policy rules, making use of machine learning algorithms.

1.4.3 Contributions per beneficiary

- **UMA**: Researchers from the UMA focused on defining the architecture of the authorization component, providing description of the context-awareness mechanism, analysis of Blockchain for authorization and auditing and finally the security policy readjustment.

- **UPRC** Researchers from NEURO provided the definition of the hybrid control access policy rules, implementation of the context-awareness mechanism and the iIntegration of Single-sign on protocols based on OpenID Connect protocol.
- **NEURO**: Researchers from NEURO provided the definition of the hybrid control access policy rules, implementation of the context-awareness mechanism and the integration of Single-sign on protocols based on OpenID Connect protocol.
- **BEIA**: Researcher from BEIA provided the implementation of the XACML policy.
- **CNIT**: Researcher from the CNIT contributed in developing the context awareness-mechanism.

1.4.4 Deliverables

Table 5 List of WP5 Deliverables

No.	Deliverable Title	Lead	Planned Delivery	Actual Delivery
D5.1	First version of the authorization component	UMA	M24	M24
D5.2	Authorization and security interoperability component	UMA	M36	M37

1.5 Work Package 6 – Platform Integration and Assessment Experiment (NEURO 34PM-48PM)

1.5.1 Objectives

The goal of this WP is twofold; first, to develop and demonstrate a system-level prototype (proof of concept) for the SG, and second, to develop and integrate in this prototype the HW/SW modules produced in the technical WPs relating to: i) key management and authentication (WP3), ii) trusted computing and privacy protection (WP4), and iii) authorization and security interoperability (WP5).

1.5.2 Description of work conducted during the first half of the project

- **Task 6.1: Proof of concept testbed (NEURO, M34-M42):** This task will continue from the system architecture specified in WP2, Task 2.3. Using this architecture as a reference, a proof of concept prototype will be designed. This prototype will be high level and generic enough in order to serve as a basic building block, upon which all SealedGRID components will be integrated.
- T**ask 6.2: Key management, authentication and trusted computing integration (UPRC, M40-M48):** This task will extend the common prototype developed in Task 6.1 and integrate the closely related key management, authentication and trusted computing components developed in WP3 and WP4.
- **Task 6.3: Authorization, security interoperability and privacy protection mechanisms integration (UMA, M40-M48):** This task will integrate the remaining components developed in WP4 and WP5 to the common prototype developed in Task 6.1, taking into consideration the characteristics of the integrated system as resulted from the activities in Task 6.2.

1.5.3 Contributions per beneficiary

In this section we will briefly analyze the contribution of each beneficiary in this WP:

- **UPRC**: UPRC researchers contribute to all tasks in order to achieve and ensure compatibility with the components developed in WP3 and WP4.

- **UMA**: UMA researchers are responsible for the design of the authorization mechanism, security interoperability component and context awareness.
- **NEURO**: NEURO researchers are responsible to develop all the authorization components and to evaluate them.
- **BEIA**: BEIA researchers aim at contributing to the validation of the evaluations and ensuring compliance with the reference architecture and scenarios.
- **CNIT**: CNIT researcher contributed to the implementation of the authorization components.

1.5.4 Deliverables

Table 6 List of WP6 Deliverables

No.	Deliverable Title	Lead	Planned Delivery	Actual Delivery
D6.1	Initial system design and prototyping	NEURO	M42	-
D6.2	Final integrated system	NEURO	M48	-

1.6 Work Package 7 – Dissemination, Standardisation, and Exploitation (UMA 1PM-48PM)

1.6.1 Objectives

The aim of WP7 is to coordinate the activities related to the dissemination of the results, to define strategies to ensure visibility into standardization groups, and to enable the exploitation of the new solutions.

1.6.2 Description of work conducted during the first half of the project

- **Task 7.1: Dissemination Activity (In progress):** The aim of this task is the coordination of all the activities related to the scientific dissemination of the results of the project. The website (www.sgrid.eu) is up, running to ensure a large visibility of objectives and results. SealedGRID maintains the accounts on the following social media to reach a large number of stakeholders. The social media accounts are the following:
  - Facebook (@SealedGRIDH2020)
  - Twitter (@SealedGRIDH2020)
  - LinkedIn (@SealedGRID Project)
  - YouTube (@SealedGrid project).

  SealedGRID project was presented in the following talks:
  - Critical Infrastructure Security and Resilience (CISaR) Workshop, Norway [9]
  - Safer Internet Day 2020, Cyprus [10]
  - 7th Information Security Conference [11]
  - EAB Cyber Meeting [12]
  - Virtual meeting of the Cyberwatching.eu [13]
  - MENSA module was presented at the University of Passau [14]
  - EPES and Smart GRIDS: Practical Tools and Methods to Fight Against Cyber and Privacy Attacks [15]
  - GoTech World 2020 [18]

  During this year, the following dissemination material was published:
  - Brochure [16]
  - Newsletter [17]

- Newsletter Issue 6 [18]
- Newsletter Issue 7 [19]

During this year, SealedGRID has been mentioned to the following third-party website:

- Cyberwatching Announced SealedGRID “Project of the Week” [20]

During this year, the following scientific publications have been published:

- Muñoz A., Farao A., Correia J.R.C., Xenakis C. (2020) ICITPM: Integrity Validation of Software in Iterative Continuous Integration Through the Use of Trusted Platform Module (TPM). In: Boureanu I. et al. (eds) Computer Security. ESORICS 2020. Lecture Notes in Computer Science, vol 12580. Springer, Cham. https://doi.org/10.1007/978-3-030-66504-3_9 , https://zenodo.org/record/4487292
- Cristina Alcaraz, Juan E. Rubio, Javier Lopez, Blockchain-assisted access for federated Smart Grid domains: Coupling and features, Journal of Parallel and Distributed Computing, Volume 144, 2020, Pages 124-135, ISSN 0743-7315, https://doi.org/10.1016/j.jpdc.2020.05.012 , https://zenodo.org/record/4487338#.YBhDCC2w1TZ
- J. Lopez, J. E. Rubio, and C. Alcaraz, "Digital Twins for Intelligent Authorization in the B5G-enabled Smart Grid", IEEE Wireless Communications, IEEE, In Press. [**Accepted/ To be published/ Will be uploaded to open repository when published**]
- G. Suciu et al., "FI-WARE authorization in a Smart Grid scenario," 2020 Global Internet of Things Summit (GIoTS), Dublin, Ireland, 2020, pp. 1-5, https://ieeexplore.ieee.org/abstract/document/9119589 , https://zenodo.org/record/4506462#.YB0g0S2w1TY
- Suciu, George, et al. "AN INTRODUCTION TO UBIQUITOUS COMPUTING IN THE MILITARY NETWORK." eLearning & Software for Education 1 (2020), https://web.b.ebscohost.com/abstract?direct=true&profile=ehost&scope=site&authtype=crawler&jrnl=2066026X&AN=145711102&h=Sb48%2f%2brbQ3SmgFSj8iT5JVqQGtgVcdjX%2fROvMztAyDF5xGQnxgp8LutBOqx7jT9LzAkCJGyXXuvjwkQaPp5Iyw%3d%3d&crl=c&resultNs=AdminWebAuth&resultLocal=ErrCrlNotAuth&crlhashurl=login.aspx%3fdirect%3dtrue%26profile%3dehost%26scope%3dsite%26authtype%3dcrawler%26jrnl%3d2066026X%26AN%3d145711102, https://zenodo.org/record/4506438#.YB0bIy2w1TY,
- F. Constantin, G. Suciu, S. Bosoc and R. Craciunescu, "Internet Controlled Car," 2020 13th International Conference on Communications (COMM), Bucharest, Romania, 2020, pp. 261-264, https://ieeexplore.ieee.org/abstract/document/9141988, https://zenodo.org/record/4506674#.YB008S2w1hE
- Suciu, George, et al. "PEER TO PEER WEBRTC MULTIPOINT VIDEO-CONFERENCE SYSTEM FOR E-LEARNING." The International Scientific Conference eLearning and Software for Education. Vol. 1. " Carol I" National Defence University, 2020. https://search.proquest.com/openview/fd238323760033483191f19aa43dd6c6/1?casa_token=YIQVKkGf2OUAAAAA:gM_gWVac-lVuN_jG3owLkQHVdhVIBpDm9KFzi1_l8ds7slxqSWHY1sBzUXiANj9NCGtj3LjAtQ&cbl=1876338&pq-origsite=gscholar, https://zenodo.org/record/4506541#.YB0nnC2w1TY
- G. Suciu, A. Scheianu, I. Petre, A. Drosu and R. Darabană, "VLC Quantum Fusion," 2020 International Workshop on Antenna Technology (iWAT), Bucharest, Romania, 2020,

pp. 1-4, https://ieeexplore.ieee.org/abstract/document/9083887, https://zenodo.org/record/3941705#.YB0kaC2w1TY

- Suciu G., Hussain I., Badicu A., Necula L., Ușurelu T. (2020) IoT Services Applied at the Smart Cities Level. In: Rocha Á., Adeli H., Reis L., Costanzo S., Orovic I., Moreira F. (eds) Trends and Innovations in Information Systems and Technologies. WorldCIST 2020. Advances in Intelligent Systems and Computing, vol 1160. Springer, Cham. https://doi.org/10.1007/978-3-030-45691-7_42, https://zenodo.org/record/3941707#.YB0j8y2w1hE

- **Task 7.2: Standardisation (In Progress):** The aim of this task is to put in place adequate actions to ensure the visibility of the project in standardisation bodies, and, if possible, to enable the inclusion of the proposed solutions in future standards for SG. Standardized components of SealedGRID solutions will be ensured by already-standardized interfaces and protocols where possible, as partners are participating or having access to several standardization bodies relevant to SealedGRID. So far, the relevant standardization groups are monitored as it is presented in the Standardization Plan in the deliverable D7.1 "Dissemination and Standardization Plan".
- **Task 7.3: Business Model, market Opportunities, and Exploitation Plan (In progress):** The aim of this task is to analyse the results of the project from a business point of view, and to identify a set of business cases for the exploitation of the results. The SMEs which participate in the consortium will create market opportunities and an exploitation plan, since that the project aims to have a direct impact on extending SMEs' products.

1.6.3 Contributions per beneficiary

All the beneficiaries have contributed to the activities of this WP so far. Major effort has been allocated to the dissemination and communication of the project to public audience and all the seconded researchers were involved in this task, actively.

1.6.4 Deliverables

Table 7 List of WP7 Deliverables

No.	Deliverable Title	Lead	Planned Delivery	Actual Delivery
D7.3	Dissemination and Standardisation	UMA	48	-
D7.4	Market Analysis and Exploitation	UMA	48	-

2 Impact

2.1 Contribution of each secondee during the third year of the project

2.1.1 UPRC

2.1.1.1 Christos Xenakis

Christos Xenakis is a seconded researcher from the UPRC to BEIA. His secondment in 2020 started on 28/02/2020 and terminated on 03/03/2020. During this perioded he supervised the work conducted in WP3 and WP4. Regarding his contribution in the WP3 he supervised the work in the implementation and evaluation of the SealedGRID authentication module. In addition, he provided useful guidelines for the design of the trusted computing module. Finally, he supported the dissemination of the project

presenting its mission, goals, and prospects in numerous events, but he also published scientific documents presenting the project’s results.

2.1.1.2 Panagiotis Bountakas

Panagiotis Bountakas is a seconded researcher from the UPRC to BEIA. His secondment started a few months before the initiation of the 2020; however, his secondment terminated on 29/01/2020. During this month he finalized the contribution regarding the WP5 since he provided the related information regarding the federated identity among the SealedGRID ecosystem. Moreover, he contributed to the design and implementation of the WP4 regarding the initial version of the trusted computing. Finally, he contributed to the design of the authentication component architecture.

2.1.1.3 Farnaz Mohammadi

Farnaz Mohammadi is a seconded researcher from the UPRC to BEIA. Her secondment terminated on 21/01/2020. During this period, she focused on designing the final version SealedGRID authentication components, part of the D3.2. Moreover, she contributed to the WP5 since she contributed to the integration of the federated identity in the SealedGRID ecosystem. Finally, she contributed in the WP4 providing input regarding the related work and similar approaches.

2.1.2 BEIA

2.1.2.1 Gheorghe Suciu

Gheorghe Suciu is a seconded researcher from the BEIA to UPRC. His secondment started on 14/12/2019 and terminated on 21/01/2020. During this period, he supervised and guided in issued related to WP4, also he contributed to WP7 by participating in online events and presentations.

2.1.2.2 George Suciu

George Suciu is a seconded researcher from the BEIA to UPRC. His secondment started late in 2019 on 19/12/2019 and terminated on 28/02/2020. During this period, he supervised, guided and contributed to WP3 and WP4 supervising and guiding in the testing process and in WP 7 by participating in online events and presentations.

2.1.2.3 Razvan-Alexandru Vuple

Razvan-Alexandru Vuple is a seconded researcher from the BEIA to UPRC. His secondment started on 25/02/2020 and terminated on 24/03/2020. During this period, he contributed in WP1, through participation in online meetings and organizing of secondments. In WP4 through running performance and regression tests using the OPTEE test suite, and contributed to D4.2. In WP5 he shared considerations on interoperability and potential implementation of policy translation mechanisms across SealedGRID domains using XACML. Defined a Policy Translation Point in conjunction with an authentication delegation mechanism. And in WP7: by supporting in the project presentations in several events and contribution to papers

2.1.2.4 Victor Suciu

Victor Suciu is a seconded researcher from the BEIA to UPRC. His secondment started on 25/02/2020 and terminated on 24/03/2020. During this period, he contributed in WP1 by participation in online meetings and supporting the organization of secondments. In WP4 by contributing to TEE state-of-the-art for testing and contributing on D4.2. In WP5 he supported in exploring the interoperability governance in federated networks And in WP7: by supporting in the project presentations in several events and contribution to papers

2.1.3 NEURO

2.1.3.1 Aristeidis Farao

Aristeidis Farao is a seconded researcher form NEURO to UMA. His secondment started in 2019 and terminated on 10/02/2020. During the 2020, he contributed to the WP3, WP4 and WP5. Regarding the WP3, he contributed to the implementation of the final SealedGRID authentication component. In addition, regarding his contribution to the WP4, he contributed to the analysis of the related works regarding the trusted computing. Moreover, regarding the contribution in the WP5, he supported the design of the context awareness mechanism. Finally, he supported the dissemination of the project publishing joint scientific documents presenting the project’s results.

2.1.3.2 Vaios Bolgouras

Vaios Bolgouras is a seconded researcher form NEURO to UMA. His secondment started in 2019 and terminated on 10/02/2020. During the 2020, he contributed to the WP3, WP4 and WP5. Regarding the WP3, he supported the implementation and development of the final SealedGRID authentication component. In addition, regarding his contribution to the WP4, he contributed design of the trusted computing architecture. Moreover, in the WP5, he contributed to the design of the context awareness mechanism, the core of the SealedGRID authorization module and part of the D5.2.

2.1.3.3 Vasileios Tsolkas

Vasileios Tsolkas is a seconded researcher form NEURO to UMA. His secondment started in 2019 and terminated on 01/02/2020. During the 2020, he contributed to the WP3, WP4 and WP5. Regarding the WP3, he contributed to the development of the final SealedGRID authentication component. In addition, regarding his contribution to the WP4, he contributed to the analysis of the state-of-the-art related works in that field (trusted computing). Moreover, in the WP5, he contributed to the design of the context awareness mechanism, the core of the SealedGRID authorization module and part of the D5.2.

2.1.3.4 Sofia Batsi

Sofia Batsi is a seconded researcher from Neurosoft to CNIT. Her secondment started on 11/09/2020 and will be terminated on 09/09/2021. During her secondment, in WP5 she contributed by designing and developing a Context Awareness mechanism based on the Opinion Dynamics method, conducting performance evaluations for the proposed mechanism and co-authoring deliverable D5.2. She also participated in all the online meetings that took place during the reporting period.

2.1.4 CNIT

2.1.4.1 Giorgio Bernadinetti

Giorgio Bernadinetti is a seconded researcher from CNIT to FOG. His secondment started on 04/10/2020 and terminated on 4/12/2020. During his secondment, in WP 5, he was involved in the design and implementation of the Opinion Decision Algorithm. The objective was to assess the security level of every smart meter based on shared opinions given by each node. The context awareness manager was based upon an Opinion Dynamics algorithm which was implemented in python. He supported in testing this algorithm using a variety of initial data. And in WP7: by supporting in the project presentations in several events and contribution to papers.

3 Deviations

During this year (2020), controlled deviation from the original planning were necessary, due to important the COVID-19 outbreak:

- Due to the recent pandemic that affected all industries across the globe, there has been an increased difficulty in travel that has created obstacles in people moving between countries.
- This has also affected the project secondments since it was neither safe nor allowed in many cases to travel between countries.

Consequently, there has been a dramatic reduction in the number of secondments during the third year of this project.

The following figure depicts the initial secondment plan (according to the agreement amendment).

Staff ID /Ref. to A form	[ER/ ESR/ MGT]	Hosting Institution	Active in WP	Start month	Total PM	First Year (Y1)												Second Year (Y2)												Third Year (Y3)												Fourth Year (Y4)											
						1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
						START																																														END
UPRC RESEARCHERS																																																			
1	UPRC-ER1	BEIA	WP2/6	13	12													2															6	6	6	6	6	6	6	6	6	6												
2	UPRC-ER2	BEIA	WP3	13	12													3				3	3	3	3	3	3	3	3	3	3	3																					
3	UPRC-ER3	BEIA	WP3/4	14	12														3								3	3	3					4	4	4	4	4	4	4	4												
4	UPRC-ER4	BEIA	WP3/4	14	6														3	3										4	4	4	4																					
5	UPRC-ESR	BEIA	WP3/5/4	15	12															3	3	3							5	5	5	5	5	5	5	5																		
UMA RESEARCHERS																																																			
6	UMA-ER1	NEURO	WP2/6	7	12							2	2																				6	6	6	6	6	6	6	6	6	6												
7	UMA-ER2	NEURO	WP5	16	12																5	5	5	5	5	5	5	5	5	5	5	5																					
8	UMA-ER3	NEURO	WP5	21	12																					5	5	5	5	5	5	5	5	5	5	5	5																
9	UMA-ER4	BEIA	WP4	25	12																									4	4	4	4	4	4	4	4	4	4	4											
CNIT RESEARCHERS																																																			
10	CNIT-ER1	NEURO	WP5/6	25	12																									5	5	5	5	5	5	5	5	5	6	6	6												
BEIA RESEARCHERS																																																			
11	BEIA-ER1	UPRC	WP4/6	14	12														4	4																		6	6	6	6	6	6	6	6	6	6							
12	BEIA-ER2	UPRC	WP5	14	12														5	5												5	5	5	5	5	5	5	5	5												
13	BEIA-ER3	UPRC	WP4	25	12																									4	4	4	4	4	4	4	4	4	4	4											
14	BEIA-ER4	UMA	WP6	37	12																																				6	6	6	6	6	6	6	6	6	6	6	6	6
15	BEIA-ESR	UMA	WP3/4	14	12														3											4	4	4	4	4	4	4	4	4	4	4											
NEURO RESEARCHERS																																																			
16	NEURO-ER1	UMA	WP5/6	25	12																									5	5	5	5												6	6	6	6	6	6	6	6	
17	NEURO-ER2	UMA	WP4/5	14	12														4	4	4									5	5	5	5	5	5	5	5	5													
18	NEURO-ER3	UMA	WP3/6	14	12														3	3	3																		6	6	6	6	6	6	6	6	6						
19	NEURO-ER4	UMA	WP2/6	14	12														2	2	2																					6	6	6	6	6	6	6	6	6			
20	NEURO-ESR	UMA	WP6	27	12																																				6	6	6	6	6	6	6	6	6	6	6	6
FOG RESEARCHERS																																																			
21	FOG-ER1	CNIT	WP5	31	6																																															

* Numbers inside the duration of secondments indicate the involvement in specific workpackages

Figure 1 Actual Secondment Plan after the first amendment

The actual secondments until the M36 (Dec/2020) (with researchers' names and IDs), and the planned secondments for the last year (Y4) to fulfill the secondments plan and the remining work are presented in the figure below (light green background; actual realized secondments in Y3 while in light red background; the plan for the final year of the project).

Staff ID /Ref. to A form	Sending Organisation [ER/ ESR/ MGT]	Hosting Institution	Fellow ID	Name	Active in WP	Start month	Total PM	First Year (Y1) 1 2 3 4 5 6 7 8 9 10 11 12	Second Year (Y2) 13 14 15 16 17 18 19 20 21 22 23 24	Third Year (Y3) 25 26 27 28 29 30 31 32 33 34 35 36	Fourth Year (Y4) 37 38 39 40 41 42 43 44 45 46 47 48
								START			END
UPRC RESEARCHERS											
1	UPRC-ESR1	BEIA	3	Dritsa, Alexandra	WP2/6	12	1.00	2			
2	UPRC-ER1	BEIA	2	Xenakis, Christos	WP3	12	1.00	2			
4	UPRC-ER2	BEIA	5	Ntantogian, Christoforos	WP3/4	14	2.00		3 3		
6	UPRC-ESR2	BEIA	6	Bountakas, Panagiotis	WP3/5/4	14	8.00		3 3 3 3 3 3 3 3		
9	UPRC-ESR3	BEIA	9	Mohammadi, Farnaz	WP3/5/4	15	6.00		3 3 3 3 4 4		
11	UPRC-ESR4	BEIA	21	Koutroumpouchos, Nikolaos	WP3/5/4	20	1.00		3		
New Secondments	UPRC	TBD	TBD	TBD	WP 6	TBD	TBD				6 6 6 6 6 6 6
New Secondments	UPRC	TBD	TBD	TBD	WP 6	TBD	TBD				6 6 6 6 6 6 6
New Secondments	UPRC	TBD	TBD	TBD	WP 6	TBD	TBD				6 6 6 6 6 6 6 6
New Secondments	UPRC	TBD	TBD	TBD	WP 6	TBD	TBD				6 6 6 6 6 6 6
New Secondments	UPRC	TBD	TBD	TBD	WP 6	TBD	TBD				6 6 6 6 6 6 6
UMA RESEARCHERS											
12	UMA-ER1	NEURO	1	Rios del Pozo, Ruben	WP2/6	7	2	2 2			
13	UMA-ER2	NEURO	20	Alcaraz, Cristina	WP2/6	19	1.07		5		
14	UMA-ER3	NEURO	23	Munoz, Antonio	WP2/6	19	3		4 4 4		
15	UMA-ESR4	NEURO	22	Ferraris, Davive	WP2/6	21	4		4 4 4 4		
New Secondments	UMA	TBD	TBD	TBD	WP 6	TBD	TBD				6 6 6 6 6 6 6
New Secondments	UMA	TBD	TBD	TBD	WP 6	TBD	TBD				6 6 6 6 6 6 6
New Secondments	UMA	TBD	TBD	TBD	WP 6	TBD	TBD				6 6 6 6 6 6 6 6
New Secondments	UMA	TBD	TBD	TBD	WP 6	TBD	TBD				6 6 6 6 6 6 6 6
New Secondments	UMA	TBD	TBD	TBD	WP 6	TBD	TBD				6 6 6 6 6 6 6 6
CNIT RESEARCHERS											
16	CNIT-ER1	FOG	25	Bernardinetti, Giorgio	WP2/6	34	2.13			5 5	
New Secondments	CNIT	TBD	TBD	TBD	WP 6	TBD	TBD				6 6 6 6 6 6 6
New Secondments	CNIT	TBD	TBD	TBD	WP 6	TBD	TBD				6 6 6
BEIA RESEARCHERS											
17	BEIA-ER1	UMA/UPRC	4	Suciu, George	WP4/6	14	9.84		3 3 4 4 4 4 4	4 4	
18	BEIA-ESR1	UPRC	7	Constantin, Claudia	WP5	14	4.07		4	4 4 4	
20	BEIA-ER2	UPRC	8	Suciu, Gheorghe	WP4/6	14	8.4		4 4 4 4 4 4 4 4	4	
23	BEIA-ESR2	UMA/UPRC	13	Suciu, Victor	WP5	15	5.1		3	5 4 4	4
24	BEIA-ESR3	UMA/UPRC	14	Istrate, Cristiana	WP5	15	4.1		3	4 4 4	
27	BEIA-ER3	UPRC	15	Plechi, Enuta-Mihaela	WP4/6	15	4.07		3	4 4 4	
29	BEIA-ESR4	UMA/UPRC	16	Vuple, Razvan-Alexandru	WP5	16	6		3 5 5 5 4		4
New Secondments	BEIA	TBD	TBD	TBD	WP 6	TBD	TBD				6 6 6 6 6
New Secondments	BEIA	TBD	TBD	TBD	WP 6	TBD	TBD				6 6 6 6 6 6 6
New Secondments	BEIA	TBD	TBD	TBD	WP 6	TBD	TBD				6 6 6 6 6
New Secondments	BEIA	TBD	TBD	TBD	WP 6	TBD	TBD				6 6 6 6 6 6
NEURO RESEARCHERS											
35	NEURO-ESR1	UMA	17	Farao, Aristeidis	WP3/5/4	14	12		3 3 3 3 3 3 3 5 4 5 5 4		
37	NEURO-ESR2	UMA	18	Bolgouras, Vaios	WP3/5/4	14	12		3 3 3 3 3 3 3 5 4 5 5 4		
39	NEURO-ESR3	UMA	18	Tsolkas, Vasileios	WP3/5/4	14	12		3 3 3 3 3 3 3 5 4 5 5 4		
41	NEURO-ESR4	CNIT	24	Batsi, Sofia	WP3/5/4	33	4			5 5 5 5	6 6 6 6 6 6 6 6
New Secondments	NEURO	TBD	TBD	TBD	WP 6	TBD	TBD				6 6 6 6
New Secondments	NEURO	TBD	TBD	TBD	WP 6	TBD	TBD				6 6 6 6
New Secondments	NEURO	TBD	TBD	TBD	WP 6	TBD	TBD				6 6 6 6
FOG RESEARCHERS											
New Secondments	FOG	TBD	TBD	TBD	WP 6	TBD	TBD				6 6 6 6 6 6

* Numbers inside the duration of secondments indicate the involvement in specific workpackages

Figure 2 Actual and Planned Secondment Plan

Also, in the following figure the analysis for the catch-up plan is presented.

Period	Years 1 to 3	Year 4											
Month	M01-M36	M37	M38	M39	M40	M41	M42	M43	M44	M45	M46	M47	M48
	N/A	Jan-21	Feb-21	Mar-21	Apr-21	May-21	Jun-21	Jul-21	Aug-21	Sep-21	Oct-21	Nov-21	Dec-21
Duration Per Month	N/A	5	9	11	13	15	15	16	14	11	9	6	4
Marginal Added Percentage (%)	N/A	2.08%	3.75%	4.58%	5.42%	6.25%	6.25%	6.67%	5.83%	4.58%	3.75%	2.50%	1.50%
Total Covered Percentage (%)	46.99%	49.08%	52.83%	57.41%	62.83%	69.08%	75.33%	81.99%	87.83%	92.41%	96.16%	98.66%	100.00%
Total PMs	112.78	117.78	126.78	137.78	150.78	165.78	180.78	196.78	210.78	221.78	230.78	236.78	240.00
Remaining PMs	127.22	122.22	113.22	102.22	89.22	74.22	59.22	43.22	29.22	18.22	9.22	3.22	0.00

The results come from the corresponding excel file including the PMs. The results are approximately presented since the most secondment period are not integers (e.g. one month or ten months) but are decimal (e.g one month and a half).
The excel table presents the active month and presents a secondment for one a half month as secondment for two months. However, the offical will be an integral result with 100% and 240 covered months.
1PM=0.41666667 %

Figure 3 Catch-up plan

As presented in the above figures, the plan for the last year is very demanding in order to make up lost time and it requires that global situation with regards to travel will return to normal and researchers will be able to safely and freely travel between countries.

4 Conclusions

During its third year, the project progressed with significant deviations due to external unprecedented events. The administrative and technical management procedures have been set up according to the SealedGRID proposal, and the collaboration among partners is flawless and efficient.

5 Bibliography

[1] "SKYPE," Online: [Last access: 01/02/2021], https://www.skype.com/en/.

[2] "GoToMeeting," Online: [Last access: 01/02/2021], https://www.gotomeeting.com.

[3] "Teams," Online: [Last access: 01/02/2021], https://www.microsoft.com/en-us/microsoft-teams/group-chat-software.

[4] "Google Meet," Online: [Last access: 01/02/2021], https://meet.google.com/.

[5] "COMODO antivirus," Online: [Last access: 01/02/2021], https://www.comodo.com/home/download/download.php?prod=antivirus-for-linux.

[6] [Online] Dropbox, “https://www.dropbox.com/?landing=dbv2”..

[7] [Online]G. Drive, “https://www.google.com/drive/”..

[8] “Zenodo, ” an interdisciplinary open data repository service maintained by CERN, Geneva. Datasets can be located via the Zenodo search engine., [Online]. Available: https://www.zenodo.org/..

[9] "[Online] OpenAire, SealedGRID Publications, https://explore.openaire.eu/search/project?projectId=corda__h2020::2b8b780985281e0c6c252e01d73344b4".

[10] "SealedGRID", a Scalable, trustEd, and interoperAble pLatform for sEcureD smart GRID (777996): [Online] https://explore.openaire.eu/search/find?keyword=SealedGRID.

[11] "SealedGRID at the Critical Infrastructure Security and Resilience (CISaR) Workshop, Norway," Online: [Last accessL 01/02/2021], https://www.sgrid.eu/2020/02/06/sealedgrid-at-the-critical-infrastructure-security-and-resilience-cisar-workshop-norway/.

[12] "Safer Internet Day 2020, Cyprus," Online: [Last access: 01/02/2021], https://www.sgrid.eu/2020/02/14/sealedgrid-at-the-safer-internet-day-2020-cyprus/.

[13] "7th Information Security Conference," Online: [Last access; 01/02/2021], https://www.sgrid.eu/2020/02/24/sealedgrid-at-the-7th-information-security-conference/.

[14] "EAB Cyber Meeting," Online: [Last access: 01/02/2021], https://www.sgrid.eu/2020/05/15/eab-cyber-meeting/.

[15] "Virtual meeting of the Cyberwatching.eu," Online: [Las access: 01/02/2021], https://www.sgrid.eu/2020/07/14/sealedgrid-attended-the-virtual-meeting-of-the-cyberwatching-eu/.

[16] "MENSA module was presented at the University of Passau," Online: [Last access: 01/02/2021], https://www.sgrid.eu/2020/10/29/mensa-module-was-presented-at-the-university-of-passau/.

[17] "SealedGRID at EPES and Smart GRIDS: Practical Tools and Methods to Fight Against Cyber and Privacy Attacks," Online: [Last access: 01/02/2021], https://www.sgrid.eu/2020/11/12/sealedgrid-participate-in-a-joint-webinar-organized-by-cybersecurity4europe/.

[18] "SealedGRID NEW Brochure," Online: [Last access: 01/02/2021], https://www.sgrid.eu/2020/02/03/new-sealedgrid-brochure/.

[19] "SealedGRID 5th Newsletter," Online: [Last access: 01/02/2021], https://www.sgrid.eu/wp-content/uploads/2020/03/SealedGRID_newsletter_issue5.pdf.

[20] "SealedGRD 6th Newsletter," Online: [Last access: 01/02/2021], https://www.sgrid.eu/wp-content/uploads/2020/07/SealedGRID_newsletter_issue6.pdf.

[21] "SealedGRID 7th Newsletter," Online: [Last access: 01/02/2021], https://www.sgrid.eu/wp-content/uploads/2020/12/SealedGRID_Newsletter_7.pdf.

[22] "Cyberwatching Announced SealedGRID “Project of the Week”," Online: [Last access: 01/02/2021], https://www.sgrid.eu/2020/05/04/cyberwatching-announced-sealedgrid-project-of-the-week/.

[23] European Commission, “Recommendation on preparations for the roll-out of smart metering systems”, March 2012.

[24] https://www.skype.com/en/get-skype/., [Online]. Available:.

[25] [Online] https://www.gotomeeting.com/en-ie.