SOFIE - Secure Open Federation for Internet Everywhere

779984

DELIVERABLE D6.11

Final Report on Communication, Dissemination and Exploitation

Project title	SOFIE – Secure Open Federation for Internet Everywhere
Contract Number	H2020-IOT-2017-3 – 779984
Duration	1.1.2018 – 31.12.2020
Date of preparation	29.12.2020
Author(s)	Liis Livin (GT), George C. Polyzos (AUEB), Francesca Santorini (ASM Terni), Dmitrij Lagutin (AALTO), Ahsan Manzoor (Rovio), Yannis Oikonomidis (SYN), Antonis Gonos (OPT), Giuseppe Raveduto (ENG), Francesco Bellesini (EMOT), Mikael Jaatinen (LMF), Priit Anton (GT)
Responsible person	Liis Livin (GT), liis.livin@guardtime.com
Target Dissemination Level	Public
Status of the Document	Completed
Version	1.00
Project web-site	https://www.sofie-iot.eu/

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 779984.

Executive Summary

SOFIE deliverables D6.4 “Initial Communication and Dissemination Plan” and D6.6 “Updated Consolidated Communication and Dissemination Plan” identified and classified the target audience, the dissemination and exploitation methods and goals, and the measures to assess the impact of those activities to ensure proper dissemination of the generated knowledge. Deliverable D6.7 “Initial Report on Communication, Dissemination and Exploitation” described the status of those activities undertaken during the first 12 months of the project as well as plans for the upcoming months and any changes in the original plan. Deliverable D6.8 “Interim Report on Communication, Dissemination and Exploitation” outlined the outcomes of communication, dissemination and exploitation activities of the project undertaken during the first 25 months.

The current deliverable D6.11 “Final Report on Communication, Dissemination and Exploitation” provides the results of communication, dissemination and exploitation activities of the project undertaken during M26-36. It also reflects on the activities from the perspective of the entire lifeline of the project, giving final overviews and assessments of the activities. The report is divided into 8 chapters, with the aim to reflect on the general strategy for communication, dissemination and exploitation (Chapter 1) and to offer an overview of related communication and dissemination activities that took place from February 2020 (M26) until December 2020 (M36) (Chapter 2). In a comprehensive and closely related Chapter 3, the deliverable presents the result of exploitation activities of the last year of the project. Expanding upon exploitation, the deliverable presents the final Business Model Canvases created for each pilot (Chapter 4). These two chapters are inherently connected to D6.9 “Exploitation Strategy and Roadmap” and D6.10 “Business Planning”, where the first among other things describes exploitable assets and offers future exploitation plans and the second offers the detailed business plans (incl. market and financial analysis) of our pilots that are the drivers to pushing SOFIE asset to the market. The following chapters of this deliverable offer insight into community related achievements (Chapter 5), open data and intellectual property rights (Chapter 6). The deliverable is concluded with Chapter 7 where an evaluation to communication, dissemination and exploitation activities is offered and analysed.

Table of Contents

1. Introduction

1.1 General Strategy for Communication, Dissemination and Exploitation

The main purpose of the SOFIE communication and dissemination strategy has been to maximize the impact created by the project. Thus result created under this strategy directly relate to plans and activities reflected described in D6.9 “Exploitation Strategy and Roadmap”. Communication and dissemination activities have aimed to address both in-project and outreach communication needs. To support those activities, clear communication messages and tools have been formulated and produced. Various external communication channels and activities have been utilised to reach the target groups.

SOFIE has conducted dissemination and exploitation on the following three verticals: 1) academic, 2) commercial, 3) community (i.e. groups related to and interested in topics that SOFIE explores). In the Interim report D6.8 we distinguished two verticals (academic and commercial), nevertheless for the benefit of more systemized presentation of our dissemination and exploitation work, it was essential to formulate the community vertical and report accordingly.

All consortium partners are contributors to the communication and dissemination activities under WP6: Communication, Dissemination, and Exploitation, led by Guardtime OÜ. The communication and dissemination activities have been managed via the communication channel on Slack as well as the project’s official mailing list. All communication materials have been uploaded to SOFIE’s webpage. Lists of publications and presentations, as well as WP6 related deliverables, are managed on the SOFIE Wiki page.

1.1.1 Key message

The key message of the project has been used to inform the targeted audiences of the value in using project SOFIE’s results. During the second part of the project’s lifetime SOFIE’s primary message has been sharpened to better reflect SOFIE’s ambitions.

The key message is as follows:

SOFIE facilitates the smooth creation of new IoT business platforms through secure open federation - powered by the SOFIE architecture, software framework, and reference implementation.

1.1.2 Objectives

The objectives of the communication and dissemination activities were determined in D6.6 and have remained the same during the lifetime of the project.

Our goal has been:

- Raising general awareness about the project and its output.
- Supporting the engagement of stakeholders for participation in the work of SOFIE technical work packages WP2-WP5.
- Gathering feedback from stakeholders that can be incorporated in SOFIE’s scientific and development activities.
- Attracting users from targeted sectors to start using SOFIE’s results.
- Ensuring high transparency and accessibility of the project output.

1.1.3 Target groups

The main audiences for communication and dissemination activities have been as follows: academic community, (potential) industrial partners for exploiting the commercial components of SOFIE, policy makers and general public. The target audiences were refined in D6.6 and have remained the same until the end of the project.

The aim has been to involve the **academic community** into SOFIE project content discussion, so that they could use and build on SOFIE results in future academic works through dissemination process with the hope to lead way to other research projects that might grow out of components and knowledge developed in SOFIE. The **industry** target audience has been kept informed about SOFIE research. We have fulfilled our aim to engage this audience with the issues addressed by the project and invite them to use/implement exploitable components of SOFIE. The **policy** target group has been invited to discuss the knowledge acquired during the lifespan of the project and its results with the possibility to have an impact on future policy making in EU and beyond. Additionally, SOFIE project developments and results have been communicated to the **general audience**, as well. We have created general support and awareness of the advantages SOFIE provides and to invited external contributors to use the SOFIE solution. In this deliverable we demonstrate that within the reporting period all the target groups have been reached out to and engaged with, using the related communication messages and value offers and designated tools and channels.

1.1.4 General out-reach channels

The main communication and dissemination channels throughout the project are:

1. Offline channels
   - Business networking
   - Conferences
   - Scientific publications
   - Workshops and seminars
   - Industry meetings
   - Policy meetings

2. Online channels
   - Official SOFIE website
   - Social Media (SOFIE Twitter and LinkedIn)
   - SOFIE Newsletter
   - SOFIE Wiki

1.1.5 Visual Identity

A visual identity for SOFIE was created at the beginning of the project. This visual identity has been used in all the dissemination outputs, such as the project website, deliverables, presentations, leaflets, etc. Primary colour codes used in visualizing SOFIE are #36bba5 for web and #01b4bc for print materials. The approach to design is simple and clean, using neutral and soft colours. The typeface for SOFIE is Barlow and its variations (Barlow Strong, Barlow Medium, Barlow Light etc.).

The SOFIE logo combines IoT with the circle O around SOFIE and stopping at the I. As SOFIE stands for Secure Open Federation of Internet Everywhere, the circle in the logo is left open to symbolize the notion of openness of the SOFIE federation.

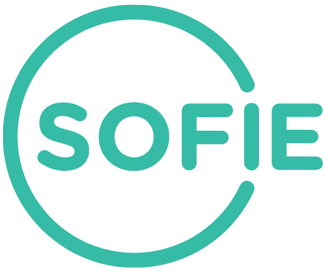
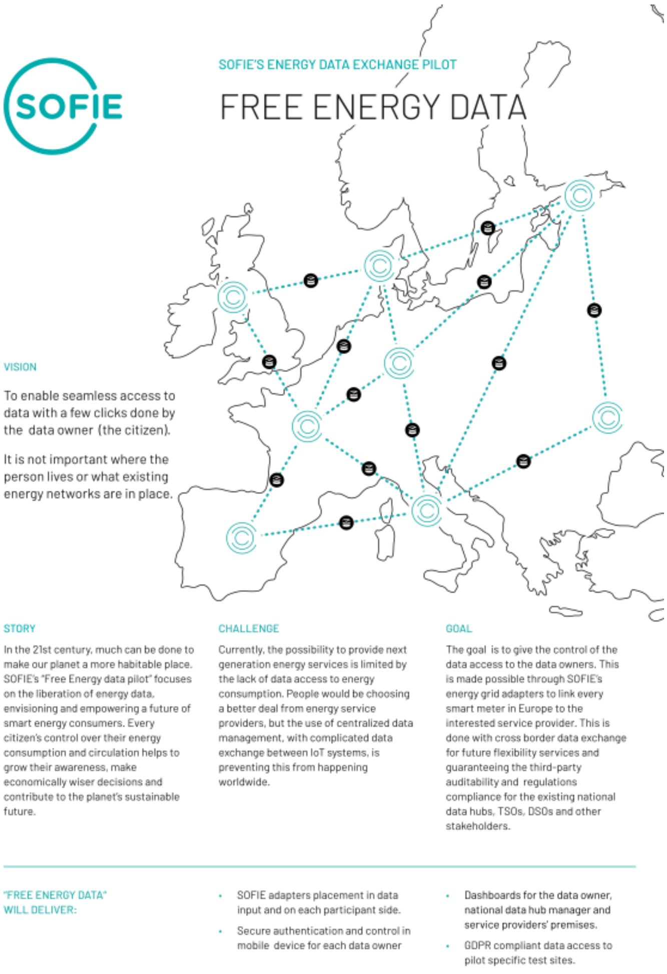


Figure 1. The SOFIE logo

Examples of visual identity in use:



SOFIE'S ENERGY DATA EXCHANGE PILOT

FREE ENERGY DATA

VISION

To enable seamless access to data with a few clicks done by the data owner (the citizen).

It is not important where the person lives or what existing energy networks are in place.

STORY

In the 21st century, much can be done to make our planet a more habitable place. SOFIE's "Free Energy data pilot" focuses on the liberation of energy data. envisioning and empowering a future of smart energy consumers. Every citizen's control over their energy consumption and circulation helps to grow their awareness, make economically wiser decisions and contribute to the planet's sustainable future.

CHALLENGE

Currently, the possibility to provide next generation energy services is limited by the lack of data access to energy consumption. People would be choosing a better deal from energy service providers, but the use of centralized data management, with complicated data exchange between IoT systems, is preventing this from happening worldwide.

GOAL

The goal is to give the control of the data access to the data owners. This is made possible through SOFIE's energy grid adapters to link every smart meter in Europe to the interested service provider. This is done with cross border data exchange for future flexibility services and guaranteeing the third-party auditability and regulations compliance for the existing national data hubs, TSOs, DSOs and other stakeholders.

"FREE ENERGY DATA" WILL DELIVER:

- SOFIE adapters placement in data input and on each participant side.
- Secure authentication and control in mobile device for each data owner
- Dashboards for the data owner, national data hub manager and service providers' premises.
- GDPR compliant data access to pilot specific test sites.

Figure 2. Decentralised Energy Data Exchange pilot's promotional material (print material)

SOFIE - Secure Open Federation for Internet Everywhere

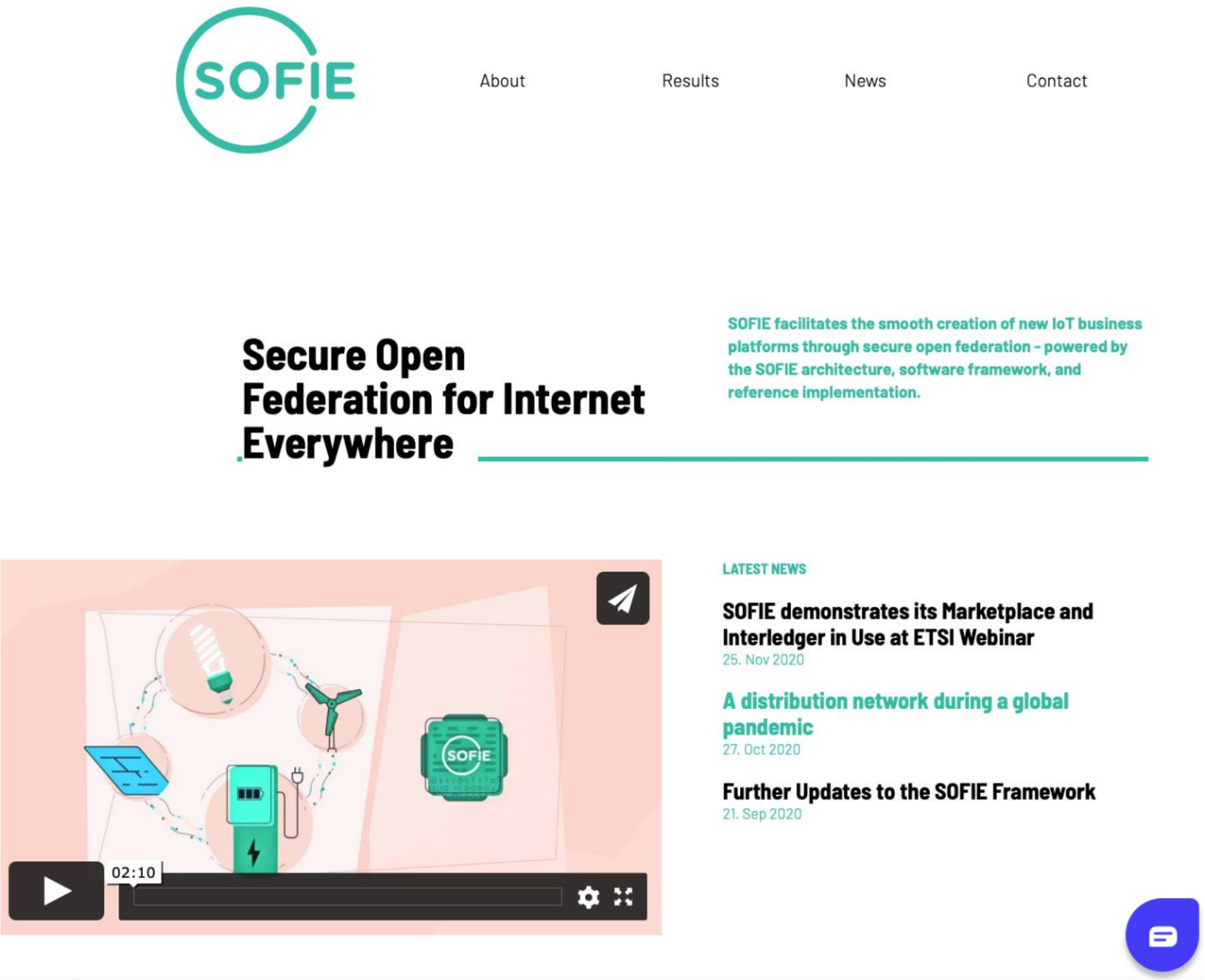
Figure 3. SOFIE video (audio-visual material)

2. Communication and dissemination during M26-36

This Chapter provides an overview of the communication and dissemination tools and activities created and conducted in the project, including the analysis of website and social media usage analysis. Additionally, lists of publications and events are presented, and an overview of various communication tools, channels and activities carried out to reach SOFIE target audiences and to promote the project is offered.

2.1 Project Website

The SOFIE website is one of the project's key dissemination tools and simple and systemized source for information about the project, especially for the wider IoT community and the general public. It is available at https://www.sofie-iot.eu.



Secure Open Federation for Internet Everywhere

SOFIE facilitates the smooth creation of new IoT business platforms through secure open federation - powered by the SOFIE architecture, software framework, and reference implementation.

LATEST NEWS

SOFIE demonstrates its Marketplace and Interledger in Use at ETSI Webinar
25. Nov 2020

A distribution network during a global pandemic
27. Oct 2020

Further Updates to the SOFIE Framework
21. Sep 2020

Figure 4. The project's main webpage.

The site contains several sections: general information about the project, news and blog items, contact information and publicly available publications and project deliverables, promotional materials, use-case introductions and components information etc. The website is regularly updated to assure that visitors get coherent and timely information about the project as it develops. The visitor numbers of the webpage were approximately 300-350 visitors per month.

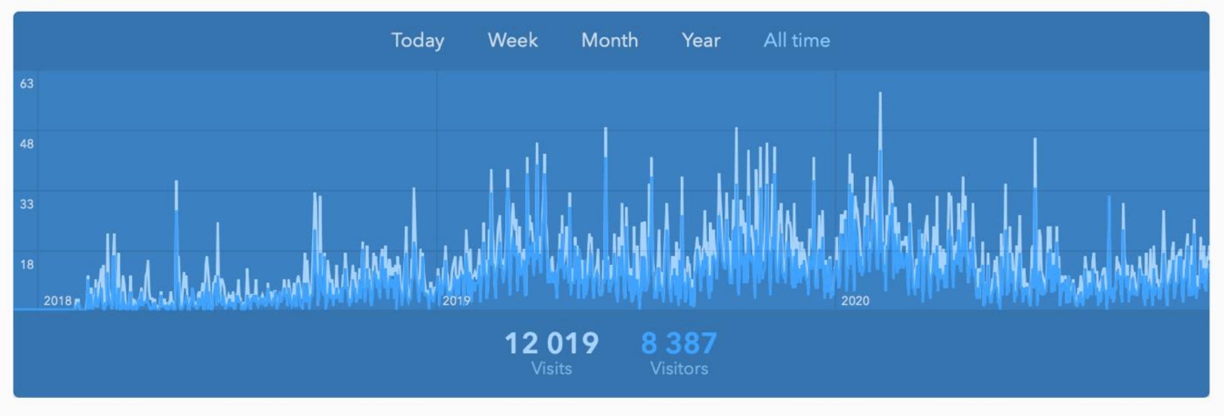


Figure 5. Overview of website visitors throughout the project lifetime (10.12.2020).

By the end of the project, the webpage had approx. 12019 visits with 8378 visitors. Two of the most visited pages besides the main page are “about SOFIE project”, project deliverables” and “project deliverables. It can be concluded that people visiting the SOFIE website want to know what SOFIE is about and (then) look for results. Out of the over 12000 visits, around half come to the SOFIE webpage directly and the second half through search results or via reference or social media. Although, we aimed to reach higher visitor numbers, the achieved attraction for the website is still substantial and proves that this source has been relevant for our audiences.

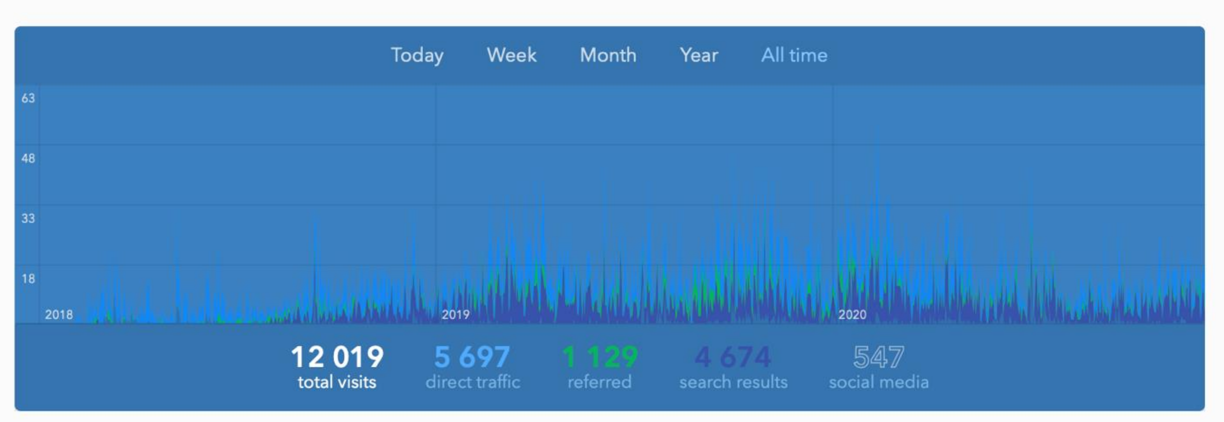


Figure 6. Overview of visit sources (10.12.2020).

In 2020 several subpages of the webpage were updated to give a more thorough insights into the project. E.g. the “About” section was updated with SOFIE components and the section with promotional materials was enhanced.

One of the most important regularly uploaded content areas for the webpage were the blog posts. The partners followed the established timetable for producing content to the blog section and we were successful in producing 31 blog posts in total. The blogs help the project followers to gain further insight into the project theory and the development of different use cases.

The list of published blog posts from February to December 2020 (M26-36) is as follows:

1. Automated Tests in Software Development
2. Leveraging Interledger Functionality in Automated Responsible Disclosure of Vulnerabilities
3. Could Decentralized Identifiers Facilitate Users’ Control over Their Data?
4. A glimpse of hope for the Food Supply Chain in the COVID-19 era

5. The SOFIE user experience from energy data exchange perspective
6. SMAUG: a decentralized marketplace for smart lockers built with SOFIE
7. Blockchains in the Food Supply Chain during a pandemic - SOFIE to the rescue!
8. DLT benefits on electric mobility cyber security improvement
9. A distribution network during a global pandemic
10. Quick guide on how to use SOFIE federated adapter in a datahub
11. Setting standards for the future
12. Achievements of the SOFIE project

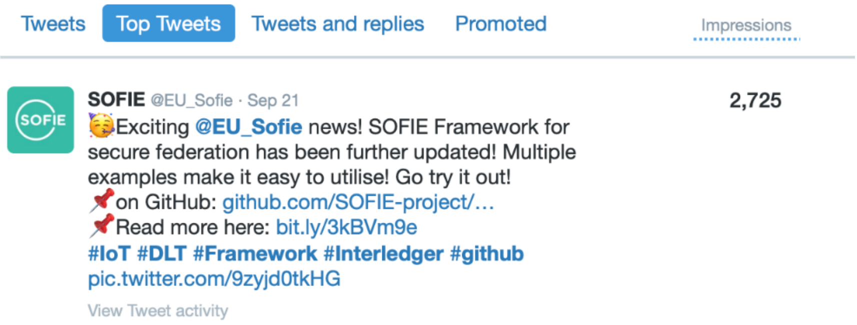
The previous 19 blog posts were reported in D6.8.

2.2 Social media

The project has two social media accounts: one on Twitter and one on LinkedIn. Through these channels the project's goals and advances have been shared and promoted.

Twitter. The purpose of SOFIE's Twitter profile (https://twitter.com/EU_Sofie) is to reach wide and targeted audiences in a fast and efficient manner. Twitter is used to communicate the main events, publications, as well as news related to the project.

By the end of December 2020 (13.12.2020) SOFIE had 279 followers on Twitter. Usually, within a 28-day period SOFIE Twitter earns 6500-12000 impressions (2500-3500 impressions during the summer). Twitter impressions show how many *total* times people have seen the tweets. In other words, e.g. 500 impressions mean that a tweet has been seen 500 times. Usually, a month's top tweet collects 700-2700 impressions (see Figure 4).



SOFIE @EU_Sofie · Sep 21

🥳Exciting @EU_Sofie news! SOFIE Framework for secure federation has been further updated! Multiple examples make it easy to utilise! Go try it out!
📌on GitHub: github.com/SOFIE-project/…
📌Read more here: bit.ly/3kBVm9e
#IoT #DLT #Framework #Interledger #github
pic.twitter.com/9zyjd0tkHG

2,725

Figure 7. Top Tweet on SOFIE Twitter in October 2020.

LinkedIn. LinkedIn is a social network targeted to engage and serve the business community. The purpose of SOFIE's LinkedIn profile (https://www.linkedin.com/company/sofie-project) has been to promote SOFIE results for this community and help to establish contacts with industry. By the end of December 2020 (13.12.2020) the page has 84 followers.

In conclusion, the number of social media followers increased throughout the project. In total, SOFIE project had over 350 followers by the end of the project, which is slightly lower than the expected goal (500) but nevertheless substantial and satisfactory to provide an interested and engaged audience. The project did not engage in paid follower building, meaning that the gained number followers are organic. Although gaining organic followers is harder, we prioritized getting people follow us "organically" to assure higher engagement with the content and long-term connectedness to the channel.

2.3 Other communication tools

SOFIE Newsletter. In 2020 the SOFIE Newsletter was sent out quarterly. It gives an overview of the deliverables, publications and other relevant events that have occurred during this time period. Everybody could sign up for the newsletter on the SOFIE website. The newsletter provides a compact overview of the project and it is a good way to summarize the project to its followers. In 2020 three Newsletters were sent out (February, June and October). They can be found from the "Promotional materials" section of the webpage: https://www.sofie-iot.eu/about/promotional-materials. By December 2020 the newsletter had 78 subscribers.

External SOFIE profiles. During the reporting period SOFIE utilized the previously established **Cyberwatching.eu profile** https://cyberwatching.eu/projects/1302/sofie to promote its events and framework components. In 2020 SOFIE also joined the **SecureIoT** project **marketplace platform:** https://secureiot.eu to primarily exhibit its components. Being a part of both initiatives has helped to wider the project's visibility and empower cooperation with other EU projects.

2.4 Scientific Publications

The SOFIE project has strong scientific foundation and many of the research results have already been published in conferences with formal proceedings and in journals. The project has exceeded its initial goal to publish 14 publications. By the end of the project, we had 34 published publications. During M26-36 we released 12 publications. In this section we present all the projects academic publications to offer a concise overview and discussion of the whole set of publications produced by and during the project. All the publications have been also made available of SOFIE website.

Journal and Scientific Magazine Publications

[J1] Y. Kortesniemi, D. Lagutin, T. Elo, N. Fotiou, "Improving the Privacy of IoT with Decentralised Identifiers (DIDs)," *Journal of Computer Networks and Communications,* vol. 2019, March 2019.

[J2] V.A. Siris, P. Nikander, S. Voulgaris, N. Fotiou, D. Lagutin, G.C. Polyzos, "Interledger Approaches," *IEEE Access,* vol. 7, pp. 89948-89966, July 2019.

[J3] S. Voulgaris, N. Fotiou, V.A. Siris, G.C. Polyzos, M. Jaatinen, Y. Oikonomidis, "Blockchain Technology for Intelligent Environments," *Future Internet,* vol. 11, no. 10, October 2019.

[J4] V.A. Siris, D. Dimopoulos, N. Fotiou, S. Voulgaris, G.C. Polyzos, "Decentralized authorization in constrained IoT environments exploiting interledger mechanisms," *Computer Communications,* Elsevier, vol. 152, pp. 243-251, February 2020. (PDF)

[J5] R. Neisse, J.L. Hernandez-Ramos, S.N. Matheu-Garcia, G. Baldini, A. Skarmeta, V.A. Siris, D. Lagutin, P. Nikander, "An Interledger Blockchain Platform for cross-border Management of Cybersecurity Information," *IEEE Internet Computing*, pp. 1-11, June 2020.

[J6] S. Paavolainen, C. Carr, "Security Properties of Light Clients on the Ethereum Blockchain," *IEEE Access*, vol. 8, pp. 124339-124358, June 2020.

[J7] A. Manzoor, M. Samarin, D. Mason, M. Ylianttila, "Scavenger Hunt: Utilization of Blockchain and IoT for a Location-Based Game," *IEEE Access*, vol. 8, pp. 204863-204879, November 2020.

Conference and Workshop Publications

[C1] A. Karila, Y. Kortesniemi, D. Lagutin, P. Nikander, S. Paavolainen, N. Fotiou, G.C. Polyzos, V.A. Siris, T. Zahariadis, "Secure Open Federation for Internet Everywhere," Proc. Workshop on Decentralized IoT Security and Standards (DISS) in conjunction with Network and Distributed System Security Symposium (NDSS), San Diego, CA, USA, February 2018.

[C2] N. Fotiou and G.C. Polyzos, “Smart Contracts for the Internet of Things: Opportunities and Challenges,” Proc. European Conference on Networks and Communications (EuCNC), Ljubljana, Slovenia, June 2018. (PDF)

[C3] S. Paavolainen and P. Nikander, “Security and Privacy Challenges and Potential Solutions for DLT based IoT Systems,” Proc. Global Internet of Things Summit (GIoTS), Bilbao, June 2018. (PDF)

[C4] A.S. Ahmed and T. Aura, “Turning Trust Around: Smart Contract-Assisted Public Key Infrastructure,” Proc. 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), New York, NY, USA, August 2018. (PDF)

[C5] S. Paavolainen, T. Elo, P. Nikander, “Risks from Spam Attacks on Blockchains for Intemet-of-Things Devices,” Proc. 9th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, USA, November 2018. (PDF)

[C6] N. Fotiou, V.A. Siris, G.C. Polyzos, “Interacting with the Internet of Things using Smart Contracts and Blockchain Technologies,” Proc. 11th International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage (SpaCCS), Melbourne, Australia, December 2018. (PDF)

[C7] N. Fotiou, V.A. Siris, S. Voulgaris, G.C. Polyzos, D. Lagutin, “Bridging the Cyber and Physical Worlds using Blockchains and Smart Contracts,” Proc. Workshop on Decentralized IoT Systems and Security (DISS) in conjunction with the Network and Distributed System Security Symposium (NDSS), San Diego, CA, USA, February 2019.

[C8] D. Lagutin, Y. Kortesniemi, N. Fotiou, V.A. Siris, “Enabling Decentralised Identifiers and Verifiable Credentials for Constrained IoT Devices using OAuth-based Delegation,” Proc. Workshop on Decentralized IoT Systems and Security (DISS) in conjunction with the Network and Distributed System Security Symposium (NDSS), San Diego, CA, USA, February 2019.

[C9] V.A. Siris, D. Dimopoulos, N. Fotiou, S. Voulgaris, G.C. Polyzos, “OAuth 2.0 Meets Blockchain for Authorization in Constrained IoT Environments,” Proc. 5th IEEE World Forum on Internet of Things (WF-IoT), Limerick, Ireland, April 2019. (PDF)

[C10] V.A. Siris, D. Dimopoulos, N. Fotiou, S. Voulgaris, G.C. Polyzos, “Interledger Smart Contracts for Decentralized Authorization to Constrained Things,” Proc. 2nd Workshop on Cryptocurrencies and Blockchains for Distributed Systems (CryBlock 2019), in conjunction with IEEE INFOCOM 2019, Paris, France, April-May 2019. (PDF)

[C11] S. Paavolainen and P. Nikander, “Interledger Demo: IoT Integration,” Proc. IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Seoul, Korea (South), May 2019. (PDF)

[C12] V.A. Siris, D. Dimopoulos, N. Fotiou, S. Voulgaris, G.C. Polyzos, “IoT Resource Access utilizing Blockchains and Trusted Execution Environments,” Proc. Global IoT Summit, Aarhus, Denmark, June 2019. (PDF)

[C13] S. Paavolainen and P. Nikander, “Decentralized Beacons: Attesting the Ground Truth of Blockchain State for Constrained IoT Devices,” Proc. Global IoT Summit (GIoTS), Aarhus, Denmark, June 2019. (PDF)

[C14] N. Fotiou, I. Pittaras, V.A. Siris, S. Voulgaris, G.C. Polyzos, “Secure IoT access at scale using blockchains and smart contracts,” Proc. 8th IEEE WoWMoM Workshop on the Internet of Things: Smart Objects and Services (IoT-SoS), Washington DC, USA, June 2019. (PDF)

[C15] V.A. Siris, D. Dimopoulos, N. Fotiou, S. Voulgaris, G.C. Polyzos, “Trusted D2D-based IoT Resource Access using Smart Contracts,” Proc. 20th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), Washington DC, USA, June 2019. (PDF)

[C16] D. Lagutin, F. Bellesini, T. Bragatto, A. Cavadenti, V. Croce, Y. Kortesniemi, H.C. Leligou, Y. Oikonomidis, G.C. Polyzos, G. Raveduto, F. Santori, P. Trakadas, M. Verber, “Secure Open Federation of IoT Platforms Through Interledger Technologies – The SOFIE Approach,” Proc. European Conference on Networks and Communications (EuCNC), Valencia, Spain, June 2019. (PDF)

[C17] E. Arzoglou, T. Elo, and P. Nikander, “The Case of iOS and Android: Applying System Dynamics to Digital Business Platforms,” Proc. 19th International Conference on Computational Science (ICCS), Faro, Portugal, published in *Lecture Notes in Computer Science*, Vol. 11540, J.M.F. Rodrigues et al. (eds), Springer, June 2019. (PDF)

[C18] P. Nikander, J. Autiosalo, S. Paavolainen, "Interledger for the Industrial Internet of Things," Proc. 17th IEEE International Conference on Industrial Informatics (INDIN), Helsinki, Finland, July 2019. (PDF)

[C19] N. Fotiou, I. Pittaras, V.A. Siris, S. Voulgaris, G.C. Polyzos, “OAuth 2.0 Authorization using Blockchain-based Tokens,” Proc. Workshop on Decentralized IoT Systems and Security (DISS) in conjunction with the Network and Distributed System Security Symposium (NDSS), San Diego, CA, USA, February 2020.

[C20] V.A. Siris, M. Tsenos, D. Dimopoulos, N. Fotiou, G.C. Polyzos “Decentralized Interledger Gateway Architectures in Authorization Scenarios with Multiple Ledgers,” Proc. Global Internet of Things Summit (GIoTS), Dublin, Ireland, June 2020. (PDF)

[C21] F. Carere, F. Bellesini, T. Bragatto, V. Croce, G. Raveduto, F. Santori. M. Veber, “Flexibility - enabling technologies using electric vehicles,” Proc. IEEE International Conference on Environment and Electrical Engineering and IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe), Madrid, Spain, June 2020. (PDF)

[C22] S. Voulgaris, N. Fotiou, V.A. Siris, G.C. Polyzos, A. Tomaras, S. Karachontzitis, “Hierarchical Blockchain Topologies for Quality Control in Food Supply Chains,” Proc. European Conference on Networks and Communications (EuCNC), June 2020. (PDF)

Published Abstracts and Posters in Conference and Workshop Proceedings

[S1] N. Fotiou, I. Pittaras, V.A. Siris, G.C. Polyzos, “Enabling opportunistic users in multi-tenant IoT systems using decentralized identifiers and permissioned blockchains,” Proc. Workshop on the Internet of Things Security and Privacy (IoT S&P), in conjunction with the 26th ACM Conference on Computer and Communications Security (CCS), London, UK, November 2019 (poster). (PDF)

[S2] N. Fotiou, I. Pittaras, V.A. Siris, S. Voulgaris, G.C. Polyzos, “Poster: Securing IoT services using DLTs and Verifiable Credentials,” Proc. Network and Distributed System Security Symposium (NDSS), San Diego, CA, USA, February 2020 (poster).

Book Chapters

[B1] D. Lagutin, et al., “SOFIE – Secure Open Federation for Internet Everywhere,” Section 7.8 in Chapter 7 of “IoT European Security and Privacy Projects: Integration, Architectures and Interoperability,” E. Ferrera et al., in *Next Generation Internet of Things, Distributed Intelligence at the Edge and Human Machine-to-Machine Cooperation*, O. Vermesan and J. Bacquet, eds., River Publishers, 2018.

[B2] D. Lagutin, P. Anton, F. Bellesini, T. Bragatto, A. Cavadenti, V. Croce, N. Fotiou, M. Haavala, Y. Kortesniemi, H. C. Leligou, A. Manzoor, Y. Oikonomidis, G.C. Polyzos, G. Raveduto, F. Santori, V.A. Siris, P. Trakadas, M. Verber, “The SOFIE Approach to Address the Security and Privacy of the IoT using Interledger Technologies,” in *Security and Privacy in Internet of Things: Challenges and Solutions*, J.L. Hernández Ramos and A. Skarmeta eds., IOS Press, (Ambient Intelligence and Smart Environments, Ebook Series, vol. 27), March 2020. (PDF)

[B3] D. Lagutin, Y. Kortesniemi, V.A. Siris, N. Fotiou, G. C. Polyzos, L. Wu, “Leveraging Interledger Technologies in IoT Security Risk Management,” in *Security Risk Management for the Internet of Things: Technologies and Techniques for IoT Security, Privacy and Data Protection*, J. Soldatos, ed., now publishers, pp. 229-246, June 2020. (PDF)

SOFIE researchers have published extensively throughout the lifetime of the project. (References in this subsection are to the above full list of SOFIE publications.) Starting with the basic ideas and plan of the project early on to a workshop [C1] and then a book chapter [B1], through studies of architectural trade-offs, e.g., [C21], to extensive and specific results of various particular investigations, e.g., [J7].

Key technologies employed and promoted and their application to the IoT have been addressed in [J2] (Interledger), [J1] (DIDs), [J3] (DLTs), and [J4] (Decentralized authorization).

The publications cover the whole spectrum of scientific publication types, from Journal articles, and one in a scientific magazine with typically wider visibility [J1-J7], through competitive and timely conference and workshop publications [C1-C22], with [S1] and [S2] being posters, but to top security conferences, ACM CCS and NDSS. Moreover, we have written book chapters [B1-B3] that are parts of focused and relevant collective works. They are accessible on the Web, and many journal ones are in open access publications. In particular, three articles are in the (relatively) new *IEEE Access* journal, which has attracted attention and interest because of its fully open access format, the importance and tradition of IEEE in the area, and fast and effective reviewing cycle.

Finally, we could categorize the SOFIE publications in the following, partially overlapping, categories, mostly as guidance about what is the main emphasis of the paper:

(i) SOFIE Overview: [C1], [C16], [B1], [B2]
(ii) Review, survey, selection and promotion of key technologies: [J1], [J2], [J3], [C3]
(iii) Architectural: [J2], [C1], [B1], [C20], [C22]
(iv) SOFIE pilot related: [J7], [C21], [C22], [C16]
(v) Solutions for constrained IoT Devices: [J4], [C6], [C7], [C9], [C10], [C13],
(vi) Business platform related: [C17], [S1], [B3], [J5]
(vii) DIDs, VCs, OAuth 2.0: [J1], [J4], [C8], [C9], [C10], [C15], [C19], [S1], [S2], [C12]
(viii) Interledger focused: [J2], [C18], [C20], [J4], [C11], [C12]
(ix) DLT focused: [J6], [J3], [C2], [J2], [C5], [C13]
(x) Trust focused: [C4], [C12], [C13], [C15]

Note that most of the papers could fit on very many of these categories, however, we limit joint membership for readability and effectiveness as guidance.

2.5 Events and presentations

All the attended events have given an excellent opportunity for project partners to interact with audiences from different domains relevant to the project. It needs to be emphasised that the global COVID-19 pandemic positioned us in a situation where we had to cancel and rethink the participation at a number of previously planned events. Especially affected were our exhibiting plans. All in all, SOFIE manged to adjust to the situation and through adjusted presentation methods we connected with our audiences despite the rapidly changed circumstances. The majority of the reported events and related presentations were given virtually with the assistance of telecommunication tools.

The table below gives a detailed overview of the presentations given by SOFIE partners between February 2020 and December 2020. The previous (M1-25) presentations were reported in D6.8.

Table 1. List of SOFIE presentations at various events.

Date	Presenter(s)	Presentation title	Place	Audience
13.2.2020	Dmitrij Lagutin	SOFIE, Distributed Ledgers, and Decentralized Identifiers	COMNET Research Workshop, Aalto University, Espoo, Finland	Scientific community
18.3.2020	Dmitrij Lagutin, Nikos Fotiou	Using Decentralized Identifiers (and Verifiable Credentials) in IoT Services	W3C Web of Things Interest Group, Virtual F2F Meeting	Industry, Scientific community
5.6.2020	Dmitrij Lagutin, Yannis Oikonomidis, Giuseppe Raveduto, Liis Livin, Max Samarin	The Interoperability between IoT Platforms: the SOFIE Framework	Webinar of NGIoT project.	Industry, Scientific Community
18.6.2020	George C. Polyzos, Santeri Paavolainen, Vassilios A. Siris, Priit Anton, Giuseppe Raveduto, Max Samarin, Spyros Voulgaris	1. An Introduction: The IoT Space and Where SOFIE fit in - G. Polyzos; 2. Combining multiple ledgers for better control - Interledger approaches in IoT - S. Paavolainen; 3. Enabling Decentralised Identifiers and Verifiable Credentials for Constrained IoT Devices - V. A. Siris.; 4. Enabling next generation secure energy services through data exchange liberation- P. Anton; 5. A marketplace for flexibility: improving	SOFIE WORKSHOP: Decentralised operation and security in the IoT Space	Industry, Scientific Community, Policy Makers

		power network efficiency using electric vehicles - G. Raveduto; 6. Exploring DLT & IoT use-cases in mobile gaming - M. Samarin; 7. Blockchain-based Architectures for Food Supply-Chain Management - S. Voulgaris.		
22.6.2020	Nikos Fotiou, Dmitrij Lagutin	Using Verifiable Credentials in IoT Services	W3C Web of Things Interest Group, Virtual F2F Meeting	Industry, Scientific Community
3.7.2020	Dmitrij Lagutin	Secure Open Federation for Internet Everywhere (SOFIE): Interledger and Identifiers	Webinar of NGIoT project	Industry, Scientific Community
22.7.2020	Nikos Fotiou	OAuth 2.0 meets verifiable credentials and blockchain-based tokens	OAuth Security Workshop 2020	Industry, Scientific Community
30.9.2020	Ahsan Manzoor	SOFIE- mobile gaming pilot	Digital Vaccination Certificates in Post-COVID Pakistan	Industry, Scientific Community
20.10.2020	Priit Anton	Solving trust and privacy challenges in the IoT field – an energy sector example	IoT Forum virtual event: Digital Around the World	Industry, Scientific Community, Policy Makers
20.10.2020	George C. Polyzos	Decentralized Identifiers and Verifiable Credentials in SOFIE with applications in aviation	3rd CHARIOT workshop: “IoT Data Security and Privacy Solutions - challenges and Opportunities for Airports”	Industry, Scientific Community, Policy Makers
12-13.11.2020	Ahsan Manzoor	Mobile Gaming Pilot: Utilization of Blockchain and IoT for a location-based Game.	DELTA (Doctoral Training Network, Finland)	Scientific
25.11.2020	Dmitrij Lagutin	Secure Open Federation for Internet Everywhere (SOFIE)	European Commission's Standardization Roundtable Discussion:	Industry, Scientific Community, Policy Makers

			Digital Society, Identity and Privacy	
2.12.2020	Vincenzo Croce	IoT Decentralized identity for electric mobility and renewable energy	Digital Identity and Distributed Systems Conference	Industry
11.12.2020	Dmitrij Lagutin	Decentralized Identifiers, Verifiable Credentials, and Internet of Things	Visions of Tomorrow event, University of Pisa	Scientific community
17.12.2020	Santeri Paavolainen, Antonio Antonino, Erik Forsgren	Interledger in use: SOFIE decentralized marketplace demonstrator	ETSI BrightTalk	Industry

2.5.1 SOFIE workshops

During the project SOFIE aimed to deliver three project specific workshops to disseminate and promote SOFIE results and the project itself.

The first SOFIE workshop took place in October 2019 and was reported in D6.8. It was dedicated to presenting and demonstrating SOFIE's use cases to specific target audiences and to gather relevant feedback. Early this year its video was realised. It is available here.

During M26-36, SOFIE organized additional two workshops: one workshop dedicated to disseminating SOFIE research results and the other one dedicated to exploitation activities and included stakeholder interviews.

The second SOFIE Workshop. On 18th of June 2020 SOFIE dedicated a workshop to "Decentralised operation and security in the IoT Space" introducing our outstanding research results and applications to showcase how decentralisation in the IoT Space helps our society and economy. The event was organized in cooperation with Cyberwatching.eu initiative.

SOFIE representatives gave the following presentations:

- "An Introduction: The IoT Space and Where SOFIE fit in" by George Polyzos.
- "Combining multiple ledgers for better control - Interledger approaches in IoT" by Santeri Paavolainen.
- "Enabling Decentralised Identifiers and Verifiable Credentials for Constrained IoT Devices" by Vasilios A. Siris.
- "Enabling next generation secure energy services through data exchange liberation" by Priit Anton.
- "A marketplace for flexibility: improving power network efficiency using electric vehicles" by Giuseppe Raveduto.
- "Exploring DLT & IoT use-cases in mobile gaming" by Max Samarin.
- "Blockchain-based Architectures for Food Supply-Chain Management" by Spyros Voulgaris.

The workshop was recorded and is available here. The virtual workshop had 70 active participants from 23 countries: 19 EU Member States and 4 Non-EU/global. For the EU, Greece and Italy were by far the most represented country, followed by Finland, Belgium and Portugal. The majority of them were from software industry (23%), followed by educational institutions

(16%), other research organisations (13%), consulting firms (10%) and telecommunications industry (7%).

As a result, SOFIE and Cyberwatching.eu compiled a whitepaper presenting IoT's societal impacts and giving recommendations for future EU funding programmes. The report is available here.

The third SOFIE Workshop. In October-December 2020 SOFIE conducted a workshop the "Close and personal with SOFIE stakeholders" comprised of 13 expert interviews with stakeholders relevant to exploiting SOFIE results. The aim of the workshop was to investigate SOFIE solution's suitability for end-users and establish mutually beneficial and sustainable relationships with the interviewed stakeholders.

The conducted 13 interviews for this workshop were segmented into four groups according to SOFIE pilots[1] and were carried out by seven SOFIE representatives who lead the work on pilots in the project. They inquired relevant stakeholders and field experts from their use-case perspective.

Two types of generated data were analysed to draw conclusions (1) content of the open-ended interviews that followed a pre-posed interview outline and (2) the interviewers' personal reflections about process of the interviews and gathered feedback.

As a result, the "Close and personal with SOFIE stakeholders" workshop interviews provide the following key take-aways:

- Most interviewees were able to articulate and discuss clear benefits of implementing SOFIE after they were introduced to the value offer and SOFIE project by the interviewers. They were able to see how they could incorporate the offered solution one way or the other now or in the future.
- The most important benefits that SOFIE can provide according to the interviewees are: access control, cross-country data access, simplicity, additional security (DEDE pilot); flexibility and avoiding installation or upgrading of power lines (DEFM pilot); food quality assurance, trust, traceability and gaining a competitive edge (FSC pilot).
- In general, the interviewees were unable to point out clear micro-level monetary benefits of SOFIE implementation. Nevertheless, in the energy and food supply chain vectors the interviewees assessed, in a generalised way, that implementing SOFIE would cut their costs and/or produce more income.
- The barriers to implement SOFIE according to the interviewees are technical integration aspects, potential additional financing requirements and general reluctance to use (and understand) emerging new technologies.
- Out of the four pilots, the context-aware mobile gaming pilot affirmed their position that within Rovio Entertainment Corporation they do not have a viable business offer at this point for the pilot. All other three pilots confirmed that their value propositions match their determined stakeholders, and they continue their commercial work.

What is more, the interviewers reported that during the interviews the interviewees were highly responsive and collaborative. In most cases the interviewees were able to expand the discussion at hand and think along with the interviewer, as well as exhibit deeper interest towards the specific value offer under discussion. The interviewees were not explicitly aware of any similar solution to SOFIE, at least not as much as to be able to name them.

As a result, the suitability of SOFIE pilots value propositions to the stakeholders was confirmed in the cases where the pilots have had business interests throughout the project (DEDE, DEFM,

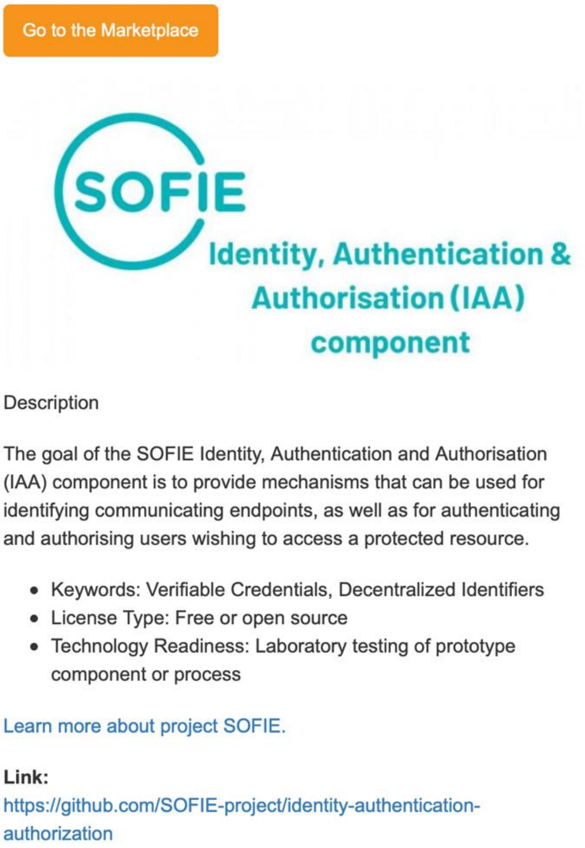
[1] Decentralised Energy Data Exchange (DEDE) pilot, Decentralised Energy Flexibility Marketplace (DEFM) pilot, Food Supply Chain (FSC) pilot, Context-Aware Mobile Gaming pilot.

FSC). These pilots will carry on their work to during and beyond the project to push their assets to the market. The workshop's report is available here (pdf).

Exhibitions

During the reporting period (M26-36) it was impossible for the SOFIE Consortium to participate at any live events where exhibiting SOFIE would have been possible. Thus, we pivoted from the traditional exhibition format and went virtual and showcased our assets online. As a result, we exhibited our results on two online platforms:

1. Cyberwatching.eu marketplace - exhibiting the SOFIE framework components, adapters and pilot use-cases, since summer 2020. On Cyberwatching.eu marketplace SOFIE was also awarded with the "Provider of the Week" award to mark the contribution we had made with exhibiting our result on the marketplace.



Description

The goal of the SOFIE Identity, Authentication and Authorisation (IAA) component is to provide mechanisms that can be used for identifying communicating endpoints, as well as for authenticating and authorising users wishing to access a protected resource.

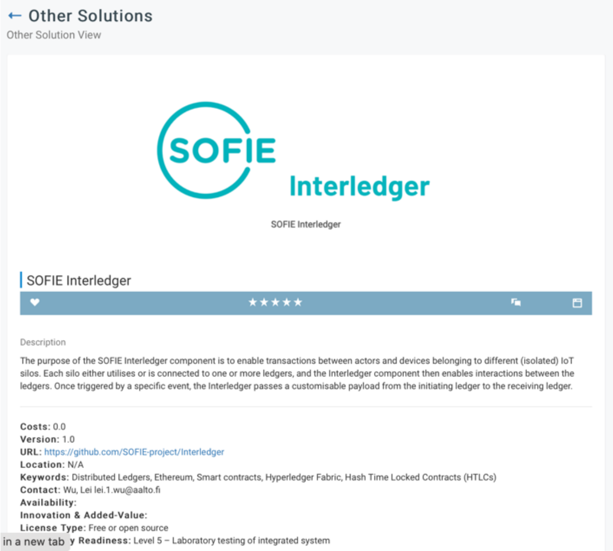
- Keywords: Verifiable Credentials, Decentralized Identifiers
- License Type: Free or open source
- Technology Readiness: Laboratory testing of prototype component or process

Learn more about project SOFIE.

Link:
https://github.com/SOFIE-project/identity-authentication-authorization

Figure 5. An example how IAA component is exhibited on the cyberwatching.eu marketplace.

2. SecureIot Marketplace - exhibiting the SOFIE framework components, adapters and pilot use-cases, since summer 2020.



← Other Solutions

Other Solution View

SOFIE Interledger

★★★★★

Description

The purpose of the SOFIE Interledger component is to enable transactions between actors and devices belonging to different (isolated) IoT silos. Each silo either utilises or is connected to one or more ledgers, and the Interledger component then enables interactions between the ledgers. Once triggered by a specific event, the Interledger passes a customisable payload from the initiating ledger to the receiving ledger.

Costs: 0.0
Version: 1.0
URL: https://github.com/SOFIE-project/Interledger
Location: N/A
Keywords: Distributed Ledgers, Ethereum, Smart contracts, Hyperledger Fabric, Hash Time Locked Contracts (HTLCs)
Contact: Wu, Lei lei.1.wu@aalto.fi
Availability:
Innovation & Added-Value:
License Type: Free or open source
in a new tab **y Readiness:** Level 5 – Laboratory testing of integrated system

Figure 6. An example how the Interledger component is exhibited on the cyberwatching.eu marketplace.

Lastly, SOFIE made the effort to exhibit at the IoTForum global event “IoT Week” on the 5th of June in Dublin, 2020. We managed to propose our exhibition plans to the organisers early 2020. Nevertheless, the event was cancelled in its original format due to the pandemic and thus we had no chance to carry out the exhibit we had envisioned for the event.

2.6 Industry outreach – meetings and networking

All SOFIE partners have made efforts to reach out to the stakeholders, through mostly online meetings, calls and networking during this reporting period, in order to communicate the SOFIE mission and progress, and to gather feedback from the potential end-users to adjust the value offer for the clients in the future. As the project’s pilots are the drivers bringing the SOFIE components to the market, the following section presents the efforts made by each pilots’ partners in M26-36. The meetings and milestones of pilots from M1-25 were reported on D6.8. (Chapter 3.7).

2.6.1 Energy data exchange pilot (Guardtime)

Guardtime’s primary agenda during this reporting period was to present the DEDE adapter in end-user’s environment, and discuss the technology, integration, and business solutions with network operators. The goal was to have 2-3 DSOs and TSOs ready to onboard the DEDE adapters and scope a more detailed PoC to agree the financing, demonstrate the DEDE functionality in relevant end-users’ systems, test the business case and cover potential technical challenges.

Parallel to work with existing stakeholders the additional goal was to find more network operators and integrators who could start using SOFIE DEDE adapter.

Guardtime’s milestones during the reporting period, M26-36.

- Business Model Canvas final version for exploitation ready.
- Onboarding DSOs/flexibility service providers (Elektrilevi, Enoco, Scener).
- Demonstration in Elering/Elektrilevi datahub to control data access, governance mechanism and evidence/audit trail.
- Writing two blog posts in energy sector published on SOFIE webpage.
- Participation at 3 workshops and 12 business meetings.

- Guardtime Management Board's approval to continue with the DEDE adapter exploitation in year 2021.
- SOFIE DEDE adapter concept used for SACCESS H2020 proposal.

Guardtime's meetings during reporting period were:

The interaction with stakeholders has been divided into meetings in the workshops (total 3 workshops during M26-M36) and B2B meetings via teleconferences. The aim of the interaction with stakeholder was to match the business problems with the value that DEDE adapter delivered. The target goal was to agree details to do a Proof of Concept for demonstration of DEDE adapter and start the commercial service offer discussion.

Meetings during reporting period M26-M36 (industry):

- In April 2020 and in October 2020, 2 virtual meetings with Elering Use of DEDE adapter in Estfeed platform, Security aspects of evidence and logs. Data access control handover mechanism.
- In February 2020, in June 2020 and November 2020, 3 virtual meetings with Elektrilevi - onboarding DSO to use DEDE adapter, business case to provide governance of 3rd party smart grid in Poland, Germany.
- In June 2020, 1 virtual meeting with Polskie Sieci Elektroenergetyczne (PSE) – onboarding Poland TSO to use DEDE adapters, potential cooperation in next generation Datahub development.
- In March 2020 and in November 2020, 2 virtual meetings with Enoco - discussing using DEDE adapters to access Estfeed data and share smart meter data to Estonian and France flexibility services providers.

Meetings during reporting period M26-M36 (technology partners):

- In September 2020 and in November 2020, 2 virtual meetings with AKKA - introduction to SOFIE DEDE adapter, potential use-cases (AKKA big data platform integration) and business case with financing mechanisms.
- In February 2020, a virtual meeting with Électricité de France (EDF) - discussing using dede adapters for smart grid data access control.
- In November 2020, a virtual meeting With Cybernetica - authorisation and message exchange and logging procedure related to Estfeed platform. SOFIE DEDE adapter use-case related to logging and audit trail.

To sum up, the exploitation activities during the last year in SOFIE can be evaluated as a success. Guardtime has been able to present the SOFIE assets to such wide range of stakeholders and have created enough interest for future collaboration. There are also three potential cases (Elektrilevi, AKKA and Enoco) where a proposal to do a PoC is in discussion with the aim to sign at least one contact during 2nd half of 2021. There is also the approved confirmation to proceed with SOFIE DEDE adapter exploitation in 2021 by Guardtime management board.

2.6.2 Energy flexibility marketplace pilot (Engineering)

Engineering's primary agenda during this reporting period was to further extend the outreach, participating to industrial workshops and conferences. The COVID-19 pandemic hit live events and networking opportunities, so we tried to exploit remote events as much as possible.

Engineering's milestones during the reporting period:

- Engineering had contacts with DLT (IOTA, Obyte) and crypto-payment solution (PumaPay) providers to discuss about their platforms and their usage in the pilot. Engineering decided to proceed with the Ethereum based solution for the decentralised marketplace. Software implementation of the pilot platform completed. The SOFIE components used in the pilot are updated to the latest released version. The DEFM Federation Adapter was released as part of the SOFIE software release.

Engineering's meetings during reporting period:

- November 2020, interview with ASSEM SpA during 3rd SOFIE workshop where we supported ASM with explaining the advantages of the blockchain-based solution from the technical point of view to the interviewee.

To sum up, during the last year of the project the focus was on consolidating the pilot's platform implementation and participating to remote events on the IoT field. In general, the target audience seems to have responded positively to the pilot platform presented during the events. The stakeholders' interviews revealed a potential interest from DSOs to use the platform operationally, should the regulatory framework change to allow direct exchanges between DSOs and final customers.

2.6.3 Food Supply Chain pilot (Synelixis and Optimum)

During the last period of the project, the focus of the pilot's outreach activities was on demonstrating the pilot's platform to potential adopters. We intensified the communication with Pegasos 7 grapes association, where the pilot platform was deployed and real operational activities have been performed, Agrinio Union[2], where on-premises deployment has also taken place in order to better highlight the functionality of the platform, and Vivartia Group[3], which is a candidate adopter of the pilot platform. In the latter case, we had contacts with two companies, members of the group, Barba Stathis and Delta, which also participated in the interviews for the third SOFIE workshop. Of course, due to the pandemic spur during this last period, physical presence was not possible during a last portion of this period. However, virtual meetings were employed.

Synelixis' and Optimum's milestones during the reporting period:

- On-premises pilot demonstration at Pegasos facilities.
- On-premises deployment and functionality demonstration an Agrinio Union facilities.
- Pilot platform on-site tests have been performed on aforementioned organizations
- Communication establishment with Vivartia Group companies; Barba Stathis and Delta were the main contacts.

Synelixis' and Optimum's meetings during reporting period were:

- During April-September 2020, several virtual meetings (at least 5) with Pegasos 7Grapes association. Discussion point was the on-site deployment of the pilot platform and planning the detail about it.
- End of September 2020, on-site deployment of the pilot platform with Pegasos 7Grapes association.
- August-November 2020, virtual meetings to discuss about the possibility of showcase our pilot platform with Agrinion Union.
- November 2020, Agrinion Union, on-premises demo of the pilot platform to showcase its functionality.
- During September - November 2020 virtual meetings to discuss how our pilot platform could fit in their operations with Vivartia group (Barba Stathis, Delta). Resulted in interview discussions in the context of the third SOFIE workshop.

To sum up, during this last period the pilot partners focused on potential adopters of the pilot platform and how they could keep their interest so as to get them on-board after the project end.

[2] https://www.e-ea.gr/en/
[3] https://www.vivartia.com/?lang=en

In two cases, we have managed to make on-site demos of the pilot platform and in another case, we have managed to establish a communication channel which resulted in two interviews with key people in the organization. Our plan is to extend the contacts and pursue further collaboration with these organizations in the context of the pilot platform and how it could be utilized in their operations. The approach that we will follow in this case is to propose a demonstration of the platform capabilities, preferably with on-site deployments. The goal is to on-board these organizations to our pilot platform eventually, so that the pool of participants in the platform increases.

2.6.4 Context-Aware Mobile Gaming Pilot (Rovio)

Rovio's primary agenda during this reporting period was to disseminate and communicate the mobile gaming pilot implemented during the M1- 25. After gathering feedback, the next goal was to look at the potential impact and business opportunities created by such a game. We also had a free form discussion with the industry leaders regarding the uses and benefits of distributed ledger technologies and IoT in mobiles games.

Rovio's milestones during the reporting period:

- In January 2020, research visit to University College Dublin Ireland discussed uses of Decentralised Identifiers in mobile gaming advertisement and started the work on a new use case.
- In April 2020, Rovio wrote a blogpost for SOFIE titled "Could Decentralised Identifiers Facilitate Users' Control over Their Data?"
- Rovio also helped to develop SOFIE provisioning and discovery for SAMUG proof of concept, which was accepted in ETSI ISG PDL-005 specification.
- Rovio had a planned internal playtest for mobile gaming pilots in 2020 but it was cancelled due to COVID-19.

Meetings during the reported period:

- In September 2020, Rovio held 5 different virtual meetings with gaming industry experts.

To sum up, from the different meetings and discussions, Rovio decided not to pursue the gaming pilot beyond the SOFIE project. Rovio open sourced Scavenger Hunt prototype use cases by releasing code and documentation that has been written throughout the project timeline. This proof-of-concept may serve as a template for future researchers who wish to further investigate IoT and blockchain technologies in the context of gaming.

3. Academic and commercial exploitation during M26-36

The exploitation of the project's results is the key element for the success of the SOFIE project. This chapter covers the knowledge advancement activities by academic partners, as well as the efforts made in commercial exploitation. This chapter provides an overview of the exploitation activities in M26-36. More detailed information is available in SOFIE deliverables D6.9 Exploitation Strategy and Roadmap and D6.10 Business Planning.

During the SOFIE project we have identified 16 assets that can be used for SOFIE exploitation (Table 2) which are explored in more detail on D6.9. but for the sake of clarity, it is important to mention them here as well:

Table 2: SOFIE assets

ID	Name of the Asset	Description of the Asset
1	Interledger	enables secure federation by providing support for atomic transactions spanning two or more ledgers
2	Identity, Authentication and Authorisation	provides IAA functionalities for the different entities in the system by supporting multiple authentication and authorisation techniques
3	Privacy and Data Sovereignty	provides mechanisms that enable data sharing in a controlled way and supports privacy preserving surveys using differential privacy techniques.
4	Semantic Representation	enables semantic level interoperability between different IoT systems, services, and data by describing what functions they provide and what interfaces and formats they utilise.
5	Marketplace	allows participants to trade resources by creating auctions, placing offers, and tracking trade completion in a secure, auditable, and decentralised way.
6	Provisioning and Discovery	enables management and discovery of IoT devices, services, and data.
7	Transportation Federation Adapter	provides the functionality required to federate the Transportation IoT platform to the Food Supply Chain pilot platform of SOFIE.
8	Decentralised Energy Data Exchange adapter[4]	provides access control and governance to smart meter data and datahub integration
9	Decentralised Energy Flexibility Marketplace federation adapter[5]	provides data exchange from IoT to energy flexibility services
10	Decentralised Marketplace for Energy Flexibility Services	provides an energy flexibility provisioning and energy supply.
11	SynField Federation Adapter	provides integration mechanism to exchange of data between an IoT platform and Food Supply Chain platform

[4] Also referred to as "DEDE adapter".

[5] Also referred to as "DEFM federation adapter".

12	SynField platform for traceability and audit services	provides access control, overview, and traceability services for Food Supply Chain participants
13	Aberon Federation Adapter	connects the warehouse automation platform (Aberon) with the SynField platform
14	Scavenger Hunt game	provides location-based game to search for events in IoT environment, solve puzzles and receive rewards (real life interaction)
15	SMAUG	prvides access control, governance, sharing of assets and payment mechanism for IoT smart locker cabins
16	System dynamics models of business platforms federations	provides models to study (IoT) data markets and business platforms

3.1 Exploitable foreground

The exploitable foreground consists of SOFIE framework components, SOFIE federation adapters, and other technologies listed below.

Interledger

The purpose of the SOFIE Interledger component is to enable secure transactions between actors and devices belonging to IoT platforms (silos) using different or separate blockchains. The Interledger component then enables interaction between the ledgers, including atomic transactions across ledgers.

The Interledger component is used in all SOFIE pilots and the Secure Marketplace for Access to Ubiquitous Goods (SMAUG) reference implementation.

Identity, Authentication and Authorisation (IAA)

The goal of the SOFIE Identity, Authentication, and Authorisation (IAA) component is to provide mechanisms that can be used for identifying communicating endpoints, as well as for authenticating and authorising users wishing to access a protected resource.

The IAA component is used by the Food Supply Chain and the Decentralised Energy Data Exchange pilots and SMAUG.

Privacy and Data Sovereignty (PDS)

The SOFIE Privacy and Data Sovereignty component provides mechanisms that allow actors to better control their data, as well as mechanisms that protect client privacy.

PDS enables the creation of privacy preserving surveys. These are surveys that allow users to add noise to their responses using local differential privacy mechanisms. The addition of the noise prevents 3rd parties from learning meaningful information about specific users, but at the same time aggregated statistics can be extracted.

PDS component is used by the Food Supply Chain and Decentralised Energy Data Exchange pilots and SMAUG.

Semantic Representation

Semantic representation is a mechanism for describing the data model and the services of IoT devices. The component defines a common representation data model for IoT devices (Things), their services and their data, which enables interoperability and automation in the deployment of services and applications on top of federated IoT environments.

The Semantic Representation component is used by Food Supply Chain, Decentralised Energy Flexibility Marketplace, and Context-Aware Mobile Gaming pilots and SMAUG.

Marketplace

The goal of the SOFIE Marketplace component is to enable the trade of different types of assets (e.g., electricity for charging a vehicle) in an automated, decentralised, and flexible way. The Marketplace is implemented on top of Ethereum blockchain, and it allows operation without a single entity owning or managing it, which in turn increases competition and enhances its security, resiliency, transparency, and traceability.

The Marketplace component is used by Decentralised Energy Flexibility Marketplace and Context-Aware Mobile Gaming pilots and SMAUG.

Provisioning and Discovery

The goal of the provisioning and discovery component is to enable the discovery of new IoT resources and their related metadata. Using this functionality, it is possible to decentralise the process of making new resources available to systems utilising the SOFIE framework and to automate the negotiations for the terms of use and the compensation for the use of these resources.

The Provisioning and Discovery component is used by the Context-Aware Mobile Gaming pilots and SMAUG.

SOFIE Federation Adapters

The SOFIE federation adapters are used to interface IoT systems with the SOFIE Architecture, which allows the IoT systems to interact with SOFIE while requiring no changes to the IoT systems themselves.

The SOFIE pilots have implemented 5 federation adapters: one adapter for Decentralised Energy Flexibility Marketplace (DEFM) and one for Decentralised Energy Data Exchange (DEDE) pilot, and 3 federation adapters for the Food Supply Chain (FSC) pilot, where they are used to adapt 3 pre-existing IoT platforms, SynField of Synelixis, Aberon of Optimum, and Transportation Federation Adapter. The Context-Aware Mobile Gaming pilot and the SMAUG reference application do not include any adapters as they are new applications designed and implemented based on SOFIE, without the need to adapt to pre-existing platforms.

Secure Marketplace for Access to Ubiquitous Goods - SMAUG

“Secure Marketplace for Access to Ubiquitous Goods” (SMAUG) has been developed as a practical realization of the SOFIE architecture and framework. SMAUG is released as open source, as a reference implementation for the SOFIE framework components. As the name suggests, the reference implementation realizes a secure and decentralised marketplace, specifically for renting access to smart lockers for short periods. SMAUG natively integrates all SOFIE framework components.

System dynamics models of business platforms federations

System dynamics models exploit causal loop diagrams, which can lead to analytic and simulation models explaining long-term platform behaviour and outcomes. Real-world data can be fed as inputs to the models, but also what-if parameters and sensitivity analysis can be performed to study various scenarios. These models can be used to study (IoT) data markets, and business platforms in general, focusing on their economic sustainability and evolution and their sensitivity to various endogenous and exogenous parameters and strategic alternatives.

3.2 Academic exploitation

This sub-chapter reports on the project’s academic partners’ exploitation in M26-36, relying heavily on deliverable D6.9 where the exploitation roadmap of each partner is explored in detail.

3.2.1 Aalto University

Main exploitation assets: Interledger, the Identity, Authentication and Authorisation (IAA), Privacy and Data Sovereignty, system dynamic models of business platform network effects, Marketplace.

The exploitation activities in M26-36: "Microservice architectures and serverless computing" course was held in Spring 2020. Aalto also supervised also a second SOFIE-related master's thesis. SOFIE results were utilised by H2020 PHOENIX, H2020 IoT-NGIN, and EMPIR SmartCom projects. Aalto also published several scientific publications and held several presentations.

Future work and impact: SOFIE results will be utilized also in the future in several EU- and national-level research projects, including H2020 PHOENIX, H2020 IoT-NGIN, and EMPIR SmartCom. Aalto will continue to offer master thesis topics, guest lectures, seminars, and/or special courses related to the results of the SOFIE project.

3.2.2 Athens University of Economics and Business

Main exploitation assets: The SOFIE framework components: Interledger, Identity, Authentication and Authorisation (IAA), Privacy and Data Sovereignty (PDS), Marketplace and the System Dynamics models of business platforms, but also the whole SOFIE concept and approach, including evaluation methodologies and results.

The exploitation activities in M26-36: Two new related research projects have been started: "Self-Certifying Names for Named Data Networking" from the 1st Open Call of H2020 NGIatlantic.eu, proposing to use DIDs as (network layer) names for the Named Data Networking internet architecture with exciting security properties and decentralisation capabilities) and "Eclipse-Resistant Network Overlays for Fast Data Dissemination," considering the Cardano blockchain with funding from IOHK/Cardano, being led by Prof. Spyros Voulgaris with extensive experience in P2P systems and overlay networks, as well as broad distributed systems expertise.

The "Blockchains and Smart Contracts" graduate course, is being taught again, this time in the Fall of 2020, by Prof. Voulgaris. Again, generating high interest, since all but one MSc CS students,14 of 15, elected to take the course.

Finally, an additional SOFIE related MSc thesis has been completed with title "Internet of Things Gateway Access Control." The approach is based on OAuth 2.0 and JSON Web Tokens, exploits the SOFIE IAA component software, and provides security and user role management for the open Home Automation Bus (openHAB), one of the most widely used open software platforms for home automation and to control the operation of smart Things.

Future plans and impact: SOFIE know-how and results will be utilized also in future research projects for which proposals have or will be submitted by AUEB. Also, AUEB will continue to offer PhD and master thesis topics, seminars, and courses related or based on the results of the SOFIE project, expecting to attract top notch talent. AUEB's expertise in SSIs, DIDs, VCs, interledger technologies, and smart contracts, accumulated mostly because of the SOFIE project, has invigorated the group and expanded its visibility within AUEB, nationally, and internationally. With respect to the IAA and PDS components, the group has plans to support and expand them beyond the end of SOFIE and to promote them for adoption as open source solutions in various practical settings. For example, AUEB considers contributing the IAA component and an extended version of the software from the above mentioned IoT Gateway Access Control thesis to the openHAB open source repository.

3.3 Commercial exploitation

3.3.1 ASM Terni SPA

Main exploitation assets: Interledger, Marketplace.

The exploitation activities in M26-36: To enable the most extensive use of the project outputs ASM Terni exploited the SOFIE's results participating to conferences, workshops, using them in further research and innovation activities, during M26-36. Moreover, ASM Terni contributed to the stakeholder consultation.

Key results:

- Interview to an IT company and a e-mobility provider.
- Publication of a scientific paper.
- Presentations of project results in scientific conferences and workshops.
- Exploitation of SOFIE results in H2020 IoT-NGIN.

Future work and impact

Apart from the aforementioned KERs, ASM Terni has reached additional results which will be internally exploited, as follows:

1. Enhanced understanding in cutting-edge smart grid solutions: The work carried out over the project had provided ASM Terni with new knowledge in terms of technical and strategic approaches. Moreover, thanks to the SOFIE's solutions new integrated functionalities will be taken in consideration for a future exploitation
2. Multinational and multidisciplinary collaboration: A significant outcome arising from working on SOFIE consists of strengthening multinational and multidisciplinary collaboration with public and private European Entities working on developing, deploying and evaluating advanced tools and ICT services for DSO and electric cooperatives, enabling active consumers' involvement. Networking activities carried out over the project lifetime have allowed ASM to go forward in terms of innovation (new businesses, advanced solutions and services, etc.), evaluating new visions and strategies suitable for DSO activities.

To sum up, ASM Terni is aware of the impact the federation concept and the specific outcomes achieved in SOFIE are going to create on the power distribution network; new grid operations and intelligent reliable techniques, like SOFIE's interledger protocols or the local energy flexibility marketplace with its consumer-centric vision, are actually vital to reach a sustainable and effective Smart Grid in a Smart City. All that considered, after the SOFIE's experience ASM Terni is ready to face innovations in the Smart Grid, exploiting SOFIE's outcomes in other EU or National projects with the aim of reaching a large-scale application in real environment.

3.3.2 Emotion SRL

Main exploitation assets: Interledger, Semantic representation, Marketplace, SOFIE Federation adapters.

The exploitation activities in M26-36: The aim in 2020 was to present to stakeholders the full capability and value proposition of Decentralised Energy Flexibility Marketplace solution together with SOFIE general concept.

Key results:

- Finalizing the demonstration of the Decentralised Energy Flexibility Marketplace solution.
- Conducting the 3rd SOFIE workshop.

Future work and impact: The SOFIE project has allowed Emotion Srl to investigate and test an innovative Demand Response mechanism which we believe will be very useful in the near future when we have more electric vehicles and renewable generation plants deployed. As shown in the paper "Flexibility - enabling technologies using electric vehicles" submitted by ASM, EMOT and ENG, published in 2020 IEEE International Conference on Environment and Electrical Engineering and 2020 IEEE Industrial and Commercial Power Systems Europe (EEEIC / I&CPS Europe) on 6 August 2020, electric mobility represents a solution for balancing high-penetration power grids of intermittent distributed renewable generation plants, thus avoiding huge investments to upgrade power lines and energy storage facilities. This solution has a double benefit: on the one hand renewable energy is integrated with greater efficiency by reducing generation from fossil sources, on the other hand electric mobility is powered by clean energy, thus obtaining a substantial reduction in CO_2 emissions in the atmosphere. This result will be exploited and improved in the new wave of research projects in which Emotion is a part, such as the BRIGHT project (GA n. 957816). Moreover, Emotion Srl will follow up legislation that is in the progress to update with technology and make exploitable in real life aforementioned virtuous mechanism. In the meantime, Emotion Srl will refine its services and products with the aim of making the most of what has been learned and developed over the course of SOFIE project, both from technical and social point of view.

3.3.3 Engineering Ingegneria Informatica SPA

Main exploitation assets: Interledger, Semantic Representation, Marketplace, Federation Adapters.

The exploitation activities in M26-36: During this reporting period the exploitation activities were focused on the deployment, validation, and demonstration of the final version of the pilot platform and the release of the pilot's Federation Adapter (FA) as part of the SOFIE software release. Preliminary market analysis and financial analysis were included in D6.10. The plan for 2020 was to exploit SOFIE outcomes via Engineering’s BU, including it to the business offer to the clients. Engineering continued to participate in workshops and conferences to present the pilot’s results and released the pilot’s Federation Adapter as part of the SOFIE software release.

Key results:

- DEFM FA release.
- DEFM pilot presentation to workshops and conferences.
- Contribution to the publication of a scientific paper.
- Market and Financial Analysis.

Future work and impact:

In the future Engineering plans to:

1. Carry on with the company innovation process in term of technical support to the internal Business Units for the knowledge transfer.
2. Engage new potential adopters, mainly DSOs, EV fleet managers, EV users, and energy retailers, interested to test the applicability of the DEFM platform for their operations.
3. Investigate potential applicability of decentralised marketplaces in different domains or in different segments within the energy domain.
4. Further dissemination of SOFIE outcomes to potential stakeholders in the energy domain and exploitation the results within other EU H2020 research and innovation projects where Engineering is currently participating, e.g. the BRIGHT project, or will participate in the future.

3.3.4 Guardtime OÜ

Main exploitation assets: Interledger, Authentication and Authorisation (IAA), SOFIE Federation adapters, KSI blockchain.

The exploitation activities in M26-36: During 2020 GT aimed to present to stakeholders the full capability and value proposition of Decentralised Energy Data (DEDE) solution together with SOFIE general concept. The questions/answers that were driving the discussion with stakeholders were: what DEDE offers, what is DEDE's added value, and what could be the next business opportunities. The 3rd SOFIE workshop enabled Guardtime to conduct one to one interview and to get answers to these questions.

The exploitation activities were also focused on presenting the full DEDE solution, that was developed to larger audience, keeping in mind the key countries that were selected during phase 2.

Key results:

- Finalizing the demonstration of the DEDE solution.
- Selection of three potential end-users to be part of post SOFIE project activities.
- Conducting the 3rd SOFIE workshop.

Future work and impact:

Future work of Guardtime related to DEDE adapters exploitation is mainly focusing in signing 2-3 Proof of Concepts. This means that we will continue to expand the list who could sign the PoC as well as make proposals to existing stakeholders. We plan to conduct the following activities:

1. Negotiations with Elektrilevi have a PoC and with the Polskie Sieci Elektroenergetyczne (PSE) for the Smart grid data access governance and control. Proposal for PoC.
2. Negotiations with Service providers of Enoco to have a PoC and Spotty energy and PSE to grant access to National level smart meter data hubs (Estonia, Finland and Poland as examples. Proposal for PoC.
3. Integration of SOFIE DEDE adapter in EU-SysFlex project data exchange demonstrations. Follow up to have a demonstration beyond project.
4. Activates towards including more stakeholders to the potential PoC demonstration list. Main focus will be on TSOs and DSOs Fingrid (Finland), Tennet (Netherlands) 50hertz (Germany) in order to reach an agreement to propose a customer specific PoC and the financing mechanism on this.
5. Preparation to bid in national level energy network upgrade procurement. Cooperation with existing system integrator and smart grid providers will be using DEDE adapters to solve part of the procurement requirements.

We believe that the impact SOFIE DEDE adapters will bring is related to Energy market services relying on seamless data feed from smart meters. The current governance and control mechanisms are not delivering the required functionality to the changing energy market. Simply put, when company starts new flexibility service in multiple countries, the bottleneck is accessing the smart grid data fast and in a secure way. The SOFIE DEDE is having strong traction with the Energy sector data exchange platform operators and in combination with these will solve this bottleneck for service providers.

3.3.5 LMF Ericsson

Main exploitation assets: Interledger, Offer Marketplace, Authentication and Authorisation (IAA), Semantic representation, Privacy and Data Sovereignty, Discovery & Provisioning

The exploitation activities in M26-36: In this reporting period, Ericsson developed the SMAUG reference implementation and started development of a pilot project related to 5G spectrum sharing which builds further on SMAUG.

Key results:

- Demonstration of the use of the SOFIE academic assets in a decentralised marketplace realization (SMAUG). This project was successfully completed, results released as open source and SMAUG accepted as a proof of concept in the ETSI ISG PDL-005 specification.
- Development of 5G Spectrum Sharing pilot that leverages further on the results from SOFIE and on the SMAUG reference implementation. The 5G Spectrum Sharing pilot was demonstrated internally. Preparations were started to create a proposal for ETSI ISG PDL to include this pilot as an additional proof of concept in the PDL-005 specification.

Future work and impact:

The following actions are planned in relation to SOFIE:

1. Prepare a proposal to include 5G Spectrum Sharing Proof of Concept in the ETSI ISG PDL-005 specification.
2. Capture SOFIE architecture, especially the open federation and interledger aspects therein, in Ericsson’s blockchain strategy
3. Continued evaluation of possible use cases that are ready for pre-commercial pilots of commercial adoption, where the problem statement includes interledger and federation aspects. Mainly these use cases are in the 5G, IoT and Security areas.

3.3.6 Optimum Anonimi Etairia Technologies Pliroforikis

Main exploitation assets: Interledger, Authentication and Authorisation (IAA), Semantic representation, SOFIE Federation adapters.

The exploitation activities in M26-36: Optimum finalized our Aberon platform according to the feedback received from several stakeholders and had several discussions within our customer network for potential collaboration. An important achievement during this phase was that we had the chance to have discussions with people from companies that are already using our platform and could potentially adopt our SOFIE-enhanced platform in a trial. We have already engaged these companies in having interviews in the context of the third SOFIE workshop and we plan to follow-up on these discussions with further collaboration after the end of the project.

Key results:

- Engagement of existing customers to consider the adoption of our SOFIE-enhanced platform for a trial.
- Finalization of the Aberon platform with a full set of SOFIE-related features.
- Compilation of a business proposal for our customers that will include the pilot’s outcomes.

Future work and impact:

The following actions are planned in relation to SOFIE:

4. Triggering discussions with a number of existing business partners for the possibility of adopting of the pilot platform. Discussions concern existing business partners in the fields of Food Retail and Electronics Retail.
5. Further improving services of Aberon tailored to the warehouse management by using blockchain technology. Investigating the possibility to embed some of the pilot platform’s

functionalities in the commercially offered product (e.g., the Federation Adapter to make the product SOFIE-compliant).

6. Further business evaluation of the implemented business platform to identify potential exploitation opportunities in the logistic area, also in other verticals.

With the above, it is believed that interest of existing customers can be retained at high levels while also additional profit by providing extra services (via the SOFIE-related functionalities) can be achieved.

3.3.7 Rovio Entertainment Corporation

Main exploitation assets: Interledger, Marketplace, Semantic representation, Provisioning and Discovery.

The exploitation activities in M26-36: Rovio's main focus during this period was on demonstrating the final version of the pilot platform highlighting the full set of features that it offers. We had the chance to conduct interviews with gaming industry experts, where we discussed the benefits of technologies used in gaming pilot and SOFIE platform in the gaming industry.

Key results:

- Demonstrating the final version of the gaming pilot.
- Conducting interviews for the 3rd SOFIE workshop.
- Presentation of the pilot in conferences and publish research papers.
- Business opportunities for using the SOFIE framework for mobile.
- Open sourcing the mobile gaming pilot.

Future work and impact:

1. Research paper to be submitted: Decentralised Identifies for mobile advertisements.
2. One PhD student will be completing a doctoral degree in 2021 that would be based on the research performed during the project timeline.
3. Business requirement assessments for the gaming pilot implemented during the SOFIE project will be used by Rovio internally for future decision making and it will also be included in the doctoral thesis.
4. The codes and documentation that has been written throughout the project timeline will be open sourced, and the proof-of-concept can be template for future researchers who wish to further investigate IoT and blockchain technologies in the context of gaming.

3.3.8 Synelixis Solutions SA

Main exploitation assets: Interledger, Authentication and Authorisation (IAA), Semantic representation, SOFIE Federation adapters.

The exploitation activities in M26-36: During the last year of the project, the main focus was on demonstrating the final version of the pilot platform, highlighting the full set of features that it offers. On top of that, the fine-tuned business proposition was in place, aiming to attract potential adopters and customers. During the 3rd SOFIE workshop, we have the chance to conduct interviews with people from companies that are considered key players in the regional food supply chain. Another aim of this phase was to identify and make contact with companies in order to form a first -basic- ecosystem after the end of the project that will draw more attention -and customers- to our platform.

Key results:

- Demonstrating the final version of the pilot platform on-site.
- Contacted new candidate adopters of the pilot platform.
- Conducting the 3rd SOFIE workshop.

Future work and impact: Future exploitation will result through main research, development, and dissemination activities of SOFIE, and especially Food Supply Chain outcomes, where Synelixis is actively involved and interested. In this scope, the following priorities are planned for the next period:

1. Evaluation of users' feedback and make any necessary adjustments to a business proposal that will include the pilot platform and SOFIE components
2. Trigger further discussions with 7GRAPES Pegasus about the possibility of adopting the pilot platform for a testing period under regular daily operations.
3. Engage new candidate adopters that have been identified (e.g., Agrinio Union, Cooperative Winery of Nemea). These candidates have already expressed their interest in Synelixis SynField platform; hence, it is planned to enhance this offering with a testing period of the pilot platform from SOFIE.
4. Investigating potential companies from the different segments of the Food Supply Chain and how to make on-boarding to the pilot platform attractive to them. The aim is to find a few (not directly competitive, i.e., from different regions) companies (from the farming sector, the logistics sector, and the retail sector) to get on-boarded and therefore form a first -basic- ecosystem.
5. Further dissemination of SOFIE outcomes to potential stakeholders in the agricultural domain and exploitation of SOFIE solutions within other EU H2020 research and development projects where SYN participates, e.g., PHOENIX.

What has been made evident from the above is that there is a clear opportunity for Synelixis to approach and make new customers (the Agrinio Union case where a deployment has already been made is an indicative example) by offering existing products (e.g., Synfield) and/or SOFIE-enhanced products. In addition, SOFIE has created opportunities in participation in other H2020 research projects.

4. Business models for pilots

The aim of SOFIE is to launch the technological capabilities and investigate in which business verticals these could create new business opportunities. The basic setup for value creation and making profit has been set by the four SOFIE pilots. They represent the examples, how we plan to implement SOFIE results in specific business verticals. Energy, food supply chain and context-aware gaming sector related prototypes demonstrate the added value to business and deliver minimal viable product that could be used to develop and offer a specific market ready product or service.

The tool that we use for each pilot to keep track on business activities and consolidate most important information together is Business Model Canvas (BMC). In this section there is an overview of the BMC development in the M26-M36 and the final stage of each pilots BMC. The previous versions of BMC's were discussed in D6.8. In the SOFIE project deliverable D6.10 Business planning, we offer a more comprehensive overview and use of BMCs and business activities.

4.1 Decentralised Energy Data Exchange (DEDE) pilot (Guardtime)

BMC developments during M26-36:

The main change of the BMC for the DEDE pilot in the final phase of SOFIE has been focusing only on Tier1 (see indication in canvas), as they need to be onboard for further business models that are related to energy flexibility services. The following BMC is the final version for DEDE pilot that will be applied to also carry out beyond project activities.

Decentralised Energy Data Exchange (DEDE) Pilot's Business Model Canvas:

The Problem

For the Datahub operators, the risk to grant access to data owner and service providers is too high. These risks are handed over to service providers to comply and creates unexpectedly high cost to access the data. This applies especially in the case where there is National Datahub approach. The **cost reduction is key busines problem** for Central datahub in order to survive in free and open energy market. For decentralised and regional data access the key problem to be solved is **prevent the duplication** of solutions that connect different parties that are involved in energy data sharing.

The Energy Data Exchange Pilot

We offer to the DSO/TSO the smart meter data access platform that enables the data gatekeeper service. We provide governance and control mechanism four your energy data. The DEDE adapters will be an effective bridge between service providers system (Tier2 stakeholders) and data access platform operators fulfilling part of the requirements that come from GDPR, Green energy deal and open data access regulations side.

The pilot and the following exploitation activities are directed towards smart meter data operators (TSOs/DSOs). We will create a novel digital infrastructure available that will allow the targeted TSO-s/DSOs to grant access to data, track the process of who gives/receives data through their platform and creates immutable evidence for auditing and security purposes. The pilot is taking advantage of the recent cutting-edge breakthroughs in blockchain technologies, which enable to increase trust among companies and transparency in data management.

The Pilot Objective

The Energy Data Exchange Pilot will deliver:

- Means to manage DSO/TSO datahub access to data with the data owners' consent and GDPR compliant evidence/audit trail;
- SOFIE adapters placement in data input and on each participant side;
- Secure authentication and control in a mobile device for each data owner;
- Visual overview of access/revocation and "whitelist" between parties involved in data access
- GDPR compliant data access to pilot specific test sites.

The Exploitation Strategy

We plan to execute a two-tiered exploitation strategy:

- **Tier 1** - we approach the DSO/TSO's operating the access control of energy consumption data. We provide them with the digital infrastructure based on SOFIE adapters on an annual license fee. The solution adds value to the existing and running platforms, so DSO/TSO can make a shortcut into sharing data and skip the planning/development phase on their existing platform.
- **Tier 2** - we aim to get service providers to start using the SOFIE solution to be able to get data and sell flexibility services. **This tier will be postponed until we have successfully integrated with 4-6 DSO datahubs to make data available.**

Key markets to be targeted – The goal is to approach Austria, Switzerland, Netherlands, Poland and Finland as main markets.
Potential customer segment - smart meter datahub managers, the industry responsible for energy data consumption/production distribution, energy flexibility service providers.
Strategic exploitation stakeholders - energy sector regulators, GDPR related data protection agencies.

Benefits for targeted end-users

- Reduction of integration costs for governance mechanism for data access and controlling the risks involved to data sharing.
- Traceability of products and ensuring the integrity of critical data without the need for centralized authority.
- Reducing the chances of fraud and data manipulation, cutting out corresponding mediation expenses and transaction costs.
- Immutable blockchain-backed energy consumption readings which are correct beyond dispute.

Enabling technologies

- Guardtime's KSI Blockchain® API provides technology for massive scale integrity verification and immutable audit trail generation.
- Hyperledger Indy-based decentralised identifiers provide a mechanism to link the data owners and service providers together (automated matchmaking functionality) and create a novel trusted way to authorize the access of data between the parties.
- SOFIE adapters to collect energy consumption data.
- The solution deployed in an operational environment (TRL-7).

SOFIE DEDE pilot is having strong traction with the energy sector data exchange platform operators. The data access control solutions currently in use are not delivering the required functionality and upgrading these is main goal of our adapters. The addressable market is growing, and the regulatory aspects are getting in the stage that country level grid operators have to comply with them in coming 2-3 years.

4.2 Decentralised Energy Flexibility Marketplace (DEFM) pilot (Engineering)

BMC developments during M26-36:

To draw the previous version of the BMC (presented on D6.8), some considerations about the key markets, potential customers, and stakeholders were made considering a potential overlap with the DEDE pilot. In the current version, those considerations were slightly refined, making the overall BMC more adherent with the DEFM pilot specifications.

Decentralised Energy Flexibility Marketplace Pilot's Business Model Canvas

The Problem

Following the advent of distributed electricity generation, the electric grid underwent an impressive change in power flows. The grid was designed with an assumption that energy had a unidirectional power flow, but today we have many renewable generation sources (solar and wind), distributed in the network and, sometimes the energy produced is higher than the energy consumed by the end users present in the same local network. The reversed power flow causes stability and safety problems in the electricity grid, which the DSO (medium/low voltage grid owner) has to solve to guarantee the continuity of the energy service. To understand the complexity of this phenomenon, we must consider that it is generated mainly by intermittent and non-programmable generation plants, strongly influenced by atmospheric conditions, making it very difficult to predict its progression.

The Energy Flexibility Marketplace Pilot

Thanks to the network equipped with devices that allow remote monitoring and management in real time, is possible to obtain useful information to receive accurate forecasts and avoid the emerging of reverse power flow. Thanks to the SOFIE project, we want to use blockchain technology and smart contracts to enable a secure and transparent mechanism to time-shift the end users' consumption according to the needs of the network (Demand-Response) involving the DSO, which needs energy flexibility, the EV Fleet Managers, which provides energy flexibility by directing the electric vehicles in the areas of interest to charge and, finally, the Energy Retailers, which manages electricity trading.

The Pilot Objective

The goal is to build a new decentralised, fair, transparent and secure marketplace, powered by the blockchain in which market operators can be sure that the best offers will be selected without any kind of bias, and, by interfacing directly with the smart meters on the grid, the payments can be settled in near real time without the need for longer verification times. In this way, electric mobility can act as a catalyst to improve the usage of renewable energy sources, acting not only as an "on-demand" energy storage but also as a novel "on-the-move" storage solution able to operate in a specific area and at a specific time contributing to the balancing of the entire network.

The Exploitation Strategy

Different paths will be followed for the exploitation strategy. As for the DSO point of view, flexibility can be used for obtaining technical data. As for the Fleet Manager point of view, SOFIE outcomes could be exploited to improve electric mobility services, achieving money savings and reduced environmental impact: the use of energy produced from renewable sources for electric mobility entails a double benefit, on the one hand harmful emissions are removed from the places where vehicles circulate, making the streets healthier, on the other hand, avoiding to produce such energy from fossil fuel power plants, dangerous emissions that contribute to sickening our planet are not released. We aim to get service providers to start using SOFIE platform to be able to get data and sell flexibility services. Also providing evidence to DSO/TSO as well as regulators and other supervisory boards in the energy network is delivered to the service providers. The business model with service providers is sharing a revenue stream based on the new customer base that they get by new data access through the digital infrastructure.

Key markets to be targeted - the key market segment is coincided with the storage and flexibility market instruments for grid operators.

Potential customer segment – Distribution System Operators, EV Fleet Managers, EV users, Energy Prosumers.

Strategic exploitation stakeholders – Local communities, stakeholders in the energy production/distribution/consumption pipeline.

Benefits for targeted end-users	**Enabling technologies**
• Use real time and historical data to forecast the occurrence of reverse power flow • Create flexibility requests on the marketplace to balance the local energy supply • Help to charge the batteries of its fleet of electric vehicles at advantageous price. • The incentive provided by the DSO can cover part of the electrical supply • Thanks to the marketplace, the most convenient energy retailer can be selected any time a charge is needed • Provides a rapid user-friendly mechanism to negotiate micro-contracts • Grants security, transparency and auditability of the operations. • Enable the interoperability among different siloed IoT systems.	• SOFIE decentralised blockchain-based marketplace • SOFIE adapters to collect data from DSO’s smart meters and fleet managers’ EVs and EVSEs
Market Trends	**Pilot Outputs**
• There is an industry-wide agreement to make the energy consumption as well as production data available and more usable. This has been also agreed in the Clean energy package. There is an organic demand and expanding the market need for technical solutions which make this industry disruptive trend possible. • Increase of distributed generation from renewable sources (solar and wind)	• The solution designed and validated with key stakeholders. • The solution deployed in an operational environment (TRL-7). • The solution replicable and scalable in any microgrid.

SOFIE DEFM pilot validation has demonstrated the viability of the solution, and the search by network operators for market solutions putting value on storage and flexibility has intensified. The current trend in RES and EV penetration is forcing traditional operators to adapt their infrastructure: flexibility can reduce capital expenditures of DSO by shaving peaks of PV and EVSE, increasing hosting capacity without higher costs on infrastructure.

4.3 Food Supply Chain (FSC) pilot (Synelixis)

BMC developments during M26-36:

During the final year of the project, the interaction of the technical partners with the end users, and the feedback from them following the on-site deployment, confirmed that the following two types of services are of significant importance for targeted end-users and stakeholders; end-to-end product traceability and audit to verify integrity of the enforced business rules. Our BMC has remained the same as it was presented in D6.8.

Food Supply Chain pilot's Business Model Canvas

The Problem

Producers, distributors, logistics and retailers want to get their products to the market quickly, safely, and in the best possible condition. They also share a common trust issue among each other in the sense that there might be multiple participants in a supply chain and not every participant is aware of all other participants. Consumers want to buy high-quality products and know how these were produced, where they came from and what is their ingredients. They also have increased expectations about the environmental sustainability or health-related issues in the production cycle, not rarely preferring brands which promote the same social and environmental values as their own.

The Food Supply Chain Pilot

The food supply chain (FSC) pilot considers the field-to-fork grapes supply chain system covering the farming, storage, distribution (logistics), and retail subdomains, and serves as a proof-of-concept for the validation and demonstration of the capabilities of the SOFIE platform to combine and interconnect, in a secure way, different IoT platforms that are involved in the food supply chain sector.

The pilot demonstrates a provenance chain Business Platform (BP) to ensure wide visibility of supply chain information, traceability of assets, and secure data exchange among heterogeneous, federated IoT environments, without forcing additional changes to their infrastructures, equipment and security policies. The pilot leverages a hierarchical topology of DLTs to improve transparency and traceability of assets and build a robust and secure data management framework that verifies integrity of exchanged data and ensures identity and authenticity control of involved entities.

The Pilot Objective

The objective is to demonstrate a provenance chain BP that secures information sharing and value exchange between organizations which participate in the food supply chain without the need of a third-party intermediary to establish trust, coordinate interaction and supervise products flow over the chain. The BP will provide end-to-end product traceability services to all involved companies as well as food consumers.

The Exploitation Strategy

FSC traceability services could be released as a mixed Platform as a Service (PaaS) and Software as a Service (SaaS) model. This model will maximize the scalability and flexibility of the platform allowing customers to access more or fewer services or features on-demand. Different releases of the platform and provided services could be possible:

- Open platform access with limited functionality and service provision on top of a basic schema to adapt existing IoT services and systems.
- Full platform access and customizable services with provision of federation adapters for existing IoT systems.

The commercial usage of the pilot platform and its services could combine a double revenue model: On the one hand, the companies which participate in the supply chain could pay a periodical fee (subscription model) to get federation adapters for their IoT platforms and share data through the SOFIE FSC platform. This is applicable to all identified chain segments (e.g. producers, logistics, etc.), under the appropriate adaptations tailored to the specific interests and activities per domain. On the other hand, retailers and/or customers which want secure traceability information and food safety assurance could directly pay a small amount per SOFIE-traceable product purchase.

Potential customer segments - suppliers in agri-food domain, logistics and transportation companies.

Strategic exploitation stakeholders - retailers, supermarkets, consumers associations.

Potential customers: Vivartia group, 7Grapes coop, Sklavenitis group

Benefits for targeted end-users and stakeholders

For suppliers:

- secure information sharing without the need of a centralized authority to supervise and control data exchange,
- easy to use and non-disruptive solution to federate local IoT business environments,
- verify goods ownership and authenticity, as well as on-time and in-full transactions and deliveries,
- cut out mediation expenses, reduce transaction costs and improve quality management of products distribution
- enhance trust between participants of the supply chain and allow rapid replacement of participants

For retailers:

- increase visibility in goods transfer from the field to the market shelf,
- improve efficiency in audits and disputes resolution when quality conditions are not met,
- enable immediate identification and recall of potential contaminated goods in cases where product quality and/or safety events are detected

Enabling technologies

- DLT-based identity authentication and role-based control management.
- SOFIE adapters to enable a common interface specification upon federation of heterogeneous IoT systems.
- SOFIE interledger protocol to bridge different DLTs.

For food consumers: • increase consumers' visibility about goods production, transportation and processing practices over the whole food supply chain.	
Market Trends • Immutable, real-time keeping of transactions among supply chain companies improves product and inventory mgmt., minimizes errors in their communication and increases trust among them. • Companies want to protect their brands and product labels against negative publicity, potential frauds and counterfeits as well as to highlight their sustainable supply chain and market practices. • Customers and customer associations push for extended visibility and traceability of products' history to ensure high standards for their quality and safety.	**Pilot outputs** • A validated platform with key stakeholders that offers two main services: i) secure product traceability for final customers, and ii) audit process allowing supply chain companies to detect product quality issues. • The solution deployed in an operational environment (TRL-7).

Food Supply Chain pilot resulted in a potential product which can be further explored for potential commercial exploitation. Given the EU Farm-To-Fork strategy, participants in this pilot are motivated to further pursue this potential. The on-site deployment on the premises of one of the potential customers for this platform highlights the ambition of the participants to continue with such activities in the future, demonstrating the functionality and benefits of the SOFIE-powered platform in various players along the Food Supply Chain.

4.4 Context-Aware Mobile Gaming pilot (Rovio)

BMC developments during M26-36:

Compared to the previous version of the canvas in D6.8, the following changes have been made for the current version:

- discussed customers in the "Pilot Outputs" part of the BMC,
- benefits of BLE positioning accuracy indoors compared with GPS specifically,
- stating the potential benefit and demand of the sense of true ownership brought with DLTs.

Context-Aware Mobile Gaming Pilot's Business Model Canvas

The Problem

If positioning players is done through ubiquitous IoT devices, new location-based mobile games require access to infrastructure in order to be attractive and to offer new ubiquitous gaming experiences. There is a high cost associated with investing into new sensors, thus making it more reasonable to use existing devices and sensors while developing new location-based games. In this process, involving the stakeholders of IoT devices is challenging. There is a hurdle of how to motivate them to be a part of the game and get the fair share of the money coming in from the game and to cover the costs of integration and implementation.

From a technical perspective we are addressing the following two problems:

- Could the existing base of fixed-location IoT devices also be used for location-based mobile gaming?
- Could DLT bring benefits to players or other stakeholders in mobile gaming?

The Context-aware Mobile Gaming Pilot

We identify and test use cases of DLT and IoT in mobile gaming in an iterative fashion. We are not working on a commercial product but experimenting with new technologies.

The Pilot Objective

Through iterative prototypes, tests and calculations, we evaluate the technical fit, performance, gameplay experience, and business potential of the use cases that we identify. The objective of the pilot is to experiment and understand whether DLT and IoT can provide new kinds of compelling player experiences.

The Exploitation Strategy

We have a working architecture (hybrid game server & DLT combination), and we receive feedback and insight from dissemination activities. We are keen on discovering whether these technologies do not stand in the way of sustaining a game with more than one million daily active users and the means of generating reasonable revenue, while bringing compelling benefits to consumers and/or other stakeholders.

Benefits for targeted end-users and stakeholders

- By using ephemeral identifiers, beacons can be harder to spoof than GPS.

Enabling technologies

- In the prototype we're using Hyperledger Fabric for a permissioned blockchain, but we are not locking into it.
- Bluetooth low-energy beacons.

Player locations can be verified, reducing the number of cheaters in competitive games.

- Indoor positions, especially altitude information, can be more accurate when compared to GPS.
- Hypothesis: DLTs can bring transparency, automation and virtual item cross-game interoperability to companies participating in an ecosystem for location-based (and other) games.
- Hypothesis: DLTs can bring a sense of true ownership of virtual items to players.

Market Trends

- The global number of IoT devices is increasing - can location-based games utilize them?
- A potential demand for "true ownership" of virtual items

Pilot outputs

- Results from testing the technical fit and performance of DLT and IoT technologies in mobile gaming (academic paper). Learning which benefits of DLT outweigh the technology's shortcomings and identifying whether such benefits cannot be achieved on a traditional game server and a database.
- An open sourced scavenger hunt game prototype (TRL-6): an example of a real location-based game that uses beacons for positioning and a server-DLT hybrid architecture, bundled with the Blockmoji virtual item management application
- In the imagined business environment described in this canvas the end users (the players) as well as points of interest (who would use a location-based game as a business platform) can be seen as customers. In practice, the global DLT & IoT research and development communities can be seen as customers of this pilot, who would be able to use the open-sourced prototypes as a base for their projects for free.

Through iterative prototypes, tests and calculations, Rovio evaluated the technical fit, performance, gameplay experience, and business potential of the use cases that they identify. The pilot yields three main prototypes – Scavenger Hunt, Blockmoji and Decent ID, out of which Rovio open-sourced the first and plans to open source the second as well for the wider research and development community so that our work may be used as a basis for future research.

As already stated above, Rovio does not currently plan to pursue the pilot beyond the SOFIE project. The reasons for not pursuing the gaming pilot further are the following:

- Gaming systems are so closed and don't support openness like other platforms, so there is little or no value of using SOFIE services. If in future the gaming systems are more open and interact with other systems like IoT then there might be some added value of SOFIE.
- An increase in the cost of running services without any majors benefit for mobile gaming.
- Blockchain games suffer from having a simple play mechanism and a short life-cycle.
- At this point DLT and IoT technologies that was used in the pilot do not provide a gaming experience that is able to be unique or differential and able to scale to tens of millions of player globally with potential to build a substantial revenue (in excess of EUR 50 million)

However, preparations are currently ongoing to potentially release also Blockmoji prototype to the wider developer community. The prototype may serve as foundations for new use cases of DLT and IoT in gaming that future developers and designers may devise.

5. Community outreach

The SOFIE consortium has used both personal and interpersonal tools to communicate SOFIE results to general audience as well as to more SOFIE related community segments (e.g. IoT community, people working with topics like energy data liberation and energy flexibility, traceability of food supply chain, blockchain opportunities in mobile gaming etc). For example, we have written 30+ blog posts that are suitable for a general reader with interest in the field of IoT and released a quarterly newsletter for our 70+ subscribers. Below we describe liaisons, standardization and open sourcing effort in more detail, to showcase our out-reach to the community.

Liaisons

In 2020 SOFIE has been participating in the work related to BRIDGE initiative (https://www.h2020-bridge.eu/). SOFIE participated in BRIDGE General Assembly in February 2020. The result of this activity is aligning the SOFIE messages towards the industry with the BRIDGE projects. In collaboration with Bridge initiative on Q1-Q2 2020 we have been focusing on cyber security of energy data access and SOFIE adapters alignment with various energy standards, initiatives.

There has also been close cooperation between SOFIE and Sysflex project (https://eu-sysflex.com/). Moreover, within the reporting period SOFIE has collaborated with SecureIot project, Cyberwatching.eu initiative, NGIoT project, and IoTCrawler project. With NGIoT SOFIE also produced two collaborative webinars in Summer 2020. SOFIE is promoting itself and its components both in cooperation with SecureIoT and Cyberwatching. Within the EC Security Cluster, SOFIE contributed to a book compilation and made a joint presentation at IoTForum's virtual event "Digital Around the World". Additionally, EU H2020 project PLANET (Progress towards Federated Logistics through the Integration of TEN-T into a Global Trade Network), which started in mid-2020 is planning to adopt Interledger component developed in SOFIE

Standardization

During the SOFIE project, we have seen an uptake of blockchain related standardization activities. The recent, increased focus towards ledger interoperability in standardization proves the relevance of the interledger research and realization that has taken place in the SOFIE project. During the reporting period we made the biggest efforts in ETSI Industry Special Group for Private Distributed Ledgers (ISG PDL) where we made significant contributions to the "ETSI PDL-004 Smart Contracts" draft, "ETSI PDL-005 Proof of Concepts Framework" draft and the "ETSI PDL-006 Interoperability" draft.

In addition to ETSI ISG PDL, SOFIE partners have also contributed to several other standards. The following table summarizes the achievements in this area. Activities by partners in standardization bodies in described in more detail in 6.9.

Table 3. SOFIE standardization activities

Activity	Responsible Partners	Area of contribution
W3C	AUEB, AALTO	Contributions in security and privacy to WoT IG and WG Participating to the Blockchain and Interledger CGs Invited presentation "Using Verifiable Credentials in IoT Services" (slides archived in W3C github repository)
IETF/IRTF	AUEB	Participation in a pre-standardization IRTF workshop on Decentralized Internet Infrastructure (DINRG, https://trac.ietf.org/trac/dinrg/wiki) with a presentation on

		SOFIE's ideas on a secure, open, decentralised IoT.
ETSI ISG PDL	LMF, AALTO, AUEB	PDL-004 Smart contracts, contributions by LMF based on research and deliverables developed in the SOFIE project PDL-005 Proof of Concepts Framework, significant contribution by LMF. SMAUG was accepted as a PoC for this draft. Plan to propose 5G Spectrum Leasing, which builds further on SMAUG, as a second PoC for this draft PDL-006 Interoperability, significant contributions by AALTO, AUEB and LMF based on research and deliverables developed in the SOFIE project

Code releases

Throughout the SOFIE project we have made five software releases, final three were made within the reporting period of this document.

1. The first code release was made in September 2018.
2. The second code release was made in October 2019.
3. The third code release was made in April 2020.
4. The fourth code release was made in September 2020.
5. The fifth and final code release was made in December 2020.

Between main releases, the code base was improved through continuous integration, deployment, and validation processes. The code is available under Apache License, Version 2.0. Everyone who is interested can use the open source software for their own developmental reasons.

6. Open data and intellectual property rights

SOFIE participates in the Open Research Data Pilot. As outlined in the updated deliverable D6.5 - Data Management Plan the open data from the SOFIE project will be deposited in an open access repository such as Zenodo (https://www.zenodo.org). The data that can compromise commercialization prospects or has inadequate protection of, e.g., personal information, which will not be published. When the data is related to a publication, it will be linked to it via OpenAIRE (https://www.openaire.eu).

The Intellectual Property Rights and future exploitation of results is treated according principles agreed in the Consortium Agreement. SOFIE open-source framework components has been released under the Apache License, Version 2.0. Licensing of pilot components is up to the pilots. Terms of licensing will be agreed between the owner of the IPR (e.g., pilot lead) and the potential user. This means that IPRs are owned by the consortium partners that generate them.

Since most of the results of the SOFIE project, such as the SOFIE federation framework, has been released under open-source license and described in scientific publications, other parties can easily utilize and exploit them.

7. Monitoring and evaluation

In order to assess the success of communication and dissemination activities, this chapter reflects on the KPI's that were set for the activities in D6.6 "Updated Consolidated Communication and Dissemination Plan" (Table 4) and that were already once discussed in D6.8 "Interim Report on Communication, Dissemination and Exploitation" (Table 5). The KPIs for communication activities are compared to the original goals presented in D6.6 to reflect on the final results and reflect upon achievements made during the last year of the project.

SOFIE made substantial efforts to promote the project and carry out the communication and dissemination of the project according to the plans we had set. Over the last year of the project, when COVID-19 hit, we had to replan several things in WP6 and take alternative routes to achieve our goals. This was the most difficult with activities related to face-to-face interaction. For example, we could not participate almost at any live exhibitions or events to promote SOFIE. Adjusting, we relied on virtual tools, and gave our maximum effort to reach the best possible outcome. Our greatest communication and dissemination effort was placed on producing high-level publications from academic side and industry outreach from the commercial side, as well as promoting those efforts through blog posts, news releases and public events. Ultimately, these activities were essential to support the exploitation of our assets.

The table below shows the final achievement of communication KPIs (monitored in December 2020) and the predicted final outcome we had planned in D6.6. The last column evaluates each KPI's final status and explains deviations in cases they occurred.

Table 4. SOFIE's KPIs for communication.

KPI	Achieved by December 2020	Target KPI	Evaluation
Publications in peer-reviewed journals and conferences	34	14	Excellent scientific work on IoT, DLTs, DIDs, VCs, OAuth 2.0, interledger, etc. has been published in journals, conference proceedings and books throughout the project with good pace.
Website visitors	8300+	12000	Fair final number of visitors of the website. The visitor number of the webpage kept constantly growing over the years. In D6.8 KPI evaluation chapter, we prognosed that there will be boost in visitor numbers during the last year, but the inflow of visitors remained steady.
Events attended representing the project	38 events 5 exhibitions	35 events 6 exhibitions	Very good effort in participating at various events targeted at different types of audiences. During the last year we mostly attended the events virtually but managed to still advance in our efforts to present and partake at a number of European and global events. We only missed our exhibiting final goal with a fraction due to COVID-19 restrictions.
Workshops of the project	3	3	Excellent result for the project. All the workshops we had promised to deliver were executed. First SOFIE workshop, Oct 2019.

			Second SOFIE workshop, Jun 2020. Third SOFIE workshop, Dec 2020.
Business events and communication (including communication with end users)	90	41	Excellent effort from industry partners' side to meet with end-users and relevant stakeholders throughout the three years of the project. Biggest proportion of the effort was carried by the pilot leads.
Blog posts	31	31	Very good and systematic progress and performance throughout the project by all partners producing the content of the blogs.
Followers on social media	360+	500	Fair final number of followers. We concentrated our efforts to organic followers. It was a steady rise with quality followers, although we were a little behind of the end goal by the end of the project.
Liaison and organization of cluster activities (meeting attendance and joint publications)	15	12	Very good cooperation with other initiatives as well with the cluster. We have had joint workshops, written pieces, meetings etc.
News items on website	19	17	Excellent number of news releases on SOFIE website. Notable effort was made especially during the last year of the project.
Mentions of SOFIE in other websites/news items	22	22	Very good result. This KPI includes news about the project, mentions on partners' websites, Cyberwatching.eu and SecureIoT profile, profiles on external event pages etc.

8. Conclusion

The SOFIE's communication, dissemination and exploitation activities were on track throughout the project, even considering the last year where we had to conduct our activities during COVID-19. This entailed a level of replanning our activities early 2020 to mitigate the risks and carry them out with maximum effort. Prevailing, we made great effort in communicating, disseminating and exploiting the results of the project and evaluate the work of WP6 a success.

During the lifespan of the project, we compiled informational materials to distribute the information about SOFIE and sent out newsletters to update our audience promptly about our regularly achieved milestones. The website was constantly updated and served as an essential vehicle to bring our results to both general audience and to our specific target groups. We actively used our internal and external networks to promote SOFIE and used the social media channels we had established for the project to spread project related news. We were successful in building meaningful liaisons throughout the project and will utilize many established connections beyond the project as well.

Throughout the project we made five open-source (three during M26-36) releases and we promoted the SOFIE Framework, its components, adapters and the pilot use-cases not only through our own website and social media but also through external online marketplaces. What is more, we complemented the scientific literature with 34 publications, which exceeded greatly our initial targets. In doing so, we covered a variety of scientific publication types, from journal articles to conference papers and book chapters, with the attempt to make SOFE results available for different types of (scientific) audiences and readers. What is more, we have demonstrated the practical realization of our developed architecture through our reference implementation “Secure Marketplace for Access to Ubiquitous Goods” (SMAUG). In the future, LMF Ericsson is dedicated to developing a proof of concept for 5G Spectrum Sharing that relies on and builds further on SMAUG. Moreover, SOFIE project has successfully engaged with several standardization bodies. The most significant contributions have been made to ETSI ISG PDL-004 and PDL-00.

Moreover, all SOFIE partners have maximized their efforts to strategically exploit the commercial assets created in the project. We have developed clear and strong value propositions and planned and carried out out-reach activities to engage in mutually beneficial collaborations with our stakeholders. A good statement for the latter is that we exceeded our industry outreach KPI with more than a double of the number of business meetings we had planned. During the final year of the project, we finalized our business planning for the pilots, on-boarded the DEDE Adapter to DSO, and released the final versions of the SynField platform for traceability and audit services and Decentralised Marketplace for Energy Flexibility Services. We also released the context-aware mobile gaming pilot's asset, Scavenger Hunt Game, as open source. The exploitation of SOFIE assets continues and will be manifested in various ways, some of which we have highlighted with our roadmap in D6.9.