SOFIE - Secure Open Federation for Internet Everywhere

779984

DELIVERABLE D6.8

Interim 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	31.1.2020
Author(s)	Liis Livin (Guardtime OÜ), Mikael Jaatinen (LMF Ericsson), George C. Polyzos (AUEB), Dmitrij Lagutin (Aalto University), Tomasso Bragatto (Terni ASM), Fancesco Bellesini (Emotion SRL), Priit Anton (Guardtime OÜ), Max Samarin (Rovio), Sotiris Karachontzitis (Synelixis), Giuseppe Ravedutto (Engineering), Antonis Gonos (Optimum).
Responsible person	Liis Livin (Guardtime OÜ), 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.

Table of Contents

1. Introduction

SOFIE deliverables 6.5 “Initial Communication and Dissemination Plan” and 6.6 “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 with regards to confidentiality, publication, and use of the knowledge. Deliverable 6.7 “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.

The current deliverable “Interim Report on Communication, Dissemination and Exploitation” outlines the outcomes of communication, dissemination and exploitation activities of the project undertaken during the first 25 months. It assesses the status of the initiatives and activities and highlights the future progress of them. The report is divided into 10 chapters, with the aim to reflect on the general strategy for communication, dissemination and exploitation (Chapter 2) and to offer an overview of related communication and dissemination activities that took place from January 2018 until January 2020 (Chapter 3). In a comprehensive and closely related Chapter 4, the deliverable presents the result of exploitation activities from January 2018 until January 2020. Expanding upon exploitation, the deliverable presents the Business Model Canvases created for each pilot (Chapter 5). The following chapters offer insight into standardization initiatives (Chapter 6), open data and intellectual property rights (Chapter 7 and 8). The deliverable is concluded with Chapter 9 where an evaluation to ongoing activities is offered and analysed.

2. General Strategy for Communication, Dissemination and Exploitation

The main purpose of the SOFIE communication and dissemination strategy is to maximize the impact created by the project. Communication and dissemination activities aim 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 are utilised to reach the target groups. As a research and innovation project, SOFIE takes two paths in dissemination and exploitation: 1) dissemination and exploitation of academic results and 2) dissemination and exploitation of commercial components, acknowledging that the academic results produced provide essential input to commercial exploitation. Those SOFIE components that end up being commercially exploitable will be exploited through the project's pilots; exploitation will be executed with the help of Business Canvas Model (see chapters 4 and 5).

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 are managed via the communication channel on Slack as well as the project's official mailing list. All communication materials are uploaded to SOFIE's webpage and maintained on Google Drive. Lists of publications and presentations, as well as WP6 related deliverables, are managed on the SOFIE Wiki page.

The key message. The key message of the project is 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.

The objectives of the communication and dissemination activities:

- Raising general awareness about the project and its output.
- Supporting the engagement of stakeholders for participation in the work of 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.

Target groups. The main audiences for communication and dissemination activities are as follows: academic community, (potential) industrial partners for exploiting the commercial components of SOFIE, policy makers and general public.

The aim is 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 is being kept informed about SOFIE research. The aim is 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 is invited to discuss 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. SOFIE project developments and results are communicated to the **general audience**, as well. The aim is to create general support and awareness of the advantages SOFIE provides and to invite 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.

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

Visual Identity. A visual identity for SOFIE was created at the beginning of the project. This visual identity is to be 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.

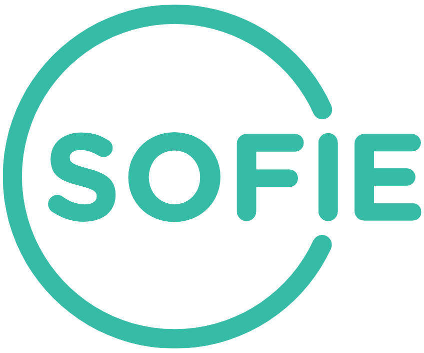


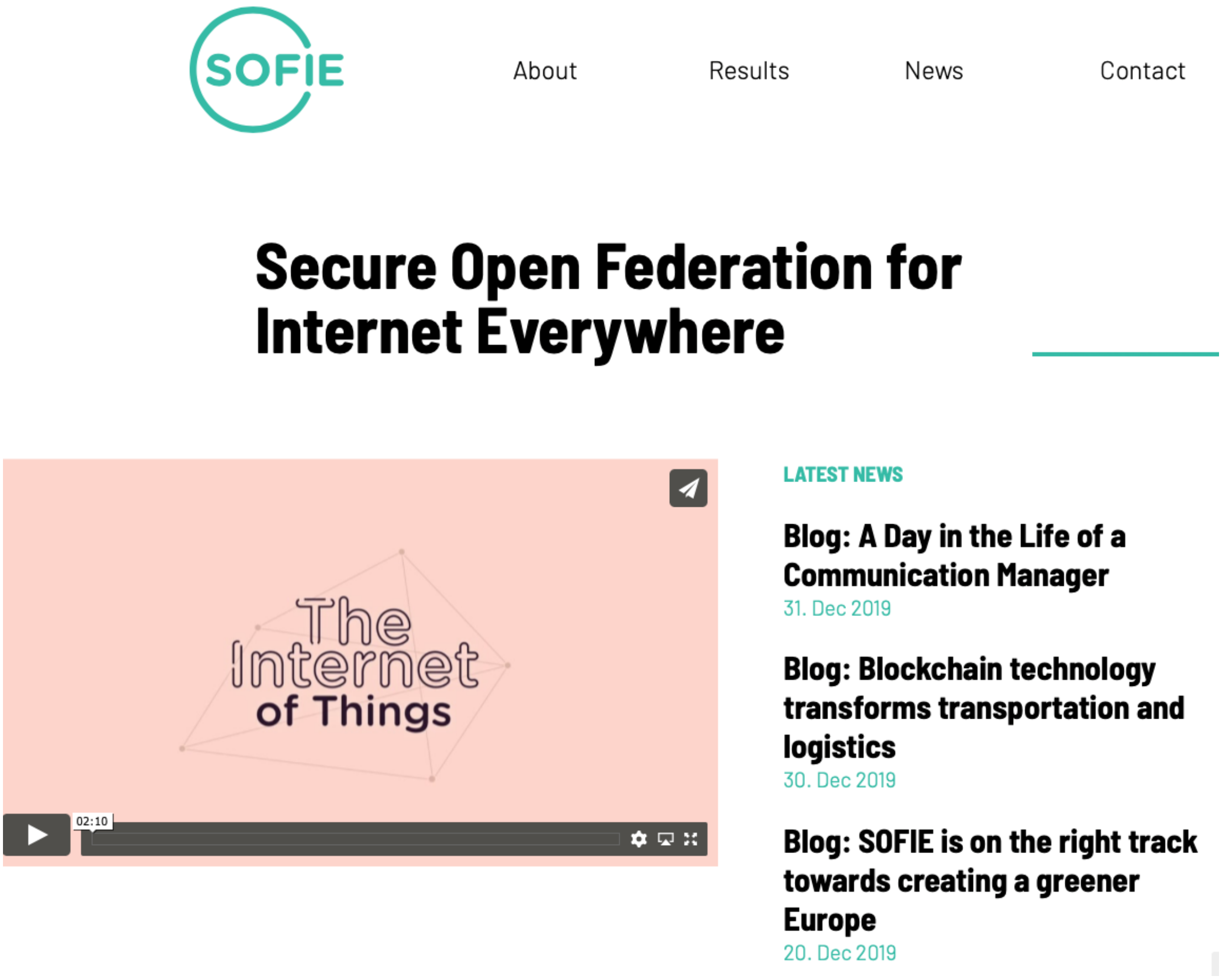
Figure 1. The SOFIE logo

3. Communication and Dissemination

This Chapter provides an overview of the communication and dissemination tools and activities created and conducted within the first 25 months of 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.

3.1 Project Website

The SOFIE website is the project's key dissemination tool and the main source of 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

LATEST NEWS

Blog: A Day in the Life of a Communication Manager
31. Dec 2019

Blog: Blockchain technology transforms transportation and logistics
30. Dec 2019

Blog: SOFIE is on the right track towards creating a greener Europe
20. Dec 2019

Figure 2. 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 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 keep growing, currently having approximately 300-450 visitors per month.

By the end of January 2020, the webpage had approx. 8000 visits with 5500 visitors. The top 5 countries where the page is visited from are: United States (13%), Finland (8,8%), Indonesia (8,5%), Greece (8,2%) and Estonia (5,8%). Two of the most visited pages besides the main page are “project deliverables” and “about SOFIE project”. So, 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 8000 visits, around half come to the SOFIE webpage directly and the second half through search results or via reference or social media.

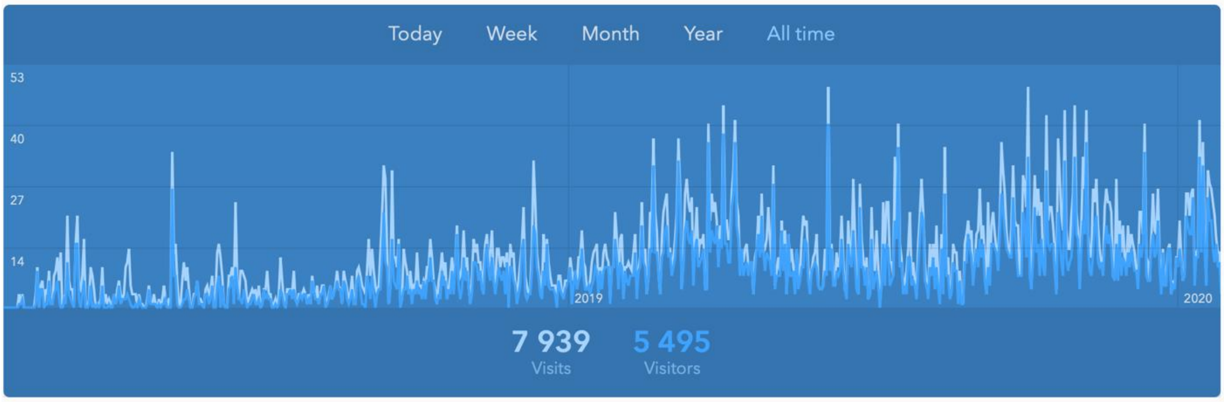


Figure 3. Overview of website visitors (27.01.2020).

In 2019 several subpages of the webpage were updated to give a more thorough insights into the project. E.g. the front page was updated with the SOFIE video. The “About” section was updated with use-case focused but also general informational materials, newsletters and gallery.

One of the most important regularly uploaded content areas for the webpage are the blog posts. The partners have established a timetable for posting, in order to assure that by the end of the project the page will have 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. Each partner contributes at least one post per year. By January 2020, nineteen blog post have been written and published on SOFIE website. The post can be found from the “News” section of the webpage: https://www.sofie-iot.eu/news.

The list of published blog posts from the beginning of the project until January 2020 (incl.) is as follows:

1. Blockchain technology to secure cross-border data exchange between smart meter platforms.
2. Utilizing blockchain technology for providing product insights from-field-to-fork.
3. A secure blockchain-based energy marketplace for load balancing in Low Voltage distribution grids.
4. State of the Art in Blockchain Technology and IoT Systems.
5. Decentralized marketplace using smart contracts.
6. The role of Distributed Ledger Technology (DLT) for authorization in environments with constrained IoT devices.
7. Are data markets necessarily failing?
8. Modelling growth and sustainability of Digital Business platforms with System Dynamics.
9. Traceability in food supply chain based on blockchain & internet of Things.
10. A liberated energy market where data owner calls the shots.
11. Using smart contracts to balance grids and integrate renewable energies via EV fleet charging - Part 1: energy scenario overview.

12. Using smart contracts to balance grids and integrate renewable energies via EV fleet charging - Part 2: the marketplace smart contract.
13. Exploring blockchain and IoT in mobile gaming: location-based games.
14. Integrating framework components and business platforms in SOFIE.
15. Exploiting flexibility marketplace for boosting smart grids.
16. Blockchain technology transforms transportation and logistics.
17. SOFIE is on the right track towards creating a greener Europe.
18. A Day in the Life of a Communication Manager.
19. Integrating Verifiable Credentials (VCs) and Decentralized Identifiers (DIDs) for identification and authorization in the IoT.

The blog schedule for the year of 2020 is as follows:

Table 1. SOFIE's blog timetable for 2020.

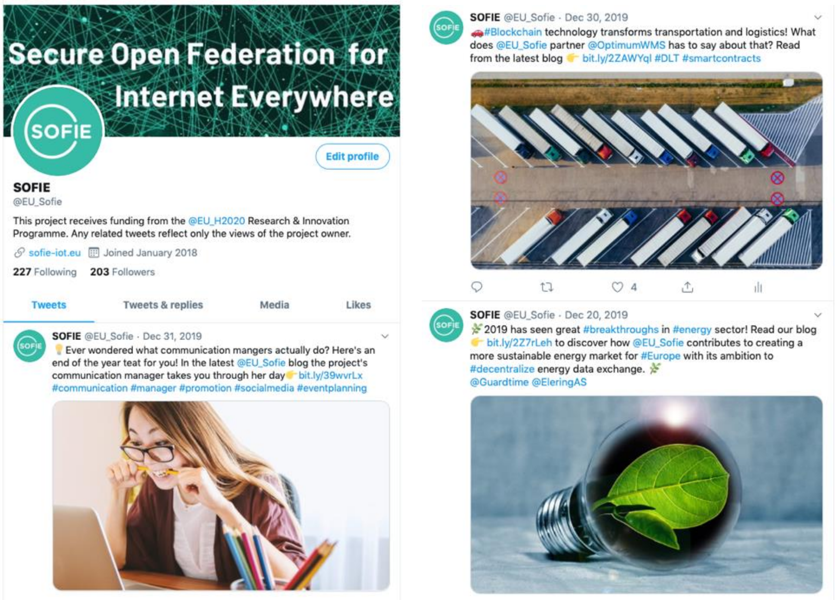
Month (in 2020)	Partner
January	AUEB (completed)
February	Engineering
March	Aalto
April	Rovio
May	Optimum
June	GT
July	Ericsson
August	Synelixis
September	Emotion and Ericsson
October	Terni
November	GT
December	Aalto

3.2 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 is 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. The project's partners help to enhance the project outreach by retweeting.

By January 2020 SOFIE has 210 followers on Twitter, out of whom 59% were men and 41% women. Their top interests are "technology" and "science news". United Kingdom, Italy, Spain, Finland, and Greece are the top 5 countries SOFIE is been followed from on Twitter. Usually, within a 31-day period SOFIE Twitter earns 400-500 impressions per day. Tweets related to events (i.e. workshop attendance) get the highest number of impressions.



SOFIE
@EU_Sofie
This project receives funding from the @EU_H2020 Research & Innovation Programme. Any related tweets reflect only the views of the project owner.
sofie-iot.eu Joined January 2018
227 Following 203 Followers

SOFIE @EU_Sofie · Dec 31, 2019
💡 Ever wondered what communication mangers actually do? Here's an end of the year teat for you! In the latest @EU_Sofie blog the project's communication manager takes you through her day👉 bit.ly/39wvrLx #communication #manager #promotion #socialmedia #eventplanning

SOFIE @EU_Sofie · Dec 30, 2019
🚗#Blockchain technology transforms transportation and logistics! What does @EU_Sofie partner @OptimumWMS has to say about that? Read from the latest blog 👉 bit.ly/2ZAWYql #DLT #smartcontracts

SOFIE @EU_Sofie · Dec 20, 2019
🌿2019 has seen great #breakthroughs in #energy sector! Read our blog 👉 bit.ly/2Z7rLeh to discover how @EU_Sofie contributes to creating a more sustainable energy market for #Europe with its ambition to #decentralize energy data exchange. 🌿
@Guardtime @EleringAS

Figure 4. SOFIE Twitter feed.

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) is to promote SOFIE results for this community and help to establish contacts with industry.

In January 2020 the page has 46 followers and when taking a look on visitors' activity, it is clear that LinkedIn users are attracted to the project page during the times when the SOFIE teams are out and about and actively approaching the business community in person. E.g. Figure 5 illustrates that during the time period where SOFIE participated at Decentralized (30-31.10. 2019) and interacted with industry in a wide set of topics, the interest toward the SOFIE LinkedIn profile also peaked. Although the number of followers doubled during the last four months of the project, it remains below was has been expected. Consequently, more effort should be placed into interactions on this channel.

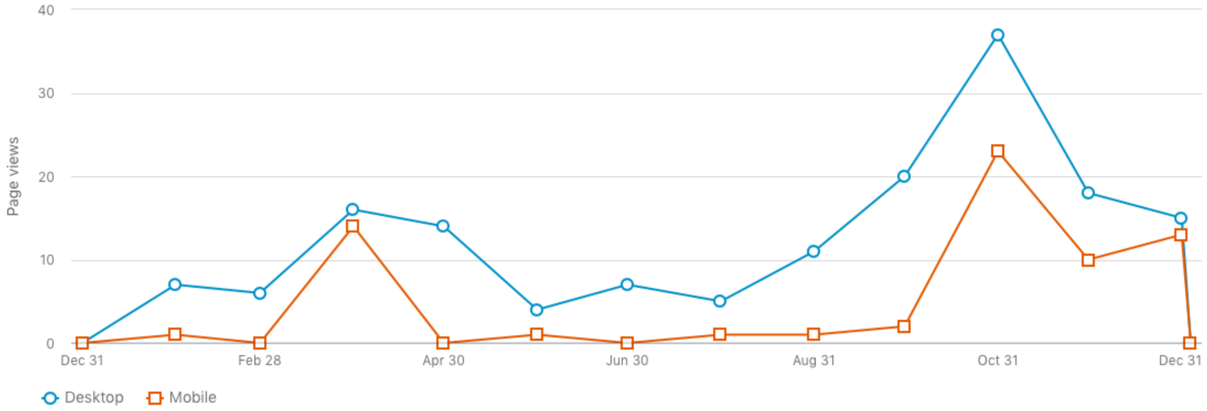
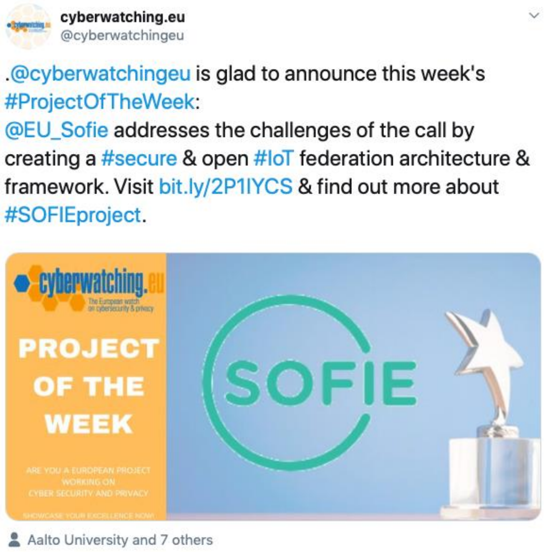


Figure 5. LinkedIn visitor's activity.

In conclusion, the number of social media followers is increasing over time and is expected to boost during the last year. The reach and impressions of posts on these mediums are in correlation with other communication activities, e.g. when SOFIE is exhibited at an event the number of followers increases and the reach of the messages posted on the social media increases as well.

3.3 Other communication tools

Cyberwatching.eu profile. In spring 2019 a cyberwatching.eu portal profile was created for SOFIE project: https://cyberwatching.eu/projects/1302/sofie. Cyberwatching.eu is the European observatory of research and innovation in the field of cybersecurity and privacy and funded under the European Commission's H2020 programme. SOFIE joined this platform to wider the project's visibility and empower cooperation with other EU projects. SOFIE was also featured as project of the week in 21 – 25 October 2019. During the promo week, cyberwatching.eu promoted SOFIE project on its web page and social media (Twitter and LinkedIn).



cyberwatching.eu
@cyberwatchingeu

.@cyberwatchingeu is glad to announce this week's #ProjectOfTheWeek:
@EU_Sofie addresses the challenges of the call by creating a #secure & open #IoT federation architecture & framework. Visit bit.ly/2P1lYCS & find out more about #SOFIEproject.

cyberwatching.eu
The European watch on cybersecurity & privacy
PROJECT OF THE WEEK
ARE YOU A EUROPEAN PROJECT WORKING ON CYBER SECURITY AND PRIVACY
SHOWCASE YOUR EXCELLENCE NOW!
SOFIE

Aalto University and 7 others

Figure 6. Cyberwatching.eu announcing SOFIE as project of the week on Twitter.

SOFIE Newsletter. In 2019 the SOFIE Newsletter was sent out quarterly starting summer 2019. It gives an overview of the deliverables, publications and other relevant events that have occurred during this time period. Everybody can sign up for the newsletter on the SOFIE website: https://www.sofie-iot.eu. The newsletter provides a compact overview of the project and it is a good way to summarize the project to its followers. In 2019 two Newsletters were sent out. They can be found from the "Promotional materials" section of the web-page: https://www.sofie-iot.eu/about/promotional-materials. By January 2020 the newsletter had 62 subscribers with the opening rate of 42,2%. In 2020 the Newsletter will be sent out in February, June and October.

3.4 Scientific Publications

SOFIE project has strong scientific foundation and many of the research results have already been published in conferences with formal proceedings and in journals. By January 2020 the project had exceeded its initial goal. The project's goal was to publish at least 14 scientific articles during the lifetime of the project. By January 2020 the project has 23 publications. The list of the publications is as follows:

Journal Publications

1. Y. Kortesniemi, D. Lagutin, T. Elo, N. Fotiou, "Improving the Privacy of Internet of Things with Decentralised Identifiers (DIDs)," ***Journal of Computer Networks and Communications***, vol. 2019 (Article ID 8706760), 2019.
2. V.A. Siris, P. Nikander, S. Voulgaris, N. Fotiou, D. Lagutin, G.C. Polyzos, "Interledger Approaches," ***IEEE Access***, vol. 7, pp. 89948-89966, 2019.

3. 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, 2019.

4. V.A. Siris, D. Dimopoulos, N. Fotiou, S. Voulgaris, G.C. Polyzos, “Decentralized Authorization in Constrained IoT Environments exploiting Interledger Mechanisms,” ***Computer Communications*** (to appear—accepted for publication January 17, 2020).

Conference and Workshop Publications

5. 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 the Network and Distributed System Security Symposium (NDSS), San Diego, CA, USA, February 2018.

6. E. Ferrera et al., “IoT European Security and Privacy Projects: Integration, Architectures and Interoperability,” in Next Generation Internet of Things: Distributed Intelligence at the Edge and Human Machine-to-Machine Cooperation, O. Vermesan, J. Bacquet, Eds., River Publishers Series in Communications, 2018.

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

8. 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.

9. A. Abu Shohel, 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 and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE 2018, IEEE International Conference on Trust, Security, July 31. 2018.

10. S. Paavolainen, T. Elo, P. Nikander. “Risks from Spam Attacks on Blockchains for Internet-of-Things Devices,” IEEE IEMCON 2018, November 2018.

11. 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.

12. 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

13. D. Lagutin, Y. Kortesniemi, N. Fotiou, V. Siris. “Enabling Decentralised Identifiers and Verifiable Credentials for Constrained Internet-of-Things Devices using OAuth-based Delegation,” DISS Workshop of NDSS 2019, May 2019.

14. S. Paavolainen, P. Nikander. “Decentralized Beacons: Attesting the Ground Truth of Blockchain State for Constrained IoT Devices,“ 2019 Global IoT Summit (GIoTS), June 2019.

15. 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.

16. 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.
17. S. Paavolainen, P. Nikander. “Interledger Demo: IoT Integration.” IEEE International Conference on Blockchain and Cryptocurrency 2019, Seoul, South-Korea, May 2019.
18. 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.
19. 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.
20. 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.
21. 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.
22. P. Nikander, J. Autiosalo, S. Paavolainen, “Interledger for the Industrial Internet of Things“, IEEE International Conference on Industrial Informatics 2019, Helsinki-Espoo, Finland, July 2019.
23. 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.

3.5 Events and presentations

All the attended events have given an excellent opportunity for project partners to interact directly with audiences from different domains relevant to the project. SOFIE partners have given many talks and presentations about the project. Those events have given an excellent opportunity to our target groups to learn more about the specific research and development as well as about the project in general. Through talks and presentations, the project’s aims and developments are reaching the designated target groups: industry, academia, policy makers and also general audience. The table below gives a detailed overview of the presentations given by SOFIE partners between January 2018 and January 2020.

Table 2. List of SOFIE presentations at various events.

Date	Presenter(s)	Presentation title	Place	Audience
20.03.2018	Dmitrij Lagutin	SOFIE - Secure Open Federation for Internet Everywhere	Cluster Workshop for IoT Security/Privacy Related Projects, Brussels.	Scientific community, industry, policy makers.

21.03.2018	George C. Polyzos	SOFIE - Secure Open Federation for Internet Everywhere	IRTF Decentralized Internet Infrastructure (DINRG) Proposed Research Group's Interim Meeting at NDSS-2018, San Diego.	Scientific community
21.03.2018	Priit Anton	SOFIE example - practical experiences with blockchain/DLT technologies	IoT and Blockchain technologies for home and energy services, Brussels.	EU policy makers, Energy sector SME-s, TSOs and DSOs related to energy smart grid developers.
02.05.2018	Francesca Santori	General Presentation of the project	Appuntamento con l'energia, Terni.	General, students
11.05.2018	Massimo Cresta	General Presentation of the project	INGEGNERIA R&D 2018: la ricerca vista da vicino, Terni.	Academic community
24.05.2018.	Vasilios A. Siris	SOFIE - Secure Open Federation for Internet Everywhere	City University of London.	Scientific community
05.06.2018.	Pekka Nikander	Blockchains and IoT: a reality check	IoT Week 2018, Bilbao, Spain.	Scientific community, industry, policy makers.
12.06.2018	George C. Polyzos	IoT Security & Privacy: Challenges and Solutions	Workshop on "Internet of Things: Smart Objects and Services" (IoT-SoS 2018) in conjunction with the 19th IEEE International Symposium on a "World of Wireless, Mobile and Multimedia Networks" (WoWMoM).	Scientific community
14.06.2018	George C. Polyzos (moderator)	Mind the Gaps - Network management, security, privacy, and interoperability in IoT spaces	19th IEEE International Symposium on a "World of Wireless, Mobile and Multimedia Networks" (WoWMoM).	Scientific community
15.06.2018	George C. Polyzos	The Brave New World of Data Analytics	19th IEEE International Symposium on a "World of Wireless, Mobile and	Scientific community

			Multimedia Networks" (WoWMoM).	
20.08 .2018	George C. Polyzos	IoT Vision and Edge Requirements, Workshop on "Mobile Edge Communications”	In conjunction with ACM SIGCOMM 2018, Budapest.	Scientific community
11.10 .2018	Giuseppe Raveduto	SOFIE - Secure Open Federation for Internet Everywhere	CHARIOT project workshop “Towards a cognitive computing platform supporting a unified approach towards privacy, security and safety (PSS) of IoT systems, Rome.	Scientific community, industry, end-users.
31.10 .2018	Francesca Santori,	General Presentation of the project	ELSA open day, Terni.	Engineers
15.11 .2018	Dmitrij Lagutin	SOFIE - Secure Open Federation for Internet Everywhere	P2P Lab, Ioannina.	Scientific community
10.12 .2018	Tommaso Bragatto	General Presentation of the project	Workshop real time data for smart grids, Terni.	Students
24.02 .2019	Pekka Nikander	Anti-rival compensation	NDSS DISS workshop, San Diego.	Scientific community
28.02 .2019	Dmitrij Lagutin	Decentralized identifiers and Enabling IoT interoperability through distributed ledgers	CAIDA: Centre for Applied Internet Data Analysis, University of California, San Diego.	Scientific community
07.03 .2019	Pekka Nikander	Breaking into Silos or Openly Federating IoT Systems with Blockchains	Taltech internal workshop, Tallinn.	Scientific community
08.03 .2019	Ivo Lõhmus	SOFIE project overview	Open Energy Marketplace and the enabling technologies, Brussels.	Scientific community, industry, policy makers.
15.03 .2019	George C. Polyzos	SOFIE Project presentation	European H2020 Cluster Workshop, Athens.	Science community
29.03 .2019	Dmitrij Lagutin	Decentralised Identifiers	Comnet department, Aalto University, Espoo.	Scientific community
17.04 .2019	George C. Polyzos	Bridging the Cyber and Physical worlds using	AUEB's School of Information Sciences and Technology, Athens.	Science community

		Blockchains and Smart Contracts		
09-10.04.2019	Priit Anton	SOFIE approach to privacy and security issues using blockchain technologies	Berlin Energy Transition Dialogue, Berlin.	EU policy makers, Energy sector SME-s, TSOs and DSOs related to energy smart grid developments.
09.05.2019	Pekka Nikander	Towards plurivalued markets	Aalto Sustainability Days, Session 6: Degrowth and Postgrowth, Espoo.	Scientific community
16.05.2019	Pekka Nikander	SOFIE - Secure and Open Federation of IoT systems	Joint workshop between SOFIE, Platform of Trust, GoWood, and Digital Twin projects, Espoo.	Scientific community, industry.
21-22.05.2019	Priit Anton	Applicability of blockchain in energy sector - SOFIE example	Eurelectric workshop blockchain discussion platform, Florence.	Energy sector SME-s, TSOs and DSOs.
10.06.2019	Vasilios A. Siris	Smart Mobility in IoT, Internet of Things: Smart Objects and Services (IoT-SoS)	In conjunction with IEEE WoWMoM 2019, Washington DC.	Scientific community
20.06.2019	Pekka Nikander	Data governance beyond ownership	IoT Week - panel on “Blockchain for IoT”, Aarhus.	Industry, scientific community, policy makers.
20.06.2019	Mikael Jaatinen	Solving business problems in IoT with blockchain	IoT Week - panel on “Blockchain for IoT”, Aarhus.	Industry, scientific community, policy makers.
20.06.2019	Vasilios A. Siris	Blockchains and Authorization in Constrained IoT Environments	IoT Week - panel on "Blockchain for the IoT", Aarhus.	Industry, scientific community, policy makers.
20.06.2019	Pekka Nikander	Inter-ledgers for IoT data markets	IoT Week - panel on "Blockchain for the IoT", Aarhus.	Industry, scientific community, policy makers.
23.09.2019	Massimo Cresta	General Presentation of the project	Terni Digital Week, Tern.	General audience
22-23.10.2019	Priit Anton	Blockchain in the energy sector: challenges and opportunities	Bridge workshop - cyber security for TSO-DSO, Brussels.	EU Policy makers, Energy sector SME-s, TSOs and DSOs.

25.10.2019	Vasilios A. Siris	The role of Distributed Ledger Technology (DLT) for Authorization in Environments with Constrained IoT Devices	ETSI IoT Workshop 2019, France.	Industry, policy makers, standardization.
31.10.2019	Tommi Elo	Using System Dynamics Models to analyse the sustainability of SOFIE Business Platforms	SOFIE Workshop at Decentralized 2019, Athens.	Industry, science community.
31.10.2019	George C. Polyzos (moderator)	SOFIE - Secure Open Federation for Internet Everywhere	SOFIE Workshop at Decentralized 2019, Athens.	Industry, science community.
31.10.2019	Priit Anton and Margus Haavala	SOFIE - Energy data exchange pilot	SOFIE Workshop at Decentralized 2019, Athens.	Industry, science community.
31.10.2019	Giuseppe Raveduto	SOFIE - Energy Flexibility Marketplace pilot	SOFIE Workshop at Decentralized 2019, Athens.	Industry, science community.
31.10.2019	Artemis Tomaras	SOFIE - Food Supply Chain pilot	SOFIE Workshop at Decentralized 2019, Athens.	Industry, science community.
31.10.2019	Ahsan Manzoor and Max Samarin	Exploring DLT & IoT use-cases in mobile gaming	SOFIE Workshop at Decentralized 2019, Athens.	Industry, science community.
19.11.2019	Priit Anton	Free energy data - Blockchain enabling energy flexibility services	Cyberwatching Webinar, online GoToWebinar.	Industry, scientific community, EU policy.

3.5.1 Exhibitions

During the first year the SOFIE project was exhibited at two conferences. The first exhibition was in IoT Week 2018 in Bilbao and the second one in ICT2018, Vienna. During both of the exhibitions the SOFIE flyers and business cards were distributed. In addition, the demos for the Estonian energy pilot and Greek from-field-to-fork pilot were introduced.

During the second year the SOFIE project was exhibited at Decentralized 2019 that took place in Athens 30.10-01.11.2019. The exhibition focused on presenting the use-cases but also distributed general information about the project and consortium. The SOFIE video was played at the exhibition booth to visually attract the visitors. Moreover, project leaflets and pilots' one-pagers were distributed to the visitors.

In 2020 SOFIE aims to exhibit its results in various conferences by having a special exhibition area, communicating via dedicated panels, and presentations. We are interested in participating in events like IoTWeek and cooperating with other EU projects while exhibiting.

3.5.2 SOFIE workshops

The aim of the project is to organize three workshops aimed to disseminate and promote SOFIE results and the project itself.

The first SOFIE workshop took place in 2019. It was dedicated to presenting and demonstrating SOFIE's use cases to specific target audiences and to gather relevant feedback.

The workshop took place in the framework of Decentralized conference in Athens, 30.10-01.11.2019. SOFIE's ambitious workshop "Interledger Technologies for Cyber-Physical Systems Federation with Security, Privacy, and Flexibility. - Practical applications to the Energy sector, the Food-Supply Chain, and Context-Aware IoT gaming" showed the audience that a federated platform enabling seamless data exchange paths between fragmented Iot systems is future of now.

The use-cases presented at the workshop were: energy data exchange pilot, presented by Priit Anton and Margus Haavala (Guardtime); energy flexibility marketplace pilot, Giuseppe Raveduto (Engineering Ingegneria Informatica); food supply chain pilot, Artemis Tomaras (Synelixis Solutions SA); mixed reality mobile gaming pilot, presented by Max Samarin and Ahsan Manzoor (Rovio Entertainment Corporation). The workshop was moderated by George Polyzos (Athens University of Economics and Business). Around 50 people attended the workshop. The SOFIE team got lot of insightful questions from the audience that allowed to discuss the topic of decentralized IoT systems on a wider manner.

Furthermore, Tommi Elo (Aalto University) from SOFIE consortium gave a speech at Decentralized as well. On the 31st of October he will spoke about using system dynamics models to analyse the sustainability of SOFIE business platforms.

Additionally, SOFIE's applications were showcased at the exhibition site at SOFIE booth during Decentralized. The consortium partners discussed the wide variety of SOFIE applications with the visitors and visualised their interaction with videos of use-case demos.

SOFIE
A new federated platfor... ling seamle... exchang... betw...
Finland
Mixed reality gaming pilot
Learn about
IoT Use Cases
Grov
Project Consortium
WORKSHOP

Figure 7. Team SOFIE at the Decentralized exhibition area.

SOFIE workshops M26-36. The second SOFIE workshop will take place on the first half of 2020. The workshop will focus on disseminating SOFIE research results. The third SOFIE workshop will take place at the end of the project and it will be dedicated to exploitation activities.

3.6 Liaisons

SOFIE participated in the EC cluster meeting for IoT projects, and established liaisons with CHARIOT and SEMIoTICS H2020 projects. Several SOFIE partners created proposals utilizing SOFIE results for the H2020 ICT56 funding call in January 2020. SOFIE participated in the IOS Press book "Security and Privacy in Internet of Things: Challenges and Solutions" edited by Jose Luis Hernandez-Ramos and Antonio Skarmeta. SOFIE participated in the Workshop on Internet of Things Security and Privacy (WISP), which was organised by the IoT Crawler project and held in conjunction with Global IoT Summit 2019. There has been also close co-operation between SOFIE and TrustNet project funded by Business Finland related to decentralised identifiers.

The SOFIE project in collaboration with five (ENACT, ARMOUR, SMESEC, IoT Crawler, CIPSEC) other H2020 IoT projects organised a joint exhibition area at ICT2018 conference in December 2018. The SOFIE project also established liaisons with GHOST H2020 projects and participated in the workshop of CHARIOT project in October 2018. The SOFIE project organised a joint international Hackathon event, IoThon (https://iothon.io), in co-operation with the H2020 POINT project. The IoThon was held in Berlin, Germany in January 2018 and attracted about 50 participants.

In 2019 SOFIE has been actively participating (Priit Anton, Guardtime) to the work related to Bridge initiative (https://www.h2020-bridge.eu/). SOFIE participated in two workshops 2019 and is planning to contribute into two more in 2020. The result of this activity is aligning the SOFIE messages towards the industry with the Bridge projects. Also, the interaction with energy companies as well as EC policy makers is a good result.

There has been close cooperation between SOFIE and Sysflex project (https://eu-sysflex.com/). In Sysflex there are 10 DSOs and TSOs that have been updated on how SOFIE is solving the energy smart grid and stand-alone data hubs challenges. It is an excellent way of getting more industry involvement in energy sector for SOFIE. On the other way, the requirements from energy industry and new developed applications related to what we are using in SOFIE are introduced from Sysflex's partners to us.

3.7 Industry outreach – meetings and networking

As the project's pilots are the drivers bringing the SOFIE components to the market, the following section presents the efforts made by each SOFIE pilot partners to reach out to the industry audience through meetings and networking until January 2020 (incl.), 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.

3.7.1 Energy data exchange pilot (Guardtime)

The primary agenda is to focus on "gate keepers" of the field of energy data and to validate the business use-case in concern of solving the access, access control, audit trail and trust issues when complying to the Green energy package, GDPR and free energy market.

Guardtime's milestones during the reporting period (M1-25)

Milestones in 2018

- Compiling the first one-pager describing the energy data exchange concept.
- Elering (Estonian TSO) confirmed as advisory boarded member for SOFIE.
- Published one blog post in energy sector on SOFIE webpage.
- Participation in 3 workshops and 14 business meetings.

Milestones 2019

- Creating the first version of business canvas model for the pilot.
- Joining the EU H2020 Bridge initiative for data and cyber security.
- Elering (Estonian TSO) participating in SOFIE advisory board.
- Writing two blog posts in energy sector published on SOFIE webpage.
- Participated at 4 workshops and 23 business meetings.
- SOFIE energy data exchange participation in Energy data access alliance (8 countries TSOs initiative to create a joint market for data access).

The interaction with stakeholders has been divided into meetings in the workshops (total 8 workshops during first 25 months) and B2B meetings and teleconferences. The aim of the interaction with stakeholders is to validate the SOFIE energy data exchange value proposition, find potential customers and technology partners.

Meetings during reporting period (industry):

1. With Elering - 6 meetings in 2018, 8 meetings in 2019.

2. With Tennet - 2 meetings in 2018, 1 meeting in 2019.

3. With Energinet - 2 meetings in 2018, 1 meeting in 2019.

4. With ESO - 2 meetings in 2018, 1 meeting in 2019.

5. With PSE - 1 meeting in 2018, 3 meetings in 2019.

6. With Spotty - 1 meeting in 2018, 1 meeting in 2019.

7. With Elektrilevi - 1 meeting in 2018, 1 meeting in 2019.

8. With Fingrid- 1 meeting in 2018, 1 meeting in 2019.

Meetings during reporting period (technology partners):

1. With AKKA - 2 meetings in 2018, 2 meetings in 2019.

2. With EDF - 3 meetings in 2018, 4 meetings in 2019.

3. With Intrinsic ID - 5 meetings in 2018, 2 meetings in 2019.

4. With Cybernetica - 2 meetings in 2018, 3 meetings in 2019.

During the last year of the project Guardtime aims to participate in 3-4 workshops, conduct 25 meetings with industry and 15 meetings with relevant technology partners.

3.7.2 Energy flexibility marketplace pilot (Engineering)

The strategy is following a two-step process. In the first part, Engineering, as tool provider and technical developer, collected and took into account feedback from ASM Terni and Emotion, as main users, to design the tools based on internal objectives and experience. In parallel, an internal knowledge transfer process towards the dedicated business unit has been started.

Engineering's milestones during the reporting period (M1-25)

- Engineering started to disseminate the project through the participation to scientific and technical conferences and Industrial exhibitions.

Meetings during reporting period:

1. Innogrid 2019 Conference

2. ENTSO-E EC/DG Energy-EIT group on Open Energy Marketplaces

During the last year of the project Engineering aims to further extend the outreach participating to the following industrial workshops and conferences:

1. Participation in EU BRIDGE working group for Data Management

2. participation to Innogrid 2020, Bruxelles (May 2020)

3.7.3 Food Supply Chain pilot (Synelixis and Optimum)

The food supply chain pilot follows an end-user centric design process where pilot platform and provided services are defined based on the business needs and challenges identified by the main end user of the pilot, i.e. Pegasos 7 grapes association.

Synelixis' and Optimum's milestones during the reporting period (M1-25)

- On site resources, equipment and facilities which will be used in the pilot demonstration activities have been identified jointly by technical partners (SYN, OPT) and end users (Pegasos). The timeline and workflow for on-site testing, validation and further dissemination of results have also been defined.
- Initial end-user requirements have been collected and used to define technical specifications for SOFIE framework components, pilot platform architecture and exposed services (i.e. tracking and audit services).
- Software implementation of pilot platform architecture has started; implementation of tracking service has been completed, while implementation of audit service is in progress.
- Initial tests about installation and configuration of IoT equipment deployed on site have been made. Complete pilot test, involving also real end-users, have been identified.

Meetings during reporting period:

1. Meeting in Kiato area (end-user premises) on M14: Initial discussions between technical partners and end users; presentation of SOFIE and Food Supply Chain pilot concepts; insights and current challenges in food (grapes) supply chain workflow; initial elicitation of end-users requirements.

2. Meeting in Kiato area (end-user premises) on M18: First tests on how to deploy equipment on-site and use local facilities/resources; agree on the roadmap and a plan for validation/demonstration activities

During the last year of the project, the Food Supply Chain pilot aims to finalized implementation and release final pilot platform, perform on-site testing and demonstration of provided services, analyze impact and lessons learned from pilot activities and disseminate final outcomes to further customers and potential stakeholders.

List of planned meetings for 2020:

1. Meeting planned for M27 with main objective to collect feedback from the end-users about pilot platform and services first release.
2. Meeting planned for M31/M32 with main objective to perform on-site demonstration of pilot platform and services final release.
3. Meeting planned for M34/M35 with main objective to jointly analyze pilot impact and perform activities to disseminate the outcomes to further stakeholders and potential customers.

3.7.4 Mobile Gaming Pilot (Rovio)

The main aim of the mobile gaming pilot is to identify and understand use cases for DLTs and IoT in gaming and test the business opportunity. Through communication and dissemination activities (internal and external), Rovio aims to gather feedback and get technical assistance with their implementation of the pilot, as well as to try to identify new use cases.

Rovio's milestones during the reporting period (M1-25)

- In 2018, Rovio held an internal hackathon where their first DLT based prototype was designed. During M13-24 Rovio had a session with GoFore, where IoT beacons were used for proximity-based location applications.
- Additionally, Rovio had several web meetings with the Amazon Web Services (AWS) team for this period, discussing the use of Amazon managed blockchain for the SOFIE mobile gaming pilot, getting assistance with technical challenges in the pilot, and discussing pilot promotion opportunities.
- Rovio also had a discussion with Dapperlabs about their new Flow blockchain and whether it could be useful in the pilot. Rovio decided not to lock in to a specific blockchain platform, as flexibility is needed for prototyping.
- In November 2019 Rovio hosted a partner challenge in the Junction hackathon in Espoo, Finland. Rovio challenged the participants to create a game over the weekend that utilizes any emerging technology in some way, including IoT devices. This was an opportunity to potentially witness new use cases for the technology. A few teams utilized Bluetooth beacons in the indoor location-based game experiences that they built. Rovio saw interesting ideas implemented by the hackathon participants, especially the ones that used detected signal strengths of beacons at small distances. This is different to Rovio pilot's beacon detection, which uses beacons at larger distances for discrete positioning - estimating whether the user is in the correct room or not.

Meetings during reporting period:

1. Internal hackathon #1: The Ethereum asset minting and trading game prototype was born out of this hackathon.
2. GoFore workshops: Learning how IoT beacons could be used in proximity-based location applications through hands-on exercises.
   AWS meetings: Receiving technical support with AWS Managed Blockchain for the development of the Scavenger Hunt prototype's backend. There were also discussions about presenting Rovio's Pilot at the AWS re:Invent conference, however Rovio did not get a presentation slot for this topic.
3. Equilibrium labs: Rovio presented their pilot's hybrid server-blockchain architecture with the objective to receive feedback from an expert company on distributed technologies.
4. Dapperlabs discussions: Rovio learned from Dapperlabs about their new Flow blockchain used for decentralized games, to which a few gaming companies have already committed. Rovio decided not to lock in to any specific blockchain platform at this research stage.

5. Internal hackathon #2: The Blockmoji decentralized avatar prototype was born in this hackathon and was presented internally.

Planned meetings 2020:

1. Invernal hackathon #3: Potentially work on a small new use case or continue developing an old use case.
2. AWS: Asking for more help with using AWS Managed Blockchain if needed.

3.8 Code releases

SOFIE has planned for 5 main software releases. The first main release code has been made available in September 2018, the second code release was made in October 2019, the third one is planned for April 2020, the fourth one for Autumn 2020, and the final one at the end of the project for December 2020.

The code is downloadable at GitHub: https://github.com/SOFIE-project. Between main releases, the code base is improved through continuous integration, deployment, and validation processes.

4. Exploitation

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.

During the first year of the project it was identified that those SOFIE results that are closely related to the pilots, will have the strongest chance to survive and move to the pipeline for commercialization. Thus, during the second year much effort was placed on planning and executing exploitation activities through the four SOFIE pilots.

The chapter starts with giving an overview of the general exploitation foreground, followed by the academic exploitation efforts. The second part of this chapter is dedicated to commercial exploitation, which will be complemented by pilots' exploitation efforts in Chapter 5.

4.1 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 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 interaction between the ledgers.

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.

Privacy and Data Sovereignty

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

Semantic Representation

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

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.

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.

SOFIE Federation adapters

The purpose of the federation adapter is to interface the SOFIE components with existing IoT platforms. This allows the IoT platforms to interact with SOFIE without requiring any changes to the IoT platforms themselves.

Reference implementation

A SOFIE reference implementation is being developed as a practical realization of SOFIE architecture and framework. It is planned to become available after the 3rd SOFIE code release, in May 2020. The reference implementation will demonstrate the use of all six SOFIE framework components in the context of an IoT marketplace application.

System dynamics models of business platform network effects

System dynamics models are causal loop diagrams, which include simulation equations and real-world data as inputs to the model. These models can be used to simulate the data markets, the economic sensitivity, and economic sustainability of the platform businesses.

4.2 Academic exploitation

4.2.1 Aalto University

Foreground to be exploited: Interledger, the Identity, Authentication and Authorisation (IAA), Privacy and Data Sovereignty, system dynamic models of business platform network effects, Marketplace.

Measures taken so far: Two PhD students and one master's student are working on the SOFIE project. Aalto has also supervised one SOFIE-related master's thesis. A graduate course "Postgraduate Seminar in Communications Engineering on Data Economics" was held in Autumn 2018, and "Microservice architectures and serverless computing" course was held in Spring 2019 at Aalto University.

SOFIE results have already been utilised by H2020 PHOENIX, EMPIR SmartCom, and EIT Climate-KIC GOWOOD projects.

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

4.2.2 Athens University of Economics and Business

Foreground to be exploited: Interledger, Identity, Authentication and Authorisation (IAA) component and technologies, the Privacy and Data Sovereignty (PDS) component and technologies, smart contracts encoding payment and authorization policies, IAA & PDS for constrained IoT devices and settings.

Measures taken and results so far: AUEB MMlab seminars on distributed ledger technology, programming for smart contracts, and blockchain security have been offered. In addition, an elective Special Topics in CS course has been offered for credit as part of the AUEB MSc CS program by Dr. Nikos Fotiou, an AUEB SOFIE researcher, on “Blockchains and Smart Contracts” in the Spring 2018-2019 semester to 11 students (who selected it among many); the same course will be offered in Spring 2019-2020 by Prof. Spyros Voulgaris, also an AUEB SOFIE researcher. The following three MSc theses related to SOFIE have been assigned and completed: (1) I. Pittaras, “Interacting with the Web of Things using Blockchains” 2019, (2) S. Drossos, “Creating a ‘Store of Value’ platform for cryptocurrencies” 2019, (3) M. Tsenos, “Interledger Approaches” 2019. One of those students, I. Pittaras, has been subsequently recruited as a PhD student at AUEB and as a SOFIE researcher exploiting the opportunity created by SOFIE. Another PhD is being pursued at AUEB because of the expertise, experience and reputation achieved due to SOFIE and without the candidate, Chr. Karapapas, being financially supported by SOFIE, in the area of smart contract programming and security. Profs. Polyzos, Siris and Voulgaris presented (in the Fall of 2019) SOFIE research topics to new MSc

CS students as part of the Research Methodology course/seminar of the program in order to recruit students for MSc theses.

Future work: AUEB will continue offering master thesis topics, seminars, and graduate courses related to SOFIE in order to exploit the specific components and other software it has developed for SOFIE, but more importantly to exploit the overall deep understanding it has achieved regarding problems in the area and various technologies employed and developed, with the ultimate goal to recruit top students at all levels and top researchers to further the mission of the lab and AUEB.

4.3 Commercial exploitation

In this section commercial exploitation of SOFIE is presented through each partner presenting the foreground they are exploiting, complemented by the description of activities undertaken during M1-25 to exploit SOFIE results, and with future exploitation plans.

4.3.1 ASM Terni SPA

ASM Terni offers specialized and public services to citizens of Terni and its surrounding area, namely water and electricity grid management that can be dramatically improved by implementing cutting-edge technologies such as a potential federation composed of different platforms connected to each other. ASM Terni as responsible for the power distribution network has the potential to offer a significant change in terms of energy availability by providing safe and secure operation and management of the Distribution Network. In this case, renewable energy has the paramount benefit to meet the local green economy.

Foreground to be exploited: Interledger, Semantic representation, Marketplace, SOFIE Federation adapters.

Measures taken so far: As foreseen in D 2.7, the adaptation of the existing metering infrastructure to the SOFIE platform has been implemented.

Future work: Block Chain installation for Smart contracts, if legally applicable, at ASM headquarters.

4.3.2 Emotion SRL

Emotion is part of the Italian Energy pilot providing monitoring and management services for electric vehicles and charging stations. The acquired knowledge is exploited to increase Emotion SRL business, offering to the market products and services enhanced with the project, with the aim of giving strength to electric mobility, for cleaner mobility, allowing an increasingly massive deployment of electric vehicles and charging stations and an increasingly intense use of renewable photovoltaic energy that is mainly produced at lunchtime, when consumption is lower and when the vehicle could be parked in charge.

Foreground to be exploited: Interledger, Semantic representation, Marketplace, SOFIE Federation adapters.

Measures taken so far: Emotion SRL has refined its skills related to smart contracts and micro payments. Electric Mobility Dashboard has been implemented: in addition to monitoring and managing electric vehicles and charging stations in real time, it is also possible to predict in advance the amount of flexibility that can be provided to the DSO thanks to the implementation of a forecasting algorithm which is based on the real data acquired by the electric vehicles and charging stations deployed in the Italian pilot site. Furthermore, since it was necessary to involve the energy retailer in the Demand Response (DR) campaigns, a panel was implemented in the dashboard to create the auctions relating to the supply of electricity and to sign smart contract between the energy retailer and fleet manager. DR campaigns, previously tested in the laboratory, have been successfully performed on the Italian pilot site. An improvement process is started for the services offered to customers by EMOT, thanks to the knowledge acquired during the SOFIE project.

Future work: Emotion SRL is implementing a service to modulate charging station power output during a charging session, with the aim of providing flexibility modulated according to the energy balance of the grid. The goal is to test it in the Italian pilot site by the end of the project, to be able to exploit it both commercially and in future research projects.

4.3.3 Engineering Ingegneria Informatica SPA

Engineering implements the Decentralized Marketplace that enables the demand response campaigns via smart contracts. The results of the project, in particular the components related to the Decentralized Marketplace and the DSO forecast and congestions detection dashboard, will be exploited in several European research projects exploring the usage of distributed ledger solutions in the Energy field; moreover these technologies will be made available to the related ENG business unit. In fact, Engineering addresses the specific market with its Business unit Energy & Utility to provide its own value proposition as complete solution for its customers. In the Engineering innovation model, the R&I activity goal is to contribute to the change in markets and companies via solutions that can create innovative experiences for the users, in order to encourage a safe and aware use of information technology. The process is composed by three macro steps: 1. Develop and consolidate the results of research projects; 2. Define and execute experimental checks of developed solutions –or components – including the activity to assure the replicability of processes; 3. Capitalize the investment providing via ENG Business Unit Business Offer to the clients according to a specific business plan. Part of this step is the actual commercialization process, including the work of the business unit to extend the company offer portfolio and address the worldwide market with a proper marketing strategy.

Foreground to be exploited: Interledger, Semantic representation, Marketplace, SOFIE Federation adapters.

Measures taken so far: Involvement of Energy & Utility Business Unit (BU). In a first stage, the BU was involved for the scenario identification, preliminary pilot use cases design and first requirement analysis. Later on, the BU participated to a live demo of the Terni pilot, to demonstrate the complete prototype functionalities end-to-end.

Future work: extend and consolidate the blockchain-based marketplace prototype and involve the internal business unit to identify the best way to extend the company solutions and, in case, start the technology transfer process.

4.3.4 LMF Ericsson

Ericsson is interested in the open federated approach defined by the SOFIE architecture and framework. Opportunities for exploitation of the SOFIE foreground have already been identified as discussed in this chapter.

Foreground to be exploited: Interledger, Identity, Authentication and Authorisation (IAA), Privacy and Data Sovereignty, Semantic Representation, Marketplace, Provisioning and Discovery, Reference Implementation.

Measures taken so far:

- SOFIE approach for distributed identifiers has been adopted so far in one completed research project.
- One Master's Thesis completed in the areas of Distributed Identifiers.
- Multiple internal demonstrations of how SOFIE Interledger approach can be used for control of resource constrained IoT devices.

- Have started development of a reference implementation that demonstrates the use of SOFIE framework components in the context of an IoT marketplace application for control of smart lockers. This reference implementation will be disseminated as part of SOFIE project results.

Future work:

- Complete the work on the reference implementation
- Demonstrate the smart lockers marketplace internally and in external events during June-December 2020.
- Leverage on the reference implementation for a research project that aims to demonstrate results in Mobile World Congress 2021 in Barcelona, Spain.
- Research on transparency for centralized identity systems such as PKI and Remote SIM provisioning (RSP) with use of decentralized and immutable structure of ledger and smart contracts for transparency of identity data.
- Security analysis of identity systems. Security analysis of blockchain and non-blockchain identity systems, considering e.g. PKI, Remote SIM provisioning and Ethereum name service. Research to evaluate automated device provisioning with use of blockchain.

4.3.5 Guardtime OÜ

Guardtime’s aims have remained the same, as reported in Deliverable 6.7. The only notable deviation is related to the interaction with the hardware and smart meters. As the data collection and access is more related to energy data hubs and the problem/solution fit can be solved on the same level, the hardware approach has been dropped from its main focus from a technical perspective.

Foreground to be exploited: Interledger, Identity, Authentication and Authorisation (IAA), Privacy and Data Sovereignty (PDS), Semantic representation, SOFIE Federation adapters.

Measures takes so far and future work:

From the commercial exploitation perspective Guardtime has not changed the priority related to SOFIE. Energy sector remains an important business vertical for Guardtime and resources that are not directly related to SOFIE (mainly interaction with CEO, sales force and marketing team), are used to achieve better results in the exploitation activities.

The energy industry target group that was listed before (TenneT, Elering, AKKA, ESO) are continuing to be an important source of information. Also, the plan to focus on the GDPR and flexible open energy market activities is still viable and future workshops and interaction with energy industry will follow this path.

4.3.6 Optimum Anonimi Etairia Technologies Pliroforikis

Optimum participates in the food supply chain pilot and implements the federation adapter of the Aberon IoT platform to support tracking of environmental conditions in the warehouse. Optimum is especially interested in the convergence of DLTs with IoT and how the first can address challenges relate to cybersecurity, data privacy and integrity, and scalability of next generation IoT services.

Foreground to be exploited: Interledger, Authentication and Authorisation (IAA), Semantic representation, SOFIE Federation adapters.

Measures taken so far: Further analysis of technical requirements for the identified services in the pilot. Presentation of the SOFIE business platform to partners and commercial customers to inform them about new business opportunities towards integrating end-to-end secure traceability in logistics and warehouse management.

Future work: the following actions are planned in relation to SOFIE:

- Improving cybersecurity and data protection mechanisms in integrating IoT functionality to Aberon.

- Improving services of Aberon tailored to the warehouse management by using blockchain technology.

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

4.3.7 Rovio Entertainment Corporation

Rovio leads the Mobile Gaming Pilot in the project. We aim to seek and identify where data platforms using DLTs can have significant impact in gaming industry. We will also build prototypes for leading use cases and validate game experience and business potential for DLTs and IoT in gaming.

Foreground to be exploited: Interledger, Marketplace, Semantic representation, Provisioning and Discovery.

Measures taken so far:

One Blockchain research developer (PhD student) working on identifying use cases, current challenges to implement those use cases and their possible solutions. A publication is being prepared for this purpose. A wider team is involved in the prototype development. To date, we have developed three prototypes in total to explore the foreground and understand the use of DLTs and IoT in games. The first one enables creating, buying and selling of in-game assets. The second one is a location-based scavenger hunt game prototype that uses IoT beacons for positioning players and stores rewards on the blockchain. The third and the most recent prototype is a distributed avatar management application and standard, allowing for a distributed avatar to be displayed and utilized in different applications and potentially enabling cross-game interoperability.

Future work:

- Paper submission for review “SOFIE Gaming - Use Cases, Challenges and Solutions” - planned for first week of March (IEEE TrustCom ’19).
- Plan to submit “Scavenger Hunt: A Location-based Game on the Blockchain Utilizing the Internet of Things” for review during first half of 2020.
- Implementation of the scavenger hunt game testing - DLT and IoT gaming use case.
- Play testing and business requirement assessments for use case for the gaming pilot. Define requirements for SOFIE platform integration with the gaming pilot use cases.
- Open sourcing the Discovery & Provisioning component for the wider developer community.

4.3.8 Synelixis Solutions SA

Synelixis is interested in the semantics schema developed in the scope of SOFIE to support supply chain management, especially that part that matches processing of data from a farming system (as it is managed by SynField IoT platform) to the other segments of the chain. SynField is a commercial, cloud based IoT solution for precision agriculture and smart water irrigation. Proper adaptation of SOFIE pilot blockchain-based data model into SynField mechanisms for data serialization and farming objects identification can be used to develop custom protocols and secure modules that allow easy adaptation and integration of the last as part of complex networks of IoT and other operational technologies enabling traceability of resources in large, multi-segment food supply chains and networks (agriculture 4.0).

Foreground to be exploited: Interledger, Authentication and Authorisation (IAA), Semantic representation, SOFIE Federation adapters.

Measures taken so far: Exploitation activities so far have focused on adapting SOFIE technology and implementing Food Supply Chain services according to the requirements and business needs highlighted by 7GRAPES Pegasus, which also is considered as an early adopter and customer of the SOFIE food supply chain environment.

Future work: 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:

- Competitor analysis of most successful blockchain-based, “farm-to-field” traceability software solutions and thorough cybersecurity analysis about how IoT platforms are integrated.
- Evaluation and development of the semantics reference model for web services discovery and provision in the food-chain supply system, especially in farming operations.
- Investigation and determination of the social/business context (e.g. structural properties of collaboration, business routines, governance issues etc.) in which the food-chain pilot will be deployed and operate. Formulation of a business proposal to clarify SOFIE added value in supply chain and develop potential business opportunities.
- 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.

5. Business Models for pilots

The following chapter presents the business models best suited to SOFIE's pilots, through which the generated innovation will be brought to the market. The Business Model Canvas (BMC) approach is used to generate, present and develop the planning of exploitation through the pilots.

The Business Model Canvases will present the exploitation strategy of each pilot, as well as the benefits for the stakeholders, enabling technologies and also an overview of market trends. The workflow and interaction between SOFIE work packages of Business Model Canvases are described in chapter 3.4 "Business outreach" in the updated version of deliverable D6.6. The first version of the models was presented in under Chapter 5 of deliverable D6.7.

5.1 Energy data exchange pilot (Guardtime)

During the first two years of the SOFIE project one of the focus points has been to validate the problem description in the energy data exchange pilot. The first version was written in the SOFIE initial proposal and was mostly focused on providing evidence of data exchange/data access to the Energy datahub operators. This problem is still currently valid but via the interaction to the end users more urgent needs have been expressed. The current problem description in the BMC has been confirmed by all relevant stakeholders (data owners, TSO/DSO, regulators). It will not be changed (unless some minor definition changes) and will be the main driver for this pilot.

The main story/scenario of the energy data exchange pilot is well understood by the stakeholders. Depending on the focus group, different focus points have been used, but the overall statement of using novel technology to grant data access, manage access rights and create evidence of conducted steps has remained the same. The story line of the data owner being the initiator of the scenario has also been accepted by the wider audience. As a result, the defined scenario is not to be changed and will be demonstrated in final review to the stakeholders.

The current exploitation strategy was defined after 18 months of the SOFIE project. During the testing of the pilot scenario the first priority was to approach the Energy Data operators and digital infrastructure managers rather than end-customers/data owners. The first integration and taking SOFIE adapters to practical use will definitely be the TSO/DSO Tier and only after that the smart grid flexibility service providers will follow. The balance between these two user groups will be investigated during the last year of SOFIE project.

The core technology stack has been selected and implemented. When exchanging information with relevant stakeholders and technology partners, it has been clarified, that the platforms and technology currently in use is very wide (despite the heavily standardized energy sector). In order to cope with this challenge, the flexibility and easy/seamless integration are selected as key parameters, that will affect the future development of the pilot in 2020.

Based on the preliminary market analysis and close cooperation with other EU H2020 energy projects, five main countries (Denmark, Norway, Estonia, Finland, the Netherlands) were selected as primary markets for our pilot. In past 6 months we have narrowed this list down by discarding Norway in the first phase. Depending on the interest from key stake holders from these countries this list can be even shorter. Eventually 2-3 countries will remain in the end of the SOFIE project while others should be shortlisted for further work.

In conclusion, the BMC approach for energy data exchange pilot has really helped to create a clear focus on what we do, who we help and how we plan to go to the market. In upcoming months much effort will be put into validating the technology, integration and business value proposition side and be as active as possible in exploiting the SOFIE results in the energy sector.

Energy data exchange pilot’s Business Model Canvas:

The Problem

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

The Energy Data Exchange Pilot

The pilot furthers the liberation of energy sector data, by providing currently missing building blocks for a future where the energy service providers and consumers have more control, freedom and flexibility over their data. The pilot establishes seamless access to the data with a few clicks done by the data owner (the citizen), regardless of where the person lives or what existing energy networks are in place.

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 is led by Guardtime throughout the project 2018-2020. The data exchange pilot is held in close cooperation with the targeted users’ groups, which will ensure the product-market-fit from the early stage of the development, allows to validate the feasibility in real-life environment, on real on-sites and thereby lay the foundation for scaling and commercial uptake.

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;
- Dashboards for the data owner, national data hub manager and service providers’ premises;
- 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. Also, 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 - we have mapped the key customer segments based on our value proposition and the target market selection is done in parallel with smart grid infrastructure development. The exploitation, and market entry strategy will focus on mature countries where smart meters and national/regional data hubs are in place (Denmark, Norway, Finland, the Netherlands etc.)
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, GSPR related data protection agencies.

Benefits for targeted end-users

- 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;
- Transparent data adaptation layer for IoT platforms and easy to deploy solution to federate heterogeneous IoT environments;
- Immutable blockchain-backed energy consumption readings which are correct beyond dispute;
- Provenance chain throughout the whole infrastructure.

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

Market Trends

- There is an industry-wide agreement to make the make 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.

Pilot outputs

- The solution validated with key stakeholders;
- The technology demonstrated in relevant environment (TRL-6);
- The pilot will set us ready for engaging business stakeholders and start with exploitation activities;
- The primary input for detailed business strategy formulation.

5.2 Energy Flexibility pilot (Engineering)

During the first two years, the focus of the energy flexibility pilot has been to define, validate and demonstrate a scenario in which Electrical Vehicles act as “mobile loads” contributing to:

- Decarbonize cities, improving the usage of EVs;
- Stabilize the network thanks to Demand Response (DR), improving RES usage and thus contributing further to Decarbonization;
- Provide a localized impact, exploiting the mobility of EVs in comparison to stationary storage solutions.

The current scenario has been developed together with relevant stakeholders (DSO, Fleet Manager) and still remains relevant to date. As a result, the defined scenario is not going to be changed.

The exploitation strategy was defined following a multiphase process aimed at: develop and consolidate the result of the research project; validate the developed solution and its replicability; eventually, provide the solution to the potential clients, extending the current offer.

The technology implemented has been designed to be easily integrated with the existing platforms used by the stakeholders, thanks to low coupling and the use of standard formats for the interfaces. This will allow us to reuse as much as possible the software platforms being tested in the pilot also in the case of deployment on third party premises. In conclusion, the approach followed defining the BMC helped to define clearly the pilot objective and the current problems and, as a result, the benefits provided to the end users.

Energy flexibility 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 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 obtain 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 provide energy flexibility by directing the electric vehicles in the areas of interest to charge and, finally, the Energy Retailers, which supply electricity.

The Pilot Objective

The goal is to build a new decentralized, 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 - we have mapped the key customer segments based on our value proposition and the target market selection is done in parallel with smart grid infrastructure development.

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 and stakeholders	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 recharge 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 recharge 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 decentralized blockchain-based marketplace • SOFIE adapters to collect data from DSO's smart meters and fleet managers' EVs and EVSEs

Market Trends

- There is an industry-wide agreement to make the make 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)

Pilot outputs

- The solution designed and validated with key stakeholders;
- The solution deployed in an operational environment (TRL-6);
- The solution replicable and scalable in any microgrid.

5.3 Food Supply Chain pilot (Synelixis)

The BMC of the food supply chain pilot is still valid, as it was defined in the updated version of D6.7. During the second year of the project, the interaction of the technical partners with the end users resulted in the conclusion 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. Furthermore, the end-users have confirmed the two main scenarios of the pilot (as described in D5.2) and the technical design of the pilot software platform have been identified. The implementation has started in M16 and the first on-site demonstration is planned for M27. The concept of the pilot business platform and part of its functionality were demonstrated during the first SOFIE workshop, which was organized as part of the 2019 decentralized conference in Athens. The feedback from attendees and potential stakeholders therein (of both technical and business expertise) confirmed both the importance and the good timing of proposing a decentralized, flexible and secure business platform to transparently collect data from different administrative domains across the supply chain, enable secure information sharing among them and open up opportunities for further analysis of their businesses and interactions. In the third year of the SOFIE project, emphasis will be given in demonstration activities and exploitation opportunities for which the business model canvas will be the main driver.

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. 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 is organized by Synelixis and Optimum with strong involvement of the 7Grapes product association which as end-user and early adopter participates in the definition of end-user requirements and the evaluation of pilot services. On-site testing and demonstration activities are taking place in Kiato area, Greece, mainly during grapes harvesting periods.

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 pay directly 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.

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,

Enabling technologies

- DLT-based identity authentication and role-based control management.

- 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

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

For food consumers:

- increase consumers' visibility about goods production, transportation and processing practices over the whole food supply chain.

- SOFIE adapters to enable a common interface specification upon federation of heterogeneous IoT systems.
- SOFIE interledger protocol to bridge different DLTs.

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-6).

5.4 Mobile gaming pilot (Rovio)

In the objective of mobile gaming's pilot, Rovio emphasizes to experiment and understand whether DLT and IoT can provide new kinds of compelling player experiences. In the current version of the BMC (below) the “benefits” section has been updated in comparison to the initial Model presented in D6.7. Additionally, the benefits of DLT have been modified to be in the form of a hypothesis to be explored, rather than a fact. In addition, minor wording modifications were done throughout the canvas, for better clarity.

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 exciting gaming experiences. There is a high cost to invest 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 cover the costs of integration and implementation.

From a technical perspective we are addressing these 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, 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 and contacts from the game industry. 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 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. Player locations can be verified, reducing the number of cheaters in competitive games.
- Indoor positions, especially altitude information, can be more accurate
- Hypothesis: DLTs can bring transparency and automation to companies participating in an ecosystem for location-based games

Market Trends

- The global number of IoT devices is increasing - can location-based games utilize them?

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.

Pilot outputs

- Results from testing the technical fit and performance of DLT and IoT technologies in mobile gaming. 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.
- A non-commercial scavenger hunt game prototype: an example of a real location-based game that uses beacons for positioning.

6. Standardization

IoT related standardisation suffers from a fragmentation similar to that of the field in general, with tens of competing standardisation organisations and well over a hundred different standards. As is often the case, proper end-to-end security and privacy remain areas with the least amount of interoperability. Moreover, measuring the standardisation contribution is not trivial as the amount of contributions does not always show the real value. Many of the mechanisms that we are using in SOFIE are already being standardized. One of the primary goals in SOFIE is to identify how this project can contribute to ongoing standardisation work in the best possible way, considering the fragmentation, the specific standardisation bodies where partners are active and the pace at which different standards evolve. The main concepts in SOFIE that may influence future standardisation relate to:

- Open, secure federation for decentralized IoT
- The use of Interledger in various use cases, by leveraging on research done in this project as well as concrete results and experiences from SOFIE pilots
- Security and privacy aspects for Interledger

In SOFIE, we have identified W3C Web of Things (WoT) and ETSI PDL ISG (Ericsson is a founding member) as the main standardization groups to liaise with for presentations and potential contributions.

Table 3. Main SOFIE standardization activities

Standardization body	Responsible Partners	Planned areas of contribution
W3C	AALTO, LMF	Security and privacy to WoT IG and WG Participating to the Blockchain and Interledger CGs
ETSI ISG PDL	LMF	Security and privacy aspects. Interoperability, including test and conformance specifications Permissioned adaptations of SOFIE architecture and principles

Other standardization groups on the radar are various IETF/IRTF groups, oneM2M, ETSI M2M and ISO TC307 SG3, AIOTI, with the following identified opportunities for contributions:

Table 4. Opportunities for additional standardization contributions

Standardization body	Responsible Partners	Potential areas of contribution
IETF/IRTF	LMF, AALTO, SYN	Continue co-chairing the IoT directorate and T2TRG Continuing contributions to IRTF T2TRG and IETF CoRE WG Active contribution to any future IoT security & privacy work

ETSI M2M / one M2M	LMF	Protocols/APIs/standard objects based on oneM2M architecture.
ISO	Aalto	ISO TC307, contributions to SG3 security and privacy.
AIOTI	ENG, SYN	ENG is a founding member of AIOTI SYN will contribute to WG 06 Smart Farming and Food Security ENG will contribute to the WG12 Smart Energy

6.1 Presentations to standardization bodies

In February 2018, George Polyzos from AUEB participated in an IRTF pre-standardisation workshop on Decentralized Internet Infrastructure (DINRG, https://trac.ietf.org/trac/dinrg/wiki) and presented SOFIE's ideas on a secure, open, decentralized IoT. The meeting's outcome was that Internet decentralization is a timely topic of interest to the community and thus further meetings of the DINRG were planned.

In October 2019, Vasilios Siris from AUEB participated in the ETSI IoT Workshop that was held in Sophia Antipolis, France. He presented SOFIE's work on the role of Distributed Ledger Technology (DLT) for authorization in environments with constrained IoT devices. The workshop included two sessions on security and privacy in the IoT, which highlighted the interrelation of privacy and trust with the need for information discovery to increase the information's value and the efficient support for a huge number of devices. The above can have a significant influence on standardization.

7. Open data

SOFIE participates in the Open Research Data Pilot. As outlined in 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).

8. Intellectual Property Rights

IPR & future exploitation of results is treated according principles agreed in the Consortium Agreement.

SOFIE open source framework components are 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. Most of the results of the SOFIE project, such as the SOFIE federation framework, will be released under open source license and/or described in scientific publications, allowing also other parties to utilize and exploit them.

9. Monitoring and Evaluation

The results of the communication and dissemination strategy are constantly being monitored in order to assess its effectiveness and progresses, as well as to formulate changes to requirements where necessary. In D6.8 the KPIs for communication activities are compared to the original goals presented in D6.6 (Table 4) to reflect on the progress and assess the progression during the last year of the project.

The table below shows the current achievement of KPI (monitored in January 2020), the predicted outcome for year 2020 and also the total value of KPI's as originally planned in D6.6. The last column evaluates the KPI's current status and explains future action to reach the planned KPI total goal according to the plan presented in deliverable 6.6.

Table 5. SOFIE's KPIs for communication

KPI	Achieved by January 2020	Planned for January – December 2020	Evaluation Planned total KPI by 36 (inlc.)
Publications in peer-reviewed journals and conferences	22	4	Excellent scientific work on IoT environments, blockchain and interledger has been published in journals and conference proceeding. More publications have been approved and will be published soon. Total KPI: 14 (*exceeded*)
Website visitors	5500	6800	The numbers are increasing in correlation with the maturity of the project. Regular content creations will be upheld and boosted to attract more visitors. Total KPI: 12000
Events attended representing the project	23 conferences 3 exhibitions	12 conferences 3 exhibitions	Excellent first two years, mostly due to active participation of research partners in conferences and various academic events. Partners have plans to participate at several conferences in 2020. Total KPI: 35 / 6
Workshops of the project	1	2	One SOFIE workshop successfully completed. Second one planned for M29-30, third one M33-34. Total KPI: 3
Business events and communication	60	20	Good results for first two years and much effort is planned to be dedicated to this activity in 2020. Business networking will intensify during 2020 when (especially)

(including communication with end users)			pilots move more aggressively towards exploitation. Total KPI: 41 (*exceeded*)
Blog posts	19	12	Very good progress that is expected to continue. Total KPI: 31
Followers on social media	254	250	The number of followers is increasing, and the plan is to promote the accounts expand the audience. Total KPI: 500
Liaison and organization of cluster activities (meeting attendance and joint publications)	8	4	Good progress so far, that the project aims to continue. Total KPI: 12
News items on website	7	10	This KPI is on track and will increase during the last year of the project. Total KPI: 17
Mentions of SOFIE in other websites/news items	12	10	Very good progress. This KPI includes news about the project, mentions on partners' websites, cyberwatching.eu profile and SOFIE Workshop on Decentralized 2019 homepage etc. Total KPI: 22

10. Conclusion

The SOFIE project has made good progress during the first two years of the project. Many informational materials have been completed, the website has been built and is constantly updated. The visitor number of the webpage is constantly growing and will hopefully be boosted even more while the project reaches its maturity's peak during the last year. The project has set up social networks and is actively using them. We also have been building meaningful liaisons with other projects, as well as presenting and exhibiting at various events.

During the first two years two open-source codes were released and two more are planned for the last year. Currently the project already has 23 publications, which means that we have exceeded the expected total KPI. SOFIE is also participating in the Horizon 2020 Pilot on Open Research Data and the data related to publications and deliverables has been made available via the project's website.

The exploitation activities have taken off well, especially during the last seven months. The Consortium has identified the SOFIE exploitable foreground the consists of SOFIE framework components, SOFIE federation adapters, and other technologies. All partners are using one or the other component in their exploitation activities. A reference implementation that demonstrates the use of all SOFIE framework components will be published before the end of the first half of 2020. As the commercial exploitation in project is executed through pilots, all SOFIE pilots have compiled Business Models Canvases that they are using to guide and execute their exploitation activities. The partners are actively meeting stakeholders in order to get feedback and improve and validate the Models constantly.

SOFIE's "Communication, Dissemination and Exploitation" work package (WP6) will also produce the following deliverables during the last year of the project:

- D6.9 (December 2020) - Exploitation strategy and roadmap. Report includes the main aspects of projects exploitation during the duration of the project and beyond.
- D6.10 (December 2020) - Business planning. Outlines the main business plans for the three use cases as well as for the general platform for potential other uses.
- D6.11 (December 2020) - Final Report on Communication, Dissemination and Exploitation. Achievements of communication, dissemination, and exploitation during the reporting period.

To sum up, the SOFIE's communication, dissemination and exploitation activities are largely on track. Key targets are expected to be successfully met at the end of this project.