Advanced Secure Cloud Encrypted Platform for Internationally Orchestrated Solutions in Healthcare

Project Acronym: **ASCLEPIOS**
Project Contract Number: **826093**

Programme**: Health, demographic change and wellbeing**
Call: **Trusted digital solutions and Cybersecurity in Health and Care to protect privacy/data/infrastructures**
Call Identifier: **H2020-SC1-FA-DTS-2018-2020**

Focus Area: **Boosting the effectiveness of the Security Union**
Topic**: Toolkit for assessing and reducing cyber risks in hospitals and care centres**
Topic Identifier: **H2020-SC1-U-TDS-02-2018**

Funding Scheme: **Research and Innovation Action**

Start date of project: 01/12/2018 Duration: 36 months

Deliverable:

D7.3 Interim Dissemination, Communication and Stakeholders' Activity Report

Due date of deliverable: 31/05/2020 Actual submission date: 02/06/2020

WPL: SUITE5

Dissemination Level: Public

Version: 1.0

ASCLEPIOS is supported by the H2020 Programme under contract no. 826093

Executive Summary

This deliverable, entitled "Interim Dissemination, Communication and Stakeholder's Activity Report", reports on the dissemination, communication and stakeholders' engagement activities conducted during first reporting period of the project (M1-M18) based on the related strategy and plan outlined in the beginning of the project. This initial plan is revisited and the foreseen activities for the second reporting period are updated based on the assessment of achieved progress until M18.

The overall ASCLEPIOS dissemination and communication strategies are designed in three phases of gradual intensification, covering the whole duration of the project, and following the project's scientific progress and outcomes. Maximum impact in the research and industry communities is promoted, through participation in events, active organisation of workshops and other open activities, scientific publications, establishment of relationships and synergies with the outer world and exploitation of internal partners' infrastructure. Active involvement in standardisation activities and the adoption of existing ones have been identified as key factors for the broader adoption of ASCLEPIOS in the healthcare sector and beyond. The organisation of multiple security awareness courses and the creation and interaction with an active focus group are two actions specifically targeted at stakeholders' engagement. ASCLEPIOS leverages for its communication purposes multiple identified communication channels, conventional and online, to publicise the concept, outcomes and news of ASCLEPIOS.

During the first reporting period ASCLEPIOS **participated in twenty events**, spanning from academic conferences, workshops, seminars and other events, where the partners presented the results of the project. **12 papers** were accepted in **conferences** and **2 journal papers were published**. The **first ASCLEPIOS security awareness workshop, with 23 attendees,** was organised and hosted by Secura in the context of stakeholders' engagement activities, while a **focus group with 4 experts** has been assembled, has already **participated in 2 ASCLEPIOS meetings** and provided valuable feedback. The first steps have been made towards active involvement in ongoing standardisation efforts, with **2 standardisation bodies** contacted and the ongoing participation of ASCLEPIOS partners in **1 online standardisation draft**. Partners have communicated the project's scope to other departments through **5 internal presentations**. The project's vision and results have been communicated to **5 industry communities/organisations,** while **6 synergies** have been established with projects in the same domain with ASCLEPIOS. The website of ASCLEPIOS is regularly updated with new content (having **13 blogposts and 11 news posts** so far) and existing pages are updated to reflect the project's progress. ASCLEPIOS has an active social media presence with **145 accumulative posts** thus far. Finally, communication material, in the form of **1 brochure, 1 poster and 1 eNewsletter,** has been created to support the dissemination and communication purposes of ASCLEPIOS.

The activities planned for the forthcoming period will exploit the foundations set during the first half of the project, i.e., the created connections and synergies, to intensify the project diffusion and maximise its visibility. Communication material will be created and published regularly. Joint activities will be organised with sister projects. Among others, the ASCLEPIOS partners will participate in conferences and publish results in domain-related journals. ASCLEPIOS will organise demonstrator events and awareness workshops.

All dissemination and communication activities performed during the second period of the project will be reported in deliverable D7.5 – "Final Dissemination, Communication and Stakeholders' Activity Report" in M36.

Table of Contents

List of Figures and Tables

Figures

Tables

Status, Change History and Glossary

Status:	Name:	Date:	Signature:
Draft:	Nefeli Bountouni, Evmorfia Billiri	26/05/2020	Nefeli Bountouni
Reviewed:	Silvia Olabarriaga	27/05/2020	Silvia Olabarriaga
Approved:	Tamas Kiss	02/06/2020	Tamas Kiss

Table 1: Status Change History

Version	Date	Pages	Author	Modification
v0.1	17/02/2020	13	SUITE5	ToC
v0.2	08/05/2020	76	SUITE5	First Input
v0.3	11/05/2020	84	Secura B.V.	Added Contribution – Sections 6.4 and 7.3
v0.4	22/05/2020	84	SUITE5	Incorporation of Activity Templates from all Partners
v0.5	25/05/2020	86	SUITE5	Polishing of Contributions and Addition of Annexes
v0.6	26/05/2020	86	SUITE5	Final Draft Version
v0.7	27/05/2020	86	AMC	Internal Review
v0.8	29/05/2020	85	SUITE5	Further Input by partners revised
v0.9	01/06/2020	84	SUITE5	Version responding to review process comments
v1.0 final	02/06/2020	83	SUITE5	Final Version to be submitted to the EC

Table 2: Deliverable Change History

Glossary

CSA	Coordination and Support Actions
DoA	Description of Action
Dx.x	Deliverable x.x
EC	European Commission
IT	Information Technology
KPI	Key Performance Indicator
Mxx	Month xx
TBA	To Be Announced
TBD	To Be Determined
Tx.x	Task x.x
WPx	Work Package x

Table 3: Glossary

1 Introduction

1.1 Purpose of Deliverable and Relation to Other WPs

The present deliverable is released within the context of WP7 – "Dissemination, Exploitation and Communication". WP7 runs through the whole project and ensures the wide and timely diffusion of information about the project and the generated results, setting the scene for the future exploitation and sustainability of the projects results.

The scope of deliverable D7.3 is to present any updates on the initial dissemination and communication strategy, along with specifying new actions and activities to be performed during the second period of the project and identifying opportunities for the project's diffusion. D7.3 also constitutes the interim report of the dissemination, communication and stakeholders' engagement activities performed during the first reporting period of the project, until [M18]. The plan will be continuously revised until the end of the project, with the assistance of the collaborative activities' identification spreadsheet, aiming for the timely identification and response to emerging opportunities.

D7.3 is associated in particular with the activities of tasks T7.1 – "Dissemination, Clustering and Standardization Activities", T7.2 – "Communication Activities", T7.3 – "eHealth Cyber Security Industrial Focus Group" and T7.6 - "Training Courses to Raise Security Awareness". It is based on previous deliverables of the WP7 and more specifically on the initial dissemination and communication plan, as devised in the context of D7.1 – "Plan for Project's Dissemination, Communication and Stakeholder's Plan". The communication and dissemination activities of the second reporting period will follow the updates plan outlined in D7.3 and their outcomes will be documented in D7.5 – "Final Dissemination, Communication and Stakeholders' Activity Report" in [M36].

1.2 Structure of Document

The remainder of the deliverable at hand is structured as follows:
Section 2 outlines the objectives and strategy underlying the ASCLEPIOS dissemination, communication and stakeholders' engagement activities. A set of appropriately defined performance indicators for the quantification of activities intensity and assessment of the achieved impact has been established and is presented along with any required updates.

Section 3 reports on the related activities undertaken until M18 of the project. The section encompasses the achieved progress thus far, as indicated through the presented values of the communication and dissemination metrics in M18, in comparison to the target values for the first reporting period. An extensive overview of the conducted activities is also provided. These refer to the various mechanisms identified in the initial planning: dissemination events in which the project participated, publications, standardisation and community building, any published communication material, the ASCLEPIOS online presence and finally the conducted awareness workshops and activities of the focus group.

Section 4 presents the planning for the dissemination, communication and stakeholders' engagement activities that will take place during the second reporting period of the project. It provides the overall target values of the performance indicators for the whole project, as well as the updated values for M19 to M36, based on the progress of the first reporting period. Upcoming communication and engagement actions are detailed, along with a list of identified events and opportunities.

Finally, Section 5 summarises the document, outlining the key takeaways, and the Annexes present the templates and spreadsheets used within the project for better coordination of the related activities, a list of reached industry communities and the full versions of the ASCLEPIOS communication material.

2 Overall Dissemination and Communication Approach

From a technical perspective, ASCLEPIOS aims to provide services for the secure storage and handling of healthcare data on cloud infrastructures, by employing modern encryption techniques, providing advanced access control mechanisms and secure analytics services.

To maximise the adoption and future exploitation of its technical outcomes, ASCLEPIOS shall undertake the appropriate dissemination and communication activities that will help reach its target audience and engage the relevant stakeholders. Furthermore, ASCLEPIOS aspires to raise security awareness in the healthcare sector through a number of targeted activities, such as workshops and training sessions. In the context of WP7, and in particular with respect to dissemination and communication, the following objectives have been identified:

- Submission of publications based on project results and related work in international conferences and journals. Other interested parties could also be involved and collaborate.
- Establishment of full online presence for the presentation of results and continuous participation of both project-related partners and the broader community.
- Participation of ASCLEPIOS in events evolving around domains of interest to the project, such as health informatics and IT security.
- Establishing a channel of communication between the project and relevant domain experts though an eHealth Cyber Security focus group.

An important task for the planning of dissemination, communication and exploitation, was the identification of the entities at which these activities should be targeted. These could be individuals, groups or organisations, which altogether comprise the potential ASCLEPIOS target audiences due to their specific interest in the project. A list of target groups along with their relation to the project has already been assembled in the context of D7.1 and is presented in Table 2-1

Table 2-1 Target Audiences for Dissemination and Communication

Target Group	Interest in the Project
A – Industry: healthcare providers, healthcare system vendors, data handling organisations (providers, brokers, collectors and processors), cloud platform providers, medical device manufacturers and vendors	• Utilisation of project's results in business operations • Strengthened innovation by blending with in-house artefacts • Training based on the project's outcomes • Participation in the project's events • Exploitation of project's open source results • Inspiration for new ideas and application

B - Researchers and Academia: Individual researchers engaged in research initiatives and/or working in research organisations relevant to the project's interest domains	• Further advancements in a series of research domains – e.g. Healthcare analytics, Data management, Data security – through extension / reuse of the project's outputs • Inspiration for future research initiatives based on the project's concept and results • Participation in the project's events
C - Industry Associations & Technology Clusters: European initiatives and clusters (e.g. IMIA (International Association of Engineering Insurers), EFMI (European Federation for Medical Informatics), FIWARE)	• Inclusion of project's results in collaborative research activities (roadmap, white papers, position papers) • Dissemination of project's results to members • Bilateral participation in events for knowledge exchange
D – Standardisation Organisations: ISO (International Organisation for Standardisation), IEC (International Electrotechnical Commission), TCG (Trusted Computer Group), etc.	• Inputs for standardisation activities • Identification of common topics • Contribution to events
E – Policy Makers: EC Directorates/ Units, Governments and Governmental Organisations, Regulatory Agencies, etc.	• Evaluation of the project's Social-Technological-Economic-Environmental-Political aspects • Definition of future research and innovation directions for the EC initiative "Digitizing the European Industry" considering the project's acquired knowledge and experience
F - Individuals providing personal, health, activity and other sensitive data as prerequisite for receiving several types of services	• Understand the way their personal data are used in a secure and trustful manner • Learn about novel technological advancements for healthcare data protection

The dissemination and standardisation strategy is driven by the objective to maximise the outreach of the project's scientific and technological results within and outside the consortium. These results shall be spread to the identified audiences, in order to be validated and assessed for their broad applicability, based on attained feedback. Knowledge and innovation exchange with other projects, as well as further involvement in new initiatives, are also within the scope of dissemination. Standardisation will facilitate the adoption of ASCLEPIOS outcomes from different environments (cross-border and cross-community). Lastly, the dissemination activities will support the exploitation strategy, as they will engage possible users and clients and consequently mobilise relevant market segments.

The dissemination and standardisation strategy is deployed in three phases covering the whole duration of the project, namely: Raise Awareness, Inform and Interact, Promote. Each phase comprises a number of dissemination mechanisms, realised through multiple actions.

The dissemination plan is dynamically adapted after the completion of each phase, where an evaluation of the achieved progress shall be performed. All partners are involved in dissemination, with each one directing efforts towards the most relevant target audiences; healthcare partners target the healthcare sector, while academic and research partners focus on engaging other research organisations across Europe. Regarding the content and intensity of the dissemination activities, they follow the expected progress of the project. During the first phase [M1-M12], the activities are mainly content-oriented and of moderate intensity. Focus is on introducing the project's concept, drive and ambition to the target audiences. The project outreach is enhanced via appropriate key messages. Early networking and establishment of communication channels are foreseen, to later provide the necessary environment for successful diffusion of actual results and knowledge within and beyond the consortium. As the project evolves, in the second and third phase ([M13-M24 and [M25-M36] respectively) the activities become more result-oriented, demonstrating high intensity. Both interactive and non-interactive activities are included depending on the most appropriate approach towards each target audience. The first tangible outcomes of ASCLEPIOS are expected in Year 2. Phase II of dissemination activities runs in parallel to the second year of the project, being therefore responsible for exhibiting these results to the community through events and publications. Liaisons with other initiatives, projects, external organisations, and interdepartmental collaborations initiated in the first phase will be intensified and put into action. Knowledge and innovation transfer, and attaining useful feedback for validation of results, are among the dissemination objectives addressed in this phase. Finally, the third phase of dissemination and standardisation [M25-M36] is focused on creating the necessary conditions for the exploitation of the project's products and results. Phase III lasts the whole third year of the project. Demo presentations, workshops and training sessions will be employed, in order to familiarize potential adopters with the ASCLEPIOS solution. This phase is targeted mainly at attracting potential users and clients, ensuring broad applicability and acceptance, and stimulating the appropriate market segments.

An early standardisation plan is also outlined from the onset of the project. Adoption and compliance to existing security standards as well as incident management directions will promote further adoption of ASCLEPIOS. Active contribution of ASCLEPIOS in healthcare and security standardisation bodies will help leverage findings to enhance cross-fertilization in the domain of healthcare and security. Partners already involved in standardisation, research and security organisations, shall ensure the effective downstream of results into standards. Standardisation activities are part of the dissemination plan.

The ASCLEPIOS communication strategy aspires to raise awareness and promote public interest in the project, while playing a supportive role in dissemination and exploitation, which take place concurrently. Potential adopters/users will be informed of the project's concept, goals and results through multiple means of communication, including key messages and relevant material. Another objective is the mobilisation of an active community. This group will not only form a pool of potential users but will also provide feedback throughout the project, via the two-way communication channels made available. Communication channels and content, constantly updated and enriched with the latest project's results, will also be adapted to community needs and emerging trends.

The communication strategy is structured in three phases of gradually increasing intensity, following the progress of the project. The three communication phases run in parallel to dissemination and are the following: Raise Awareness, Diffuse Knowledge, Intensify Communication.

The communication plan is adapted after the end of each phase, where the effectiveness of taken actions is evaluated and forthcoming activities and targets are appropriately adjusted. A social media strategy has been designed to make the most of the available channels, while the regular update of communication material and content with the commitment and contribution from all partners is considered essential for the success of the overall

communication task. The communication plan follows the project's progress; from increasing awareness in the beginning of the project, to providing actual knowledge on results and supporting exploitation towards the end of it.

More specifically, Phase I [M1-M12] covering the first year of ASCLEPIOS, includes all preparatory actions to establish the project's identity and make its presence felt through available media. Furthermore, the website and social media accounts constitute a bilateral communication channel with the broad community, both for broadcasting and receiving information. Moving on to the second year of the project, the communication efforts of Phase II become more substantial, as they are backed up with actual project outcomes. Communication material and media will be updated accordingly to reflect the latest progress and will be used supportively in dissemination activities. Liaisons, events and other important news regarding dissemination shall be fed back into available media. This phase is also related to actively engaging as many members of the community as possible. Interaction with the public through public comments or private messages will be encouraged and intensified. Finally, Phase III [M25-M36] is planned for the last year of the project. Its main focus is the preparation of the ground for the exploitation. The developed ASCLEPIOS solution shall be demonstrated and promoted through the online media. The business case, developed in parallel exploitation-related activities, shall also provide input for the communication mechanisms. The frequency of posts and updates reflect exactly this intention to intensify communication and build strong ties with potential adopters and clients.

Various mechanisms and conduits have been identified for the realisation of the project's dissemination and communication aims, with their main objective being the generation of publicity for the project in the scientific and industrial community, as well as in other targeted audiences. These dissemination and communication mechanisms include:

- organisation of project events (including the organisation of security awareness courses),
- participation in conferences and workshops,
- dissemination of scientific results in relevant journals and conferences, in alignment with the EC Guidelines on Open Access to Scientific Publications and Research Data in Horizon 2020,
- creation and distribution of communication material (such as brochures, newsletters etc.),
- circulation of press releases,
- deployment and continuous update of the project's website as main online information point, as well as the integration of a blogging space for the communication of scientific results in a reader-friendly manner for the general public,
- maintenance of an active social media presence,
- establishment of synergies with other projects,
- community building with stakeholders (including the engagement of stakeholders through the focus group activities),
- diffusion of results and news in the internal networks of the project partners, as for example in other departments,
- contribution to standardisation efforts

These mechanisms are integrated in the communication and dissemination strategies, which foresee the gradual intensification of their use as well as the evolution of the disseminated content, following the progress of the project.

For progress evaluation purposes, a set of measurable evaluation indicators has been derived from the key mechanisms that implement the dissemination and communication objectives of the project. This list was included in the initial plan of D7.1 along with the total and intermittent target values for each indicator. In the context of this deliverable, the actual achieved values for the period [M1-M18] are presented in the reporting section and the target values for the second period are updated accordingly in the planning section, in order to finally add up to the desired total in [M36].

Table 2-2 WP7 Measurable Indicators and Target Total Values for M36 according to DoA

Measurable Indicator	M1-M18	M19-M36	Total
Number of workshops organised	1	2	3
Number of demo events organised	0	3	3
Number of European healthcare professionals reached by various ASCLEPIOS events	200	1.000	1.200
Number of unique stakeholders (IT security professionals, IT specialists in hospitals and healthcare institutions, healthcare professionals) reached by the ASCLEPIOS demonstrators	20	100	120
Number of events where ASCLEPIOS has participated	5	15	20
Number of events attended where ASCLEPIOS has a presentation	2	8	10
Number of project's demo booths	0	1	1
Number of conference papers	6	14	20
Number of journal papers submitted	0	10	10
Number of articles in corporate magazines	0	5	5
Number of unique industry contact points	30	70	100
Number of industry communities informed about the project	2	3	5
Number of webinars	0	3	3
Number of synergies with other projects	2	6	8
Number of joint activities (with other projects)	1	4	5
Number of internal partners' events / presentations	3	7	10
Number of links to the project's website	5	25	30
Number of training sessions	0	3	3
Number of standardisation working groups contacted	1	2	3

Number of individually or jointly submitted draft standardization documents	0	>=2	>=2
Number of blueprint documents of developed security enablers	0	>=3	>=3
Number of project's presentations in standardisation meetings	0	1	1
Number of unique visitors in the project's website	1.500	3.500	5.000
Average duration of visits in the project's website	1 min	2 min	-
Number of views of the project's website	2.000	8.000	10.000
Number of accumulative followers in social media	200	800	1.000
Number of accumulative posts in social media	100	300	400
Number of blogposts	18	18	36
Number of press releases	2	3	5
Number of project's factsheets / brochures and banners	2	3	5
Number of e-Newsletters	2	4	6
Number of videos	1	1	2
Number of blog posts in EC dissemination mechanisms	2	4	6

3 Activities Reporting [M1-M18]

In terms of dissemination, ASCLEPIOS showcased a very active presence in the academic field, participating in a multitude of events and conferences. The ASCLEPIOS partners communicated the core concept of the project to researchers and members of the academia, but also presented some of the key initial research results to the community through a number of academic publications. Liaisons with other projects have been established, creating the foundations for the organisation and conduction of joint activities in the upcoming period, while some initial steps towards standardisation were taken.

ASCLEPIOS has achieved a strong online presence with regular posting of content in the established social media channels (Twitter and LinkedIn), and ongoing updates of the project's website. A number of traditional media such as industry magazines and EC dissemination mechanisms have also been employed for the promotion of ASCLEPIOS activities. The first issues of communication material have been produced to facilitate the communication objectives of ASCLEPIOS.

3.1 Dissemination and Standardisation Activities Performed in [M1-M18]

3.1.1 Events/Conferences/Workshops

3.1.1.1 Participation in Conferences and Workshops

The participation of ASCLEPIOS in some of the most prominent conferences and events in related scientific and industry fields is a key part of the project's dissemination activities. Identified scientific fields of interest to ASCLEPIOS included, but were not limited to: biomedicine, cybersecurity and encryption and cloud computing. ASCLEPIOS's presence in these events has initiated interactions and exchange of knowledge with the community and fuelled networking, while keeping the consortium informed with the latest advances in technology.

Participated in 11 Conferences
Representation of ASCLEPIOS in 5 Workshops
1 Seminar Attended
Took Part in 3 Events of Other Types[1]

In some of these events, the partners presented the scope and vision of ASCLEPIOS, increasing awareness about the project, while in others, project participation was enhanced by the publication of conference papers, thus promoting the project's scientific results and progresses. Events of other types were also attended where ASCLEPIOS was represented, such as university-hosted seminars and workshops and roundtable discussions, which enabled face-to-face interactions with other researchers, academia and key persons in the field of cybersecurity. Please note that the presentation of ASCLEPIOS by HTW in the context of the "HTW Symposium "Kreativität + X = Innovation" is included in the table with the participated events, but is not counted in the respective KPIs, as it took place before the project's official beginning. Unfortunately, "Multi-Clouds and Mobile Edge Computing Workshop (M2EC), 34th International Conference on Advanced Information Networking and Applications (AINA 2020)" where an ASCLEPIOS paper was accepted, was cancelled due to COVID19 crisis. We have it listed for completeness, but do not count it in the relevant KPIs.

[1] E.g. roundtable discussion, social evening talk, etc.

Figure 3-1 Highlights from ASCLEPIOS in events: SAC 2019 (up-left), Healthcom 2019 (up-right), ICT Security World (bottom-left), NordSec 2019 (bottom-right)

Table 3-1 Events ASCLEPIOS Participated during [M1-M18]

Date	Place	Event Name	Type	Action	Participating Partner
November 2018	Berlin, Germany	* HTW Symposium "Kreativität + X = Innovation	Other	Project Presentation	HTW
April 8-12, 2019	Limassol, Cyprus	34th ACM/SIGAPP Symposium on Applied Computing (SAC 2019)	Conference	Paper	TUNI
June 12-14, 2019	Ljubljana, Slovenia	11th International Workshop on Science Gateways (IWSG 2019)	Workshop	Paper	UOW
June 11, 2019	Brussels, Belgium	Roundtable EU Event	Other	Project Communication/ Networking	TUNI
June, 2019	Berlin, Germany	Long Night of Sciences Berlin 2019	Other	Project Communication/ Networking	HTW
July 23-27, 2019	Berlin, Germany	IEEE Engineering in Medicine and Biology Society: Workshop (EMBS 2019)	Conference with Workshops	Project Communication/ Networking	CHARITE
August 19-24, 2019	Beijing, China	ACM Special Interest Group on Data	Conference	Poster	RISE

		Communication (SIGCOMM 2019)			
September 19, 2019	Helsinki, Finland	ICT 2019 Proposers Day	Conference	Networking	SUITE5
September 19-20, 2019	London, UK	RE-WORK Deep Learning Summit 2019	Conference	Networking	SUITE5
October 10, 2019	Florida, USA	Florida Institute for Cybersecurity Weekly Seminar (FICS)	Seminar	Paper and project presentation	AMC
October 14-16, 2019 -	Bogota, Colombia	IEEE International Conference on E-health Networking, Application & Services (Healthcom 2019)	Conference	Paper	AMC
October 23, 2019	Orlando, USA	15th EAI International Conference on Security and Privacy in Communication Networks (SecureComm 2019)	Conference	Paper	TUNI
November 11, 2019	London, UK	ACM Cloud Computing Security Workshop (CCSW 2019)	Workshop	Short Paper	UOW
November 12-14, 2019	Dallas TX, USA	IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN 2019)	Conference	Paper	RISE
November 14, 2019	Athens, Greece	5th ICT Security World: Digital transformation & Cybersecurity	Symposium / Conference	Project presentation and panel discussion	ICCS
November 18-20, 2019	Aalborg, Denmark	24th Nordic Conference on Secure IT Systems (NordSec 2019)	Conference	Paper	TUNI
December 11, 2019	London, UK	Knowledge Technical Social evening talk at University College London	Other	MiCADO[2] presentation	UOW
February 20, 2020	London, UK	2nd Annual Research Software London Workshop (RSLondonSouthEast 2020)	Workshop	MiCADO presentation	UOW
March 3, 2020	London, UK	UKRI Cloud Workshop 2020	Workshop	Lightning talk	UOW
March 11-13, 2020	Kiel, Germany	Biosignal Conference by DGBMT / VDE (BIOSIGNALE 2020)	Conference	Networking	CHARITE
April 15-17, 2020 - CANCELLED	Caserta, Italy	Multi-Clouds and Mobile Edge Computing Workshop	Workshop	Paper	ICCS

[2] https://micado-scale.eu/

		(M2EC), 34th International Conference on Advanced Information Networking and Applications (AINA 2020)			
May 7-9, 2020	Prague, Czech Republic / online	5th International Conference on Internet of Things, Big Data and Security (IoTBDS 2020)	Conference	Paper	TUNI

3.1.1.2 Organisation of Project Events

The organisation of informative and training sessions is of paramount importance in the context of raising cyber security awareness among stakeholders in the healthcare sector (patients, healthcare and IT personnel, cloud and third-party providers).

1 Awareness Workshop with 23 Attendees Organised

During the first reporting period, the **first ASCLEPIOS awareness workshop** has been organised and hosted by SECURA on January 16th 2020, in its premises in Amsterdam. The workshop themed "Protecting vital assets, the art and science of working with medical data", focused on the limitations concerning the handling of sensitive patient's medical data and how ASCLEPIOS attempts to solve these. The workshop admission was free of charge and had the goal of bringing together both technical and non-technical personnel involved with medical data processing. The impact and results of the workshop are detailed in the dedicated section 3.3.2.

Figure 3-2 1st ASCLEPIOS Awareness Workshop

3.1.2 Publications

During the first reporting period of the project, several scientific publications by the partners of the ASCLEPIOS project were accepted both in conferences and journals.

2 Journal Papers Published
12 Conference Papers Accepted

These publications are a means of diffusing the project outcomes to the scientific community and contributing to the broader research. Furthermore, they act as an instrument of verification and validation of the project's results and findings. The published papers evolve around the development and validation of the novel encryption schemes and security protocols, which will be the foundations of the final solution provided by ASCLEPIOS in the end of the project.

In alignment with the EC Guidelines on Open Access to Scientific Publications and Research Data in Horizon 2020, ASCLEPIOS followed a combination of Gold and Green Open Access strategy to its scientific publications. One publication is Gold Open Access, while the rest of the publications were granted Green Access. A ZENODO repository (url: https://zenodo.org/communities/asclepios-project-h2020/?page=1&size=20) and a project page in ResearchGate (url: https://www.researchgate.net/project/ASCLEPIOS-Advanced-Secure-Cloud-Encrypted-Platform-for-Internationally-Orchestrated-Solutions-in-Healthcare) are used complementary to the website of the project, for sharing publications and deliverables with the research and academic community.

Table 3-2 ASCLEPIOS Publications [M1-M18]

Date	Publication Type	Title	Authors	Conference/Journal Name	Contributing Partner
2019	Conference	The Lord of the Shares: Combining Attribute-Based Encryption and Searchable Encryption for Flexible Data Sharing	Michalas, A.	34th ACM/SIGAPP Symposium On Applied Computing (SAC 2019)	TUNI
2019	Conference	A Secure Cloud-based Platform to Host Healthcare Applications	Pierantoni, G., Kiss, T., Terstyanszky, G., Dang, H., Delgado Olabarriaga, S., Tuler de Olivera, M., Yigzaw, K. Y., Belika, J. G., Krefting, D., & Penzel, T	11th International Workshop on Science Gateways (IWSG 2019)	UOW, AMC, NSE, HTW, CHARITE
2019	Conference	Protecting OpenFlow Flow Tables with Intel SGX.	Paladi, N., Svenningsson, J., Medina, J., & Arlos, P.	ACM Special Interest Group on Data Communication (SIGCOMM 2019)	RISE
2019	Conference	Red Alert: Break-Glass Protocol to Access Encrypted Medical Records in the Cloud	T. de Oliveira, M., Michalas, A., Groot, A., Marquering, H. A., & Olabarriaga, S.	IEEE International Conference on E-health Networking, Application & Services (Healthcom 2019)	AMC, TUNI
2019	Conference	Modern Family: A Hybrid Encryption Scheme Based on Attribute-Based	Bakas, A., & Michalas, A.	15th EAI International Conference on Security and	TUNI

		Encryption, Symmetric Searchable Encryption and SGX		Privacy in Communication Networks (SecureComm 2019)	
2019	Conference	Access Control in Searchable Encryption with the Use of Attribute-based Encryption and SGX	Michalas, A., Bakas, A., Dang, H. V., & Zalitko, A.	ACM Cloud Computing Security Workshop (CCSW 2019)	TUNI, UOW
2019	Conference	Protecting OpenFlow using Intel SGX	Medina, J., Paladi, N., & Arlos, P.	IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN 2019)	RISE
2019	Conference	MicroSCOPE: Enabling Access Control in Searchable Encryption with the use of Attribute-based Encryption and SGX	Michalas, A., Bakas, A., Dang, H. V., & Zalitko, A.	24th Nordic Conference on Secure IT Systems (NordSec 2019)	TUNI, UOW
2020	Conference	A generic cloud-agnostic platform to support the execution of deadline-constrained workloads	Ullah, A., Deslauriers, J., & Kiss, T.	2nd Annual Research Software London Workshop (RSLondonSouth East 2020)	UOW
2020	Conference	Deploying and auto-scaling scientific applications in the cloud using Terraform and MiCADO	Ariyattu, R., Deslauriers, J., & Kiss, T.	2nd Annual Research Software London Workshop (RSLondonSouth East 2020)	UOW
2020	Conference	A context-aware security model for a combination of attribute-based access control and attribute-based encryption in the healthcare domain	Psarra, E., Verginadis, Y., Patiniotakis, I., Apostolou, D., & Menztas, G	Multi-Clouds and Mobile Edge Computing Workshop (M2EC), 34th International Conference on Advanced Information Networking and Applications (AINA 2020) – event cancelled, but papers published in WAINA 2020 https://link.springer.com/chapter/10.1007/978-3-030-44038-1_104	ICCS
2020	Conference	Do not tell me what I cannot do! (The constrained device shouted under the cover of the fog):	Frimpong, E. Bakas, A., Dang, H-V., & Michalas, A.	5th International Conference on IoT, BigData and Security (IOTDBS 2020)	TUNI, UOW

		Implementing Symmetric Searchable Encryption on Constrained Devices			
2019	Journal	Network Physiology in Insomnia Patients: Assessment of Relevant Changes in Network Topology with Interpretable Machine Learning Models	Christoph, J., Penzel, T., Hodel, S., Breuer, S., Spott, M., & Krefting, D.	Chaos: An Interdisciplinary Journal of Nonlinear Science	CHARITE, HTW
2020	Journal	A Break-Glass Protocol based on Ciphertext-Policy Attribute-Based Encryption to Access Medical Records in the Cloud	T. de Oliveira, M., Bakas, A. Frimpong, E., Groot, A., Marquering, H.A, Michalas, A., & Olabarriaga, S.	Annals of Telecommunications (2020)	AMC, TUNI

3.1.3 Community Building, Synergies and Internal Dissemination

The creation of a scientific and industry community around the project, even from its early stages, is of great importance for the wide adoption of the project outcomes and the attraction of potential future clients. It is also a means of validation of project results.

Synergies Established with 6 Projects
5 Industry Communities Reached
20 Links from Partners' Networks to ASCLEPIOS
Organised 5 Internal Events

During the first reporting period, ASCLEPIOS joined forces with other European projects in the domain of security in the healthcare domain, in the context of **H2020 Synergy**[3], which aims to increase cross-project collaboration and promotion of results. The H2020 Synergy initiative comprises the following projects in the domain of cybersecurity in healthcare: ASCLEPIOS, CUREX[4], FeatureCloud[5], Panacea[6], SAFECARE[7] and SPHINX[8]. ASCLEPIOS is in touch with the European observatory of research and innovation in the field of cybersecurity and privacy, Cyberwatching.eu,[9] and is already part of its online hub for cybersecurity and privacy projects (url: https://cyberwatching.eu/projects/2012/asclepios).

Additionally, the first steps have been made towards actual exchange of knowledge and results with other projects, including COLA (ASCLEPIOS services will be deployed on MiCADO[10] the exploitable asset of project COLA: an open-source multi-cloud orchestration and auto-scaling framework for Docker containers, orchestrated by Kubernetes) and MELITY[11] (with the participation of a MELITY project partner in the ASCLEPIOS Focus Group).

A number of unique industry contact points with key players in the domains of cloud technologies, secure analytics and hardware have been created after communication actions

[3] https://mailchi.mp/bcc06f9a3f59/h2020-synergy-newsletter
[4] https://curex-project.eu/
[5] https://featurecloud.eu/
[6] https://www.panacearesearch.eu/
[7] https://www.safecare-project.eu/
[8] https://sphinx-project.eu/
[9] https://cyberwatching.eu/
[10] https://micado-scale.eu/
[11] https://melity.cs.unipi.gr/en/

performed by the ASCLEPIOS partners, aiming for knowledge exchange to facilitate the project's research and development activities.

UOW organised an initial on-line meeting with the REMEDI project[12] to discuss synergies. Both projects presented their aims and work and it was agreed that potential joint funding opportunity will be pursued. This is currently under investigation. The participation of ASCLEPIOS in REMEDI, an evidence-based community focusing on medical device informatics, will boost the outreach of ASCLEPIOS to healthcare personnel that are part of the community and increase the visibility of the project to national organisations (e.g. AAMI[13], ASHP[14], The Joint Commission[15] etc.), while the meetings and virtual conferences held by the community will serve as a means of results' validation. The full list of reached communities and conducted activities can be found in Annex II. Industry Communities/Organisations

Finally, the internal networks and infrastructures of partners have been exploited both for the employment of existing communication channels and for the accommodation of the ASCLEPIOS dissemination activities, such as the organisation of workshops in the partners' premises. Several posts have been published in the partners' communication channels, outlining the project's scope and their involvement and containing links back to the official ASCLEPIOS website (Table 3-3).

Table 3-3 Mentions and Links to ASCLEPIOS Website from Partners' Networks

#	Entry Description	URL	Contributing Partner
01	ASCLEPIOS Project description	https://www.suite5.eu/asclepios	Suite5
02	ASCLEPIOS Project description	http://imu.ntua.gr/project/asclepios	ICCS
03	ASCLEPIOS Project description and involvement of ICCS	https://www.ece.ntua.gr/en/article/303	ICCS
04	ASCLEPIOS Project description	https://ehealthresearch.no/en/projects/advanced-secure-cloud-encrypted-platform-for-internationally-orchestrated-solutions-in-healthcare-asclepios	NSE
05	ASCLEPIOS Project blogpost	https://ehealthresearch.no/en/news/2019/secure-e-health-in-the-cloud	NSE
06	ASCLEPIOS Kick off Press Release by SECURA	https://www.secura.com/C789-Press-release---Secura-joins-the-international-H2020-ASCLEPIOS-project-4.html	SECURA
07	1st ASCLEPIOS Awareness Workshop by SECURA	https://www.secura.com/asclepios-awareness-workshop	SECURA
08	ASCLEPIOS Kick off Press Release by AMC	https://www.ebioscience.amc.nl/2019/02/06/asclepios-project-started/	AMC
09	Link to blogpost "Stroke acute care: ASCLEPIOS demonstrator"	https://www.ebioscience.amc.nl/2019/07/25/stroke-acute-care-asclepios-demonstrator/	AMC

[12] https://www.purdue.edu/discoverypark/rche/centers/remedi/remedi-overview.php
[13] https://www.aami.org/
[14] https://www.ashp.org/?loginreturnUrl=SSOCheckOnly
[15] https://www.jointcommission.org/

10	ASCLEPIOS Project thumbnail	https://HTW.htw-berlin.de/en/projects	HTW
11/ 12	2 x links to ASCLEPIOS (kickoff and plenary meeting entries)	https://HTW.htw-berlin.de/en/news	HTW
13	Project description	https://research.tuni.fi/nisec/projects/	TUNI
14	Plenary Meeting @Limassol News entry	https://research.tuni.fi/nisec/event/event-example/	TUNI
15	Short project description	https://www.westminster.ac.uk/research/groups-and-centres/centre-for-parallel-computing/projects	UOW
16	Mention in Kiss T. (UOW) About page	https://www.westminster.ac.uk/about-us/our-people/directory/kiss-tamas	UOW
17	Announcement of the start of the ASCLEPIOS project:	https://www.westminster.ac.uk/news/university-of-westminsters-centre-for-parallel-computing-awarded-major-funding-to-investigate?fbclid=IwAR06ysXQBSZ2taYs7wlehqpST8XT9UVC1oo1pzNLbi7P5LtsJCUW-nFxDgQ	UOW
18	Mention in Pierantoni G. About page	https://www.westminster.ac.uk/about-us/our-people/directory/pierantoni-gabriele	UOW
19	ASCLEPIOS Project description	https://www.ri.se/en/what-we-do/projects/advanced-secure-cloud-encrypted-platform-internationally-orchestrated	RISE
20	ASCLEPIOS Project Kickoff	https://www.ubitech.eu/ubitech-participates-in-the-asclepios-research-and-innovation-action-on-secure-cloud-encrypted-solutions-for-healthcare/	UBITECH

Internal presentations of ASCLEPIOS to other departments and employees not directly involved in the project led to sharing of know-how and ideas and facilitated the research objectives of the project with the help of questionnaires. The internal events that took place during the first reporting period are enlisted in Table 3-4.

Table 3-4 Internal ASCLEPIOS Events in [M1-M18]

Date	Place	Event Description	Activity	Audience	Participating Partner
April, 2019	Berlin, Germany	Inauguration of the IT-Security Lab at the HTW Berlin[16]	Poster Presentation	40-50	HTW
September, 2019	Online	MiCADO webinar	Presentation of MiCADO	65	UOW
November, 2019	Limassol, Cyprus / Online	Internal Presentation	ACLEPIOS Presentation	20	SUITE5
March/April 2019	Amsterdam, Netherlands	Presentation at Biomedical Engineering Department	ASCLEPIOS Pitching and Questionnaires/Surveying for WP1 activities	23	AMC

[16] https://www.htw-berlin.de/en/

February, 2020	Tromsø, Norway	Weekly lunch seminar	Presentation to Employees with medical and technical background	10 – 15	NSE

3.1.4 Standardisation

ASCLEPIOS aims to contribute to standardisation efforts, recognising the importance of common standards in achieving cross-border and cross-community collaboration in cyber security.

2 Standardisation Bodies Contacted
Ongoing Participation in 2 Standardisation Efforts

Interested partners have showed interest in such efforts and approached the leading standardisation groups already from the initial stages of the project. In particular, RISE in collaboration with the Internet Engineering Task Force[17] is currently working towards contributing to the Trusted Execution Environment Provisioning Architecture active online draft[18]. Secondly, CHARITE in conjunction with the standardisation body for mathematical informatics in Germany (DIN NAMed[19]) is developing encryption requirements for telemedicine in general, and for sleep medicine in particular with the German Society for Sleep Medicine (DGSM[20]). The adoption of popular standards in the project also plays an important role in the applicability of results outside the closed-project environment and demonstrators and will contribute to the exploitation and sustainability after the project's end.

Table 3-5 Standardisation-Related Activities

Standartisation Body	Sector	ASCLEPIOS involvement	URL	Involved Partner
OASIS	Information Technology	Adoption of XACML v3.0 OASIS Standard	http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html	ICCS
OASIS	Information Technology	Adoption of TOSCA OASIS Standard	https://docs.oasis-open.org/tosca/TOSCA-Simple-Profile-YAML/v1.3/TOSCA-Simple-Profile-YAML-v1.3.pdf	UOW
FIHR	Healthcare Data Exchange	Adoption of standard in AMC demo	https://www.hl7.org/fhir/	AMC
IETF	Internet Technology, Cybersecurity	Contribution to TEE Architecture - in progress	https://datatracker.ietf.org/doc/draft-ietf-teep-architecture/	RISE
DIN NAMed	Medical Informatics Telemedicine	Encryption requirements for telemedicine in sleep medicine	https://www.din.de/en/getting-involved/standards-committees/named	CHARITE

[17] https://www.ietf.org/
[18] https://datatracker.ietf.org/doc/draft-ietf-teep-architecture
[19] https://www.din.de/en/getting-involved/standards-committees/named
[20] https://www.dgsm.de/dgsm_arbeitsgruppen_telemedizin.php?language=english

3.2 Communication Activities Performed in [M1-M18]

3.2.1 ASCLEPIOS Online Presence

3.2.1.1 ASCLEPIOS Website

The ASCLEPIOS public website (https://www.asclepios-project.eu) is the project's main communication and information point. It gathers in one place all public information about the project: general project information and partners, public outcomes including the ASCLEPIOS architecture, public deliverables and scientific publications.

6.137 Total Website Page Views
1.310 Unique Website Visitors
Published 13 Blogposts and 11 News posts

The website is updated with news entries about project meetings and participation in events (**Error! Reference source not found.**), while a Twitter plugin is deployed to present the latest tweets of ASCLEPIOS. A dedicated page has been created to host the project's blog, where the partners collaboratively contribute and compose articles targeted towards the general public, which are related to the ASCLEPIOS scientific results and demonstrators. The website has been enhanced with a section for the distribution of the produced communication material. The website is regularly updated with content, as a trigger for visitors to return at a later stage.

Figure 3-3 The Home page of ASCLEPIOS Website

A web analytics service has been deployed to measure and monitor the website traffic and provide some insights regarding the visitors' behaviour, which are accessible from the website's backend. Website analytics provide insights regarding the traffic volume of a website, the characteristics of the visiting audience (e.g. country) and the navigation of the visitors inside the website. It is a useful tool for better understanding the website's impact in the overall communication of the project, as well as updating content and even the website's structure based on visitors' behaviour and whether some sections should gain more visibility for dissemination. The latest update from the website analytics reveals that the majority of visitors come from the USA (22.16%). In the second and third position are Greece and the Netherlands with 15.10% and 9.17% respectivelly. The most viewed page is by far the home page (40.05%). Second most viewed page is the consortium page (7.89%) and in the third and fourth place we can find the news (6.50%) and blog (4.89%) sections. These insights could be leveraged towards slightly restructuring the website, so that the home page also contains some news and blog material, in order for the constantly updated content of the website to be more easily accessible to the visitors.

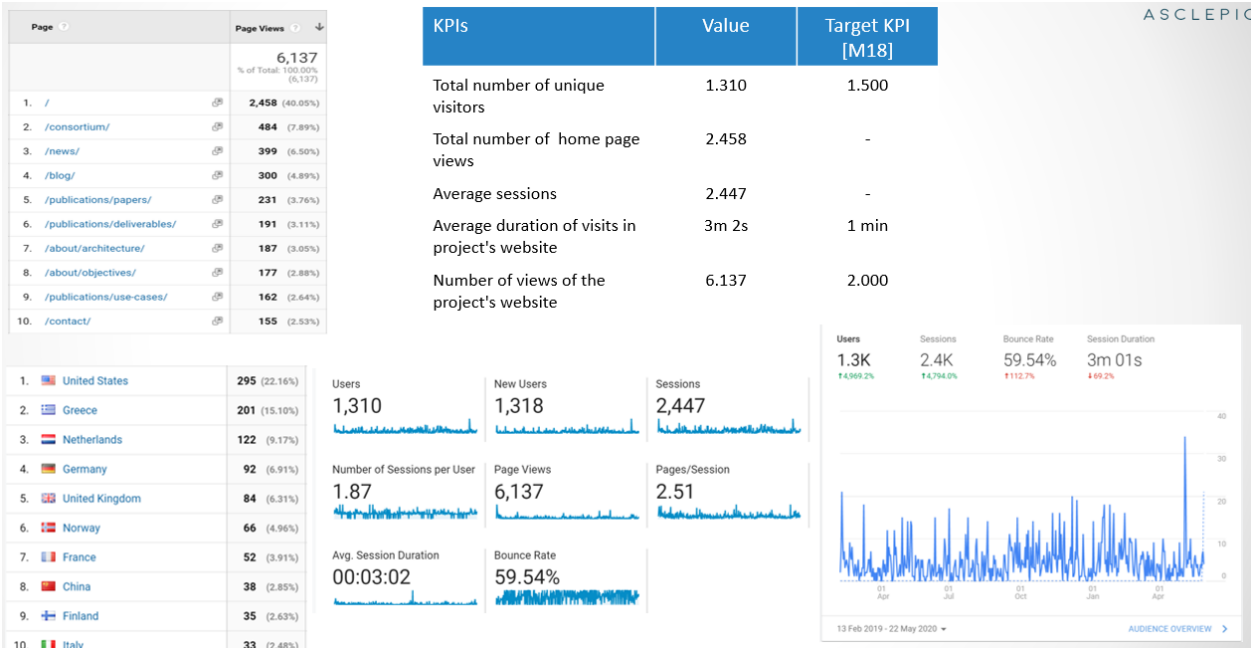


Figure 3-4 ASCLEPIOS Website Analytics on 24/5/2020

3.2.1.2 ASCLEPIOS Blog

The project's blog is part of the website. It is an active section of the website, which is regularly updated with new content provided by the responsible partners. These blogposts are promoted through the ASCLEPIOS social media, increasing their outreach and bringing more visitors to the website. So far, 13 blogposts directly associated to the scope of ASCLEPIOS have been created and shared.

Table 3-6 ASCLEPIOS Published Blogposts until [M18]

#	Blogpost Title	URL	Responsible Partner
01	The ASCLEPIOS vision – Making the cloud a secure place for eHealth services	https://www.asclepios-project.eu/blog-post/the-asclepios-vision-making-the-cloud-a-secure-place-for-ehealth-services/	SUITE5
02	Intro to ASCLEPIOS Demonstrators – part 1: Stroke acute care	https://www.asclepios-project.eu/blog-post/intro-to-asclepios-demonstrators-part-1-stroke-acute-care/	AMC
03	Intro to ASCLEPIOS Demonstrators – part 2 Inpatient and outpatient sleep medicine	https://www.asclepios-project.eu/blog-post/intro-to-asclepios-demonstrators-part-2-inpatient-and-outpatient-sleep-medicine/	HTW
04	Intro to ASCLEPIOS Demonstrators – part 3: Privacy-preserving monitoring and benchmarking of antibiotics prescriptions	https://www.asclepios-project.eu/blog-post/intro-to-asclepios-demonstrators-part-3-privacy-preserving-monitoring-and-benchmarking-of-antibiotics-prescriptions/	NSE
05	ASCLEPIOS Data handling and ethical issues	https://www.asclepios-project.eu/blog-post/asclepios-data-handling-and-ethical-issues/	CHARITE
06	IT and security requirements in healthcare	https://www.asclepios-project.eu/blog-post/it-and-security-requirements-in-healthcare/	RISE

07	Eliciting healthcare providers' requirements for a cloud-based e-health framework	https://www.asclepios-project.eu/blog-post/eliciting-healthcare-providers-requirements-for-a-cloud-based-e-health-framework/	NSE
08	Towards secure eHealth – The ASCLEPIOS Architecture	https://www.asclepios-project.eu/blog-post/towards-secure-ehealth-the-asclepios-architecture/	TUNI
09	Insights from searchable encryption schemes and their application in ASCLEPIOS	https://www.asclepios-project.eu/blog-post/insights-from-searchable-encryption-schemes-and-their-application-in-asclepios/	TUNI
10	Context-aware access control in ASCLEPIOS	https://www.asclepios-project.eu/blog-post/context-aware-access-control-in-asclepios/	ICCS
11	Insights from attribute-based encryption and ciphertext delegation schemes	https://www.asclepios-project.eu/blog-post/insights-from-attribute-based-encryption-and-ciphertext-delegation-schemes/	TUNI
12	Isolated and Trusted Execution Environments in Healthcare	https://www.asclepios-project.eu/blog-post/isolated-and-trusted-execution-environments-in-healthcare/	RISE
13	The ASCLEPIOS Access Control Mechanisms and Models Editor	https://www.asclepios-project.eu/blog-post/the-asclepios-access-control-mechanisms-and-models-editor/	ICCS

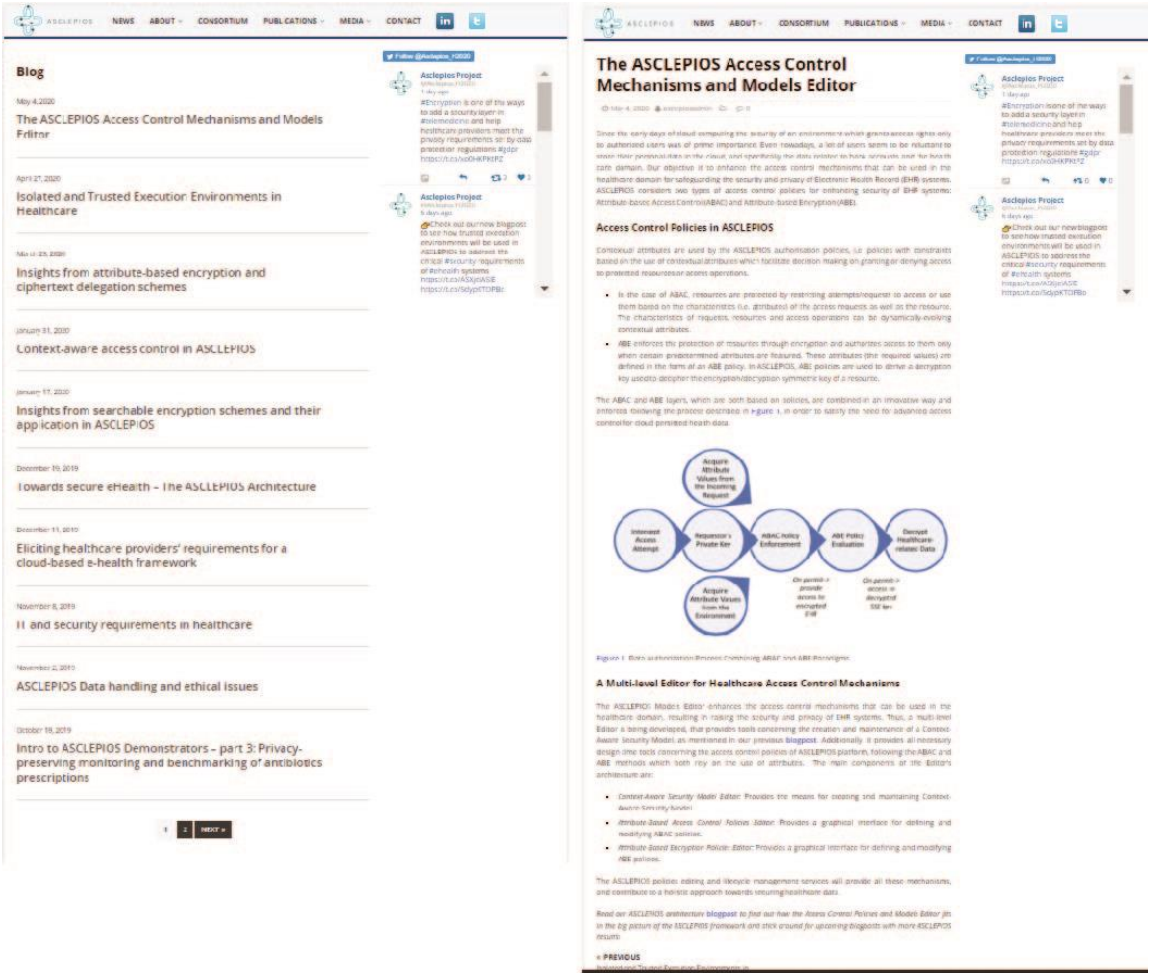


Figure 3-5 The main ASCLEPIOS Blog Page (left) and Indicative Blogpost (right)

3.2.1.3 Social Media Channels

In order to increase the visibility of the project and create room for the exchange of experiences among professionals and stakeholders, a LinkedIn showcase page (https://www.linkedin.com/showcase/asclepios-project) and a Twitter account (https://twitter.com/Asclepios_H2020) have been created.

145 Posts in Twitter and LinkedIn
Followed by 161 Accounts
72.117 Tweet Impressions

The activity of the consortium is promoted through these channels in a timely manner and with the use of appropriate hashtags to allow wider outreach. Additionally, third party content on related subjects is reposted and the relevant hashtags and activity of influencers in the domain (e.g. cybersecurity, encryption, telemedicine etc.) are monitored to identify trending themes. The list of followed accounts in Twitter is constantly enhanced with new related projects and also with accounts of influencers in order to engage the research community in the ASCLEPIOS vision and to capitalise on the networking effect of social media. The followed accounts are selected based on three criteria: their relevance to ASCLEPIOS, the high quality of uploaded content and their network size.

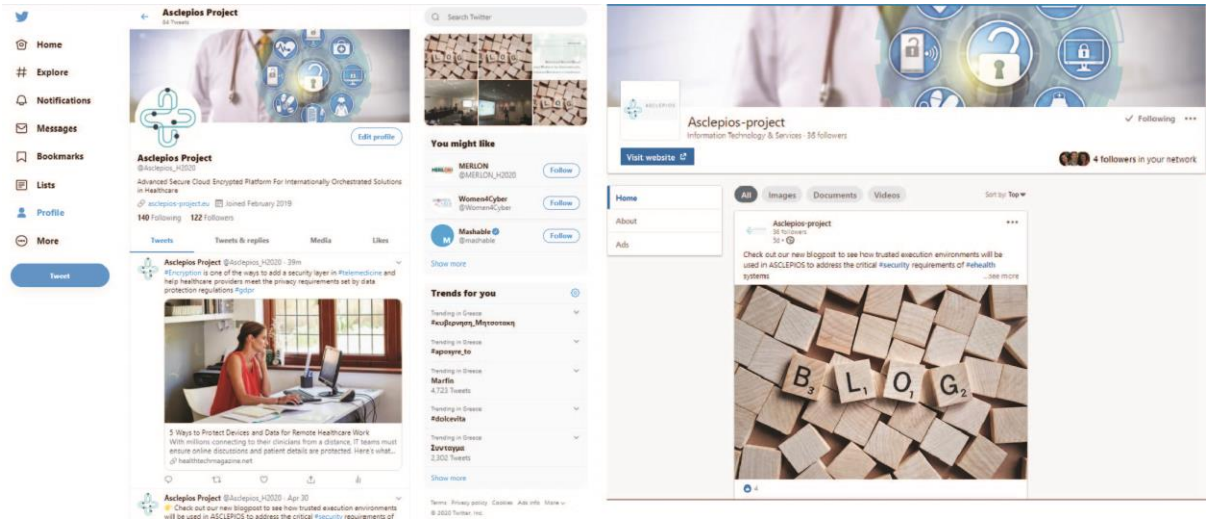


Figure 3-6 ASCLEPIOS Twitter and LinkedIn Pages

The progress of the ASCLEPIOS social media channels is presented in the following Table 3-7. The results of social media activities, expressed in metrics such as "Mentions", "Likes" and "Impressions" are satisfactory, as they show that in general the content circulated through the social accounts of ASCLEPIOS has achieved high visibility in the selected social media and contributes to the diffusion of the project's objectives, results, and news.

Table 3-7 ASCLEPIOS Social Media Metrics M1-M18

Social Network	Metric	Actual Value M1-M18
Twitter	Tweets	88
	Followers	125
	Impressions	72.117
	Mentions	70
	Retweets of ASCLEPIOS Tweets	115
	Likes	261
LinkedIn	Posts	57
	Followers	36
	Likes	167

3.2.2 Traditional Media and Press Releases

ASCLEPIOS takes advantage of news media such as corporate magazines and EU dissemination mechanisms, to communicate significant project events and results.

ASCLEPIOS Featured in 1 Industrial Magazine
1 Entry for the ASCLEPIOS Security Awareness Workshop in CORDIS
1 Project Kick-Off press Release

So far, the project's launch and the organisation of its 1st Cybersecurity Awareness Workshop have been distributed to traditional media through the publication of press releases, articles and announcements (Figure 3-7). More specifically, one article has been published in the printed edition of the leading Norwegian business magazine "Kapital"[21], featuring the ASCLEPIOS project and vision. One press release was created and circulated through the network of SECURA, announcing the launch of ASCLEPIOS and the role of

[21] https://kapital.no/

SECURA in the project[22]. Furthermore, the announcement and invitation to the 1st ASCLEPIOS Awareness Workshop[23] was hosted in the CORDIS portal for European Projects, offered by the European Commission.

Figure 3-7 ASCLEPIOS in Kapital Magazine (up-left), Press Release by SECURA (up-right), Workshop Invitation in CORDIS (bottom-left)

[22] https://www.secura.com/press-release-secura-joins-asclepios
[23] https://cordis.europa.eu/event/id/147543-workshop-on-security-of-healthcare-data

3.2.3 Communication Material

A combination of material -brochure, newsletter, poster – comprises the communication kit created during [M1-M18] both for the communication purposes of ASCLEPIOS as well as to support the ongoing dissemination and exploitation activities.

1 Trifold Brochure Designed
1 Poster Created for Event
1 e-Newsletter Published

It exhibits the unique ASCLEPIOS branding and visual identity, featuring the ASCLEPIOS logo and colour palette that has been designed from the beginning of the project. The content of the material was focused on the vision of ASCLEPIOS, presenting the key objectives, the three use cases, the architecture of ASCLEPIOS and highlights from ASCLEPIOS presence in events. The eNewsletter (Annex III. 1st Issue of ASCLEPIOS eNewsletter) was exported in PDF format with hyperlinks to material in the ASCLEPIOS website and the project's social media, in order to further promote the ASCLEPIOS online presence. This material was circulated through the project's website, social media, and the networks of sister projects. The brochure (Annex IV. 1st ASCLEPIOS Brochure) was exported as high-quality images in RGB and CMYK colour modes, appropriate both for digital exposure and printing. The ASCLEPIOS Poster was presented in the Inauguration of the IT-Security Lab that took place at the HTW Berlin.

Figure 3-8 ASCLEPIOS Poster created by HTW for the Inauguration of the IT-Security Lab at HTW Berlin- April 2019

Figure 3-9 1st Issue of ASCLEPIOS Brochure – January 2020

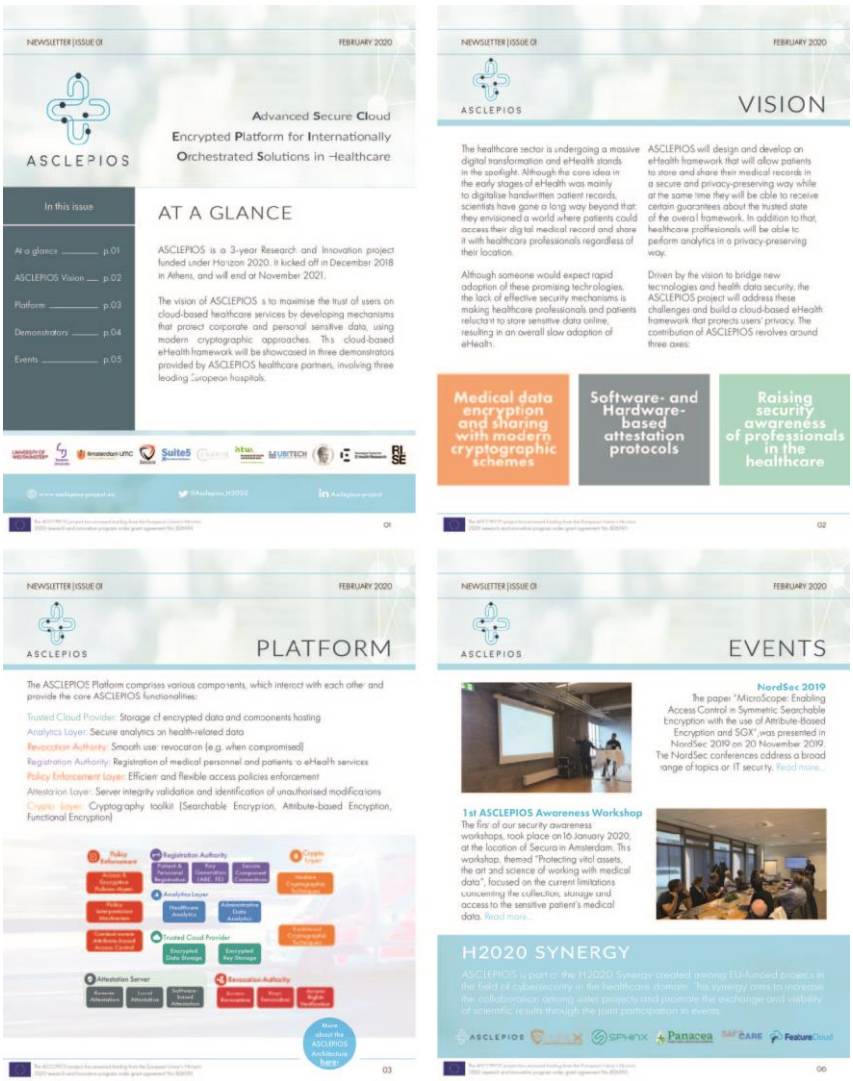


Figure 3-10 Indicative Pages from the 1st Issue of ASCLEPIOS Newsletter – February 2020 (full Issue in Annex III.)

3.3 Stakeholders' Engagement Activities Performed in [M1-M18]

3.3.1 Focus Group

Secura was in charge of setting-up and managing the Industrial Focus Group established around the ASCLEPIOS project.

Establishment of Focus Group with 4 Experts
2 ASCLEPIOS Events attended by members of the Focus Group

The objectives that the Focus Group aims to achieve are:

- Broad and efficient dissemination of the ASCLEPIOS progress and deliverables, such that the results of the project can reach a considerably wider audience
- Relevant technical input provided towards the members of ASCLEPIOS, which will be used to guide the research and development activities
- Relevant input regarding the possible limitations that certain parts of the project could have in practice, from an industry perspective

The target groups of people considered for the Focus Group included:

- Manufacturers of medical devices and systems for personal use (e.g. insulin pumps, pacemakers, etc.)
- Manufacturers of medical devices and systems for use within hospitals and clinics (e.g. medical imaging systems, brain stimulators, life sustaining systems, etc.)
- Manufacturers of medical devices software
- Pharmaceutical manufacturers
- Service providers involved with the processing or storage of health data
- Medical institutions such as hospitals and clinics
- Security assessment companies with an internationally recognized track record in testing the security of medical devices, systems or healthcare infrastructures
- EU level regulators and policy makers directly involved in the drafting of regulations and directives related to the healthcare domain (covering both security and privacy aspects)

Finally, some additional criteria were considered for the selection of the Focus Group members:

- Geographical spread
- Possibility to actively travel to the ASCLEPIOS plenary meetings

In the first half of the ASCLEPIOS project, the Focus group was created to include the following experts:

- Mr. Mario Dagrada – Forescout Technologies
- Mr. Guido van 't Noordende – Whitebox Systems BV
- Mr. Panagiotis Kotzanikolaou – University of Piraeus, Greece
- Ms. Bergling Smaradottir – University of Adger, Norway

The current componence of the Focus Group ensures a strong focus on technical concepts (especially cryptography), resulting from both academia, as well as private companies.

The following ASCLEPIOS project meetings were already attended by the members of the Focus Group:

- Plenary meeting Tampere, Finland – 17, 18 September 2019 – attended by Mr. Guido van 't Noordende
- Plenary meeting Athens, Greece – 11, 12 February 2020 – attended by Mr. Panagiotis Kotsanikolaou

The involvement in the plenary meetings is considered up to this moment satisfactory. The members of the Focus Group managed to get quickly up to speed with the objectives and current status of the ASCLEPIOS framework. They got actively engaged in the technical discussions, as well as providing feedback concerning practical implementation limitations or concerns. Finally, all the input resulting from the Focus Group members was collected in individual deliverables and documented in the archive of the project.

The second part of the ASCLEPIOS project envisions similar interaction and collaboration with the members of the Focus Group.

3.3.2 Security Awareness Courses

Secura is in charge of preparing and delivering security and privacy awareness courses integrated as part of the ASCLEPIOS project.

1 ASCLEPIOS Security Awareness Workshop organised with 23 Attendees

The target groups of such courses are highlighted in the Table 3-8 below.

Table 3-8 Target Groups for Security Awareness Courses

Type of entity	Knowledge regarding the types of data generated	Knowledge regarding the technology behind generating/storing data	Knowledge regarding the sensitivity of data
Patients	Limited	Limited	Moderate
Hospitals and clinics personnel	Extensive	Limited	Moderate
Cloud service providers	Limited	Extensive	Limited
Third party service providers	Limited	Moderate	Moderate

Based on these target groups, the following awareness courses objectives were derived.

Table 3-9 Awareness Courses Objectives

Target group	Awareness objectives to be followed in the course
Patients	• Increased awareness on types of data that do not have to be shared (according to the GDPR) • Increased awareness on secure ways in which data can be shared • Increased awareness on identifying a secure sharing platform for hosting personal data • Increased awareness regarding third-party entities that have access to shared data, as well as the type of data analytics conducted • Increased awareness on the external parties that will have access to the results of the conducted analytics
Hospitals and clinics personnel	• Increased awareness on the types of data that need to be collected from the patients (according to the GDPR) • Increased awareness about secure handling of collected medical data (e.g. secure local storage, erasure after use, etc.)
Cloud service providers	• Increased awareness on the types of cybersecurity risks that could impact the storage platform (the public cloud), as well as the security best practices that need to be deployed in order to minimize these risks

Third party service providers	• Increased awareness about the types of patient data that can be collected (according to the GDPR) • Increased awareness about secure handling of collected medical data (e.g. secure local storage, erasure after use, etc.)

Secura worked in the first half of the ASCLEPIOS project on preparing the necessary materials for delivering such courses. The materials prepared include:

- Course presentations
- Interactive exercises
- Project feedback forms
- Project results processing method and template

Based on the created materials, Secura conducted up to this moment one security awareness and privacy workshop, at its office in Amsterdam, The Netherlands. The workshop was held on 16 January 2020.

The agenda of the workshop can be found below.

Time	Topic	Description	Speaker
9:15	**Welcoming the guests**		
9:45	**Welcome message and context of the workshop**	Relevance and importance of the topic; Overview of the talks throughout the day; Attendees background	**Razvan Venter** (Secura)
10:00	**GDPR in healthcare environments**	Importance of the regulation, explanation of the concepts and topics and applicability to healthcare data	**Christiaan Hillen** (Secura)
10:45	**Coffee break**		
11:15	**Working with medical data – Patient awareness**	Threats and risks relevant to the medical data, while being processed. Best practices for secure processing of data.	**Christiaan Hillen** (Secura)
12:00	**Lunch**		
13:00	**Threat modelling in healthcare context**	Threat modelling on a state of the art medical data processing platform	**Christiaan Hillen** (Secura)
13:30	**Interactive exercise – Threat modelling**	Deriving the threat model and attack avenues for a healthcare environment	**Christiaan Hillen** (Secura)
14:00	**Working with medical data – Attacker perspective**	Attacker perspective on healthcare environments, with a strong focus on social engineering	**Christiaan Hillen** (Secura)
14:30	**Interactive exercise – Social engineering**	Social engineering scenario in a practical situation	**Christiaan Hillen** (Secura)
15:00	**Coffee break**		
15:30	**State of the art in a connected healthcare environment**	Practical way of processing medical data in a healthcare institution, risks and	**Ewald Beekman** (AMC)

		limitations	
16:15	**Applying the ASCLEPIOS concepts for improving the state-of-the-art.**	Practical demonstrator from AMC in the context of the ASCLEPIOS project	**Marcela Tuler** (AMC) **Razvan Venter** (Secura)
16:45	**Closing statement**		

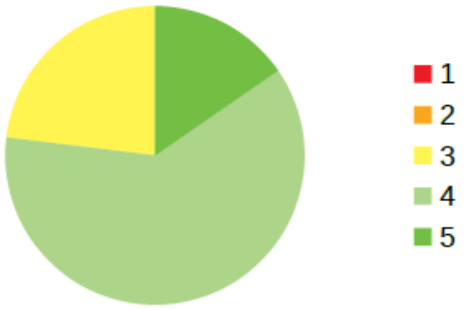
Figure 3-11 Agenda of the 1st ASCLEPIOS Awareness Workshop A

As it can be seen, the workshop included a combination of Secura presentations, as well as presentation given by speakers from AMC.

As a result of the workshop, Secura collected feedback concerning the results and the opinion of the attendees. The questions used for collecting the feedback were drafted in consultation with SUITE5. The feedback was centralised in a separate deliverable that was shared with the members of the ASCLEPIOS project. Some of the relevant statistics collected at the end of the workshop are presented in the images below.

Overall, how do you rate the event? (1 – lowest quality, 5 – highest quality)

Response	# of people
1	0
2	0
3	3
4	8
5	2
Total	**13**

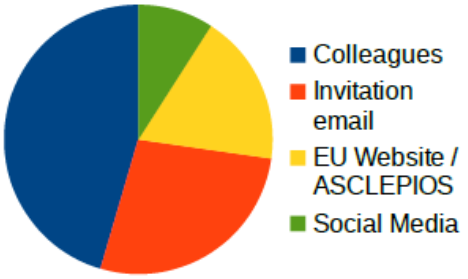


What is your background?

Response	# of people
Legal	2
Academia	1
Data Management	3
Computer Science	6
Healthcare	1
Total	**13**

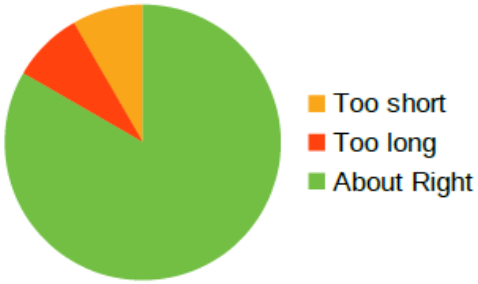
How did you find out about this event?

Response	# of people
Colleagues	5
Invitation email	3
EU Website / ASCLEPIOS	2
Social Media	1
Total	**11**



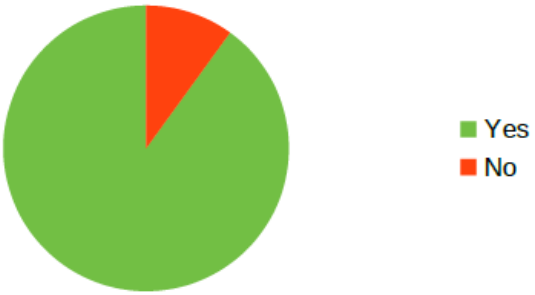
What did you think about the length of the sessions?

Response	# of people
Too short	1
Too long	1
About Right	10
Total	**12**



Do you think that the event met its goals?

Response	# of people
Yes	9
No	1
Total	**10**



How did you think the event can be improved?

Response
Less basic knowledge
More detail into cloud data transfers
More detail into ASCLEPIOS implementation
Too many sessions that were too short
Language specific courses
Having multiple Speakers
Stricter timeline (shorter breaks)

Secura will make use of the collected feedback in order to improve the next editions of the provided awareness workshops. Overall, the lessons learned after the first workshop can be summarised as:

- The agenda of the workshop needs to be made more focused, in order to ensure the quality of the presentations and reduce the total duration
- The involvement of external guest speakers was appreciated by the audience
- The usefulness of the topics was mostly shared by the audience
- For future editions, the possibility to join the workshop remotely in real time would be a very appreciated feature

3.4 KPIs in [M1-M18]

The following Table 3-10 includes the defined KPIs with respect to communication, dissemination and stakeholder engagement activities, the intermittent target values for [M1-M18] and the achieved (actual) values during that period.

Table 3-10 Dissemination and Communication KPIs for [M1-M18]

Measurable Indicator	Target for [M1-M18]	Actual Value M18
Number of workshops organised	1	1
Number of demo events organised	0	0
Number of European healthcare professionals reached by various ASCLEPIOS events	200	approx. 400
Number of unique stakeholders (IT security professionals, IT specialists in hospitals and healthcare institutions, healthcare professionals) reached by the ASCLEPIOS demonstrators	20	25
Number of events where ASCLEPIOS has participated	5	20
Number of events attended where ASCLEPIOS has a presentation	2	14
Number of project's demo booths	0	0
Number of conference papers	6	12
Number of journal papers submitted	0	2
Number of articles in corporate magazines	0	1
Number of unique industry contact points	30	5
Number of industry communities informed about the project	2	1
Number of webinars	0	1
Number of synergies with other projects	2	6
Number of joint activities (with other projects)	1	0
Number of internal partners' events / presentations	3	5

Number of links to the project's website	5	20
Number of training sessions	0	1
Number of standardisation working groups contacted	1	2
Number of individually or jointly submitted draft standardization documents	0	1
Number of blueprint documents of developed security enablers	0	0
Number of project's presentations in standardisation meetings	0	0
Number of unique visitors in the project's website	1.500	1.310
Average duration of visits in the project's website	1 min	3 min 2 sec
Number of views of the project's website	2.000	6.137
Number of accumulative followers in social media	200	161 (125 Twitter, 36 LinkedIn)
Number of accumulative posts in social media	100	145
Number of blogposts	18	24 (13 blogposts, 11 newsposts)
Number of press releases	2	1
Number of project's factsheets / brochures and banners	2	2
Number of e-Newsletters	2	1
Number of videos	1	0
Number of blog posts in EC dissemination mechanisms	2	1

4 Activities Plan [M19-M36]

4.1 Dissemination and Standardisation Plan for [M19-M36]

4.1.1 Dissemination and Standardisation Schedule for [M19-M36]

The second reporting period of the project covers the second half of Phase II: "Inform and Interact" and the whole Phase III: "Promote" of the Dissemination Schedule. The tangible results of ASCLEPIOS will be exhibited to the community through events and publications. Liaisons with other initiatives, projects, external organisations, and interdepartmental collaborations initiated in the first period, will be intensified and put into action through the organisation of joint activities. Knowledge and innovation transfer and attaining useful feedback for validation of results are among the dissemination objectives addressed in this phase. During the third year of the project, dissemination will be oriented mainly to attracting potential users and clients, ensuring applicability and acceptance of the provided solution. The ASCLEPIOS demonstrators will showcase the value of ASCLEPIOS with the collaboration of the partners from the healthcare domain. In this stage, the organisation of demo presentations, workshops and training sessions will be instrumental in familiarising potential adopters with the ASCLEPIOS solution and engaging the identified stakeholders.

The dissemination setup that was created during the first reporting period, has set the ground for the intensification of dissemination activities and will be exploited for the focused activities until the end of the project. The schedule for the key dissemination mechanisms is presented in the table below, which shows their anticipated progression during [M18-M36].

Table 4-1: Dissemination Activities Schedule

Dissemination Mechanism	Phase I: Raise Awareness (M1-M12)	Phase II: Inform and Interact (M13-M24)	Phase III: Promote (M25-M36)
Project Events	• Workshops in scientific conferences	• Workshops in scientific conferences, industry events & fairs • Hackathons	• Workshops in industry events • Hackathons • Demo events
Conferences and Workshops	• Presentation of project's scope • Interaction with participants	• Presentation of project's results • Project's booths	• Presentation of project's results and business case • Demo sessions
Scientific Publications	• Position papers / review papers in conferences	• Methodology papers in conferences	• Overall project's results published in journals & industry magazines
Community Building	• Establishment of contact points • Liaison with industry communities and networks • Communication material	• Result validation from stakeholders (events/online) • Interaction with industry communities and networks • Invitation to project's events	• Creation of potential users' network • Promotion of project's application stories • Invitation to demo events • Training webinars
Internal Dissemination	• Project's links & news in partners' website, social media accounts, newsletters	• Projects' results in partners' events	• Results' demonstration in partners' premises; • Training • Reuse of results

Standardisation Contributions	• Registration / participation in relevant working groups • Alignment with existing standards	• Participation in working groups' telcos and events • Presentation of project's results	• Participation in working groups' telcos and events • Presentation of project's demos

4.1.2 Upcoming Events/Conferences/Workshops and Opportunities

ASCLEPIOS has already scheduled its participation in 4 events in the beginning of the second reporting period (Summer of 2020) and is waiting the review results for submitted papers in other 5 conferences (Table 4-2).

Table 4-2 Upcoming Participation in Conferences and Events

Date	Place	Event Name	Type	Action	Participating Partner
June 11, 2020	Cardiff, UK / online	12th International Workshop on Science Gateways (IWSG 2020)	Workshop	Two papers accepted	UOW
June 16-18 2020	Palermo, Italy / online	IEEE 20th Mediterranean Electrotechnical Conference, MELECON 2020	Conference	One paper accepted	TUNI & UOW
July 2020	Montreal, Canada / online	IEEE EMBS 2020 Conference (EMBS 2020)	Conference	Networking	CHARITE
July 7-10, 2020	Brussels, Belgium / online	25th IEEE International Conference on Communications (ISCC 2020)	Conference	Paper Accepted	TUNI
July 15-17, 2020	Piraeus, Greece / physical and online	11th IEEE International Conference on Information, Intelligence, Systems and Applications (IISA 2020)	Conference	Paper Submitted, Under Review	ICCS
September 22-25, 2020	Singapore	14th International Conference on the theme of Provable and Practical Security (ProvSec 2020)	Conference	Paper to be Submitted	TUNI
September 14-18, 2020	Guildford, UK	25th European Symposium on Research in Computer Security (ESORICS 2020)	Symposium	Paper Submitted, Under Review	TUNI
October 21-23, 2020	Washington D.C., USA	16th EAI International Conference on Security and Privacy in Communication Networks (SecureComm 2020)	Conference	Paper Submitted, Under Review	TUNI

December 6-10, 2020	Daejeon, Korea	26th Annual International Conference on the Theory and Application of Cryptology and Information Security (ASIASCRYPT 2020)	Conference	Paper Submitted, Under Review	TUNI

Some of the most prominent upcoming conferences in the domains of cloud computing, cybersecurity, encryption, healthcare informatics and biomedicine are listed in the following Table 4-3. This list is available to partners through the Future Activities collaborative spreadsheet[24] for the timely tracking of dissemination opportunities. When partners participate in events on behalf of ASCLEPIOS, they shall provide further information regarding their participation (e.g. type of participation, name of publication – if any) to facilitate the monitoring and communication of performed activities.

Table 4-3 Identified Events/Conferences/Workshops of Interest to ASCLEPIOS

Date	Place	Event Name	Type	Deadlines	Event URL
December 12-15, 2020	Shenzhen, China	IEEE International Conference on E-health Networking, Application & Services (Healthcom 2020)	Conference	Papers: 30 June 2020 Workshop Proposals: 1June 2020 Demos/Posters/Short papers:20 September 2020	https://healthcom2020.ieee-healthcom.org/
November 23-25, 2020	Linköping, Sweden	25th Nordic Conference on Secure IT Systems (Nordsec 2020)	Conference	Papers: 25 August 2020 Poster Abstracts: 13 October 2020	https://nordsec2020.on.liu.se/
December 14-16, 2020	Vienna, Austria	19th International Conference on Cryptology and Network Security (CANS 2020)	Conference	Papers: 21 June 2020	https://cans2020.at/
August 21-25, 2021	Sydney, Australia	18th World Congress on Medical and Health Informatics - MedInfo 2021	Congress	To be announced	https://medinfo2021.org/
February 11-13, 2021	Vienna, Austria	12th International Conference on Bioinformatics Models, Methods and Algorithms (BIOINFORMATICS 2021)	Conference	Papers: 14 September 2020	http://www.bioinformatics.biostec.org/
February 11-13, 2021	Vienna, Austria	14th International Conference on Health Informatics (HEALTHINF 2021)	Conference	Papers: 14 September 2020	http://www.healthinf.biostec.org/
October 15-17, 2020	Cali, Colombia	EAI International Conference on Digital Healthcare Technologies for the Global South (EAI DigiHealthSouth 2020)	Conference	Papers: 2 July 2020	http://digihealthsouth.org/
Decemb	Viana do	7th EAI International	Conferen	Papers: 22 June	http://healthyio

[24] https://docs.google.com/spreadsheets/d/1siEstpXeEeZ6jD3j1VvvIrFZOw50-MI5uO9x3x0_DH8/edit#gid=1380995237

er 2-4, 2020	Costelo, Portugal	Conference on IoT Technologies for HealthCare (HealthyIoT 2020)	ce	2020	t.org/
Dec 29, 2020 – Jan 1, 2021	Guangzhou, China	19th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom 2020)	Conference	papers: 29 July 2020	http://ieee-trustcom.org/TrustCom2020/
November 13, 2020	Orlando, USA	4th Workshop on Attacks and Solutions in Hardware Security (ASHES 2020)	Workshop	Papers: 3 July 2020	http://ashesworkshop.org/
October 5-7, 2020	Hangzhou, China	International Conference on Computer, Information and Telecommunication Systems (CITS 2020)	Conference	Papers: 6 July 2020	http://atc.udg.edu/CITS2020/
October 17, 2020	Depok, Indonesia	5th International Workshop on Big Data and Information Security (IWBIS 2020)	Workshop	Papers: 17 June 2020	https://iwbis.cs.ui.ac.id/
September 26-28, 2020	Berlin, Germany	4th International Conference on Algorithms, Computing and Systems (ICACS 2020)	Conference	Papers: 25 June 2020	http://www.icacs.org/
September 14-18, 2020	Ghent, Belgium	Workshop on IoT, Edge, and Mobile for Embedded Machine Learning (ITEM 2020)	Workshop	Abstract: 9 June 2020 Papers: 24 June 2020	https://www.item-workshop.org/
October 20, 2020	Washington D.C. USA	International Workshop on Security, Privacy, and Trust for Emergency Events (EmergencyComm 2020)	Workshop	Papers: 29 June 2020	http://securecomm.org/emergencycomm-2020/
November 21-23, 2020	City University of Macau, Macau	11th International Conference on Networking and Information Technology (ICNIT 2020)	Conference	Papers: 5 July 2020	http://www.icnit.org/
September 17-19, 2020	Chongqing, China	9th International Workshop on Cyber Security and Privacy	Workshop	Papers: 21 June 2020	http://cyberc.org/Program/Security
October 18-22, 2020	Porto, Portugal	9th International Conference on Communications, Computation, Networks and Technologies (INNOV 2020)	Conference		https://www.iaria.org/conferences2020/INNOV20.html
November 18-19, 2020	Rennes, France	European Interdisciplinary Cybersecurity Conference (EICC 2020)	Conference	Papers: 14 June 2020	https://www.fvv.um.si/eicc2020/
TBA	London, UK	Infosecurity Europe	Exhibition	TBA	https://www.infosecurityeurope.com/exhibit/

4.1.3 Upcoming Publications and Opportunities

ASCLEPIOS has already 4 conference papers accepted for the upcoming period and is waiting the review results for 7 submitted papers (in 5 conferences and 2 journals) (Table 4-4).

Table 4-4 ASCLEPIOS Upcoming Publications

Date	Publication Type	Title	Authors	Conference/Journal Name	Status	Contributing Partner
2020	Conference	Industry Simulation Gateway on a Scalable Cloud	Kovacs, J., Kiss, T., Taylor, S.J.E., Farkas, A., Anagnostou, A., Pattison, G., Emodi, M., Kite, S., Petry, J., Snookes, G., Kacsuk, P., & and Lovas, R.	12th International Workshop on Science Gateways (IWSG 2020)	Paper Accepted	UOW
2020	Conference	Science Gateways with Embedded Ontology-based E-learning Support,	Kiss, T., Bolotov, A., Pierantoni, G., Deslauriers, J., Mosa, A., Kagialis, D., Terstyanszky, G., & Chan, D.	12th International Workshop on Science Gateways (IWSG 2020)	Paper accepted	UOW
2020	Conference	Charlie and the CryptoFactory: Towards Secure and Trusted Manufacturing Environments	Michalas, A., & Kiss, T.	IEEE 20th Mediterranean Electrotechnical Conference, MELECON 2020	Paper accepted	TUNI, UOW
2020	Conference	Power Range: Forward Private Multi-Client Symmetric Searchable Encryption with Range Queries Support	Bakas, A., & Michalas, A.	25th IEEE International Conference on Communications (ISCC 2020)	Paper Accepted	TUNI
2020	Conference	Securing Access to Healthcare Data with Context-aware Policies	Psarra, E., Patiniotakis, I., Verginadis, Y., Apostolou, D., & Mentzas, G.	11th IEEE International Conference on Information, Intelligence, Systems and Applications (IISA 2020)	Paper Submitted Under Review	ICCS

2020	Conference	Attribute-Based Symmetric Searchable Encryption	Dang, H-V, Ullah, A., Bakas, A., & Michalas, A.	14th International Conference on the theme of Provable and Practical Security (ProvSec 2020)	Paper to be Submitted	UOW, TUNI
2020	Conference	Finally, a (F)unctional President! Privacy-Preserving E-Voting Through Multi-Input Functional Encryption	Bakas, A., & Michalas, A.	25th European Symposium on Research in Computer Security (ESORICS 2020)	Paper Submitted Under Review	TUNI
2020	Conference	Nowhere to Leak: A Forward and Backward Private Symmetric Searchable Encryption in the Multi-Client Setting	Bakas, A., & Michalas, A.	16th EAI International Conference on Security and Privacy in Communication Networks (SecureComm 2020)	Paper Submitted Under Review	TUNI
2020	Conference	Searching in the Dark: A Multi Client Symmetric Searchable Encryption Scheme with Forward Privacy	Bakas, A., & Michalas, A.	26th Annual International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2020)	Paper Submitted Under Review	TUNI
2020	Conference	Towards a Cloud Native Big Data Platform using MiCADO	Mosa, A., Kiss, T., Pierantoni, G., Deslauriers, J., Kagialis, D., & Terstyanszky, G.	ISPDC 2020, 19th International Symposium on Parallel and Distributed Computing	Paper Submitted Under Review	UOW
2020	Journal	Blockchain Reputation-Based	T. de Oliveira, M., Medeiros, L.R-D,	Computer Network,	Paper Submitted	AMC

		Consensus: A Scalable and Resilient Mechanism for Distributed Mistrusting Applications	Carrano, R., Sílvia D. Olabarriaga, S., & Matto, D.	Elsevier	Under Review	
2020	Journal	Cloud Apps To-Go: Cloud Portability with TOSCA and MiCADO	Deslauriers, J., Kiss, T., Ariyattu, R., Dang, H-V., Ullah, A., Bowden, J., Krefting, D., Pierantoni, G., & Terstyanszky, G.	Concurrency and Computation: Practice and Experience	Paper Submitted Under Review	UOW, HTW Berlin

The majority of the upcoming events in Table 4-5 offer Calls for Papers, providing the opportunity to ASCLEPIOS for publication and diffusion of its scientific results in the context of prestigious conferences. With regard to journal publications, the following is an indicative list of high reputation journals that shall be considered for the future ASCLEPIOS publications.

Table 4-5 Journals of Interest to ASCLEPIOS

Journal Name	Publisher	URL
Journal of Grid Computing (JOGC)	Springer	https://www.springer.com/journal/10723
Future Generation Computer Systems (FGCS)	Elsevier	https://www.journals.elsevier.com/future-generation-computer-systems
ACM Transactions on Computing for Healthcare (HEALTH)	ACM	https://dl.acm.org/journal/health
Medical Image Analysis	Elsevier	https://www.journals.elsevier.com/medical-image-analysis
IEEE Transactions on Image Processing	IEEE	https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=83
Journal of Medical Systems	Springer	https://www.springer.com/journal/10916
International Journal of Technology Assessment in Health Care	Cambridge University Press	https://www.cambridge.org/core/journals/international-journal-of-technology-assessment-in-health-care
Health Information Management Journal (HIMJ)	SAGE Journals	https://journals.sagepub.com/home/himd
IEEE Journal of Biomedical and Health Informatics	IEEE	https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=6221020
IEEE Security and Privacy	IEEE	https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=8013
Informatics for Health and Social Care	Taylo & Francis	https://www.tandfonline.com/loi/imif20
Journal of Medical Internet Research (JMIR)	JMIR	https://www.jmir.org/
International Journal of Medical Informatics	Elsevier	https://www.journals.elsevier.com/international-journal-of-medical-informatics
Journal of the American Medical Informatics Association (JAMIA)	OXFORD Academic	https://academic.oup.com/jamia
Journal of Cryptographic Engineering (JCEN)	Springer	https://www.springer.com/journal/13389
IEEE Transactions on Cloud Computing	IEEE	https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=6245519

Journal of Information Security and Applications	Elsevier	https://www.journals.elsevier.com/journal-of-information-security-and-applications

4.1.4 Standardisation Opportunities

The following standardisation efforts (Table 4-6) have been identified as potential opportunities either for the adoption of domain standards in the data models of ASCLEPIOS or for active contribution by ASCLEPIOS to the drafting of new standards or to discussions of the different working groups and task forces.

Table 4-6 Identified Standardisation Opportunities

Standardisation Body	Sector	URL
DIN	NAMED 063 Medical Informatics	https://www.din.de/en/getting-involved/standards-committees/named
CEN	TC251 Medical Informatics	https://standards.cen.eu/dyn/www/f?p=204:7:0::::FSP_ORG_ID:6232&cs=18CA078392807EDD402B798AAEF1644E1
OASIS	Information Technology	https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=tosca
CEN/CLC/JTC 13	Cybersecurity and Data Protection	https://www.cenelec.eu/dyn/www/f?p=104:7:21553073082501::::FSP_ORG_ID,FSP_LANG_ID:2307986,25
IETF	Internet Engineering	https://www.ietf.org/
HL7	Electronic Health Information	http://www.hl7.org/
CEN-CENELEC-ETSI 'Cyber Security Coordination Group' (CSCG):	IT security, Network and Information Security (NIS) and Cyber Security (CS)	https://www.cencenelec.eu/standards/sectors/defencesecurityprivacy/security/pages/cybersecurity.aspx
ETSI Cyber Security Technical Committee (TC CYBER):	Cybersecurity	https://www.etsi.org/technologies/cyber-security

4.2 Communication Plan for [M19-M36]

4.2.1 Communication Schedule for [M19-M36]

The second reporting period of the project covers the second half of Phase II: "Diffuse Knowledge" and the whole Phase III: "Intensify Communication" of the Communication Schedule.

The actual project outcomes provide input for the intensification of communication efforts. The knowledge produced by the other project activities shall be diffused to the identified audiences through the communication channels that were established during the first phase, with the appropriate use. Additionally, associated communication material will be created to inform the general public about the ASCLEPIOS solution and promote it to potential users. Heading towards the end of the project, the ground must be prepared for the exploitation of the developed solution. The social media shall be used for promotional purposes, while the communication material shall also acquire input from the parallel exploitation activities. The frequency of posts and updates will reflect exactly this intention to intensify communication and build strong ties with potential adopters and clients. The intensification of activities for

the second reporting period is depicted in the target values of the performance indicators (Table 4-9), which indicate that the actions will be oriented towards creating the main body of the ASCLEPIOS communication material in terms of quantity and content, as well as increasing the audience.

Below (Table 4-7) is the ASCLEPIOS communication schedule for the second reporting period, containing the target objectives and activities of each communication mechanism until the end of the project.

Table 4-7 Communication Activities Schedule

Communication Mechanism	Phase I: Raise Awareness (M1-M12)	Phase II: Diffuse Knowledge (M13-M24)	Phase III: Intensify Communication (M25-M36)
ASCLEPIOS Website	• Website design and development • Search engine optimisation	• Main online information point • Project news, events & results • Links to other liaison initiatives and projects • Increased awareness	• Regular updates of content • Clear visibility of results • Interactive demo / application material
ASCLEPIOS Blog	• Blog deployment • Blogposts related to project's positioning & technologies	• Frequent blogposts on issues relevant to the project • Initiate discussions • Receive feedback	• Frequent blogposts to demonstrate and promote project's results
Social Media Channels	• Establishment of ASCLEPIOS presence • Re-post of relevant content • Monitoring of relevant hashtags • Upload public material • Follow relevant domain influencers • Engagement with other projects and initiatives	• Promotion of project outcomes and events • Interaction with followers and feedback • Answer to comments and private messages on the various channels • Upload public material • Repost of relevant content and monitoring of relevant hashtags	• Promotion of project's outcomes and events • Interact with followers to get feedback • Answer to comments and private messages on the various channels • Upload public material • Repost of relevant content (more sporadically)
Press Releases	• Press release to announce the project's launch	• Press releases to announce the significant events / results	• Press releases to promote the business case of project results

Communication Material	• ASCLEPIOS logo and project identity • Preparation of project factsheet, brochure, banner, e-Newsletter and promo video	• Revision of brochure, banner and frequent releases of e-Newsletter • blogs / news in EU dissemination instruments	• Prepare final brochure, banner, frequent releases of e-Newsletter and video demonstrators • Publish blogs / news in EU dissemination instruments

4.2.2 Online Presence Intensification

A blogpost calendar has been devised to better organise the continuous update of the website's content. Blogposts will emerge from the deliverables of the project, providing information on the ASCLEPIOS outcomes and aspects on the relevant scientific domains, in a user-friendly manner. The blogposts shall be provided by the partners approximately one month after the submission of the respective deliverable and will be published to the website accordingly on a near to monthly basis.

Table 4-8 Scheduled Blogposts for [M19-M36]

#	Indicative Title/ Related Deliverable	Responsible Partner	Publication Date
14	Private vs public cloud for healthcare data analysis / D6.1	UOW	[M18] - May 2020
15	Prescriptive analytics for healthcare providers (+ analytics over encrypted data) / D2.3	SUITE5	[M19] - June 2020
16	Analytics for identification of emerging threats and monitoring of encryption activities for CSPs / D2.3	SUITE5	[M20] - July 2020
17	ASCLEPIOS Access control enforcement / D3.3	UBITECH	[M21] - Aug 2020
18	Insights from the state-of-the-art in remote attestation of firmware and workloads in ITEEs / D4.2	RISE	[M22] - Sep 2020
19	ASCLEPIOS Interoperability across ITEEs in eHealth / D4.3	TUT	[M23] - Oct 2020
20	ASCLEPIOS Technical architecture / D5.1	UBITECH	[M24] - Nov 2020
21	ASCLEPIOS Testing and technical evaluation plan / D5.1	UBITECH	[M25] - Dec 2020
22	Market Analysis	SUITE5	[M26] - Jan 2020
23	The three selected healthcare applications of ASCLEPIOS	UOW	[M27] - Feb 2020
24	Techniques for computation on distributed data / privacy-preserving analytics	NSE	[M29] - Apr 2021
25	ASCLEPIOS Early platform release / D5.2	UBITECH	[M30] - May 2021
26	ASCLEPIOS Final platform release / D5.3	UBITECH	[M31] - June 2021
27	ASCLEPIOS Early Demonstrator 1: Evaluation and feedback / D6.3	AMC	[M32] - July 2021
28	ASCLEPIOS Early Demonstrator 2: Evaluation and feedback / D6.3	CHARITE/HTW	[M34] - Sep 2021
29	ASCLEPIOS Early Demonstrator 3: Evaluation and feedback / D6.3	NSE	[M35] - Oct 2021

30	ASCLEPIOS Final Demonstrator 1: Evaluation and operation experiences / D6.4	AMC	[M36] - Nov 2021
31	ASCLEPIOS Final Demonstrator 2: Evaluation and operation experiences / D6.4	CHARITE/HTW	[M36] - Nov 2021
32	ASCLEPIOS Final Demonstrator 3: Evaluation and operation experiences / D6.4	NSE	[M36] - Nov 2021

4.3 Stakeholders' Engagement Activities' Plan for [M19-M36]

4.3.1 Focus Group

In general, the activities of the Focus Group during the second half of the ASCLEPIOS project are envisioned to be similar with the ones which were followed during the first half. As the composition of the Focus Group is at this point stable and fixed to four experts, it is likely that the Focus Group will remain with the same members until the end of the project. As discussed with the members of the Focus Group, the main objectives expected from their involvement in the project are:

- Actively participate in the plenary meetings of ASCLEPIOS.
- Provide feedback concerning the technical discussions within the plenary meetings, as well as flag any possible issues or concerns related to the practical applicability of the design elements.
- Summarise the provided feedback in individual deliverables, to share with the rest of the project members at the end of each plenary meeting.

In order to better organise the involvement of the Focus Group members, individual Confidentiality Agreements were signed between the project and the members. Based on these confidentiality agreements, it is agreed that the exchange of information between the members and ASCLEPIOS will remain confidential until the moment when this information is published in one of the project deliverables.

4.3.2 Security Awareness Courses

Secura aims to further conduct security and privacy awareness courses, following the successful experience of conducting the first of such workshops in January 2020. As a result of the first workshop, course materials are already available. Based on the collected feedback taken from the first workshop, the materials will be slightly updated in order to provide a better and more efficient experience to the workshop attendees.

The current intention is to hold at least one workshop per year. The location of such workshops can be either the office of Secura (Amsterdam, The Netherlands), as well as other possible locations. Based on the collected feedback, as well as the internal discussions following the first workshop, it was confirmed that there is interest from other ASCLEPIOS partners to co-host future editions of the workshop. Such editions could for example be combined with the dates of the project plenary meetings, therefore also making the necessary logistics smoother.

Currently, the date of the next edition of the awareness and privacy workshop is under discussion. The intention was to organise this workshop in October/November 2020. Due to the current circumstances around the COVID-19 virus, Secura is carefully monitoring the development of the situation to ensure that public meetings can be safely organised towards the end of 2020. As a viable alternative, Secura is currently considering the option of hosting the next edition of the workshop fully online, with the attendees being able to follow the presentations in real time. This approach will also allow a potentially higher number of persons in the audience of the workshop, as it will eliminate the travel effort. On the other hand, having the courses fully online will strongly limit the interaction between the participants, which was one of the most appreciated features of the first workshop edition.

For 2021, envisioned dates for the workshop are also considered towards the end of the third quarter/beginning of fourth quarter of the year. Secura will continue to record and process the feedback resulting from the attendees of these workshops. This feedback will be centralized in individual deliverables and used in order to improve the contents and the quality of the future editions.

4.4 KPIs for [M19-M36]

The initial target values for [M19-M36] of the dissemination-related performance indicators that were defined in D7.1, have been updated based on their actual values on M18, in order to achieve the desired total in [M36]. For some KPIs that exceeded the expected target value for the first reporting period, the final total targets for M36 have been increased accordingly, to reflect and make the most out of the created momentum.

Table 4-9 Dissemination and Communication KPIs for [M19-M36]

Measurable Indicator	Actual Value M18	Updated M19-M36	Total
Number of workshops organised	1	2	3
Number of demo events organised	0	3	3
Number of European healthcare professionals reached by various ASCLEPIOS events	400 (approx.)	800	1.200
Number of unique stakeholders (IT security professionals, IT specialists in hospitals and healthcare institutions, healthcare professionals) reached by the ASCLEPIOS demonstrators	25	75	100
Number of events where ASCLEPIOS has participated	20	15	35
Number of events attended where ASCLEPIOS has a presentation	14	8	22
Number of project's demo booths	0	1	1
Number of conference papers	12	8	20
Number of journal papers submitted	2	8	12
Number of articles in corporate magazines	1	5	6
Number of unique industry contact points	5	95	100
Number of industry communities informed about the project	1	4	5
Number of webinars	1	3	4
Number of synergies with other projects	6	2	8
Number of joint activities (with other projects)	0	5	5
Number of internal partners' events / presentations	5	7	12

Number of links to the project's website	20	25	40
Number of training sessions	1	3	4
Number of standardisation working groups contacted	2	2	4
Number of individually or jointly submitted draft standardization documents	1	>=1	>=2
Number of blueprint documents of developed security enablers	0	>=3	>=3
Number of project's presentations in standardisation meetings	0	1	1
Number of unique visitors in the project's website	1.310	3.700	5.000
Average duration of visits in the project's website	3 min 2 sec	2 min	2 min
Number of views of the project's website	6.137	6.000	12.000
Number of accumulative followers in social media	161 (125 Twitter, 36 LinkedIn)	840	1.000
Number of accumulative posts in social media	145	260	400
Number of blogposts	24 (13 blogposts, 11 newsposts)	15	36
Number of press releases	1	4	5
Number of project's factsheets / brochures and banners	2	3	5
Number of e-Newsletters	1	5	6
Number of videos	0	2	2
Number of blog posts in EC dissemination mechanisms	1	5	6

5 Conclusions

This deliverable contained a reiteration of the ASCLEPIOS dissemination and communication objectives, strategy and activities plan, which will ensure the outreach of the project's results towards the related stakeholders. Additionally, the activities performed during the first reporting period (M1-M18) were reported in detail, the defined KPIs were evaluated and the overall progress of the activities was assessed. The plan for the upcoming period (M19-M36) has been updated based on these results and insights.

During the second reporting period, communication and dissemination activities will be intensified and monitored constantly to maximise their effectiveness. They aim at demonstrating the actual scientific outcomes of ASCLEPIOS through a number of targeted events, publications and other dissemination mechanisms, with the support of the communication infrastructure that has already been set up. These activities will set the ground for the exploitation of ASCLEPIOS after the project's end.

All dissemination and communication activities performed during the second period and the achieved results, will be reported in the context of deliverable D7.5 – "Final Dissemination, Communication and Stakeholders' Activity Report" in M36.

Annex I. Activities Templates for [M1-M18]

Events / Conferences / Workshops ASCLEPIOS Participated in during M1-M18
Following are the completed reporting templates for the events ASCLEPIOS participated in during the first reporting period:

Table AI-1 * HTW Symposium "Kreativität + X = Innovation, November 2018 / HTW

	Event Reporting Template
Type	Participation in Conference.
Event Name	HTW Wissenschaftssymposium Kreativität + x = Innovation
Venue	Berlin, Germany
Date	8.11.2018
Event objectives	Presentation of Research Activities of HTW Berlin, Networking with local partners, in particular SME
Size of audience (approx.)	100
Dissemination Level	Regional
URL	https://www.htw-berlin.de/files/Presse/Pressemitteilungen/2018/PM__13_2018_Kreativitaet_Innovation.pdf
Description of activity	Annual conference of the HTW Berlin where research activities are presented in form of lectures, workshops and poster sessions. Audience is a wide variety of regional partners from politics, sciences, industry and small and medium enterprises.
Title	Asclepios – Sichere Cloudlösung für die Schlafmedizin
Presenter	Michael Witt, Maryna Khvastova
Partners Involved	HTW (HTW)
Type of Audience	• Academia and Research • Industry (Mixed)
Dissemination Level	International, National/Regional/Local
Hash tags for Social Media Dissemination	-
URL	-
Relevant Resources	-

Table AI-2 34th ACM/SIGAPP Symposium On Applied Computing (SAC 2019), April 2019 / TUNI

	Event Reporting Template
Type	Participation in Conference
Event Name	The 34th ACM/SIGAPP Symposium On Applied Computing (SAC'19)
Venue	Limassol, Cyprus.
Date	April 8–12, 2019
Event objectives	-
Size of audience (approx.)	>500
Dissemination Level	International
URL	https://www.sigapp.org/sac/sac2019/

Description of activity	The main idea on the core cryptographic parts of ASCLEPIOS was presented at on April the 12th 2019 at ACM SAC. The paper entitled "*The Lord of the Shares: Combining Attribute-Based Encryption and Searchable Encryption for Flexible Data Sharing*" was presented by Prof. Antonis Michalas from Tampere University. The ACM Symposium on Applied Computing (SAC) has been a primary and international forum for applied computer scientists, computer engineers and application developers to gather, interact and present their work. The ACM Special Interest Group on Applied Computing (SIGAPP) is the sole sponsor of SAC. In addition to that, ACM SAC is considered as a very important conference in the field of computer science and with a great track on security-related papers.
Title	The Lord of the Shares: Combining Attribute-Based Encryption and Searchable Encryption for Flexible Data Sharing.
Presenter	Antonis Michalas
Partners Involved	TUNI
Type of Audience	Academia and Research, Industry (mixed)
Hash tags for Social Media Dissemination	#ACMSAC #SearchableEncryption #SSE #AttributeBasedEncryption #ABE #Cryptography #SecureStorage #CloudSecurity
Relevant Resources	• **Photo:** ASCLEPIOS_2019_04_SAC.jpeg • **Agenda:** http://www.sigapp.org/sac/sac2019/file2019/SAC19-FinalProgram-v8.pdf • **Slideshare presentation:** https://www.slideshare.net/amihalas/the-lord-of-the-shares-combining-attributebased-encryption-and-searchable-encryption-for-flexible-data-sharing

Table AI-3 11th International Workshop on Science Gateways (IWSG 2019), June 2019 / UOW

	Event Reporting Template
Type	Participation in Workshop
Event Name	11th International Workshop on Science Gateways (IWSG 2019)
Venue	Ljubjana, Slovenia
Date	11-14th June 2019
Event objectives	The workshop presents the latest trends in science gateways. Science gateways are a community-specific set of tools, applications, and data collections that are integrated together via a Web portal or a desktop application, providing access to resources and services of Distributed Computing Infrastructures (DCIs). Participants discuss how science gateways are used in hybrid Clouds that combine Cloud, Fog, Edge with the Internet of Things (IoT) and various off-the-shelf methods of Artificial Intelligence (AI). At the workshop both developers and researchers also present how science gateways are used business, public sector and research applications..
Size of audience (approx.)	ca. 50
Dissemination Level	International
URL	http://www.iwsg2019.eu
Description of activity	Three UOW researchers attended IWSG 2019. G. Pierantoni presented a paper how to use the MiCADO platform to manage Healthcare applications
Title	A Secure Cloud-based Platform to Host Healthcare Applications
Presenter	Pierantoni, G
Partners Involved	UOW, AMC, HTW Berlin, NSE
Type of Audience	Academia and Research
Hash tags for Social Media Dissemination	#cloud #MiCADO #security #science gateway
Relevant Resources	-

Table AI-4 Roundtable EU Event, June 2019 / TUNI

	Event Reporting Template
Type	Summit
Event Name	iCPS Cyber Security Roundtable 2019
Venue	Brussels
Date	11/06/2019
Event objectives	Roundtable discussion regarding the direction that EU must follow in the forthcoming years regarding the field of cyber security and privacy.
Size of audience (approx.)	30
Dissemination Level	International
URL	N/A
Description of activity	Roundtable discussion regarding the direction that EU must follow in the forthcoming years regarding the field of cyber security and privacy.
Title	-
Presenter	-
Partners Involved	TUNI
Type of Audience	-
Hash tags for Social Media Dissemination	-
Relevant Resources	-

Table AI-5 Long Night of Sciences Berlin 2019, June 2019 / HTW

	Event Reporting Template
Type	Participation Summit
Event Name	Long Night of Sciences Berlin
Venue	Berlin, Germany
Date	15.6.2019
Event objectives	Show research activities to broad audience, outreach
Size of audience (approx.)	1000
Dissemination Level	Local
URL	https://events.htw-berlin.de/hochschule/lange-nacht-der-wissenschaften/
Description of activity	Presentation of the Asclepios project as a poster in the context of the tours through the Cyber Security Lab of the HTW Berlin.
Title	Asclepios – Sichere Cloudinfrastrukturen für die Gesundheit
Presenter	Maryna Khvastova
Partners Involved	HTW (TW)
Type of Audience	• Academia and Research • Industry (Health) • Industry (Tech) • Industry (mixed) • Policy Makers • Other – public audience
Hash tags for Social Media Dissemination	-
Relevant Resources	-

Table AI-6 IEEE Engineering in Medicine and Biology Society: Workshop (EMBS 2019), July 2019 / CHARITE

	Event Reporting Template
Type	Participation in Conference with a workshop

Event Name	IEEE Engineering in Medicine and Biology Society Annual Congress
Venue	City Cube, Berlin Germany
Date	23. – 27. July 2019
Event objectives	The conference is the largest Biomedical Engineering Conference annually worldwide. The specific Workshop was on biosignals and their processing using a secure cloud encryption as developed in Asclepios
Size of audience (approx.)	Conference participation: 3000 and Workshop participation: 70
Dissemination Level	International
URL	https://embc.embs.org/2019/
Description of activity	The workshop within the conference was on biosignal processing and on biosignal integration using different sources such as sleep laboratory, wearables, clinical data, questionnaires, reported data, medication data. The integrated data are stored in a cloud for quality control of medical cases and for biosignal processing in order to develop phenotyping of patients with sleep disorders.
Title	Biosignal encryption in a medical cloud
Presenter	Thomas Penzel
Partners Involved	Charite, HTW
Type of Audience	• Academia and Research • Industry (Health) • Industry (Tech) • Industry (mixed) • Policy Makers
Hash tags for Social Media Dissemination	@ieeeEMBS
Relevant Resources	-

Table AI-7 ACM Special Interest Group on Data Communication (SIGCOMM 2019), August 2019 / RISE

	Event Reporting Template
Type	Participation in Workshop
Event Name	SIGCOMM 2019 Posters and Demos
Venue	Beijing, China
Date	August 19-24, 2019
Event objectives	The objectives of the event were: (1) Present to a specialized audience the RISE work on using Intel SGX to protect information about network flows; (2) Establish new collaborations on the topic of confidential computing using Trusted Execution environments.
Size of audience (approx.)	950
Dissemination Level	International
URL	https://dl.acm.org/doi/proceedings/10.1145/3342280

Description of activity	This was a poster presentation of the work on protecting openflow flow tables using Intel SGX. Abstract: Commodity software switches do not currently implement confidentiality or integrity protection of flow tables. An attacker can exploit software vulnerabilities to access the switch host memory and observe or modify installed flows. Observing installed flows allows an attacker to learn security-sensitive information: topology, flow patterns between endpoints, and flow priority. Modifying installed flows allows an attacker to exploit routing loopholes and avoid certain packet steps - e.g. route around a firewall or prevent mirroring packets to an intrusion detection system. In this demo we present OFTinSGX, an approach to protect the confidentiality and integrity of network flows installed on software switches. Our approach is based on decomposing the network switch to reduce the attack surface by isolating the OpenFlow flow tables and the flow rules from the rest of the code base. OFTinSGX allows to prevent attacks on the confidentiality and integrity of flow rules in software switches
Title	Protecting OpenFlow Flow Tables with Intel SGX
Presenter	Jacob Svenningsson
Partners Involved	RISE Research Institutes of Sweden.
Type of Audience	• Academia and Research • Industry (Tech)
Hash tags for Social Media Dissemination	#SIGCOMM, #SGX, #Openflow
Relevant Resources	Paper: https://dl.acm.org/doi/epdf/10.1145/3342280.3342339

Table AI-8 ICT 2019 Proposers Day, September 2019 / SUITE5

	Event Reporting Template
Type	Participation in Conference.
Event Name	ICT 2019 Proposers Day
Venue	Helsinki, Finland
Date	19/09/2019
Event objectives	ICT Proposers' Day focuses on the upcoming calls of the Horizon 2020 work programme in the field of Information & Communication Technologies, Future and Emerging Technologies (FET), and Societal Challenges. The event provides an excellent opportunity to present and discuss the main policy drivers of the digital transformation of European industry and society. It also presents how the EU research & innovation agenda can best contribute to these objectives.
Size of audience (approx.)	2000
Dissemination Level	International
URL	https://ec.europa.eu/digital-single-market/en/ict-proposers-day
Description of activity	The event was an exceptional opportunity for ASCLEPIOS to discuss its goals and challenges and build quality partnerships with academics, researchers, healthcare stakeholders, SMEs and government actors from all over Europe.
Title	-
Presenter	-
Partners Involved	Suite5
Type of Audience	• Academia and Research • Industry (Tech) • Policy Makers
Hash tags for Social Media Dissemination	#ICTpropday #H2020 #
Relevant Resources	-

Table AI-9 RE-WORK Deep Learning Summit 2019, September 2019 / SUITE5

	Event Reporting Template
Type	Participation in Conference .
Event Name	RE-WORK Deep Learning Summit 2019
Venue	London, UK
Date	19-20/09/2019
Event objectives	The Deep Learning Summit focuses on bridging the gap between the latest technological research advancement and real-world applications in business and society. Sessions present Generative Models, Automated Learning, Reinforcement Learning, Computer Vision and Applied Deep Learning and explore real-world case studies that highlight the business value of AI.
Size of audience (approx.)	600
Dissemination Level	International
URL	https://www.re-work.co/events/deep-learning-summit-london-2019
Description of activity	The summit was an excellent networking opportunity due to the diverse audience it brings together, which is a mix of academia and industry. Through our participation we managed to discuss the technological challenges that ASCLEPIOS faces with AI pioneers both in research and in industry, present its vision and get valuable feedback.
Title	-
Presenter	-
Partners Involved	Suite5
Type of Audience	• Academia and Research • Industry (Tech)
Hash tags for Social Media Dissemination	#DeepLearningSummit #reworkDL
Relevant Resources	-

Table AI-10 Florida Institute for Cybersecurity Weekly Seminar (FICS), October 2019 /AMC

	Event Reporting Template
Type	Seminar
Event Name	Florida Institute for Cybersecurity Weekly Seminar
Venue	University of Florida - Gainesville, FL, USA
Date	10/10/2019
Event objectives	Text describing the objectives of the event
Size of audience (approx.)	30
Dissemination Level	International
URL	https://fics.institute.ufl.edu/about-fics/
Description of activity	Presentation of the Red Alert Paper and talk about main idea of ASCLEPIOS project with the audience. Marcela was invited by Dr.Daniela Seabra Oliveira, Diversity Director of FICS. Presentation abstract: Availability of medical records during an emergency is of paramount importance since it allows healthcare professionals to access patient's data on time and properly plan the next steps that need to be taken. Cloud storage has the potential to provide a solution to the problem of data unavailability during an emergency. However, sharing medical records raises several concerns about security and privacy. To overcome this, the project ASCLEPIOS (Advanced Secure Cloud Encrypted Platform for Internationally Orchestrated Solutions in Healthcare) has the goal of maximizing and fortifying the trust of users on cloud-based healthcare services by developing

	cryptography mechanisms for protecting both corporate and personal sensitive data. The Amsterdam University Medical Centres, Location AMC, is a leading player in stroke treatment in the Netherlands and one of the partners of the ASCLEPIOS consortium hosting a use case real-life demonstrator. In this talk I present one of the first results, the Red Alert protocol, a dynamic granting and revoking data access protocol which a team of healthcare professionals can securely decrypt the medical records of a patient who is under an emergency (e.g. acute stroke). Furthermore, our protocol ensures that a team of healthcare professionals will only have access to the patient's data for the time needed to complete a specific process related to the patient's situation (e.g. transfer patient to the hospital).
Title	Red Alert: Break-Glass Protocol to Access Encrypted Medical Records in the Cloud
Presenter	Marcela Tuler de Oliveira
Other Partners Involved	AMC/TUNI
Type of Audience	Academia and Research
Hash tags for Social Media Dissemination	#UF #FICS #RedAlert
Relevant Resources	-

Table AI-11 IEEE International Conference on E-health Networking, Application & Services (Healthcom 2019), October 2019 / AMC

	Event Reporting Template
Type	Participation in Conference
Event Name	IEEE International Conference on E-health Networking, Application & Services (Healthcom 2019)
Venue	Bogota, Colombia
Date	14-16 October 2019
Event objectives	To bring together interested parties from around the world working in the healthcare field to exchange ideas, discuss innovative and emerging solutions, and develop collaborations.
Size of audience (approx.)	60
Dissemination Level	International
URL	https://healthcom2019.ieee-healthcom.org/about
Description of activity	Articles presentations and social lunch/dinner
Title	Red Alert: Break-Glass Protocol to Access Encrypted Medical Records in the Cloud
Presenter	Marcela Tuler de Oliveira, AMC
Partners Involved	AMC and TUNI
Type of Audience	• Academia and Research • Industry (mixed)
Hash tags for Social Media Dissemination	#healthcom2019 #RedAlert
Relevant Resources	• https://ieeexplore.ieee.org/abstract/document/9009598

Table AI-12 15th EAI International Conference on Security and Privacy in Communication Networks (SecureComm 2019), October 2019 / TUNI

	Event Reporting Template

Type	Participation in Conference
Event Name	15th EAI International Conference on Security and Privacy in Communication Networks – SecureComm 2019
Venue	Crown Plaza Orlando Downtown
Date	23-25/10/2019
Event objectives	SecureComm seeks high-quality research contributions, which have not been previously published or in parallel submission to another conference or journal. Topics of interest encompass research advances in ALL areas of secure communications and networking.
Size of audience (approx.)	100
Dissemination Level	International,
URL	http://securecomm2019.eai-conferences.org/
Description of activity	In the paper *"Modern Family: A Revocable Hybrid Encryption Scheme Based on Attribute-Based Encryption, Symmetric Searchable Encryption and SGX",* we extended the work presented in the *"Lord of the Shares"* by providing a formal description of the proposed scheme. Moreover, we focused on the cryptographic security of the underlying ABE and SSE schemes that were used throughout the paper.
Title	Modern Family: A Revocable Hybrid Encryption Scheme Based on Attribute-Based Encryption, Symmetric Searchable Encryption and SGX
Presenter	Alexandros Bakas
Partners Involved	Involved ASCLEPIOS partners for this activity you should indicate that here.
Type of Audience	Select one or more of the following: 1. Academia and Research 2. Industry (Tech) 3. Industry (mixed)
Hash tags for Social Media Dissemination	#SecureComm2019
Relevant Resources	-

Table AI-13 ACM Cloud Computing Security Workshop (CCSW 2019), November 2019 / UOW

	Event Reporting Template
Type	Participation in Workshop
Event Name	ACM Cloud Computing Security Workshop (CCSW 2019)
Venue	London, United Kingdom
Date	11th November 2019
Event objectives	CCSW brings together researchers and practitioners in all security aspects of cloud-centric and outsourced computing topics, such as practical cryptographic protocols for cloud security, secure cloud resource virtualization mechanisms, secure data management outsourcing (e.g., database as a service), practical privacy and integrity mechanisms for outsourcing, remote attestation mechanisms in clouds, sandboxing and VM-based enforcement, trust and policy management in clouds and secure identity management mechanisms
Size of audience (approx.)	ca. 100
Dissemination Level	International
URL	https://ccsw.io/
Description of activity	UOW researchers attended the CCSW 2019, Dang, H-V presented a short paper on the ASCLEPIOS security solutions.
Title	Access Control in Searchable Encryption with the Use of Attribute-based Encryption and SGX
Presenter	Dang, H-V.
Partners Involved	TUNI and UOW
Type of Audience	• Academia and Research • Industry (mixed)

Hash tags for Social Media Dissemination	#Attributre Based Encryption #Searchable Encryption #Software Guard Extensions
Relevant Resources	-

Table AI-14 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN 2019), November 2019 / RISE

	Event Reporting Template
Type	Participation in Conference
Event Name	IEEE Conference on Network Function Virtualization and Software Defined Networks
Venue	Dallas, USA
Date	12-14 November 2019
Event objectives	Present the conference paper "Protecting OpenFlow using Intel SGX"
Size of audience (approx.)	500
Dissemination Level	International
URL	https://nfvsdn2019.ieee-nfvsdn.org/
Description of activity	Presentation of a research paper by Jorge Medina. Abstract: OpenFlow flow tables in Open vSwitch contain valuable information about installed flows, priorities, packet actions and routing policies. Their importance is emphasized when collocated tenants compete for the limited entries available to install flow rules. OpenFlow flow tables are a security asset that requires confidentiality and integrity guarantees. However, commodity software switch implementations - such as Open vSwitch - do not implement protection mechanisms capable to prevent attackers from obtaining information about the installed flows or modifying flow tables. We adopt a novel approach to enabling OpenFlow flow table protection through decomposition. We identify core assets requiring security guarantees, isolate OpenFlow flow tables through decomposition and implement a prototype using Open vSwitch and Software Guard Extensions enclaves. An evaluation of the prototype on a distributed testbed both demonstrates that the approach is practical and indicates directions for further improvements.
Title	Protecting OpenFlow using Intel SGX
Presenter	Jorge Medina
Partners Involved	RISE Research Institutes of Sweden
Type of Audience	• Academia and Research • Industry (mixed)
Hash tags for Social Media Dissemination	#IntelSGX; #OpenFlow; #Security
Relevant Resources	-

Table AI-15 5th ICT Security World: Digital transformation & Cybersecurity, November 2019 / ICCS

	Event Reporting Template
Type	Participation in Industrial Conference (including public administrations and policy makers)
Event Name	ICT Security World
Venue	Athens, Greece.
Date	November 14, 2019
Event objectives	Discuss digital transformation and cybersecurity issues in Cloud
Size of audience (approx.)	>200
Dissemination Level	Greek
URL	https://www.ictsecurity.gr/

Description of activity	Presentation of the main aspects of ASCLEPIOS security services and panel discussion with top executives from the cloud and cybersecurity industry. The presentation was held in Greek language and focused, among others, on the security challenges in cloud-based healthcare applications, while it analysed the main aspects of the ASCLEPIOS authorization (based on the combination of ABAC and ABE paradigms). The audience (>200 people) included among others: representatives from the cloud computing industry, CEOs and CTOs from the top cybersecurity-focused Greek SMEs and General Secretaries from the Greek Ministry of Digital Governance. The presentation attracted significant positive comments for the ASCLEPIOS potential impact.
Title	Cybersecurity in Cloud: Research challenges and results
Presenter	Yiannis Verginadis (ICCS)
Partners Involved	ICCS
Type of Audience	• Industry, • Public Administrations
Hash tags for Social Media Dissemination	#CloudSecurity #H2020 #ICTSecurityWorld #ABE #ABAC
Relevant Resources	• **Photo:** ictworld.jpg • **Agenda:** https://www.ictsecurity.gr/programma

Table AI-16 24th Nordic Conference on Secure IT Systems (NordSec 2019), November 2019 / TUNI

	Event Reporting Template
Type	Participation in Conference .
Event Name	The 24th Nordic Conference on Secure IT Systems (NordSec 19)
Venue	Aalborg, Denmark
Date	November 18-20, 2019
Event objectives	Text describing the objectives of the event
Size of audience (approx.)	30
Dissemination Level	International
URL	https://nordsec2019.cs.aau.dk/
Description of activity	In the paper *"MicroScope: Enabling Access Control in Symmetric Searchable Encryption with the use of Attribute-Based Encryption and SGX",* we extended the works presented in the *"Lord of the Shares"* and *"Modern Family".* We proved that our construction is secure against a stronger threat model. Moreover, we conducted thorough experiments using Intel's SGX to test the overall performance of the construction. NordSec is an annual research conference series that has been rNSEing since 1996. The NordSec conferences address a broad range of topics on IT security. The events bring together security researchers from the Nordic countries, Northern Europe, and beyond. In addition to being venue for academic publishing, NordSec is an important meeting place for university faculty, students, and industry researchers and experts from the region.
Title	*"MicroScope: Enabling Access Control in Symmetric Searchable Encryption with the use of Attribute-Based Encryption and SGX"*
Presenter	Alexandros Bakas, Alexandr Zalitko
Other Partners Involved	University of Westminster (Hai-Van Dang)
Type of Audience	• Academia and Research • Industry (mixed)
Hash tags for Social Media Dissemination	#NordSec, #SearchableEncryption #SSE #AttributeBasedEncryption #ABE #Cryptography #SecureStorage #CloudSecurity

Relevant Resources	• Photo: ASCLEPIOS_2019_11_NordSec.jpg • https://nordsec2019.cs.aau.dk/#program

Table AI-17 UCL Research Programming Technical Socials at University College London, December 2019 / UOW

	Event Reporting Template
Type	Participation in Technical Social Event.
Event Name	KQ Codes Technical Socials
Venue	London, United Kingdom
Date	11th December 2019
Event objectives	These informal events are for anyone with an interest in the computational methods and technology behind research and innovation. They are an opportunity to get to know fellow practitioners, and to discuss and learn about useful tools and techniques which may help with your work.
Size of audience (approx.)	ca. 70
Dissemination Level	Regional
URL	https://rslondon.ac.uk/
Description of activity	J. Deslauriers gave a short introduction on cloud computing, presented the MiCADO framework and how researchers can benefit using this framework.
Title	Building a Cloud Toolkit
Presenter	Deslauriers, J.
Partners Involved	UOW.
Type of Audience	Academia and Research
Hash tags for Social Media Dissemination	#cloud #MiCADO #JQueuer
Relevant Resources	-

Table AI-18 2nd Annual Research Software London Workshop (RSLondonSouthEast 2020), February 2020 / UOW

	Event Reporting Template
Type	Participation in Workshop
Event Name	RSLondonSouthEast 2020
Venue	London, United Kingdom
Date	6th February 2020
Event objectives	The workshop provides a regional focus on research software activities and offer an opportunity to present work to a regional audience, but it also aims to help participants develop links with the wider national and international RSE community. The workshop is open to participants from elsewhere in the UK and beyond.
Size of audience (approx.)	ca. 150
Dissemination Level	National
URL	https://rslondon.ac.uk/rslondonse-2020/
Description of activity	UOW researchers attended the UKRI Cloud Workshop to present the MiCADO framework and how it can be used to describe, deploy and execution in multiple clouds. They gave one lightning and one poster lightning talk.
Title	Deploying and auto-scaling scientific applications in the cloud using Terraform and MiCADO
Presenter	Ariyutta, R.
Partners Involved	UOW
Title	A generic cloud-agnostic platform to support the execution of deadline-constrained workloads
Presenter	Ullah, A.

Partners Involved	UOW
Type of Audience	Academia and Research
Hash tags for Social Media Dissemination	#cloud #MiCADO #TOSCA
Relevant Resources	-

Table AI-19 UKRI Cloud Workshop 2020, March 2020 / UOW

	Event Reporting Template
Type	Participation in Workshop
Event Name	UKRI Cloud Workshop 2020
Venue	London, United Kingdom
Date	3rd March 2020
Event objectives	The workshop presented the latest trends in Cloud Computing, such as hybrid clouds, managing and using private and public clouds, HPC in the Cloud, integrating data access and storage interfaces, and how to use clouds in research.
Size of audience (approx.)	ca. 150
Dissemination Level	National
URL	https://cloud.ac.uk/
Description of activity	The UOW researchers attended the UKRI Cloud Workshop to present the MiCADO framework and how it can be used to describe, deploy and execution in multiple clouds.
Title	Describing portable applications with TOSCA
Presenter	Deslauriers, J.
Partners Involved	UOW
Title	ASCLEPIOS – Health Care Security
Presenter	Pierantoni, G
Partners Involved	UOW
Relevant Resources	-

Table AI-20 Biosignal Conference by DGBMT / VDE (BIOSIGNALE 2020), March 2020 / CHARITE

	Event Reporting Template
Type	Participation in Conference
Event Name	Workshop Biosignale 2020
Venue	University Kiel, Auditorium
Date	11. – 13. March 2020
Event objectives	The conference and workshop was dedicated to biosignal analysis
Size of audience (approx.)	60
Dissemination Level	National
URL	https://www.vde.com/en/events/event-detailpage?id=17114&type=vde%7Cvdb
Description of activity	The workshop was on all kinds of biosignal processing and storage. A major problem of biosignals is storing the data together with clinical data, patient data, annotations and interpretations. The interpretations are derived from the data itself or with the help of physicians investigating the patients. Sometimes medical image data are included, and required as well. The data are stored in encrypted storage systems and are accessible through secure data transfer. A solution as prepared by Asclepios is the desirable goal for all stakeholders involved.
Title	Secure integration of biomedical signal data in a medical cloud for sleep medicine
Presenter	Thomas Penzel
Partners Involved	Charite
Type of Audience	Academia and Research

Hash tags for Social Media Dissemination	-
Relevant Resources	-

Table AI-21 5th International Conference on Internet of Things, Big Data and Security (IoTBDS 2020), May 2020 / TUNI

	Event Reporting Template
Type	Participation in Conference
Event Name	5th International Conference on Internet of Things, Big Data and Security (IoTBDS)
Venue	Online
Date	The date that the event took place
Event objectives	The internet of things (IoT) is a platform that allows a network of devices (sensors, smart meters, etc.) to communicate, analyse data and process information collaboratively in the service of individuals or organisations. The IoT network can generate large amounts of data in a variety of formats and using different protocols which can be stored and processed in the cloud. The conference looks to address the issues surrounding IoT devices, their interconnectedness and services they may offer, including efficient, effective and secure analysis of the data IoT produces using machine learning and other advanced techniques, models and tools, and issues of security, privacy and trust that will emerge as IoT technologies mature and become part of our everyday lives. Big Data (BD) has core values of volume, velocity, variety and veracity. After collecting much data from IoT, BD can be jointly used with machine learning, AI, statistical and other advanced techniques, models and methods, which can create values for people and organizations adopting it, since forecasting, deep analysis and analytics can help identify weaknesses and make improvements based on different analysis. Maintaining a high level of security and privacy for data in IoT are crucial and we welcome recommendations, solutions, demonstrations and best practices for all forms of security and privacy for IoT and BD
Size of audience (approx.)	-
Dissemination Level	International
URL	http://iotbds.org/Home.aspx?y=2020
Description of activity	In the paper "*Do not tell me what I cannot do! (The constrained device shouted under the cover of the fog): Implementing Symmetric Searchable Encryption on Constrained Devices*" we showed that rNSEing an SSE scheme in constrained devices is feasible. Thorough experimentation was conducted to prove the efficiency of our construction which also preserved the important security notion of forward privacy.
Title	Do not tell me what I cannot do! (The constrained device shouted under the cover of the fog): Implementing Symmetric Searchable Encryption on Constrained Devices
Presenter	Eugene Frimpong
Partners Involved	TUNI-UOW
Type of Audience	• Academia and Research • Industry (mixed)
Hash tags for Social Media Dissemination	#IoTBDS2020
Relevant Resources	-

Events ASCLEPIOS Organised during M1-M18

Table AI-22 1st ASCLEPIOS Awareness Workshop, January 2020 / SECURA

	Event Reporting Template
Type	Organisation of Workshop
Event Name	Protecting vital assets, the art and science of working with medical data
Venue	Secura's offices, Amsterdam, The Netherlands
Date	16 January 2020
Event objectives	Increase awareness towards the security and privacy of medical data, as well as increase awareness towards the ASCLEPIOS architecture goals and objectives
Size of audience (approx.)	25
Dissemination Level	International
URL	https://www.secura.com/asclepios-awareness-workshop
Description of activity	The first of this series of workshops took place on the 16 January 2020, at the location of Secura in Amsterdam, the Netherlands. This workshop, themed "Protecting vital assets, the art and science of working with medical data" will focus on the current limitations concerning the collection, storage and access to the sensitive patient's medical data and how ASCLEPIOS attempts to solve these. The topics discussed in the workshop addressed the topics of security and privacy in both technical and non-technical way. While parts of the talks did go deeper into topics of security or GDPR, the core of the workshop was designed such that all the members of the audience have the chance of getting involved in the topics. Exercises focused on the discussed items aimed at increasing the interaction between the audience members, helping in a better understanding of the topics.
Title	Protecting vital assets, the art and science of working with medical data Various presentations were provided during the workshop, aimed at threat modeling, attacker/defender perspective, ASCLEPIOS architecture, state of the art in a connected healthcare environment
Presenter	Christiaan Hillen (Secura), Ewald Beekman (UMC), Marcela Tuler (UMC)
Partners Involved	Secura (organiser), UMC (guest speakers)
Type of Audience	• Academia and Research • Industry (Health) • Industry (Tech) • Policy Makers
Hash tags for Social Media Dissemination	N/A
Relevant Resources	Attachments such as: (please indicate filenames or URLs) Please refer to files: • Security Awareness Workshop 16 January 2020 - Photos and Agenda • Security awareness workshop 16 January 2020 – Agenda • Presentations were shared with the attendees, but not made public

ASCLEPIOS Publications during M1-M18

Following are the completed reporting templates for the ASCLEPIOS scientific publications during the first reporting period:

Table AI-23 The Lord of the Shares: Combining Attribute-Based Encryption and Searchable Encryption for Flexible Data Sharing. (SAC 2019) / TUNI

Publication Reporting Template

Full citation	Antonis Michalas. "The Lord of the Shares: Combining Attribute-Based Encryption and Searchable Encryption for Flexible Data Sharing". In Proceedings of the 34th ACM/SIGAPP Symposium On Applied Computing (SAC). Limassol, Cyprus, April 08 – 12, 2019.
Responsible	Antonis Michalas
Partners Involved	The name of the ASCLEPIOS partners involved in this paper
Hash tags for Social Media Dissemination	#ACMSAC #SearchableEncryption #SSE #AttributeBasedEncryption #ABE #Cryptography #SecureStorage #CloudSecurity
Dissemination Level	International
Type of Audience	• Academia and Research • Industry (mixed)
URL	Provide a relevant URL, if one exists
Attachment	*../Pydio\ASCLEPIOS Project\WP7 - Dissemination, Exploitation and Communication/Dissemination Archieve/***2019 - P1 - SAC - LotS.pdf**

Table AI-24 A Secure Cloud-based Platform to Host Healthcare Applications. (IWSG 2019 / UOW, AMC, NSE, HTW, CHARITE

	Publication Reporting Template
Full citation	Pierantoni, G., Kiss, T., Terstyanszky, G., Dang, H., Delgado Olabarriaga, S., Tuler de Olivera, M., Yigzaw, K. Y., Belika, J. G., Krefting, D. and Penzel, T: A Secure Cloud-based Platform to Host Healthcare Applications, 11th International Workshop on Science Gateways, IWSG 2019, Ljubjana, Slovenia, 12-14th June 2019
Responsible	Pierantoni, G
Partners Involved	UOW, AMC, NSE, HTW, CHARITE
Hash tags for Social Media Dissemination	#cloud #security #Healthcare
Dissemination Level	International
Type of Audience	Academia and Research
URL	https://research.westminster.ac.uk/qv2xz/a-secure-cloud-based-platform-to
Attachment	The final (camera ready) version of the publication e.g. in .pdf

Table AI-25 Protecting OpenFlow Flow Tables with Intel SGX. (SIGCOMM 2019) / RISE

	Publication Reporting Template
Full citation	Nicolae Paladi, Jakob Svenningsson, Jorge Medina, and Patrik Arlos. 2019. Protecting OpenFlow Flow Tables with Intel SGX. In Proceedings of the ACM SIGCOMM 2019 Conference Posters and Demos (SIGCOMM Posters and Demos '19). Association for Computing Machinery, New York, NY, USA, 146–147. DOI:https://doi.org/10.1145/3342280.3342339
Responsible	Nicolae Paladi
Partners Involved	RISE Research Institutes of Sweden
Hash tags for Social Media Dissemination	#IntelSGX; #OpenFlow; #ConfidentialComputing
Dissemination Level	International
Type of Audience	• Academia and Research • Industry (mixed)
URL	https://dl.acm.org/doi/pdf/10.1145/3342280.3342339
Attachment	(Open Access) https://dl.acm.org/doi/pdf/10.1145/3342280.3342339

Table AI-26 Red Alert: Break-Glass Protocol to Access Encrypted Medical Records in the Cloud. (Healthcom 2019) / AMC, TUNI

	Publication Reporting Template

Full citation	"Red Alert: Break-Glass Protocol to Access Encrypted Medical Records in the Cloud". Marcela Tuler de Oliveira, Antonis Michalas, Adrien E. D. Groot, Henk A. Marquering, Sílvia Delgado Olabarriaga. In 2019 IEEE 21th International Conference on e-Health Networking, Applications and Services (Healthcom) 2019 Oct0 15. IEEE
Responsible	Marcela Tuler de Oliveira
Partners Involved	Amsterdam University Medical Centre (AMC) and Tampere University (TUNI)
Hash tags for Social Media Dissemination	#Healthcom2019 #IEEE
Dissemination Level	International
Type of Audience	• Academia and Research
URL	https://ieeexplore.ieee.org/xpl/conhome/1002408/all-proceedings (NOT available yet)
Attachment	The final (camera ready) version of the publication e.g. in .pdf or .doc

Table AI-27 Modern Family: A Hybrid Encryption Scheme Based on Attribute-Based Encryption, Symmetric Searchable Encryption and SGX. (SecureComm 2019) / TUNI

	Publication Reporting Template
Full citation	Bakas, A., & Michalas, A. (2019). *Modern Family: A Revocable Hybrid Encryption Scheme Based on Attribute-Based Encryption, Symmetric Searchable Encryption and SGX*.
Responsible	Alexandros Bakas.
Partners Involved	TUNI
Hash tags for Social Media Dissemination	#SecureComm2019
Dissemination Level	International
Type of Audience	• Academia and Research • Industry (mixed)
URL	-
Attachment	*…/Pydio/ASCLEPIOS Project/WP7-Dissemination,Exploitation and Communication/Dissemination Archive/***2019 – P2 – SecureComm – MF.pdf**

Table AI-28 Access Control in Searchable Encryption with the Use of Attribute-based Encryption and SGX. (CCSW 2019) / TUNI, UOW

	Publication Reporting Template
Full citation	Michalas, A., Bakas, A., Dang, H-V., & Zalitko, A. (2019). *Access Control in Searchable Encryption with the use of Attribute-Based Encryption and SGX*.
Responsible	Antonis Michalas.
Partners Involved	TUNI-UOW
Hash tags for Social Media Dissemination	#CCSW19
Dissemination Level	International
Type of Audience	• Academia and Research • Industry (mixed)
URL	Provide a relevant URL, if one exists
Attachment	The final (camera ready) version of the publication e.g. in .pdf or .doc

Table AI-29 Protecting OpenFlow using Intel SGX. (NFV-SDN 2019)) / RISE

	Publication Reporting Template

Full citation	J. Medina, N. Paladi and P. Arlos, "Protecting OpenFlow using Intel SGX," 2019 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), Dallas, TX, USA, 2019, pp. 1-6, doi: 10.1109/NFV-SDN47374.2019.9039980.
Responsible	Nicolae Paladi
Partners Involved	RISE Research Institutes of Sweden
Hash tags for Social Media Dissemination	#IntelSGX; #OpenFlow; #ConfidentialComputing
Dissemination Level	International
Type of Audience	• Academia and Research • Industry (mixed)
URL	https://ieeexplore.ieee.org/document/9039980
Attachment	Published version - Open Access: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9039980

Table AI-30 MicroSCOPE: Enabling Access Control in Searchable Encryption with the use of Attribute-based Encryption and SGX. (Nordsec 2019) / TUNI, UOW

	Publication Reporting Template
Full citation	Antonis Michalas, Alexandros Bakas, Hai-Van Dang, Alexandr Zalitko. "MicroSCOPE: Enabling Access Control in Searchable Encryption with the Use of Attribute-Based Encryption and SGX". In Proceedings of the 24th Nordic Conference on Secure IT Systems. Aalborg, Denmark, November 18 – 12, 2019.
Responsible	Antonis Michalas.
Partners Involved	Tampere University, University of Westminster
Hash tags for Social Media Dissemination	#NordSec, #SearchableEncryption #SSE #AttributeBasedEncryption #ABE #Cryptography #SecureStorage #CloudSecurity
Dissemination Level	International
Type of Audience	• Academia and Research • Industry (mixed)
URL	https://nordsec2019.cs.aau.dk
Attachment	*…/Pydio/ASCLEPIOS Project/WP7-Dissemination,Exploitation and Communication/Dissemination Archive/***2019 – P3 – MicroSCOPE – MSCOPE.pdf**

Table AI-31 A generic cloud-agnostic platform to support the execution of deadline-constrained workloads. (RSLondonSouthEast 2020) / UOW

	Publication Reporting Template
Full citation	Ullah, A., Deslauriers, J., Kiss, T.: A generic cloud-agnostic platform to support the execution of deadline-constrained workloads, lightning talk, 06th February 2020
Responsible	Ullah, A.
Partners Involved	UOW
Hash tags for Social Media Dissemination	#cloud orchestration TOSCA policies MiCADO
Dissemination Level	Regional
Type of Audience	Academia and Research
URL	Not available
Attachment	The final (camera ready) version of the publication e.g. in .pdf

Table AI-32 Deploying and auto-scaling scientific applications in the cloud using Terraform and MiCADO. (RSLondonSouthEast 2020) / UOW

	Publication Reporting Template
Full citation	R. Ariyattu, Deslauriers, J., Kiss, T Deploying and auto-scaling scientific applications in the cloud using Terraform and MiCADO, poster lighting talk, 06th February 2020
Responsible	R. Ariyattu
Partners Involved	UOW
Hash tags for Social Media Dissemination	#cloud #auto-scaling #TerraForm #MiCADO
Dissemination Level	Regional
Type of Audience	Academia and Research
URL	Not available
Attachment	The final (camera ready) version of the publication e.g. in .pdf

Table AI-33 A context-aware security model for a combination of attribute-based access control and attribute-based encryption in the healthcare domain. (M2EC/WAINA 2020) / ICCS

	Publication Reporting Template
Full citation	Psarra, E., Verginadis, Y., Patiniotakis, I., Apostolou, D., & Mentzas, G. (2020, April). A Context-Aware Security Model for a Combination of Attribute-Based Access Control and Attribute-Based Encryption in the Healthcare Domain. In Workshops of the International Conference on Advanced Information Networking and Applications (pp. 1133-1142). vol 1150 Springer, Cham.
Responsible	Evgenia Psarra
Partners Involved	ICCS
Hash tags for Social Media Dissemination	#Context-AwareSecurityModel, #ABE, #ABAC, #HealthcareDataSecurity
Dissemination Level	International
Type of Audience	• Academia and Research • Industry (health) • Industry (Tech) • Policy Makers
URL	https://link.springer.com/chapter/10.1007/978-3-030-44038-1_104
Attachment	The final (camera ready) version of the publication in .pdf.

Table AI-34 Do not tell me what I cannot do! (The constrained device shouted under the cover of the fog): Implementing Symmetric Searchable Encryption on Constrained Devices. (IOTDBS 2020) / TUNI, UOW

	Publication Reporting Template
Full citation	Frimpong, E., Bakas, A., Dang, H-V., & Michalas, A. (2020). *Do not tell me what I cannot do! (The constrained device shouted under the cover of the fog): Implementing Symmetric Searchable Encryption on Constrained Devices (Extended Version)*
Responsible	Eugene Frimpong.
Partners Involved	TUNI-UOW
Hash tags for Social Media Dissemination	#IoTBDS20
Dissemination Level	International
Type of Audience	• Academia and Research • Industry (mixed)
URL	Provide a relevant URL, if one exists
Attachment	The final (camera ready) version of the publication e.g. in .pdf or .doc

Table AI-35 Network Physiology in Insomnia Patients: Assessment of Relevant Changes in Network Topology with Interpretable Machine Learning Models. (Chaos Journal, 2019) / CHARITE, HTW

	Publication Reporting Template
Full citation	Jansen C, Penzel T, Hodel S, Breuer S, Spott M, Krefting D. Network Physiology in Insomnia Patients: Assessment of relevant changes in network topology with interpretable machine learning models. Chaos 2019;
Responsible	Christoph Jansen (and Dagmar Krefting and Thomas Penzel)
Partners Involved	Charite, HTW
Hash tags for Social Media Dissemination	
Dissemination Level	International
Type of Audience	Academia and Research, Industry (mixed)
URL	doi: 10.1063/1.5128003
Attachment	The final (camera ready) version of the publication is available at APS

Table AI-36 A Break-Glass Protocol based on Ciphertext-Policy Attribute-Based Encryption to Access Medical Records in the Cloud. (Annals of Telecommunication Journal, 2020) / AMC

	Publication Reporting Template
Full citation	de Oliveira, M. T., Bakas, A., Frimpong, E., Groot, A. E., Marquering, H. A., Michalas, A., & Olabarriaga, S. D. (2020). A break-glass protocol based on ciphertext-policy attribute-based encryption to access medical records in the cloud. *Annals of Telecommunications*, 1-17.
Responsible	Marcela Tuler de Oliveira and Alexandros Bakas
Partners Involved	Amsterdam UMC and TUNI
Hash tags for Social Media Dissemination	#Break-glass #AccessControl #EMR
Dissemination Level	International
Type of Audience	• Academia and Research • Industry (health) • Industry (Tech) • Industry (mixed)
URL	https://link.springer.com/content/pdf/10.1007/s12243-020-00759-2.pdf
Attachment	Open access publication

Annex II. Industry Communities/Organisations

Following is the list of Industry Communities/Organisations that were reached during the first reporting period:

Table AII-1 Industry Communities/Organisations Approached during [M1-M18]

Industry Community/ Organisation	Industry Community/Organisation Scope	Purpose of Communication/ Type of Activity	Participating Partner
ARM[25]	Vendor of microprocessor cores and technologies	Communication of ASCLEPIOS project and objectives regarding TEEs	RISE
SContain[26]	Services for confidential computing of containers and host programs using Intel SGX	Communication of ASCLEPIOS objectives and technical discussions about usage of Intel SGX	SUITE5
CloudSME[27]	Provision of vendor independent cloud technology	Commercialising the MiCADO framework (MiCADOscale), providing support to deploy and run application in the Cloud	UOW
Balasys[28]	Vendor of proxy-based gateway technologies	Balasys developed the security components of MiCADO used for the deployment of the ASCLEPIOS demonstrators. UOW has taken over the future development and maintenance of these components from Balasys.	UOW
REMEDI	Community for medical device informatics	The two projects can cooperate with each other to further advance research in Healthcare.	UOW

[25] https://www.arm.com/
[26] https://scontain.com/index.html?lang=en
[27] https://cloudsme.eu/
[28] https://www.balasys.hu/

Annex III. 1st Issue of ASCLEPIOS eNewsletter

Following is the full version of the 1st Issue of the ASCLEPIOS eNewsletter – February 2020:

NEWSLETTER | ISSUE 01 FEBRUARY 2020

ASCLEPIOS

Advanced Secure Cloud Encrypted Platform for Internationally Orchestrated Solutions in Healthcare

In this issue

AT A GLANCE

ASCLEPIOS is a 3-year Research and Innovation project funded under Horizon 2020. It kicked off in December 2018 in Athens, and will end at November 2021.

The vision of ASCLEPIOS is to maximise the trust of users on cloud-based healthcare services by developing mechanisms that protect corporate and personal sensitive data, using modern cryptographic approaches. This cloud-based eHealth framework will be showcased in three demonstrators provided by ASCLEPIOS healthcare partners, involving three leading European hospitals.

www.asclepios-project.eu @Asclepios_H2020 Asclepios-project

The ASCLEPIOS project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 826093

01

NEWSLETTER | ISSUE 01 FEBRUARY 2020

ASCLEPIOS

VISION

The healthcare sector is undergoing a massive digital transformation and eHealth stands in the spotlight. Although the core idea in the early stages of eHealth was mainly to digitalise handwritten patient records, scientists have gone a long way beyond that: they envisioned a world where patients could access their digital medical record and share it with healthcare professionals regardless of their location.

Although someone would expect rapid adoption of these promising technologies, the lack of effective security mechanisms is making healthcare professionals and patients reluctant to store sensitive data online, resulting in an overall slow adoption of eHealth.

ASCLEPIOS will design and develop an eHealth framework that will allow patients to store and share their medical records in a secure and privacy-preserving way while at the same time they will be able to receive certain guarantees about the trusted state of the overall framework. In addition to that, healthcare proffesionals will be able to perform analytics in a privacy-preserving way.

Driven by the vision to bridge new technologies and health data security, the ASCLEPIOS project will address these challenges and build a cloud-based eHealth framework that protects users' privacy. The contribution of ASCLEPIOS revolves around three axes:

Medical data encryption and sharing with modern cryptographic schemes

Software- and Hardware-based attestation protocols

Raising security awareness of professionals in the healthcare

The ASCLEPIOS project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 826093

02

NEWSLETTER | ISSUE 01 FEBRUARY 2020

ASCLEPIOS

PLATFORM

The ASCLEPIOS Platform comprises various components, which interact with each other and provide the core ASCLEPIOS functionalities:

Trusted Cloud Provider: Storage of encrypted data and components hosting

Analytics Layer: Secure analytics on health-related data

Revocation Authority: Smooth user revocation (e.g. when compromised)

Registration Authority: Registration of medical personnel and patients to eHealth services

Policy Enforcement Layer: Efficient and flexible access policies enforcement

Attestation Layer: Server integrity validation and identification of unauthorised modifications

Crypto Layer: Cryptography toolkit (Searchable Encryption, Attribute-based Encryption, Functional Encryption)

More about the ASCLEPIOS Architecture here!

The ASCLEPIOS project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 826093

03

NEWSLETTER | ISSUE 01 FEBRUARY 2020

ASCLEPIOS

DEMONSTRATORS

Three demonstrators provided by the ASCLEPIOS healthcare partners will showcase the functionalities of ASCLEPIOS in different use cases. Leading European hospitals and research centres will be involved.

Monitoring & Benchmarking of Antibiotic Prescription

Provision of feedback to clinicians on their antibiotics prescriptions, while protecting privacy

Aggregated performance indicators, across healthcare organisations, using secure multiparty computation

Pilot: Norwegian Centre for E-health Research

Stroke Acute Care Treatment & Research

Dynamic access authorisation to patient information during the stroke hyper-acute phase

Privacy-preserving analytics on cloud-based medical data for predictive modelling in stroke care research

Pilot: Amsterdam UMC

In- and Outpatient Sleep Medicine

Remote processing of home sleep testing and inpatient recordings, using dynamic access policies

Assessment of signal quality and the patient's health status using functional encryption analytics

Pilot: Charité & CBMI-HTW

The ASCLEPIOS project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 826093

NEWSLETTER | ISSUE 01 FEBRUARY 2020

ASCLEPIOS

EVENTS

ACM SAC 2019

The main idea on the core cryptographic parts of ASCLEPIOS was presented on 12 April 2019 in Limassol, Cyprus at ACM SAC. The paper entitled "The Lord of the Shares: Combining Attribute-Based Encryption and Searchable Encryption for Flexible Data Sharing" was presented by Prof. Antonis Michalas from Tampere University. Read more...

FICS Research Weekly Seminar

The approach of ASCLEPIOS for the stroke acute care demonstrator was presented at the weekly seminar for graduate and undergraduate students, at Florida Institute for Cybersecurity Research, on 10 October 2019. The presented work has been published in the paper "Red Alert: Break-Glass Protocol to Access Encrypted Medical Records in the Cloud". Read more...

ICT Security World 2019

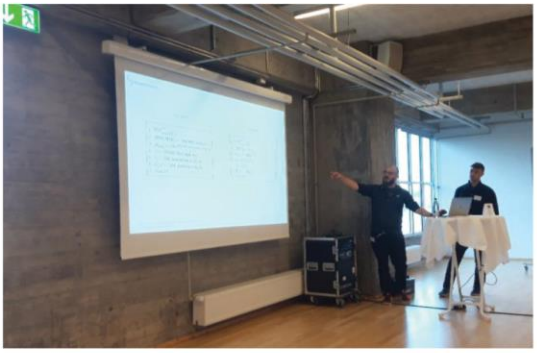
A presentation of the main aspects of ASCLEPIOS security services and panel discussion with top executives from the cybersecurity industry took place in the 5th ICT Security World 2019 on 14 November 2019. The presentation focused, among others, on the security challenges in cloud-based healthcare applications. Read more...

The ASCLEPIOS project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 826093

NEWSLETTER | ISSUE 01 FEBRUARY 2020

ASCLEPIOS

EVENTS



NordSec 2019

The paper "MicroScope: Enabling Access Control in Symmetric Searchable Encryption with the use of Attribute-Based Encryption and SGX",was presented in NordSec 2019 on 20 November 2019. The NordSec conferences address a broad range of topics on IT security. Read more...

1st ASCLEPIOS Awareness Workshop

The first of our security awareness workshops, took place on 16 January 2020, at the location of Secura in Amsterdam. This workshop, themed "Protecting vital assets, the art and science of working with medical data", focused on the current limitations concerning the collection, storage and access to the sensitive patient's medical data. Read more...

H2020 SYNERGY

ASCLEPIOS is part of the H2020 Synergy created among EU-funded projecs in the field of cybersecurity in the healthcare domain. This synergy aims to increase the collaboration among sister projects and promote the exchange and visibility of scientific results through the joint participation in events.

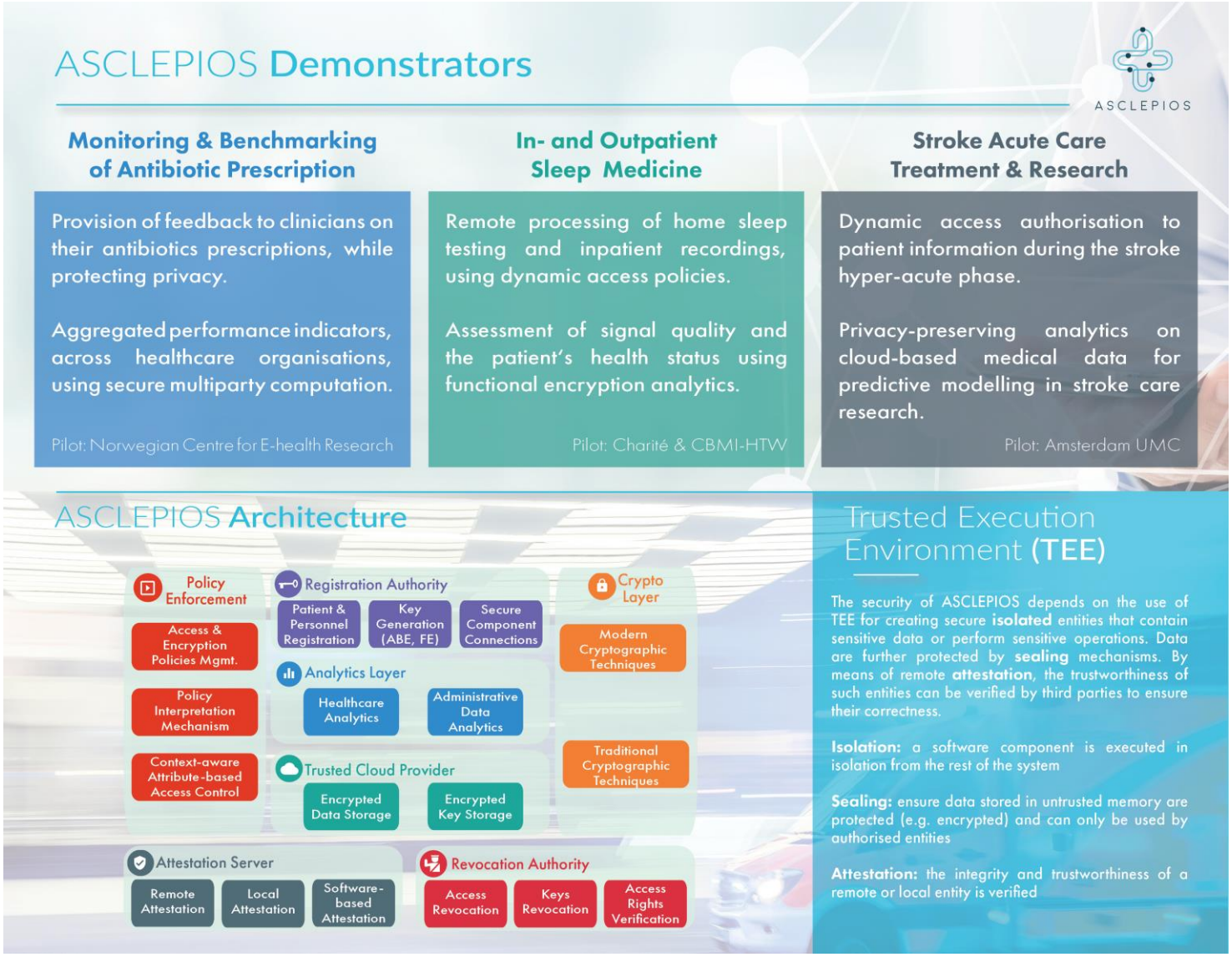
ASCLEPIOS CUREX SPHINX Panacea SAFECARE FeatureCloud

The ASCLEPIOS project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 826093

06


NEWSLETTER | ISSUE 01
FEBRUARY 2020
ASCLEPIOS
WHAT'S NEXT?
New challenges and new adventures for the ASCLEPIOS Project! Stay tuned to discover more...
WE ARE SOCIAL
@Asclepios_H2020
Asclepios-project
www.asclepios-project.eu
Project Coordinator
Tamas Kiss, University of Westminster
t.kiss@westminster.ac.uk
The ASCLEPIOS project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 826093
07

Annex IV. 1st ASCLEPIOS Brochure


ASCLEPIOS Demonstrators
ASCLEPIOS
Monitoring & Benchmarking of Antibiotic Prescription
Provision of feedback to clinicians on their antibiotics prescriptions, while protecting privacy.
Aggregated performance indicators, across healthcare organisations, using secure multiparty computation.
Pilot: Norwegian Centre for E-health Research
In- and Outpatient Sleep Medicine
Remote processing of home sleep testing and inpatient recordings, using dynamic access policies.
Assessment of signal quality and the patient's health status using functional encryption analytics.
Pilot: Charité & CBMI-HTW
Stroke Acute Care Treatment & Research
Dynamic access authorisation to patient information during the stroke hyper-acute phase.
Privacy-preserving analytics on cloud-based medical data for predictive modelling in stroke care research.
Pilot: Amsterdam UMC
ASCLEPIOS Architecture
Policy Enforcement
Access & Encryption Policies Mgmt.
Policy Interpretation Mechanism
Context-aware Attribute-based Access Control
Registration Authority
Patient & Personnel Registration
Key Generation (ABE, FE)
Secure Component Connections
Analytics Layer
Healthcare Analytics
Administrative Data Analytics
Trusted Cloud Provider
Encrypted Data Storage
Encrypted Key Storage
Crypto Layer
Modern Cryptographic Techniques
Traditional Cryptographic Techniques
Attestation Server
Remote Attestation
Local Attestation
Software-based Attestation
Revocation Authority
Access Revocation
Keys Revocation
Access Rights Verification
Trusted Execution Environment (TEE)
The security of ASCLEPIOS depends on the use of TEE for creating secure isolated entities that contain sensitive data or perform sensitive operations. Data are further protected by sealing mechanisms. By means of remote attestation, the trustworthiness of such entities can be verified by third parties to ensure their correctness.
Isolation: a software component is executed in isolation from the rest of the system
Sealing: ensure data stored in untrusted memory are protected (e.g. encrypted) and can only be used by authorised entities
Attestation: the integrity and trustworthiness of a remote or local entity is verified