PaaSword

Dissemination Activities Report
Deliverable D7.2 Interim version 1

Editors
Yiannis Verginadis (ICCS)
Ioannis Patiniotakis (ICCS)
Gregoris Mentzas (ICCS)
Reviewers
Simone Braun (CAS)
George Moldovan (SIE)

Date
31 December 2015
Classification
Public

Contributing Author

Name	Partner
Yiannis Verginadis	ICCS
Yiannis Verginadis	ICCS
George Moldovan	SIEMENS
Yiannis Verginadis	ICCS
Charles Loomis	SixSQ
Spyros Mantzouratos	INTRASOFT
Giannis Ledakis	SINGULAR LOGIC
Simone Braun	CAS
Simos Veloudis	SEERC
Gunther Schiefer	KIT
Charles Loomis	SixSQ
Panagiotis Gouvas	UBITECH
Efi Papatheocharous	SICS
Spyros Mantzouratos	INTRASOFT
Thomas Carnehult	SICS
Gunther Schiefer	KIT
Yiannis Verginadis	ICCS
Yiannis Verginadis	ICCS
George Moldovan	SIEMENS
Simone Braun	CAS
Yiannis Verginadis	ICCS
George Moldovan	SIEMENS
Simone Braun	CAS
Yiannis Verginadis	ICCS
Simone Braun	CAS

Version History

#	Description
1	Table of Contents circulated (10/09/15)
2	Dissemination Templates sent to partners (03/10/2015)
3	Filled in templates (23/10/2015)
4	Filled in templates (23/10/2015)
5	Filled in templates (29/10/2015)
6	Filled in templates (02/11/2015)
7	Filled in templates (12/11/2015)
8	Filled in templates (18/11/2015)
9	Filled in templates (19/11/2015)
10	Filled in templates (27/11/2015)
12	Updated inputs (01/12/2015)
13	Filled in templates (08/12/2015)
14	Filled in templates (08/12/2015)
15	Report on CS-IFG (15/12/2015)
16	Updated inputs (16/12/2015)
17	Updated inputs (18/12/2015)
18	Updated inputs (21/12/2015)
19	Deliverable sent for STC review (16/12)
20	Updated inputs (18/12/2015)
21	Updated inputs (21/12/2015)
22	Pre-final version sent for internal review (23/12/2015)
23	Internal review comments and suggestions (28/12/2015)
24	Internal review comments and suggestions (29/12/2015)
25	Final version (31/12/2015)
26	Final version for submission (31/12/2015)

Table of Contents

List of Figures

List of Tables

Executive Summary

This deliverable reports all the conducted dissemination activities during the first project year while it elaborates on a dissemination plan for the upcoming project period. Specifically, this report documents the dissemination activities, the envisioned relation to standards as well as the Cloud Security Industrial Focus Group (CS-IFG) related activities of the project partners. Moreover, it briefly reports on the status of the data management plan (DMP). It constitutes one of the interim versions of the D7.2 – Dissemination Activities Report. Thus, it provides details on current and anticipated individual and collaborative dissemination activities to be conducted during the second year of the project while it quantifies the target for the dissemination results over the lifespan of the project.

1 Introduction and Scope

This deliverable reports all the conducted dissemination activities, performed at consortium and individual level, during the first project year. In addition, it elaborates on a dissemination plan for the upcoming project period. It includes details of any publications, seminars and other dissemination activities already performed or planned for presenting the results of the PaaSword project. Specifically the scope along with the structure of this deliverable is summarized below:

- Present all the research publications produced during the first project year. This refers to journal, conference and workshop papers (section 2)
- Present all the other dissemination-related activities that took place during the first project year. This refers to scientific networking events, seminars, tutorials, university lectures, and workshop organization (section 3)
- Present the planned research publications to be produced over the period of M13-M24 of the PaaSword project (section 4)
- Present all the other dissemination-related activities to be conducted over the project period of M13-M24 (section 5)
- Elaborate on the consortium's individual dissemination plans (section 6)
- Present certain key performance indicators for the PaaSword dissemination overall plan (section 7)
- Report on the status of the PaaSword's data management plan (section 8)
- Report on the CS-IFG related activities (section 9)
- Discuss the relation to relevant standards and standardization working groups (section 10)

2   Research Publications

The following Table 1, describes the research outputs, in terms of journal, conference and workshop papers produced during the first project year. Specifically, for each research output we provide the publication title, its type (i.e. Journal, Conference, Workshop), its details (i.e. Journal, Conference/Workshop title, date and location), responsible partner from the PaaSword consortium and its status (Submitted, Accepted, Presented, Published).

Table 1: PaaSword's research publications – 1st Year

Publication Title	Type	Details	Authors	Responsible Partner	Status
Automated Security Assessment & Audit of Remote Platforms using TCG-SCAP synergies	Journal	Journal of Information Security and Applications, February 2015	A. Mudassar, C. Gehrmann, M. Björkman	SICS	Published[1]
PaaSword: A Holistic Data Privacy and Security by Design Framework for Cloud Services	Conference	5th International Conference on Cloud Computing and Services Science (CLOSER 2015), 20-22 May, Lisbon, Portugal	Y. Verginadis, A. Michalas, P. Gouvas, G. Schiefer, G. Hübsch, I. Paraskakis	ICCS	Accepted[2] & Presented
Towards Secure Multi-tenant Virtualized Networks	Conference	1st IEEE International Workshop on 5G Security held in conjunction with IEEE TrustCom-15, 20-22, August , Helsinki, Finland	N. Paladi and C. Gehrmann	SICS	Accepted[3] & Presented
A Survey on Context Security Policies in the Cloud	Workshop	1st International Workshop on Cloud Security and Data Privacy by Design (CloudSPD'15), 10 December, Limassol, Cyprus	Y. Verginadis, G. Mentzas, S. Veloudis, I. Paraskakis	ICCS	Accepted[4] & Presented
Towards Trusted eHealth Services in the Cloud	Workshop	1st International Workshop on Cloud Security and Data Privacy by Design (CloudSPD'15), 10 December, Limassol, Cyprus	A. Michalas, R. Dowsley	SICS/KIT	Accepted[5] & Presented

---

[1] There is a copyright by Elsevier B.V. with an embargo period of 24 months (starting Feb 2015). This paper is included in the PaaSword's research publications table but it will not be counted for a PaaSword publication until it has been self-archived (Green Open Access) according to the Horizon 2020, guidelines on open access to scientific publications and research data.

[2] Available online at: http://imu.ntua.gr/biblio/holistic-data-privacy-and-security-design-framework-cloud-services

[3] Available online at: http://soda.swedishict.se/5875/1/Towards_Secure_Multitenant_Virtualized_Networks.pdf

[4] Available online at: http://imu.ntua.gr/biblio/survey-context-security-policies-cloud

[5] To be available online at: http://soda.swedishict.se, still pending proceeding reference from CloudSPD'15

Towards Efficient and Secure Data Storage in Multi-Tenant Cloud-Based CRM Solutions	Workshop	1st International Workshop on Cloud Security and Data Privacy by Design (CloudSPD'15), 10 December, Limassol, Cyprus	S. Braun, J. Vuong	CAS	Accepted[6] & Presented
Towards secure SDN policy management	Workshop	1st International Workshop on Cloud Security and Data Privacy by Design (CloudSPD'15), 10 December, Limassol, Cyprus	N. Paladi	SICS	Accepted[7] & Presented
PaaSword: A Holistic Data Privacy and Security by Design Framework for Cloud Services	Journal	Journal of Grid Computing - Special Issue on Cloud Computing and Services Science	Y. Verginadis, A. Michalas, P. Gouvas, G. Schiefer, G. Hübsch, I. Paraskakis	ICCS	Submitted[8]
Providing user Security Guarantees in Public Infrastructure Clouds	Journal	IEEE Transaction on Cloud Computing	N. Paladi	SICS	Submitted[9]

---

[6] Available online at: http://paasword.eu/wp-content/uploads/2015/12/CloudSPD_CloudSPD2015_TowardsEfficientAndSecureDataStorageInMultiTenantCloudBasedCRMSolutions_final.pdf

[7] To be available online at: http://soda.swedishict.se, still pending proceeding reference from CloudSPD'15

[8] This is a hybrid open access journal. Once this publication is accepted it will published under open access license (Gold OA)

[9] This is a hybrid open access journal. Once this publication is accepted it will published under open access license (Gold OA)

3 Other Dissemination-Related Activities

The following Table 2 describes other dissemination-related activities that took place during the first year of the PaaSword project and arose out of the partners' organization or participation in some of the conferences and networking events. In this list, we include all the rest of the activities (i.e. not included in the above Table 1) that they were conducted in order to disseminate the PaaSword vision, objectives and generated scientific knowledge among the research community and potential early adopters (e.g. during scientific networking events, seminars, tutorials, university lectures, workshop organization). We note that some of these activities have been also reported in the deliverable D7.3 as communication activities, since the audience involved both the research and the industrial community. Specifically, for each result in the table below, we provide the title of the activity, its type (e.g. networking event, seminar, poster presentation, flyer dissemination etc.), the date and location where it took place, a short summary of its main outcomes, the responsible partner of the PaaSword consortium and its status.

Table 2: Other dissemination-related activities – 1st Year

Title	Activity	Date/Location	Type of Activity	Outcomes	Responsible Partner	Status
5th Exhibition on Informatics, Technology and Telecommunications	Flyers dissemination	6th of February, 2015	Contribution	Communicated PaaSword vision and objectives	SILO	Completed
SILO half-day event	Networking event	19th of February, 2015, Limassol, Cyprus	Presentation	Communicated PaaSword objectives to company's customer portfolio	SILO	Completed
SICS Open House, 2015	Scientific networking event	19th of March 2015, Kista, Stockholm Sweden	Contribution	Communicated and discussed with industrial and research participants the goals and scope of the project	SICS	Completed
ICEIS'15 European Project Space	Poster presentation & flyers dissemination	29th of April, 2015, Barcelona Spain	Contribution & Presentation	Present the research goals and expected benefits of the project	SICS	Completed
SICS Security Seminar 2015	Seminar	19th of May 2015, Lund, Sweden	Contribution	Communicated and discussed with industrial and research participants the goals and scope of the project	SICS	Completed

Presentation of current research topics regarding security and privacy to external, commercial SIE departments	Scientific networking event	21st of September, 2015 Teleconference	Presentation	Presentation of PaaSword's goals and approach in solving secure storage problems	SIEMENS	Completed
PaaSword at CloudWATCH, 6th workshop on cloud standards profiles	Workshop	24th of September, 2015, Brussels, Belgium	Contribution	Communicated PaaSword's activities on standards	CAS	Completed
PCI 2015 Conference	Presentation at the "Critical Infrastructure Protection" workshop"	2nd of October, 2015, Athens, Greece	Presentation	Main security threats, challenges and opportunities for the design of advanced security solutions were presented, followed by open discussion, taking into account different NFV deployment models	UBITECH	Completed
PaaSword Overview	Joint workshop on Cyber Defence and Security	8th-9th of October, 2015, Brussels, Belgium	Contribution	Gained feedback directly from participating stakeholders as cloud providers, cloud users and large enterprises	CAS	Completed
PaaSword Networking Session in ICT 2015 – "No More Dark Clouds"	Scientific networking event	20th of October 2015, Lisbon, Portugal	Organization & Contribution	Presented PaaSword's objectives and ongoing work. Reached out to find potential members for CS-IFG	CAS, ICCS, UBITECH, SICS, SEERC, INTRA, SILO	Completed
RERUM project presentation	Scientific Networking event	28th of October – 1st of November 2015, Heraklion, Greece	Participation	Presentation of PaaSword's security and privacy approaches regarding data and it's virtualized	SIEMENS	Completed

				databases		
Theatre Session at European Security Research – The next wave	Congress	5th of November, 2015, Dublin, Ireland	Contribution	Gained feedback and discuss PaaSword concepts with stakeholders and researchers	CAS	Completed
DockerCon Europe	Participation in the Security sessions	16th-17th of November, 2015, Barcelona, Spain	Participation	Participated in the discussion about trust design concepts in software engineering	UBITECH	Completed
1st International Workshop on Cloud Security and Data Privacy by Design (CloudSPD'15)	Workshop in conjunction to the 8th IEEE/ACM International Conference on Utility and Cloud Computing	10th of December 2015, Limassol, Cyprus	Organization, Contribution & Presentation	Created awareness context-aware privacy issues and solutions in cloud computing	ICCS, SICS, KIT	Completed

4   Planned Research Publications

The following Table 3 describes the planned research publications, in terms of journal, conference and workshop papers that we expect to be produced over the period of M13-M24 of the PaaSword project. Specifically, for each planned research output we provide the publication title, its type (i.e. Journal, Conference, Workshop, Article), the scheduled date (i.e. the submission deadline of a conference or the planned date until when the basic structure of the publication will be ready), the responsible partner from the PaaSword consortium, the themes to be covered through this publication, the related Task or Work Package and its status (Under Discussions, Planned, Ongoing Work, Abstract Submitted).

Table 3: PaaSword's planned research publications

Publication Title	Type	Scheduled Date	Involved Partner (s)	Themes to be covered	WP/Task related	Status
A conceptual architecture of a mechanism for contextualized access control for cloud-based applications	Conference /Workshop	End of February, 2016	SEERC, ICCS	PaaSword Reference Architecture	WP1, Task 1.3	Planned
The PaaSword Context- aware Security Model	Conference	End of February, CLOSER 2016	ICCS, SEERC	PaaSword Context- aware Security Model	WP2, Task 2.1	Planned
Ontologically describing access policies based on the PaaSword context-aware security model	Conference	End March 2016	SEERC, ICCS	Access policies model	WP2, Task 2.2	Planned
CAS Research Report	Article	Q2, 2016	CAS	PaaSword overview	All	Planned
Converting ontologically-expressed access policies into XACML	Conference	Mid of May 2016	UBITECH ICCS, SEERC	XACML-based Context-aware Policy Access Model	WP2, Task 2.3	Planned
Towards Multipath TCP over TLS Accelerator Clusters	Conference	Q3, 2016	SICS	Cloud Security	WP1	Planned
Bootstrapping Trust in SDN Infrastructure	Conference	Q3, 2016	SICS	Cloud Security, SDN	WP1	Planned
CAS@Work	Article	Q4 2016	CAS	PaaSword overview and first results	WP6	Planned
PaaSword overview for practitioners (in German)	Journal	October 2016	KIT	Overview of the PaaSword ideas	WP1	Abstract sent for review

Using XACML for Context Aware Access Control	Conference	TBD	SICS	XACML, Access Control	WP3	Planned
Security analysis of DB encryption protocols	Conference	TBD	SICS	DB encryption protocols	WP4	Planned
Database Encryption: column level encryption vs row level encryption & queries on encrypted data	Conference	TBD	SICS, KIT	DB encryption	WP4	Discussions
Security of NOSQL databases	Conference	TBD	SICS, KIT	NOSQL databases security	WP4	Under Discussions
PaaSword security-oriented software engineering methodology	Conference	TBD	SICS, Ubitech	Technical requirements, security requirements and specifications	WP1	Planned
Searchable Encryption (SE) schemes A survey	Journal	TBD	SICS, KIT	Searchable encryption	WP1	Planned
PaaSword architecture	Conference	TBD	Many	PaaSword Reference Architecture	WP1, T1.3	Under Discussions
Context-Aware Access Control with Deny-Rules	Conference	TBD	KIT, others	Address special problems about deny-rules in CAAC	WP2	Ongoing work
TBA	Conference	TBA	KIT, SICS	Database Outsourcing Security	WP4	Under Discussions
Cont. CloudSPD'15 paper with results on implementation (CloudSPD'16)	Workshop	TBA	CAS	Data encryption based on user defined policies in multi-tenant cloud-based CRM systems	WP1, WP6	Under Discussions
Joint paper on 1st Cluster Workshop Data Protection, Security and Privacy in the Cloud	Workshop paper / white paper	TBD	CAS, others	Workshop outcomes	All	Planned

4.1 Updated Indicative List of Scientific Journals and Conferences

In the following two Tables 4, 5, we repeat from PaaSword's description of work and update, a number of indicative lists of scientific journals and conferences that have already been considered or will be considered in the future for submitting PaaSword results. In both of these tables we have highlighted (in blue colour) the journals, conferences and workshops where PaaSword publications have already been submitted, presented or published.

Table 4: Indicative list of scientific Journals

Cloud Computing	IT and Cloud Security
Journal of Cloud Computing (Springer)	International Journal of Information Security (IJIS)
International Journal of Cloud Computing (IJCC)	ACM Transactions on Information & System Security (TISSEC)
IEEE Transactions on Cloud Computing	Information Management & Computer Security
International Journal of Cloud Applications and Computing (IJCAC)	Journal of Computer Security
International Journal of Cloud Computing and Services Science	International Journal of Information and Computer Security
International Journal of Cloud-Computing and Super-Computing	International Journal of Information Security Science
Open Journal of Mobile Computing and Cloud Computing	Journal of Information Security and Applications (Elsevier)
Journal of Cloud Computing (JCC) (IBIMA)	EURASIP Journal on Information Security
The International Journal of Grid Computing and eScience	Computers & Security (Elsevier)
Int. Journal of Cyber-Security & Digital Forensics (IJCSDF)	
Int. Journal of Information Privacy, Security & Integrity	

Table 5: Indicative list of International scientific conferences

Cloud Computing	IT and Cloud Security
IEEE CLOUD	International Conference on Cloud Security Management
IEEE Int. Conference on Cloud Networking (IEEE CloudNet	IEEE Int. Conference on Software Security and Reliability (SERE)
IEEE Int. Conf. on Cloud Computing for Emerging Markets (CCEM)	Int. Conference on Security and Cryptography (SECRYPT)
IEEE International Conference on Cloud Computing Technology and Science (CloudCom)	International Conference on Applied Cryptography and Network Security (ACNS)
IEEE/ACM Int. Conference on Utility and Cloud Computing (UCC)	International Workshop on Cloud Security and Data Privacy by Design (CloudSPD)
International Conference on Cloud Computing and Services Science, CLOSER	Int. Conference on Cryptography and Information Security

International Conference on Cloud Computing, GRIDs, and Virtualization	International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)
Int. Conference on Cloud and Autonomic Computing (CAC)	IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom)
International Conference on Cloud Computing (CloudComp)	Workshop on Provisioning and Management of Portable and Secure Cloud-Services
International Conference on Enterprise Information Systems (ICEIS)	

5 Other Dissemination-Related Activities – Planned

The following Table 6 describes other planned dissemination-related activities for the period of M13-M24. In this list, we include all the rest of the activities (i.e. not included in the above Table 3) that have been planned in order to disseminate the PaaSword vision, objectives and generated scientific knowledge among the research community and potential adopters (e.g. during scientific networking events, seminars, tutorials, university lectures, workshop organization). Specifically, for each planned activity in the table below, we provide the title of the activity, its type (e.g. joint workshop, networking event, seminar etc.), the date and location where it will take place, a short summary of its main objectives, the responsible partner of the PaaSword consortium and its status.

Table 6: Other dissemination-related activities – Planned

Title	Activity	Date/ Location	Type of Activity	Objectives	Respon-sible Partner	Status
Joint Workshop with PANOPTESEC project	Joint workshop	Q1/Q2, 2016, Brussels, Belgium	Organization	Gain feedback and discuss PaaSword concepts and results with stakeholders and researchers	CAS	Planned
Joint Cluster Workshop Data Protection, Security and Privacy in the Cloud	Joint workshop	23rd of February, 2016, Naples, Italy	Participation	Gain feedback and discuss PaaSword concepts and results with stakeholders and researchers	CAS	Planned
Seminar in the MSc "Advanced S/W Engineering" course	Seminar	May 2016, Thessaloniki, Greece	Organization	Present PaaSword's context-aware policy model	SEERC	Planned
Technology forum 2016 (to be organised by CERTH – the Greek Forum for Research and Technology)	Presentation	June 2016, Thessaloniki, Greece	Participation	Present PaaSword's context-aware policy model	SEERC	Planned
Paasword related workshop in ESOCC 2016	Workshop	September 2016, Vienna, Austria	Organization	Organize workshop with topics related to cloud security	SEERC	Planned
Trust and Security in a connected World	Symposium (in German)	28th of October, 2016, Karlsruhe, Germany	Organisation & Contribution	Create awareness about privacy issues and solutions in cloud computing	KIT	Planned
SICS Open House, 2016	Scientific networking event	Q4, 2016, Kista, Stockhol Sweden	Contribution	Communicate and discuss with industrial and research participants the goals and scope of the project	SICS	Planned

SICS Security Seminar 2016	Seminar	Q4, 2016, Kista, Stockhol Sweden	Contribution	Communicate and discuss with industrial and research participants the goals and scope of the project	SICS	Planned
SICS Activities Booklet 2015-2016	Article related to the project	Q4, 2016	Organization	Visibility of project goals, overview to SICS partners and customers	SICS	Planned
2nd International Workshop on Cloud Security and Data Privacy by Design (CloudSPD'16)	Workshop	Q4, 2016, Location TBA	Organization	Organize workshop with topics related to cloud security	ICCS, SICS	Under Discussi ons

6   Individual Dissemination Plans

This section discusses the individual disseminations plans of the partners which have been updated from the original description of work. For each one of the partners the relevant dissemination channels are mentioned; a summary description about ongoing and planned dissemination activities is given; the future dissemination plans over the lifespan of the PaaSword project are explained.

6.1   CAS

In addition to the continuous project communication and awareness creation, CAS will put strong emphasis on the wide dissemination of the project results upon availability of the first exploitable project outcomes.

Dissemination Channels:

CAS will disseminate the PaaSword results through non-interactive (such as publications) and interactive activities (such as face-to-face meetings) among relevant scientific communities, business networks, as well as direct and indirect customers, so as to achieve maximum visibility and sustainability.

Description:

CAS will contribute to scientific publications and present PaaSword results in relevant conferences such as CLOSER[10] or CloudCom[11]. CAS serves worldwide more than 250.000 users, over 10.300 customer companies and maintains an elaborated partner model with more than 200 software houses and consultants across the globe, developing and representing solutions based on CAS technology in 30 countries. These will be the primary target of dissemination activities. Moreover, CAS is chairing a number of renowned associations in Germany. CAS will contribute collaborating with the federal association umbrella of IT SME's (BITMi) in Germany, acting as dissemination catalyst. One particularly important association is the CyberForum[12] cluster, an association for ICT stakeholders with more than 1.000 members (incl. software and hardware companies, consultants, universities, research institutes, business angels, etc.).

Future Plans:

CAS will initiate large public press coverage and employ social networks. Dissemination regarding our partner network and existing and potential customers will be achieved also on future events, i.e. fairs, congresses and round tables including internal meetings. Events of interest include CAS IT Lounge, CeBIT[13], EuroCloud[14] or IEEE events.

6.2   SICS

Dissemination Channels:

The dissemination channels for the diffusion of scientific knowledge generated within the project from SICS are driven by digital content but are also complemented by physical interactive activities. The digital content produced is disseminated mainly through scientific publications in international peer-reviewed journals and conference/workshop proceedings. Scientific knowledge is also disseminated through websites, newsfeeds, social media, mailing lists, booklets (magazines), press releases and public presentations, seminars and talks.

---

[10] http://closer.scitevents.org/
[11] http://2015.cloudcom.org/
[12] http://www.en.cyberforum.de/cyberforum/about-cyberforum/
[13] http://www.cebit.de/
[14] http://www.eurocloud.org/

The receivers of the dissemination (target groups) are the research community, industry, standardisation organisations, policy makers and the general public. Important dissemination channels utilised by SICS are the open source channels and communities, such as GitHub and OpenStack, where software produced from the project can become available.

Description:

SICS objective is to enable the wider awareness of the project to the academic, industry and research community in order to make visible the project progress, the developed technologies and all the results outside the project consortium. The intended target groups are the research community, industry, standardisation organisations, policy makers and the general public. Throughout the project several activities are planned involving a variety of dissemination channels to ensure that the dissemination is carried out for the industrial, research and academic communities so that we increase the visibility of the project direction, results and benefits.

Future Plans:

During the project, SICS intends to participate in a number of outreaching research activities including conferences, workshops, seminars, tutorials, as well as introduction of our work in other research groups with similar interests. Security in PaaS environments is considered as an emerging and unexplored research area that allows for novel research and publications in several related topics. Therefore, within the project we plan to explore such opportunities. Furthermore, we plan to introduce PaaSword in several industrial partners that we believe can benefit from such an application framework. At the same time we expect valuable feedback from them, regarding the possible adoption or extension of the PaaSword results in the industry. A total of four publications are planned to be produced per year and also yearly a workshop will be organized targeting mainly industry participants where the research results from the project will be presented and discussed. A project web page will be created and maintained on the main Swedish ICT website and project results will be also discussed in direct meetings with industry partners.

6.3 KIT

Dissemination Channels:

KIT will use the following main dissemination channels for presenting PaaSword results in the research and business communities:

- Conferences and Workshops
- Articles
- Talks, Seminars
- Symposia
- Website

Description:

KIT uses these channels to create awareness about the outcomes of PaaSword. The scientific community is the main target through publications in scientific conferences, proceedings and journals. Besides these, KIT will present the results of the PaaSword project in talks during, e.g., symposia, workshop, and conference presentations. The project results will be also introduced to Bachelor, Master as well as PhD students through presentations during lectures and in a more interactive way during seminars. The business community is

addressed through the publication of articles in professional journals and on symposia, which address related enterprises. Through these channels multiple audiences are reached addressing the full spectrum of interested groups. I.e., KIT will not only spread the PaaSword ideas and outcomes to the typical scientific and professional communities, but also to future researchers and professionals through presentations and seminars for students. In addition, updates on the progress of the project will be published on the project website.

Future Plans:

During the PaaSword project, KIT plans to produce two publications per year. Furthermore, KIT will organize a symposium promoting the ideas and solutions of the PaaSword project to local scientists and enterprises from the local industry. Moreover, the website will be constantly updated with the newest results of the project.

6.4 ICCS

Dissemination Channels:

The main channels that ICCS will use for disseminating the scientific knowledge generated in terms of the PaaSword project include:

- Scientific publications in international peer-reviewed journals
- Scientific publications in international conferences and workshops
- Public presentations, seminars and lectures
- Website, Social Media and Newsletters

Description:

As a research institute, ICCS dissemination plans focus on the R&D community, especially in domains such as: information systems, situational and context-aware systems, recommender systems and self-adaptable systems. ICCS plans to collaborate with other partners of the PaaSword consortium in order to diffuse the generated scientific knowledge among the research community and the general audience. In particular, several dissemination activities will take place by ICCS during the lifespan of the PaaSword project, including: conference presentations, scientific articles in various high impact journals, organization of workshops and dissemination of the project results to other related research projects. ICCS, as the dissemination leader of PaaSword, will create additional dissemination channels for allowing the consortium to present the project's results in relevant research audiences. Specifically, ICCS led the successful organization of the 1st International Workshop on Cloud Security and Data Privacy by Design (CloudSPD'15) in the frame of the UCC'15 conference held in Limassol, Cyprus, 7-10/12/2015. Details on the CloudSPD'15 organization will be reported in the deliverable D7.5. In this context, ICCS has already participated in the ICT event in Lisbon ("No more dark Clouds"), where the challenges regarding context-aware access controls in the cloud domain were presented and discussed. In addition, ICCS will use communication channels, accordingly, such as our website, social media (e.g. Twitter, ResearchGate, LinkedIn) for raising awareness on the PaaSword scientific results.

Moreover, ICCS' key personnel are faculty at the National Technical University of Athens (NTUA) and at the University of Piraeus (UNIPI) enhancing the dissemination opportunities of the project results in terms of academic presentation and lectures. The scientific methodological and technological results emerging from the PaaSword project lifecycle and work may become part of teaching material for undergraduate and postgraduate courses of NTUA or UNIPI. Additionally, specific advancements of the state-of-the-art will be used directly or indirectly for driving and inspiring post-doctorate research work.

Future Plans:

ICCS future plans involve the continuation of concrete dissemination activities that will constitute PaaSword results available to a wide research audience. These planned dissemination activities include the:

- Provision of descriptive posters, videos and presentations
- Demonstration of the PaaSword context-aware security and policy models along with their relevant mechanisms to the research community
- Conferences participation
- Production of high-impact scientific publications
- Organization of the 2nd International Workshop on Cloud Security and Data Privacy by Design (CloudSPD'16)

6.5 INTRASOFT

Dissemination Channels:

INTRASOFT will use as the main communication channel for presenting PaaSword results their Corporate Magazine.

Description:

PaaSword overall objectives and activities have already been shared by using the corporate magazine, INTRAbuzz. INTRASOFT has a large network of about 1600 professionals and INTRAbuzz magazine is the most efficient way to inform colleagues from other departments. During the project duration, updates regarding PaaSword results will be also shared to existing and potential customers.

Future Plans:

Internal meetings and corporate events will be used for the dissemination of PaaSword. Moreover, INTRASOFT plans to organize a workshop in order to present the overall progress of PaaSword during the Q2 of 2016. This will aim mainly the members of Cloud Security Industrial Focus Group (CS-IFG).

6.6 SEERC

Dissemination Channels:

The main dissemination channels for the diffusion of scientific knowledge generated in the frame of the PaaSword project include:

- Scientific publications in international peer-reviewed journal and conference/workshop proceedings.
- The SEERC and the University of Sheffield website.
- Public presentations, seminars and talks.
- Newsfeeds, social media, mailing lists, brochures/flyers.
- Open source channels and communities such as Github.

Description:

Ever since cloud computing entered the mainstream, security has been one of its controversial aspects and an important obstacle to its wider adoption. Security as a PaaS offering is a new and promising area of research that is expected to produce novel results and technologies that will alleviate such security concerns. Naturally,

a multitude of relevant stakeholders may potentially benefit from such results and technologies. The main objective of SEERC's dissemination plan is to render SEERC's scientific work carried out as part of the PaaSword project (i.e. the various developed models and technologies) known beyond the confines of the project's consortium. More specifically, our intended target audience is the relevant research community as well as the relevant industry. In this respect, throughout the PaaSword project several dissemination activities will take place involving the aforementioned dissemination channels in order to ensure increased visibility for project results and findings as they become available.

<u>Future Plans:</u>

During the PaaSword project, SEERC will participate in a number of outreaching research activities including conferences, workshops, seminars and tutorials. More specifically, a total of two publications are planned to be produced per year and at least one tutorial will be organized in the frame of a relevant conference. Moreover, SEERC will exploit its extensive network of partnerships and collaborations, both in the academia and in the local industry, in order to make the PaaSword framework, and the benefits that its adoption brings about, more widely known. More specifically, SEERC intends to participate in events organized by universities, research centres and IT enterprises in the Thessaloniki area in Northern Greece, as well as throughout Europe, which aim at bridging the academic with the industrial world and promote their collaboration. In addition, SEERC will constantly update its website to report PaaSword results and findings as they become available.

6.7 SIXSQ

<u>Dissemination Channels:</u>

SIXSQ will use their Website and social media as the main channels for disseminating PaaSword's technological outcomes.

<u>Description:</u>

An overview of the PaaSword project has already been published on the SixSq website under the rubric Research and Development[15]. It gives an additional backlink to validate the project's website, which is important for Search Engine Optimisation. SixSq will continue to update its website with news and progress of the project. PaaSword social media postings have systematically been shared with the SixSq audience with this continuing throughout the life of the project.

<u>Future Plans:</u>

SixSq will publish short articles in the form of a blogs to share the objectives and progress of the project. This will be aimed at a non-technical audience with the intention of raising general awareness of the project, the H2020 platform and its successes. In addition to the general benefits of the PaaSword components, these blogs will also highlight how the PaaSword components have been integrated into SlipStream, SixSq's cloud application management platform, and how SlipStream simplifies the use of those components. These will be published twice a year in 2016 and 2017.

SixSq will host a face-to-face meeting of the project in March 2016. Dissemination efforts before this meeting will focus on the objectives of the meeting and the project in general. Afterwards, the outcomes and their expected impacts on the European research community and general public will be highlighted.

---

[15] http://sixsq.com/r-and-d/password/

To improve awareness of the project within the company, the objectives and progress will be presented at internal meetings. It is also planned to present this to the wider RHEA group[16], of which SixSq is a part and which is also involved in several European projects.

6.8 UBITECH

Dissemination Channels:

UBITECH will use their corporate website, physical meetings and conferences as the main channels for disseminating PaaSword's technological outcomes.

Description:

PaaSword activities has already been announced by using the corporate website. This process will continue during the project duration with providing updates regarding PaaSword. Moreover, additional channels for disseminating PaaSword in the Greek market will be employed such as ictplus.gr and other widely known online media and blogs in Greece.

Additionally, UBITECH has already contributed and plans to keep on contributing in the main scientific publications of the project, as UBITECH leads the design and implementation one of the two main subsystems of PaaSword, namely the "Policies Access, Decision and Enforcement Middleware" (outcome of WP3). The first outcome of this activity has been the co-authoring of a scientific paper for CLOSER 2015 with ICCS, SICS, KIT and SEERC.

Finally, UBITECH is looking forward to participating in scientific, industrial and clustering events focusing on Cloud Computing and ICT technologies for presenting and sharing PaaSword related material. In this context, UBITECH has already participated in the ICT event in Lisbon, wherein UBITECH has presented – in the course of a special networking session – the architectural design and the technological principles of PaaSword. In addition to this, UBITECH has introduced and discussed about PaaSword concepts in other initiatives (in the fields of Cloud computing and Software technologies), wherein UBITECH participates, namely PaaSport, INPUT and ARCADIA, so as to exploit the concepts of the PaaSword project and gain feedback from other user communities.

Future Plans:

Dissemination regarding business and scientific partners will be achieved also on future conferences, workshops and exhibitions, including the demonstration (during the last year of the project) of mature project results (e.g. integrated PaaSword framework and public sector related demonstrator) to potential customers in Latin America through the company's subsidiary in Buenos Aires.

6.9 SIEMENS

Dissemination Channels:

SIEMENS will use the following channels for disseminating PaaSword's technological outcomes:

- IERC meetings and presentations
- Internal interdepartmental meetings, reports and collaborations
- Presentations to external and academic partners involved in related research projects

---

[16] http://www.rheagroup.com/

Description:

Siemens has reported on PaaSword's goal and expected results in internal and external meetings, and plans to continue this effort, especially towards the end and concretization of the access and context models, and of the encrypted persistence layer.

The meetings are attended by fellow research or production departments, providing the opportunity to align the technical progress resulting from PaaSword with efforts produced by other research projects in which the department or its partners are involved (i.e. RERUM, which holds the IERC chair of AC5 -- security, privacy, trust and governance), as well as with the overall requirements of concrete Siemens services and products.

Future Plans:

Planned participation in outreach programs i.e. local and international workshops and (academic or industrial-focused) conferences. SIEMENS also plans an implementation of joint demos with other security and related research projects (and their results) which will focus on a composed scenario.

The Siemens internal IoT and security community will be engaged, in order to evaluate and expand the project's effort and outcome towards a viable product.

6.10 SINGULARLOGIC

Dissemination Channels:

SINGULARLOGIC will use their corporate website and physical meetings as the main channels for disseminating PaaSword's technological outcomes.

Description:

Sharing of content regarding PaaSword activities has already been achieved by using the corporate website. This process will continue during the project duration by providing updates regarding PaaSword, and if SingularLogic Cyprus will use social media more actively in the future, PaaSword will be disseminated through these channels   as well.

Moreover, physical events can present PaaSword to different audience types, including SingularLogic's existing customers, potential customers and SingularLogic colleagues from other departments. Already the following events have taken place and are provided as an example of the different dissemination approaches for different audience types:

- 06/02/2015 – The company held a booth at 5th Exhibition and Conference on Informatics, Technology and Telecommunications. Flyers of PaaSword project were also distributed during this event.
- 19/02/2015 – Half-day event to highlight the upcoming products of SingularLogic Cyprus. (The event captured the product Galaxy and its new functionalities, presentations on upcoming products related to mobile applications.) Among others, the outline of the PaaSword project was presented so as to inform the company's customer portfolio of the company's dedication in bringing cutting-edge solution to market.
- 08/06/2015 - Dissemination of the PaaSword project internally. The project outline was presented to the Cloud Business Division of SingularLogic S.A. (Athens, Greece). The presentation was followed by a discussion during which colleagues from SingularLogic Greece shared their experiences and provided their viewpoints concerning the project's planned work. In this way, internal awareness was raised, whereas feedback concerning the execution of future tasks was gained from a relatively early stage.

<u>Future Plans:</u>

Dissemination regarding existing and potential customers will be achieved also on future events, including internal meetings, corporate presentations and international exhibitions or conferences. Dissemination of project results with other divisions of SingularLogic (e.g. SingularLogic Romania) is also planned.

7 Target Dissemination Numbers

The PaaSword consortium attempted to quantify some of the aspects of the dissemination plan that was discussed in the previous sections, in order to set specific minimum and measurable goals to be achieved during the lifespan of the project. For this purpose, we classify the planned dissemination activities across the Cloud Computing and the IT & Cloud Security ICT themes that are relevant for the PaaSword project. Specifically, we provide Table 7 for quantifying the project's scientific publications plan that include figures for both individual (i.e. Project Target) but also for notable joint research publications that involve inter-consortium collaborations. Similarly, in Table 8, we provide target numbers for planned dissemination activities that involve training seminars and university courses. Finally, in Table 9, we mention our planning concerning the yearly organization of scientific workshops in conjunction to relevant conferences.

Table 7: Scientific Publications Plan over the PaaSword lifespan

ICT Theme	Type	Project Target	Joint Target
Cloud Computing	Journal	1	1
IT & Cloud Security	Journal	3	1
Cloud Computing	Conference/ Workshop	3	2
IT & Cloud Security	Conference/ Workshop	5	4

Table 8: Training Seminars and Input to Courses over the PaaSword lifespan

ICT Theme	Type	Project Target	Joint Target
Cloud Computing	Training Seminar	2	1
Cloud Computing	Input to University Course	1	n/a
IT & Cloud Security	Training Seminar	3	n/a
IT & Cloud Security	Input to University Course	2	1

Table 9: Workshops organization over the PaaSword lifespan

ICT Theme	Type	Project Target	Joint Target
Cloud Computing & Cloud Security	Workshop organization	3	n/a

As it was detailed in the previous sections, the PaaSword consortium has already performed the following dissemination activities with respect to the basic directions of the PaaSword dissemination plan (Table 7, Table 8, Table 9):

- o 1 joint conference publication under the cloud computing ICT theme
- o 1 individual conference publication under the IT & cloud security ICT theme
- o 2 joint workshop publications under the IT & cloud security ICT theme
- o 2 individual workshop publications under the IT & cloud security ICT theme
- o 1 seminar under the IT & cloud security ICT theme
- o 1 workshop organized by the PaaSword consortium under both the cloud computing and cloud security ICT themes

8 Data Management Plan

There is no update on the PaaSword's data management plan (DMP) in comparison to the presented plan in terms of D7.6 deliverable (reported on the 25th of June 2015). Specifically, that document described the datasets related to the four (out of five) PaaSword pilots: 1) Intergovernmental Secure Document and Personal Data Exchange (led by Ubitech), 2) Secure Sensors Data Fusion and Analytics (led by Siemens), 3) Protection of personal data in a multi-tenant CRM environment (led by CAS) and 4) Protection of Sensible Enterprise Information in Multi-tenant ERP Environments (led by SingularLogic). For each of these datasets, the document presented its name, description, standards and metadata that will be used, data sharing options along with archiving and preservation details. During the second year of the project the consortium will decide on the time planning for publishing each of these datasets and it will further examine and decide on platform solutions (e.g. https://joinup.ec.europa.eu/ and http://ckan.org/) that will allow the sustainable archiving of all the PaaSword datasets after the lifespan of the PaaSword project.

9   Report on CS-IFG

This section presents an overview of the main activities and achievements of the Cloud Security Industrial Focus Group (CS-IFG) within the first year of the project (M1-M12, January– December 2015). Within that period, INTRASOFT undertook the leadership of task 7.4 substituting SIEMENS, and thus becoming the main responsible for the CS-IFG.

The scope of CS-IFG (see Figure 1) is the wide communication and scientific dissemination of the innovative PaaSword results to the research, academic, and international community as well as the exploitation and business planning of the PaaSword concepts and tools to the market in order to identify end-users and potential customers.
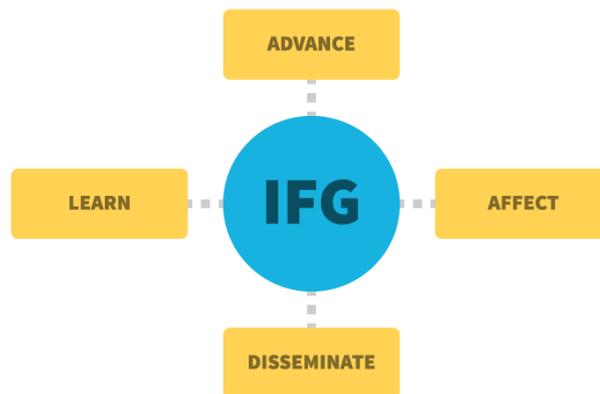

Figure 1: Cloud Security Industrial Focus Group

Figure 2: Online IFG registration form

During the first year of the project, a plan for the establishment and maintenance of the CS-IFG was prepared, including the definition of the registration process for CS-IFG membership, and the establishment of agreement between consortium members upon the first set of material to be shared to CS-IFG members. Then, a list of the first group of people to join the CS-IFG was generated and approved by all partners.

After publishing the project website, the registration process of new members was introduced. A potential member uses the online registration form in order to express its interest of becoming CS-IFG member (Figure 2). The applicant will not be able to use the newly created member account before the applicant is approved by the consortium (the account will be inactive until the approval of the applicant).

A Non-Disclosure Agreement (NDA) is available for download via the project website, which should be signed and sent to the CS-IFG manager. There are two ways to send the signed NDA; the first one is via email and the second one via fax. If the CS-IFG manager receives the signed NDA and no objections are raised by the consortium members, the applicant is approved and the account is activated. The Figure 3 below depicts the described registration process:
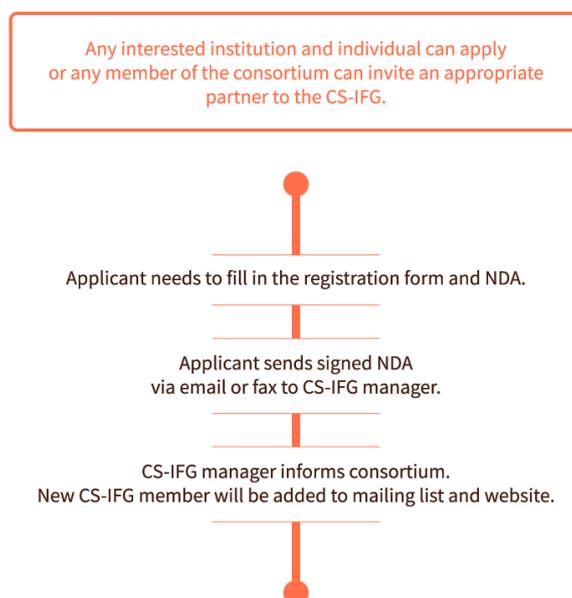
Any interested institution and individual can apply or any member of the consortium can invite an appropriate partner to the CS-IFG.

Applicant needs to fill in the registration form and NDA.

Applicant sends signed NDA via email or fax to CS-IFG manager.

CS-IFG manager informs consortium. New CS-IFG member will be added to mailing list and website.

Figure 3: IFG registration process

CS-IFG provides an environment (private area available only for members), which is available through the website of the project. This environment provides privileged and early access to information about PaaSword, as well as deliverables, publications submitted by partners, binary files etc.

As the dissemination of the project is one of the CS-IFG's main objectives, PaaSword's networking session "No more dark clouds" at the ICT2015 event in Lisbon was a great opportunity for finding more members for CS-IFG. A lot of professionals participated in this session, showing their interest in PaaSword and they were therefore invited to join CS-IFG.

In order to conclude this section, the second year of the project is expected to be more active than the first one with respect to CS-IFG. One of the main objectives of the consortium for the next year is the enlargement of the CS-IFG network. In this context, the organization of a workshop during the second quarter of 2016 is already scheduled.

10 Relation to Standards

This section captures the envisioned relation of PaaSword to specific standards (see Table 10) and standardization working groups (see Table 11). Specifically, it presents the standards upon which the PaaSword methodological and technological tools will be designed and developed.

Table 10: PaaSword & Standards

Standard	Standard brief description	Envisioned Adoption/ Contribution ("A" for adoption, "C" for contribution)	Description of the planned adoption/contribution to Standard	Responsible Partner(s)
X.509[17]	X.509 is an ITU-T standard for a public key infrastructure (PKI) and Privilege Management Infrastructure (PMI). It specifies standard formats for public key certificates, certificate revocation lists, attribute certificates, and a certification path validation algorithm.	A	X.509 will be considered for adoption in order to reassure that encryption and decryption keys are included in existing standardized digital certificates.	KIT, SICS
XACML[18]	The eXtensible Access Control Markup Language (XACML) defines a declarative access control policy language implemented in XML. In addition it is a processing model describing how to evaluate access requests according to the rules defined in policies.	A	PaaSword will deliver the XACML-based Context-aware Policy Access Model realizing the XACML combination of the context-aware security model and the access policies model.	Ubitech, SEERC, ICCS
SAML[19]	OASIS Security Assertion Markup Language (SAML) is an XML-based open standard data format dedicated for exchanging authentication and authorization data between parties.	A	PaaSword considers to use SAML as a data format to exchange policies among PaaSword mechanisms and certified third-parties components.	KIT, SICS, Ubitech, SEERC
SA-REST[20]	Semantic Annotations for REST (SA-REST) is a poshformat that adds meta-data to REST API descriptions in HTML or XHTML.	A	PaaSword considers to comply with this technology for the development of DAO annotations related to context-aware access policies in the Java SE and Java EE	Ubitech, Intrasoft, ICCS, SEERC, KIT, CAS
JSR 250[21]	JSR 250 is a Java Specification Request with the objective to develop annotations for common	A	PaaSword considers to comply with this technology for the	Ubitech, Intrasoft, ICCS,

---

[17] http://www.itu.int/rec/T-REC-X.509/en

[18] https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml

[19] https://wiki.oasis-open.org/security/FrontPage

[20] http://www.w3.org/Submission/SA-REST/

[21] https://jcp.org/en/jsr/detail?id=250

	semantic concepts in the Java SE and Java EE platforms.		development of DAO annotations related to context-aware access policies in the Java SE and Java EE	SEERC, KIT, CAS
JSR 175[22]	JSR 175 is a metadata facility for Java that allows classes, interfaces, fields and methods to be marked as having particular attributes.	**A**	PaaSword considers to comply with this technology for the development of DAO annotations related to context-aware access policies in the Java SE and Java EE	Ubitech, Intrasoft, ICCS, SEERC, KIT, CAS

Table 11: PaaSword & standardization working groups

Standardization Working Group	Brief description	Contribution ("AM" for actively monitoring group's activities, "P" for participation to group meetings, "M" for being/becoming a member of the group, "C" for contributing)	Responsible Partner(s)
ISO/IEC JTC 1/SC 27[23]	ISO/IEC JTC 1/SC 27 IT Security techniques is a standardization subcommittee of the Joint Technical Committee ISO/IEC JTC 1 of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). This subcommittee develops and facilitates International Standards, Technical Reports, and Technical Specifications within the IT security domain.	**AM**	All
ETSI CSC[24]	The ETSI Cloud Standards Coordination initiative (ETSI CSC) is launched by the European Commission (EC) and the European Telecommunications Standards Institute (ETSI) with the objective to identify a detailed map of the standards required to support a series of policy objectives defined by the EC, in particular in critical areas such as security, interoperability, data portability and reversibility.	**AM, C**	SICS, CAS, ICCS, SixSq
CSA[25]	The Cloud Security Alliance (CSA) is a dedicated organization for defining and raising awareness of the best practices that ensure a secure cloud computing environment. We note that one of the PaaSword's advisory board members, Daniele Catteddu is the Managing Director of CSA, which will allow for a closer monitoring and potential collaboration with this working group.	**AM, C**	All

---

[22] https://jcp.org/en/jsr/detail?id=175

[23] http://www.iso.org/iso/iso_technical_committee?commid=45306

[24] http://csc.etsi.org/

[25] https://cloudsecurityalliance.org/

ENISA[26]	The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU. ENISA develops recommendations on good practices in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks.	**AM**	All

10.1 Contribution to ETSI CSC

We note that the PaaSword consortium took actively part in the call for comments on a special report published by the ETSI Cloud Standards Coordination initiative. Specifically, PaaSword's partners submitted to this standardization working group a consolidated list with several comments and suggestions regarding the ETSI special report (SR 003 391) entitled as: Interoperability and Security in Cloud Computing. Analysis, conclusions and recommendations from Cloud Standards Coordination Phase 2[27].
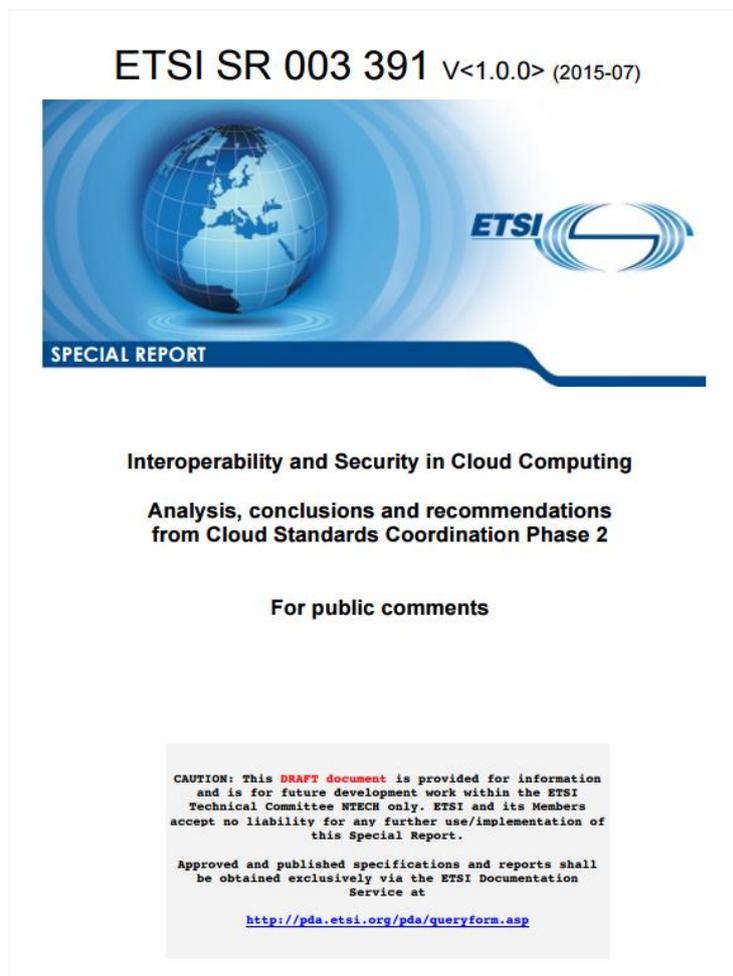

Figure 4: ETSI special report on Interoperability and Security in Cloud Computing

---

[26] https://www.enisa.europa.eu/
[27] http://csc.etsi.org/resources/STF_486_WP3_Report-v1.0.0.pdf

This Special Report (SR) has been produced by ETSI Specialist Task Force 486 "Cloud Standards Coordination Phase 2" as the result of Work Item NTECH(15)000008 "STF 486 WI on Cloud Computing interoperability and conformance: the case of security". It presents the initial results of the analysis of interoperability and security in Cloud Computing with respect to areas of concern that were not covered during CSC (phase 1)[28]. Specifically, this report addresses, from the user's perspective, the relationship between interoperability and security and how a global approach to both can increase the level of trust in Cloud Computing[29]. The PaaSword consortium consolidated a list of 12 comments that were submitted to the ETSI CSC. These comments were mostly related to challenges relevant to the PaaSword project and included, among others, the consideration of internal adversaries in the analysis of the use scenarios and the addition of context awareness issues with respect to data security and access control.

[28] http://csc.etsi.org/phase1/phase1/CSC_report.html
[29] http://csc.etsi.org/resources/STF_486_WP3_Report-v1.0.0.pdf

11 Conclusions

Concluding this interim version of the deliverable D7.2 – Dissemination Activities Report, we note that we reported the current dissemination activities, performed at consortium and individual level, during the first project year and we consolidated a dissemination plan for the upcoming project period. We focus on activities that involve the presentation of the project progress, technologies and results outside the scope of the PaaSword consortium in order to ensure large awareness of the academic, ICT, Cloud computing and Cloud security research communities through scientific and research publications and participation to relative events (e.g. conferences, workshops, symposiums and exhibitions). Specifically, we reported on:

- research publications produced (2 Conferences, 4 Workshops, 2 Submitted Journals)
- other dissemination-related activities performed (contribution to 14 Events)
- planned research publications (13 Conferences, 3 Workshops, 4 Journals planned or under discussion)
- other dissemination-related activities to be conducted (contribution to 10 Events)
- consortium's individual dissemination plans
- key performance indicators for the PaaSword dissemination overall plan
- status of the PaaSword's data management plan
- CS-IFG related activities
- relation to relevant standards and standardization working groups

The next interim version of the deliverable D7.2 – Dissemination Activities Report, will be delivered on M24 and it will include a comparison against the presented plan, a report on the project's second year activities and a consolidation of the detailed dissemination plan for the last year and beyond of the PaaSword project.

Acronyms

ACM	Association for Computing Machinery
CRM	Customer Relationship Management
CSA	Cloud Security Alliance
CS-IFG	Cloud Security Industrial Focus Group
DAO	Data Access Object
DB	Database
DDE	Data Distribution and Encryption
DDL	Data Definition Language
DMP	Data Management Plan
ENISA	European Union Agency for Network and Information Security
ERP	Enterprise Resource Planning
ICT	Information and Communications Technology
IEEE	Institute of Electrical and Electronics Engineers
NDA	Non-Disclosure Agreement
PaaS	Platform-as-a-Service
PKI	Public Key Infrastructure
PMI	Privilege Management Infrastructure
RBAC	Role-Based Access Control
RDF	Resource Description Framework
RDFS	Resource Description Framework Schema
SAML	OASIS Security Assertion Markup Language
SA-REST	Semantic Annotations for REST
SCAP	Security Content Automation Protocol
SDN	Software-defined Networking
SE	Searchable Encrytpion
TBD	To Be Discussed
TBA	To Be Announced

TCG	Trusted Computing
TCP	Transmission Control Protocol
TLS	Transport Layer Security
XACML	eXtensible Access Control Markup Language
XML	eXtensible Markup Language