RESEARCH & INNOVATION
Horizon 2020

Privacy and Security Maintaining Services in the Cloud

Contract Number: 644962
Call: H2020-ICT-2014-1

Deliverable D9.2

DISSEMINATION AND EXPLOITATION REPORT 1

Deliverable due date: 01.02.2016
Deliverable submission date: 01.02.2016

Document Information	
Title	Dissemination and Exploitation Report 1
Creator	Agi Karyda (AIT)
Deliverable no.	9.2
Work Package No.	9
Nature	R
Dissemination Level	PU
Release Date	01.02.2016
Document description	This deliverable marks the start of a series of periodic reports of WP9 activities. This report summarizes the various activities on dissemination and exploitation of the PRISMACLOUD results obtained in the first year. Additionally, it contains information about the project's, as well as individual partners', strategies for dissemination, exploitation and communication.

Authors List

Organization	Name	E-mail
AIT	Agi Karyda	agi.karyda@ait.ac.at
UNI PASSAU	Henrich C. Pöhls	hp@sec.uni-passau.de
ALL	All PRISMACLOUD partners	

Reviewers List

Organization	Name	E-mail
ALL	All PRISMACLOUD partners	

Versioning

Version	Date	Reason/Change	Editor
0.1	24.06.2015	Initial Content	Agi Karyda
0.2	05.01.2016	Some minor additions	Henrich C. Pöhls
0.3	14.01.2016	Update on exploitation plans	Santiago Cáceres
0.4	14.01.2016	Update on exploitation plans; merging and minor edits	Domenica Gallo; Henrich C. Pöhls
0.5	15.01.2016	Updates on exploitation plans	All authors
0.6	25.01.2016	Executive summary; finishing touches; last version for final internal review	Henrich C. Pöhls; all authors
1.0	29.01.2016	Changes by all partners; final editorial finishing; Final stable version to be submitted.	Henrich C. Pöhls; all authors

The work described in this document has been conducted within the PRISMACLOUD project. This document reflects only the PRISMACLOUD Consortium view and the European Union is not responsible for any use that may be made of the information it contains.

List of Contents

List of Tables

List of Figures

1. Executive Summary

This deliverable presents the dissemination, communication, and exploitation[1] strategies of the PRISMACLOUD project. Further it documents and summarises all the activities undertaken during the first year of the project. There are three points that PRISMACLOUD had put its focus on, which is also reflected by the structure of this deliverable: General communication, scientific dissemination and exploitation. From the many general communication activities we want to highlight the frequent update of the webpage, the designation of dissemination material such as brochures and flyers and the publication of a first newsletter. As a research project PRISMACLOUD is happy to announce that 17 scientific publications as well as several highly technical deliverables that summarize the state of the art in the research areas of PRISMACLOUD have been published. Further, we like to point out that the results and topics of PRISMACLOUD are actively used in the academic teaching, e.g. lectures are given as well as PhD and MSc and BSc students that are supervised. Highlights from the exploitation activities are the presentation at a jointly organised event at the ICT 2015 and at The Future of Cloud 2015, that were possible by the liaisons with several other projects that PRISMACLOUD established within the first year. Finally, there has been many outreach activities that brought the ideas and potential results of PRISMACLOUD to various stakeholders in the industry.

[1] For convenience when we refer to all the above mentioned activities the acronym DEC will be used.

2. Abbreviations and acronyms

DEC	Dissemination, Exploitation and Communication
DoA	Description of Action
PRISMACLOUD	PRivacy and Security MAintaining services in the CLOUD
SC	Steering Committee
TM	Technical Management
UAB	User Advisory Board
WP	Work Package

3. Introduction

PRISMACLOUD is an EU Horizon 2020 research project of 42 month duration (February 2015 – July 2018) developing the next generation of cloud security technologies. With a budget of 8.5 Million Euro over 3.5 years, the project brings together European leading companies, universities and research institutes with strong expertise and experience in the fields of cryptography, information security and cloud computing.

As the growth of cloud computing is increasing constantly, the traditional computing paradigm is experiencing a fundamental shift. Organisations using cloud computing services do no longer completely control their own data, but hand them over to external untrusted parties, i.e. cloud service providers, for processing and storage. Currently there exist no satisfactory approaches to protect data during its lifetime from cloud providers and from other users of the cloud. PRISMACLOUD develops innovative solutions based on efficient cryptographic techniques for cloud computing. These techniques improve the security of data at rest, data in move, and data in use, as well as the privacy of cloud users.

The project brings novel cryptographic concepts and methods to practical application to improve the security and privacy of cloud based services and makes them usable for providers and users. The main idea and ambition of PRISMACLOUD is to enable end-to-end security for cloud users and to provide tools to protect user privacy with the best technical means possible - by cryptography.

To make this vision come true, PRISMACLOUD plans innovation in the fields of verifiability of data and infrastructure use, user privacy and anonymisation, securing data at rest, secure and efficient implementations, methodology, tools and guidelines for fast adoption.

The consortium with 16 partners from 7 different EU member states and two associated countries (Switzerland and Israel) is led by AIT Austrian Institute of Technology (Vienna, Austria) as project coordinator, and IAIK-TUG Graz University of Technology (Graz, Austria) as Technological Manager. Further partners include Atos Spain, S.A. (Spain), CEA - Commissariat à l’énergie atomique et aux énergies alternatives (France), TUDA - Technische Universität Darmstadt (Germany), ETRA - ETRA Investigación y Desarrollo S.A. (Spain), FCSR - Fondazione Centro San Raffaele (Italy), IBM - IBM Israel Science & Technology Ltd. (Israel), IRT - Interoute S.p.a. (Italy), KAU - Karlstad University (Sweden), LISPA - Lombardia Informatica S.p.A. (Italy), MPL – MikroPlan GmbH (Germany), UNEW - University of Newcastle upon Tyne (UK), UNIL - Université de Lausanne (Switzerland), UNI PASSAU - Universität Passau (Germany), XT – XiTrust Secure Technologies GmbH (Austria). Furthermore, PRISMACLOUD has initiated a User Advisory Board which consists of end-user organizations and (Cloud) security experts.

The dissemination and communication of information is a key requirement of the PRISMACLOUD project and has been considered as a special topic, due to the research nature of the project and the number of contributions that PRISMACLOUD could make to the state of the art. Additionally, exploitation is a key enabler for the success of the project’s outcomes sustainability after the project ends.

3.1. Purpose of the document

The PRISMACLOUD dissemination and exploitation plan is based on identifying and organising the activities to be performed in order to promote the project's results with the widest dissemination of knowledge from the project. Dissemination is a horizontal activity and concentrates on disseminating the results of the project itself to a wide range of existing or potential stakeholders. The PRISMACLOUD consortium will promote project's results with:

- the dissemination of the project results in the scientific domain;
- the promotion of the project in the industrial world;
- the dissemination via centres and networks of excellence.

In addition, advertising material has been developed and will be updated during the lifecycle of the project; in particular an interactive website and social networks profile will help to support both external dissemination and interaction between the project partners.

The aim is to form a critical mass of key industrialists and academics to promote the PRISMACLOUD concept. Effective dissemination is important in order to:

- make key individuals and groups aware of the work;
- enable them to understand the concepts and potential benefits;
- obtain critical feedback from them to assess the perceived value of the approach.

3.2. Scope of the document

The Dissemination and Exploitation Report 1 is a deliverable of the PRISMACLOUD project, which sets out the dissemination, communication and exploitation strategy as well as the means that are used to promote the project objectives and results by providing a detailed description of the carried out dissemination and communication activities during the first year of project's execution.

3.3. Structure of the document

The document is structured in three parts. Part one starts with a short description on the general objectives of the dissemination, communication and exploitation for the project (Section 4). Part two continues with the descriptions of the strategies for general communication (Section 5), scientific dissemination (Section 6) and exploitation (Section 7) to promote the project results the and PRISMACLOUD approach. Finally, part three presents the dissemination and exploitation activities performed during the first year of the project (Section 8).

4. Dissemination, Exploitation and Communication Objectives

The planned dissemination, exploitation and communication (DEC) actions endeavour to create a large awareness of PRISMACLOUD innovations and results in order to generate a worldwide market in which European players can expect to have an important role.

4.1. Target audience

PRISMACLOUD project distinguishes between internal and external audiences.

4.1.1. Internal audience

The internal audience of the PRISMACLOUD project is directly involved in the project and comprises both academic and industrial PRISMACLOUD partners and the European Commission.

- **Academic Organisations**
  - Graz University of Technology (TU Graz)
  - Karlstad University (KAU)
  - University of Passau (UNI PASSAU)
  - University of Lausanne (UNIL)
  - Technical University of Darmstadt (TUDA)
  - Newcastle University (UNEW)

- **Institutional Research Organisations**
  - Austrian Institute of Technology GmbH (AIT)
  - Commissariat à l'énergie atomique et aux énergies alternatives (CEA)

- **Industrial Research Organisations**
  - ATOS
  - IBM

- **Service and Solution Providers**
  - ETRA Investigación y Desarrollo, S.A. (ETRA)
  - Fondazione Centro San Raffaele (FCSR)
  - Lombardia Informatica S.p.A. (LISPA)
  - Interoute S.p.A. (IRT)

- **Small and Medium Sized Enterprises**
  - MikroPlan GmbH (MPL)
  - XiTrust Secure Technologies GmbH (XiTrust)

- **European Commission**

4.1.2. External audience

The external target audience is not directly involved in the PRISMACLOUD project and an indicative initial list comprises of:

- **Research Community** – industrial as well as academic communities
- **Industry** – Cloud Providers and Cloud Users (including, but not limited to existing and potential future clients of industrial project partners), especially in the areas of
  - Public sector (government, health, industry)
  - Telco operators
- **Projects** – Other European (H2020 and FP7) and national projects
- **Standardisation Bodies and Alliances**
- **Students and Trainees** – Employees, Students (PhD/M.Sc./B.Sc./other), or anyone else interested in the PRISMACLOUD research area, namely for training and educational purposes
- **General public**
  - Potential customers that might buy services supported by PRISMACLOUD developments
  - End users of applicants that benefit from PRISMACLOUD results
  - Policy makers
  - Media
  - Members of civil societies
- **Citizens representations bodies**

4.2. The objectives

The objectives for PRISMACLOUD's DEC have been classified into four levels (ordering of levels is arbitrary). Depending on their targeted audience the means to achieve them differ. This section will first discuss the four levels (subsections 4.2.1-4.2.4) and then present some suggested means to achieve in relation to the targeted audience (subsection 4.2.5).

4.2.1. Level 1: Dissemination objectives within PRISMACLOUD consortium

The main objectives of the dissemination activities that are directed to the internal communication are to:

- ensure and establish clear channels of responsibility between the coordinator, the different management bodies and the PRISMACLOUD consortium;
- share knowledge within the consortium;
- focus consortium on research goals;
- identify and establish contacts with additional projects of interest to the research activities of PRISMACLOUD.

4.2.2. Level 2: Dissemination activities towards the Research Community

The main objectives for the dissemination activities towards the research communities, which is external communication, are to share the knowledge. In more detail the objectives are to:

- transform suitable relevant scientific results into scientific publications to inform scientist in the research communities of PRISMACLOUD results;
- plan and execute joint meetings and workshops with suitable research projects to promote research exchange and share knowledge;
- deepen, broaden and prolong the knowledge by engaging young researchers and students;
- establish new or strengthen scientific co-operations, e.g. foster academic exchanges.

4.2.3. Level 3: Communication activities towards the General Public

The main objectives for the external communication activities in level 3 are to inform the general public. In some more detail the objectives are:

- identify other stakeholders who would benefit from the knowledge acquired by the PRISMACLOUD consortium;
- establish a correct communication towards the identified stakeholders.

4.2.4. Level 4: Exploitation activities towards Industry

The main objectives for the exploitation activities toward the Industry, which is obvious external communication, in level 4 are to:

- establish contact with suitable industrial associations on a national and European level;
- attend main international events relevant to the interest of Industry in the domain of the PRISMACLOUD project.

4.3. Means to achieve the objectives in relation to the target audience

The above objectives, and the means to achieve them, are tackled considering the different dissemination and communication materials and actions available to promote the project. If the target audience identified in the previous section is considered, different strategies and goals can be pointed out:

4.3.1. Means to address the internal target audience

- Dissemination of knowledge within the consortium is crucial for the success of the project. The international and geographically distributed nature of PRISMACLOUD partners emphasizes the importance for information exchange and location independent co-working. PRISMACLOUD installed a functional and a secure knowledge management system through the use of a project collaboration tool (SharePoint). It is used as repository for all PRISMACLOUD relevant documents and allows fast and easy access via Internet.

- Furthermore, project meetings (physical and teleconferences) will be held regularly to disseminate results within the consortium and to focus all partners on the research goals.

Especially, plenary meetings will be arranged at least twice a year where the members of the SC, the TM and the sub-units will participate, and consortium teleconferences will be held once a month.

- Moreover, focused ad-hoc WP meetings on specific issues will be also organised by the WP leaders.
- Furthermore, the research addressed in PRISMACLOUD can be useful for other departments and units within each of the involved organisations. Internal promotion does not only serve to grant an efficient collaboration among partners in the consortium, but also to extend the results of the project internally. In this way, synergies may arise with other research or business groups that could help the taking over of the project's results after its finalisation.

4.3.2. Means to address the external target audience

- Make target audience aware of PRISMACLOUD.
  This is a primary communication goal since it is a prerequisite to achieve further goals. A various number of means will be used for this purpose including the PRISMACLOUD website, participation at conferences and workshops, presentation of PRISMACLOUD at trade fairs and exhibitions, distribution of leaflets, white papers, fact sheets, posters etc.
- Share results with other research groups.
  The PRISMACLOUD approach and results will be presented to other research groups (in particular other H2020 and FP7 projects) working on alternative approaches to gain feedback and to ensure that the results will converge to a maximum extent. Hence, PRISMACLOUD will participate in and/or organizes scientific conferences and workshops.
- Promoting deployment of PRISMACLOUD results.
  One primary target audience for the deployment of PRISMACLOUD results is the PRISMACLOUD User Advisory Board (UAB). Additionally to already indirectly addressing industry and universities through the respective members of the UAB the planned means to promote the results include scientific dissemination activities and standardisation activities.
- Attracting students to participate in the PRISMACLOUD project.
  All participating research organisations will incorporate research results in their courses thereby promoting and disseminating the idea and content of PRISMACLOUD. These activities will attract students to participate in the PRISMACLOUD project, e.g. by choosing their PhD, Bachelor's or Master's thesis from the PRISMACLOUD field, which in turn deepens existing and generates new knowledge.

4.3.3. Summary of means of DEC activities for external target audiences

A suitable mean to reach the dissemination and exploitation objectives depends on the target audience. The following table lists the dissemination and exploitation goals and suggests some selected means to reach the objective for each target audience.

Audience	Dissemination, Exploitation and Communication Goals	Dissemination Means
Academic and Industrial Partners	Share knowledge, focus on research goals	Distribution of documents via project collaboration tool; project meetings and internal presentations to other units and departments; research visits.
Research Community	Share knowledge, gain feedback	Journal articles; presentations at conferences and workshops; papers; posters; research visits.
Industry	Share knowledge, gain feedback, promoting deployment of PRISMACLOUD results	Standardisation activities; workshops; members of the user advisory board; conferences; exhibitions and trade fairs; newsletters; white papers; posters.
Other Projects	Share knowledge, gain feedback, establish cooperation	Organize joint workshops or conferences; newsletters; research visits.
Students and Trainees	Attract students to share the existing knowledge (training/education) and generate new insights (foster research in PRISMACLOUD related problems), and to train employees	Attract students by lectures, summer schools, PhD/MSc/BSc-thesis topics that include solutions or problems related to PRISMACLOUD; research visits.
General Public	Inform general public about the key ideas behind and the results of PRISMACLOUD	Website; social networks; newsletters and public demonstrations; articles and videos (YouTube) for non-scientists.
Citizens representations bodies	Approach and inform selected interest group in order to promote the results	Website; newsletters; address them indirectly through members of the user advisory board; videos (YouTube) and public demonstrations; standardisation activities.

Table 1: Dissemination, exploitation and communication goals and means (order is arbitrary)

4.4. Roles

The communication, dissemination and exploitation activities are carried out mainly by the following boards:

Innovation Management

Innovation management in PRISMACLOUD is based on a decision framework that is implemented within the Technical Management, which will identify the type of innovations and evaluate these in terms of potential, impact and the scope required to turn innovations to effective market success. The Innovation Management panel in PRISMACLOUD is represented by one person per partner and includes a variety of researchers with different views (cryptography, applied cryptography, information security, security by design and usability) as well as a good mix between players from academics and industry so to cover a broad perspective that also addresses market needs and new business models.

Exploitation Committee

The exploitation Committee is represented by one person per partner. It aims to coordinate the exploitation and dissemination plan of PRISMACLOUD taking into account market data, business plans of the partners, and opportunities for dissemination and collaboration with other initiatives/projects.

User Advisory Board

The User Advisory Board Members will contribute to the dissemination and exploitation of the PRISMACLOUD project since they are coming from industry as well as universities around Europe.

Consortium

In addition to the overall project communication, dissemination and exploitation plans, PRISMACLOUD partners have individual plans according to their countries, their expertise and the type of their organisation. Moreover, they are encouraged to publish PRISMACLOUD related information on their organizations' websites.

5. Strategy for General Communication

The strategy for general dissemination – not scientific specific – is first based on the promotion of a common corporative graphical identity for the project in order to facilitate the identification of any PRISMACLOUD material and result. This is done, not only by creating a project logo and visual identity, but also by making use of a common set of templates to publish information internally and externally.

5.1. PRISMACLOUD identity

5.1.1. PRISMACLOUD logo and acronym usage

prisma cloud

Logo without text

Logo with text

Figure 1: PRISMACLOUD logos

It is advised that the PRISMACLOUD logo appears in all PRISMACLOUD related documents. Any material co-funded with the project budget needs to make explicit reference to it and if possible make use of the PRISMACLOUD Logo. It has been developed in two different types in order to be able to use it in different formats and for different purposes.

In this way, the first logo is the official and corporative image of the project to be used by default. The Acronym of the project – i.e., PRISMACLOUD – is the main representative mark. When possible it has to be used with the above mentioned logo, respecting the font and colours. Otherwise, it should be written with capital letters.

5.1.2. Templates for documentation and presentation

As already mentioned in D1.1 Project Handbook, the templates for documentation and presentation are located in PRISMACLOUD SharePoint and are available from the early beginning of the project.

Moreover, a general PRISMACLOUD presentation which provides a quick look to the project objectives and innovations can be found in the PRISMACLOUD SharePoint. This set of slides will be updated periodically with the new results as the projects advances.

5.2. PRISMACLOUD Website

The PRISMACLOUD website (https://www.prismacloud.eu) is online since February 2015 and is the main general dissemination and communication tool, available to anyone with access to the internet. It all serves as a distribution channel of the rest of communication material used until now: brochures, presentations, and posters.

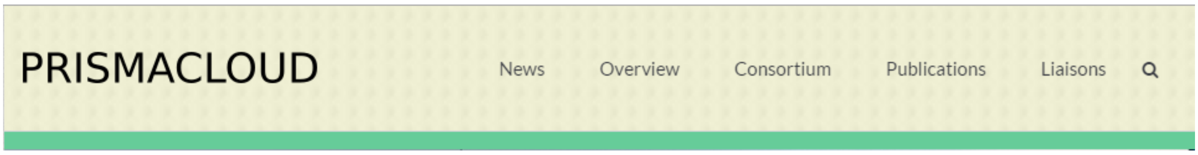


Figure 2: PRISMACLOUD website - navigation bar

The website will be periodically updated with project's news, publications, and summaries on the progress of the project in order to reflect the project's advancement.

The structure of the website is divided into the following six main headings:

- PRISMACLOUD: This section is the home page and contains the project's vision and a general brief description, as well as a feed to the PRISMACLOUD twitter account where news about the project is published.
- News: This section contains all the news and events internal and external to the project that keep a tight relation with PRISMACLOUD, including the project workshops, meetings, seminars, summer schools and academic seminars.
  - Project News: This section contains news about project's evolution.
  - Events: This section contains events relevant to the project's topic.
- Overview: Under this heading a description of the project's objectives and innovation as well as the project's metadata.
- Consortium: Description of the project consortium members and their role in the project.
- Publications: An updated list of publications including:
  - White Paper: This section contains white papers of the project
  - Scientific Publications: All the scientific publications are published during project's evolution can be found here.
  - Presentations: Project partners' presentations in conferences and workshops.
  - Press Releases: Press releases which are published in scientific printed and online magazines or other communication means containing important news about the project.
  - Media Centre: It contains the project's communication material such as the poster, the folder and the project's general presentation.
- Liaisons: This section contains the User Advisory Board members as well as liaisons established with other projects and initiatives.

Statistics for Webs: All the web site transactions are logged, in order to track any kind off attack, wrong usage or similar situations. The following statistic shows the unique visitors aggregated over two weeks.

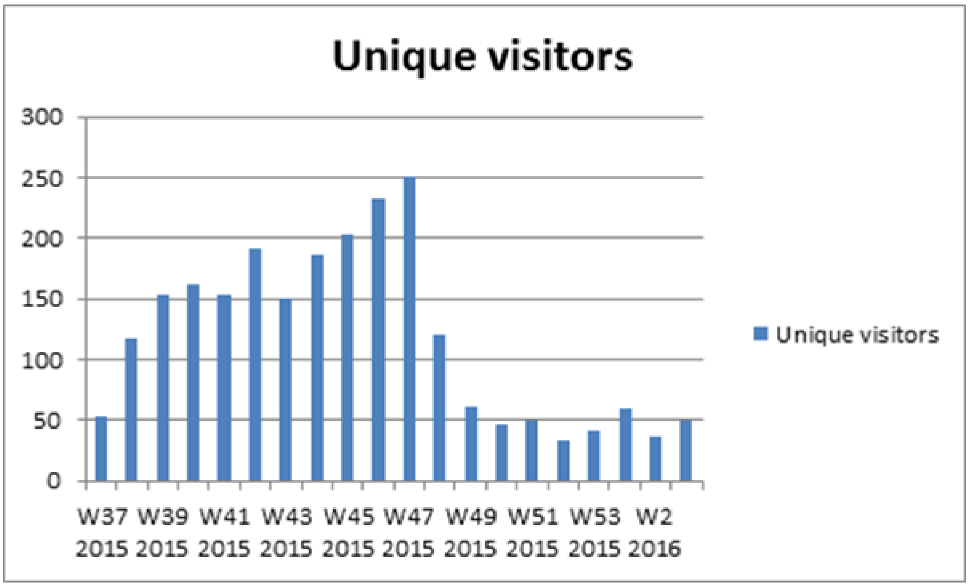
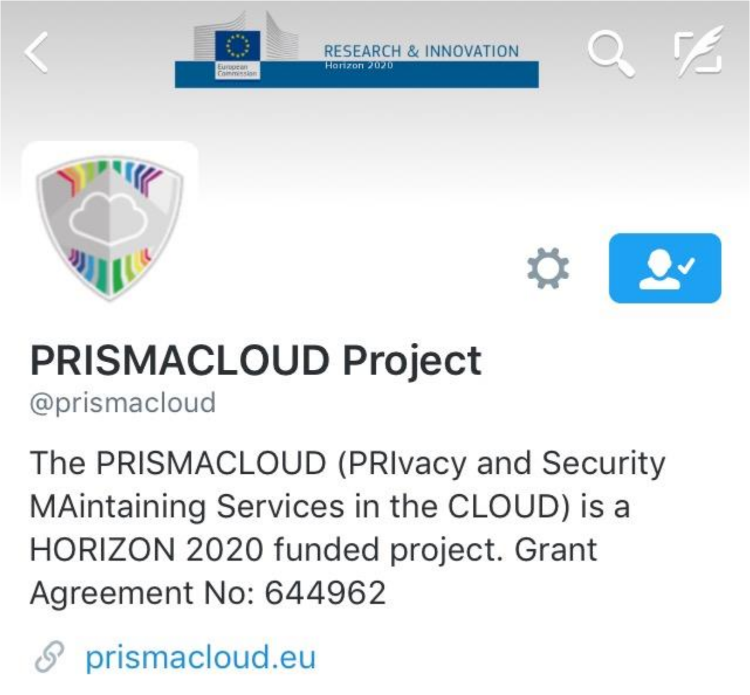


Figure 3: PRISMACLOUD website statistic of unique visitors

5.3. Social media

In order to maximise the awareness and impact of the project, the PRISMACLOUD Consortium has set up profile accounts of the project in Twitter and LinkedIn. The statistics were updated end of January 2016.



PRISMACLOUD Project
@prismacloud

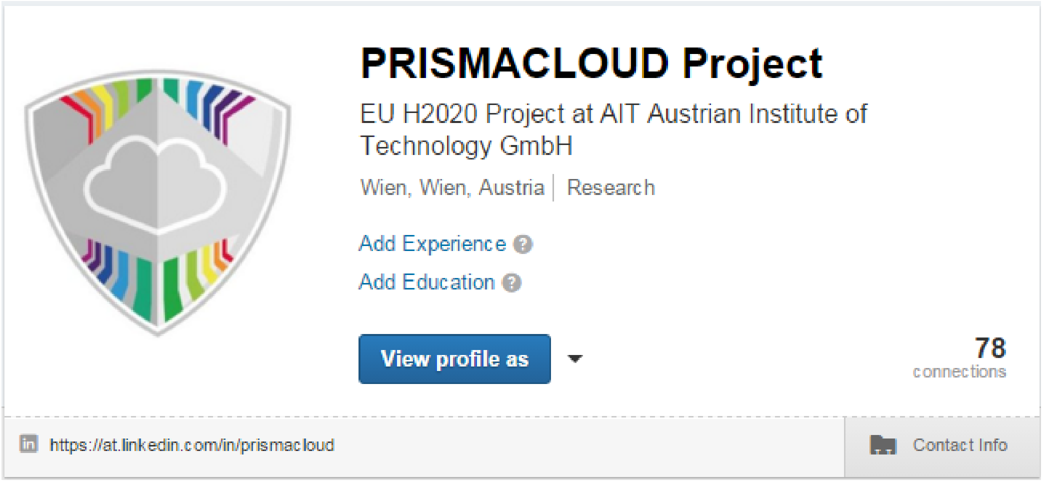
The PRISMACLOUD (PRIvacy and Security MAintaining Services in the CLOUD) is a HORIZON 2020 funded project. Grant Agreement No: 644962

prismacloud.eu

Figure 4: PRISMACLOUD twitter profile

Statistics from Twitter:		
	TWEETS	50
	FOLLOWERS	61

last updated 25.01.2016

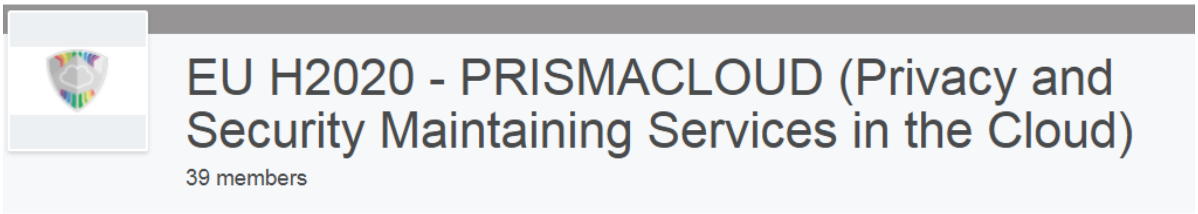


PRISMACLOUD Project

EU H2020 Project at AIT Austrian Institute of Technology GmbH

Wien, Wien, Austria | Research

Figure 5: PRISMACLOUD LinkedIn profile



EU H2020 - PRISMACLOUD (Privacy and Security Maintaining Services in the Cloud)

39 members

Figure 6: PRISMACLOUD LinkedIn group:

Statistics from LinkedIn:		
	PROFILE CONNECTIONS	78
	GROUP MEMBERS	39

last updated 25.01.2016

5.4. PRISMACLOUD newsletters

There is the strategic plan to produce a periodic e-newsletter containing summaries of the project’s achievements. The newsletter shall get distributed by any of the consortium members participating at European or national events dealing with related subjects, and by post or e-mail to the User and Advisory board members and relevant bodies. Preparation of the first newsletter has started.

5.5. PRISMACLOUD communication material

5.5.1. PRISMACLOUD Flyer

The PRISMACLOUD Flyer has been designed to promote and enhance the visibility of the project. It will be distributed to potential interested group members at conferences, workshops and exhibitions. The primary goal is to introduce the PRISMACLOUD project to the general public. In the flyer's cover page the PRISMACLOUD and European Commission logos, the QR Code, the web page, the consortium members and the contact details are demonstrated, whereas in the inside pages the project's vision, metadata, objectives and innovations are provided.

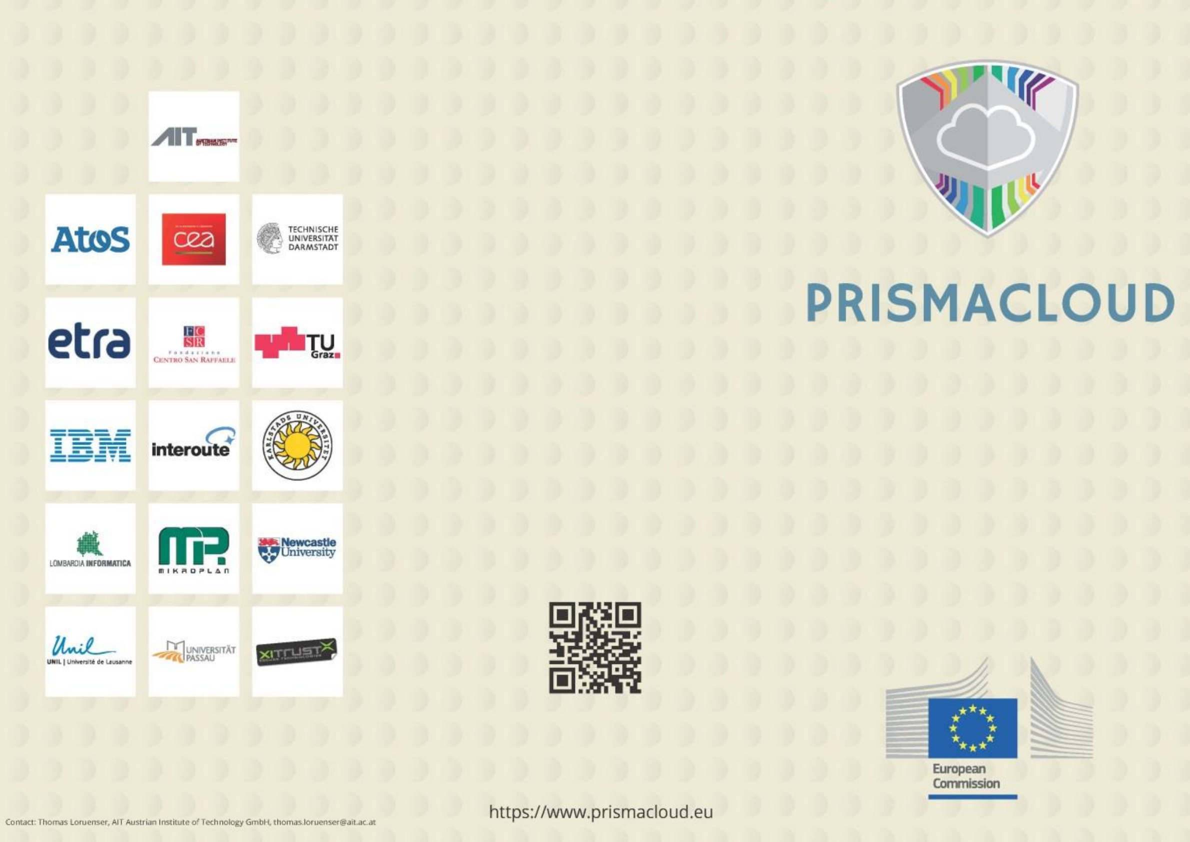
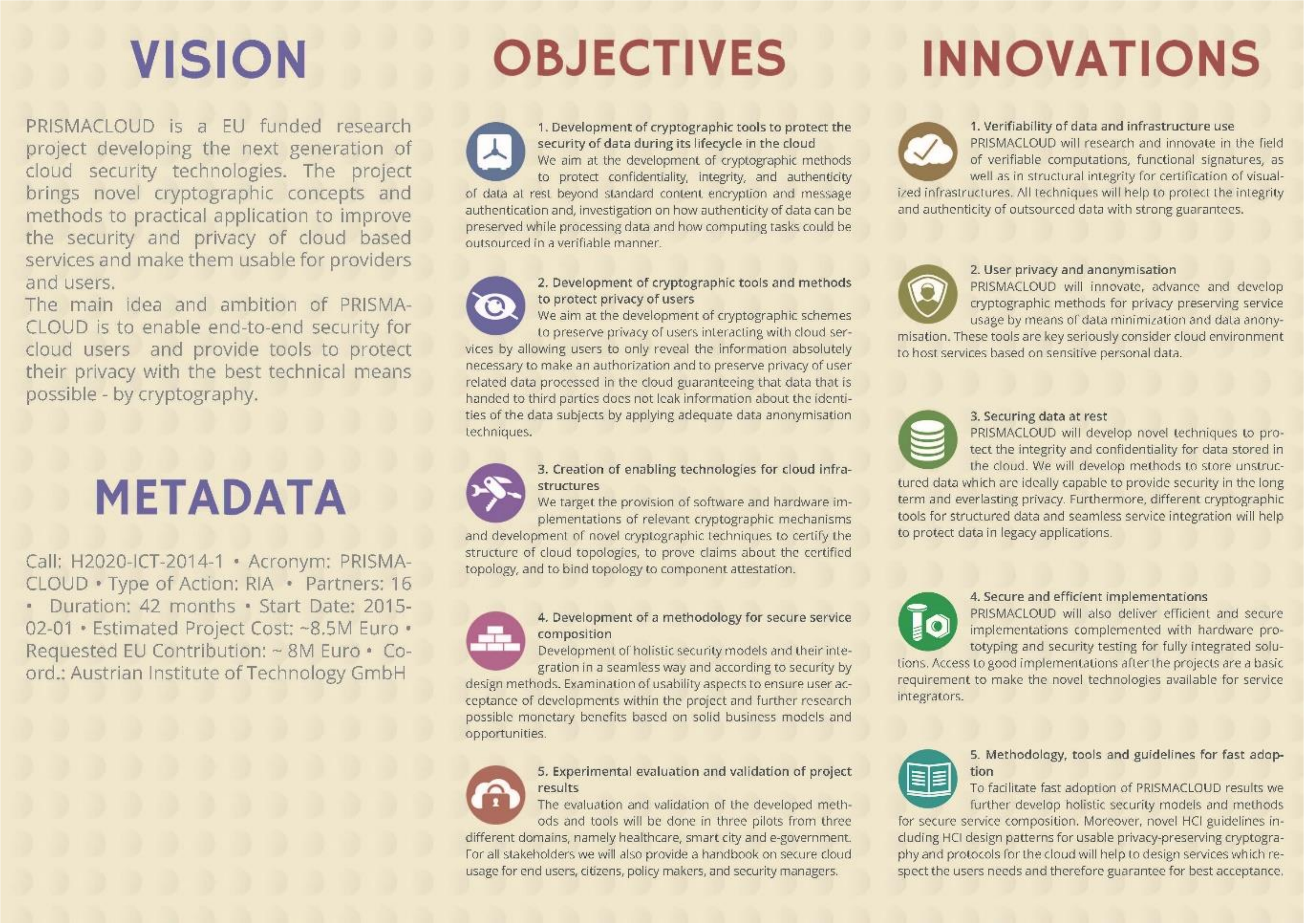

PRISMACLOUD
European Commission
https://www.prismacloud.eu
Contact: Thomas Loruenser, AIT Austrian Institute of Technology GmbH, thomas.loruenser@ait.ac.at

Figure 7: PRISMACLOUD flyer cover page



VISION

PRISMACLOUD is a EU funded research project developing the next generation of cloud security technologies. The project brings novel cryptographic concepts and methods to practical application to improve the security and privacy of cloud based services and make them usable for providers and users.

The main idea and ambition of PRISMACLOUD is to enable end-to-end security for cloud users and provide tools to protect their privacy with the best technical means possible - by cryptography.

METADATA

Call: H2020-ICT-2014-1 • Acronym: PRISMACLOUD • Type of Action: RIA • Partners: 16 • Duration: 42 months • Start Date: 2015-02-01 • Estimated Project Cost: ~8.5M Euro • Requested EU Contribution: ~ 8M Euro • Co-ord.: Austrian Institute of Technology GmbH

OBJECTIVES

1. Development of cryptographic tools to protect the security of data during its lifecycle in the cloud

We aim at the development of cryptographic methods to protect confidentiality, integrity, and authenticity of data at rest beyond standard content encryption and message authentication and, investigation on how authenticity of data can be preserved while processing data and how computing tasks could be outsourced in a verifiable manner.

2. Development of cryptographic tools and methods to protect privacy of users

We aim at the development of cryptographic schemes to preserve privacy of users interacting with cloud services by allowing users to only reveal the information absolutely necessary to make an authorization and to preserve privacy of user related data processed in the cloud guaranteeing that data that is handed to third parties does not leak information about the identities of the data subjects by applying adequate data anonymisation techniques.

3. Creation of enabling technologies for cloud infrastructures

We target the provision of software and hardware implementations of relevant cryptographic mechanisms and development of novel cryptographic techniques to certify the structure of cloud topologies, to prove claims about the certified topology, and to bind topology to component attestation.

4. Development of a methodology for secure service composition

Development of holistic security models and their integration in a seamless way and according to security by design methods. Examination of usability aspects to ensure user acceptance of developments within the project and further research possible monetary benefits based on solid business models and opportunities.

5. Experimental evaluation and validation of project results

The evaluation and validation of the developed methods and tools will be done in three pilots from three different domains, namely healthcare, smart city and e-government. For all stakeholders we will also provide a handbook on secure cloud usage for end users, citizens, policy makers, and security managers.

INNOVATIONS

1. Verifiability of data and infrastructure use

PRISMACLOUD will research and innovate in the field of verifiable computations, functional signatures, as well as in structural integrity for certification of visualized infrastructures. All techniques will help to protect the integrity and authenticity of outsourced data with strong guarantees.

2. User privacy and anonymisation

PRISMACLOUD will innovate, advance and develop cryptographic methods for privacy preserving service usage by means of data minimization and data anonymisation. These tools are key seriously consider cloud environment to host services based on sensitive personal data.

3. Securing data at rest

PRISMACLOUD will develop novel techniques to protect the integrity and confidentiality for data stored in the cloud. We will develop methods to store unstructured data which are ideally capable to provide security in the long term and everlasting privacy. Furthermore, different cryptographic tools for structured data and seamless service integration will help to protect data in legacy applications.

4. Secure and efficient implementations

PRISMACLOUD will also deliver efficient and secure implementations complemented with hardware prototyping and security testing for fully integrated solutions. Access to good implementations after the projects are a basic requirement to make the novel technologies available for service integrators.

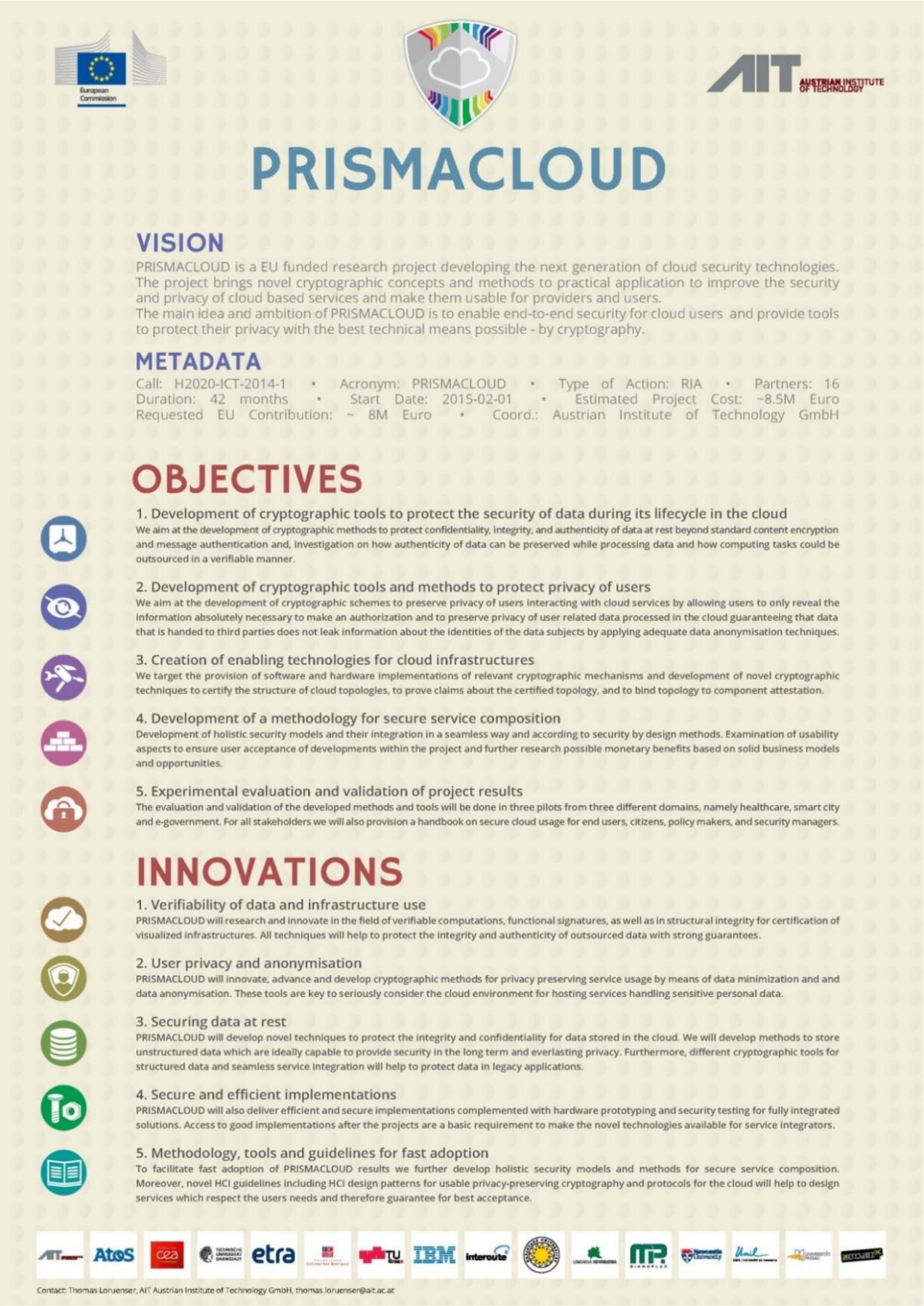
5. Methodology, tools and guidelines for fast adoption

To facilitate fast adoption of PRISMACLOUD results we further develop holistic security models and methods for secure service composition. Moreover, novel HCI guidelines including HCI design patterns for usable privacy-preserving cryptography and protocols for the cloud will help to design services which respect the users needs and therefore guarantee for best acceptance.

Figure 8: PRISMACLOUD flyer inside page

5.5.2. PRISMACLOUD poster

A poster of A0 size has been designed as a generic communication material and can be found in PRISMACLOUD SharePoint. It presents the project's vision, metadata, objectives and innovations, as well as the consortium members, and the contact details.



PRISMACLOUD

VISION

PRISMACLOUD is a EU funded research project developing the next generation of cloud security technologies. The project brings novel cryptographic concepts and methods to practical application to improve the security and privacy of cloud based services and make them usable for providers and users.

The main idea and ambition of PRISMACLOUD is to enable end-to-end security for cloud users and provide tools to protect their privacy with the best technical means possible - by cryptography.

METADATA

Call: H2020-ICT-2014-1 • Acronym: PRISMACLOUD • Type of Action: RIA • Partners: 16
Duration: 42 months • Start Date: 2015-02-01 • Estimated Project Cost: ~8.5M Euro
Requested EU Contribution: ~ 8M Euro • Coord.: Austrian Institute of Technology GmbH

OBJECTIVES

1. Development of cryptographic tools to protect the security of data during its lifecycle in the cloud

We aim at the development of cryptographic methods to protect confidentiality, integrity, and authenticity of data at rest beyond standard content encryption and message authentication and, investigation on how authenticity of data can be preserved while processing data and how computing tasks could be outsourced in a verifiable manner.

2. Development of cryptographic tools and methods to protect privacy of users

We aim at the development of cryptographic schemes to preserve privacy of users interacting with cloud services by allowing users to only reveal the information absolutely necessary to make an authorization and to preserve privacy of user related data processed in the cloud guaranteeing that data that is handed to third parties does not leak information about the identities of the data subjects by applying adequate data anonymisation techniques.

3. Creation of enabling technologies for cloud infrastructures

We target the provision of software and hardware implementations of relevant cryptographic mechanisms and development of novel cryptographic techniques to certify the structure of cloud topologies, to prove claims about the certified topology, and to bind topology to component attestation.

4. Development of a methodology for secure service composition

Development of holistic security models and their integration in a seamless way and according to security by design methods. Examination of usability aspects to ensure user acceptance of developments within the project and further research possible monetary benefits based on solid business models and opportunities.

5. Experimental evaluation and validation of project results

The evaluation and validation of the developed methods and tools will be done in three pilots from three different domains, namely healthcare, smart city and e-government. For all stakeholders we will also provision a handbook on secure cloud usage for end users, citizens, policy makers, and security managers.

INNOVATIONS

1. Verifiability of data and infrastructure use

PRISMACLOUD will research and innovate in the field of verifiable computations, functional signatures, as well as in structural integrity for certification of visualized infrastructures. All techniques will help to protect the integrity and authenticity of outsourced data with strong guarantees.

2. User privacy and anonymisation

PRISMACLOUD will innovate, advance and develop cryptographic methods for privacy preserving service usage by means of data minimization and and data anonymisation. These tools are key to seriously consider the cloud environment for hosting services handling sensitive personal data.

3. Securing data at rest

PRISMACLOUD will develop novel techniques to protect the integrity and confidentiality for data stored in the cloud. We will develop methods to store unstructured data which are ideally capable to provide security in the long term and everlasting privacy. Furthermore, different cryptographic tools for structured data and seamless service integration will help to protect data in legacy applications.

4. Secure and efficient implementations

PRISMACLOUD will also deliver efficient and secure implementations complemented with hardware prototyping and security testing for fully integrated solutions. Access to good implementations after the projects are a basic requirement to make the novel technologies available for service integrators.

5. Methodology, tools and guidelines for fast adoption

To facilitate fast adoption of PRISMACLOUD results we further develop holistic security models and methods for secure service composition. Moreover, novel HCI guidelines including HCI design patterns for usable privacy-preserving cryptography and protocols for the cloud will help to design services which respect the users needs and therefore guarantee for best acceptance.

Contact: Thomas Loruenser, AIT Austrian Institute of Technology GmbH, thomas.loruenser@ait.ac.at

Figure 9: PRISMACLOUD poster

5.5.3. Press Releases

The consortium will inform the press regularly on interesting results of the PRISMACLOUD project.

5.5.4. Other promotional material

In addition to the PRISMACLOUD poster and folder other communication material such as USB sticks and T-Shirts will be designed, based on projects established identity, and distributed during exhibitions and conferences

5.6. PRISMACLOUD Lectures, PhD/MSc/BSc-thesis, and other training

As an additional means to communicate the findings and results the PRISMACLOUD project will be presented in several courses at different universities. The list of partners where lectures could be given includes, obviously, the academic institutions participating in the project. An additional goal is to attract students to contribute to PRISMACLOUD, e.g. by choosing their PhD, Master’s or Bachelor’s thesis from the field of PRISMACLOUD. Details can be found in the exploitation sections, as for the purpose of this Deliverable these activities are considered exploitations.

6. Strategy for Scientific Dissemination

The considerations made above for general dissemination (communication) should be considered also for the specific scientific dissemination strategy. The strategy for the scientific dissemination of PRISMACLOUD is naturally concerned with scientific publications, conferences and workshops.

6.1. Journals and other scientific publications

Scientific publications usually require detailed research results and they are planned for the later phase of the project when the results and findings of the project research will be available. The PRISMACLOUD project consortium will target scientific journals and magazines to disseminate its research results and findings.

Some relevant Security Journals include (but are not limited to):

- Journal of Computer Security (IOS)
- International Journal of Information Security (Springer)
- IEEE Transactions on Cloud Computing
- International Journal of Secure Software Engineering (IJSSE)
- Computers and Security (Elsevier)
- IEEE Security and Privacy
- IEEE Transactions on Services Computing
- Journal of Services and Cloud Computing
- International Journal of Cloud Computing

6.2. Conferences and workshops / summer schools

The list of conferences and workshops relevant to the project is kept updated in the PRISMACLOUD repository. Each partner detecting a new opportunity is expected to circulate the information to the consortium, update the list of Upcoming Events and if possible upload to the repository the relevant call-announcement.

The objective of PRISMACLOUD is to be present – through the submission of papers and posters – in the most relevant conferences. The project partners keep each other informed of upcoming dissemination opportunities to plan joint activities.

A list of candidate outlets has been drawn up, many of which the project consortium already have previous experience of attending.

- IEEE Symposium on Security and Privacy
- USENIX Security Symposium
- CCS – ACM Conference on Computer and Communications Security
- PETS – Privacy Enhancing Technologies Symposium
- SOUPS – Symposium on Usable Privacy and Security
- ESORICS – European Symposium on Research in Computer Security
- FC – Financial Cryptography

- ASIACRYPT - Conference on the Theory and Application of Cryptology and Information Security
- EUROCRYPT - International Conference on the Theory and Applications of Cryptographic Techniques
- CRYPTO - International Cryptology Conference
- ISOC Network and Distributed System Security Symposium
- IEEE Computer Security Foundations Symposium
- The International Conference on Dependable Systems and Networks
- Annual Computer Security Applications Conference
- ACM Symposium on Access Control Models and Technologies
- IEEE International Conference on Cloud Computing
- USENIX HotCloud (http://www.usenix.org/events/hotcloud/)
- The ACM Cloud Computing Security Workshop
- ACNS – International Conference on Applied Cryptography and Network Security

The above list is in no particular order.

6.3. Exhibitions

PRISMACLOUD wants to make its results and objectives visible with a booth or at panel discussions, round tables or with presentations at important high level events. The current plan was to attend events like:

- ICT 2015 Innovate, Connect, Transform, 20-22 October 2015, Lisbon, Portugal
- CSP Innovation Forum 2015, 28-29 April 2015, Brussels, Belgium
- The Future of Cloud, 17 June 2015, Vienna, Austria
- Cloud World Forum, 24-25 June 2015, London, United Kingdom

6.4. Technical reports

The public technical Deliverables that will be produced as result of the project, will be also considered and used as scientific dissemination tools. They will be published as public technical reports by the respective academic partners on their websites. They should be as self-contained as possible, in order to facilitate the reading and understanding of the proposed scientific advances. This allows a fast and wide scientific distribution of the technical results.

The public technical Deliverables will become available at the PRISMACLOUD website as well as white papers produced during the course of the project.

6.5. Publication procedure

Publication procedure must follow the rules already defined in PRISMACLOUD D1.1 Project Handbook, the Grant Agreement and the Consortium Agreement.

7. Strategy for Exploitation

The PRISMACLOUD project involves partners form all areas of the spectrum of cloud computing. PRISMACLOUD consortium consists of large European service and solution providers with access to end-users (ATOS, ERTRA, FCSR, LISPA), middleware developers (IBM, ATOS, ETRA) and also an end-user for PRISMACLOUD tools (FCSR) in the project, small system solution providers and developers for dedicated local markets (MPL, XiTrust) and infrastructure provider (IRT, LISPA) with European roots and infrastructure. All this industrial partners have direct access to their markets and a large user basis all over Europe. The collaboration of the main players in European industry will help to lead the development of trustworthy services for European industry and to strengthen the position in the global cloud security market.

Moreover, academic partners (TUDA, TU Graz, KAU, UNEW, UNIL, UNI PASSAU) and research centres (AIT, CEA, IBM) are in the project to generate new ideas and transfer the technology from academia to industry. The exploitation of results of the project will be done in each institution. However, many partners in the consortium are involved in standardisation bodies, where they can push the PRISMACLOUD ideas in an international scope.

An exploitation Committee is established as a sub-unit of the Steering Committee, represented by one person per partner. It aims to coordinate the exploitation and dissemination plan of PRISMACLOUD taking into account market data, business plans of the partners and opportunities for dissemination and collaboration with other initiatives/projects.

7.1. Assets most likely to be subject to exploitation

At this early stage there are not yet any products singled out yet. Some initial products that were foreseen to benefit from PRISMACLOUD' results have already been named on individual project partner's exploitation plans in the DoW. At the end of year one PRISMACLOUD partners have identified a number of assets from PRISMACLOUD's body of research that they see most suitable to become exploited and eventually will generate products.

Those asset/areas could be identified as:

- Verifiability of data and computations on data
- Verifiability of infrastructure to use
- User privacy and anonymization
- Security protection for data at rest

Some updates and clarifications for partners that occurred in year one (period 1) have been collected in section 7.3. Note, that the two subsequent future deliverables will document the future exploitation also with regards to products.

7.2. Types of exploitation activities

Each project partner has special plans to exploit the project's results by:

- consulting activities especially in the public sector (government, health and energy);
- contacting telecom operators;
- the know-how gained from the PRISMACLOUD project will be leveraged in future research projects;
- providing high quality scientific publications covering the technologies developed within the project;
- training and educating employees or (PhD/M.Sc./B.Sc./other) students;
- devising and exploiting from an industrial point of view state-of-the-art technological innovations;
- impacting on the huge business area of the company;
- enhancing partners companies service offering;
- delivering the new services either within organisation or towards the market;
- improving industrial project partners' top-level products and make their services more attractive.

The academic partners can transfer their research results to industrial partners. This is done either by direct bilateral projects, in larger consortia involving additional partners or by the formation of spin-off companies. An exploitation of the project results in follow-up project proposals on a national or European level is planned as well. Moreover patent filing is one of the major goals. All academic partners are also encouraged to release part of their work in form of open source software after approval by the exploitation management board.

7.3. Updates / Details of individual partner's strategy for exploitation

The DoA already states individual partners' exploitation plans. However, when available updates with additional details of some individual exploitation plans are given in the following subsections after one year of the project.

7.3.1. ETRA Research and Development

ETRA is a large industry with international presence, its areas of activity are centred on the delivery of Smart Cities solutions related to Mobility, Energy, Public Services and Security. Over the last years Security has evolved into a Business Area (BA) which not only has developed vertically but also horizontally, cutting across the rest of the Bas, in this case the introduction of state of the art encryption and privacy mechanisms are of paramount importance.

There are two outcomes of the PRISMACLOUD project that are at this time considered as of exploitation interest:

- The use of anonymous credentials in the current development of the European parking disable badge. ETRA is currently delivering an ICT solution for the European disable parking badge, which among other issues will prevent fraud or malicious use, and it is expected to deliver a high degree of security, the addition of techniques such as anonymous credentials open up a way to deliver a solution with privacy at its core.

- And the PRISMACLOUD data security for database applications, especially all techniques delivering solutions using Format / Order Preserving Mechanisms (FPE or OPE). These solution can be applied to a range of products using cloud present in our current portfolio, and it is expected that they will be tested in a demonstrator within the project in the area of transportation (Image processing and storing in CCTV systems).

As the project has just started, it is expected that in future reports we will identify the best way to exploit these results in an efficient way.

7.3.2. Interoute

Interoute as Cloud provider and Network Operator confirm the interest in the project main purposes and its potential outcomes. As industrial partner, Interoute is interested in project areas which might evolve in technological enablers for an enhanced security framework. Such outcomes can be exploited in the following main directions:

- As a set of tools to be deployed over owned Corporate Data Network to enhance secure access to employees/third party partners
- As a set of tools to be deployed over owned Corporate Data network to provide a new security framework for distributed secure backups and data at rest
- As an additional infrastructure layer to provide enhanced security framework for Interoute VDC (Virtual Data Center) products
- As an additional software layer to be deployed on top of VDC and to be offered to Interoute customers, i.e. a new service like EnhancedSecurityAsAService which can boost hybrid cloud deployment for Interoute premium customers

Given the current status of the project, it is not possible to quantify the impact that the potential PRISMACLOUD solutions can have on Interoute infrastructure.

7.3.3. ATOS

It is becoming more common to require security deals to include outsourcing of IT infrastructures into secure clouds, for instance using Atos' cloud offerings **Canopy and Yunano:**

- **Canopy** is a new force in enterprise cloud powered by Atos, EMC2 and VMware, combining Atos' depth of sector-specific knowledge and business transformation; EMC2's leadership position in security and storage; and VMware's accepted dominance in virtualization. (http://atos.net/en-us/home/we-are/joint-ventures/canopy.html)

- **Yunano** (transliteration "cloud & safe") offers a new cloud experience in a safe SaaS environment. (http://atos.net/en-us/home/we-are/joint-ventures/yunano.html).

The results that PRISMACLOUD will produce will be used as well to enhance the Atos Sphere Cloud service offering (http://atos.net/en-us/home/we-do/cloud.html) towards first-class privacy protection and enhanced trust solutions for cloud.

In conjunction with the Atos High Performance Security offering, Atos intends to use PRISMACLOUD to provide our customers with reliable cloud solutions for the management of their IT control systems. In this respect, Atos will seek synergies by ensuring close collaboration and coordination with important initiatives where Atos is participating like Helix Nebula (a federated and secure high-performance computing cloud platform to be used by large research centres like CERN, EMBL and ESA).

In addition, Atos could be interested in the exploitation of the **Privacy and Security Assessments (PIAs) consulting services** following the concepts defined by **Privacy by Design**. At this moment the best methodology available that complies with this philosophy is the methodology proposed by the PRIPARE Project (http://pripareproject.eu/). Nevertheless the application of this methodology is in its very early stages so Atos could be interested in using the know-how acquired in the implementation of this methodology in PRISMACLOUD for use in future projects and products.

There is also interest from **Atos Health area** in the integration of different cryptographic tools, for data and computer integrity and security verification as those foreseen as PRISMACLOUD assets.

It could enhance the following services, that could be included in the Atos Health portfolio:

- Certification of electronic data, and integrity of electronic medical records.
- Encrypted storage of medical records in **private cloud**.
- mHealth: secure data interchange and storage using mobile devices as smartphones (for example to encrypt personal information).
- Verification of diagnosis or treatments recommended through medical apps
- As PRISMACLOUD project advance and specify more detailed outcomes, Atos will define concrete applications in Health field.

As PRISMACLOUD project advance and specify more detailed outcomes, Atos will define concrete applications in Health field.

In conclusion, Atos is recognizing the potential reach of the service orientation, and the necessity to implement a woven-in application level security together with defence-in- depth and layered security strategy. In other words, the strategy must include appropriately addressed and agile implementation and balancing of Privacy by Design approach, security controls in infrastructure and applications, as well as development and run-time security processes and procedures that span over people, process, and technology. Only a comprehensive and consistent approach ensures that all risks in critical infrastructures managed by ICT systems are evaluated and can be properly mitigated with proper and secure data protection technology. Atos will use the results of PRSIMACLOUD to enhance its Cloud and Managed Operations services and ISRM offering for critical infrastructure control (i.e. Olympic Games Atos High-Performance Security) and the protection of personal information across Europe and beyond.

7.3.4. IBM

The IBM Lab in Haifa has strong connections with several IBM product groups in the area of security and privacy, specifically the development of IBM Infosphere Guardium, and IBM Infosphere Optim Data Management Solutions as well as with IBM Cloud provider teams (IaaS, PaaS). The Lab serves as an advanced research and development team for these products. The technologies and tools developed in PRISMACLOUD will contribute to differentiating these products in the market and provide IBM's European offices with greater opportunities in the provision of software and services for privacy compliance.

There are two main outcomes of the PRISMACLOUD project which have the most exploitation interest for IBM

- The use of techniques for Format and Order preserving encryption mechanisms – we are currently exploring with different product groups (e.g. Infosphere Guardium) how these solutions can be applied to enhance and differentiate one or more of their products.
- Anonymization of big data – we are investigating several ways to exploit the anonymization solution. Firstly, we will explore within different product groups to identify where such a solution can be utilized. Second we will examine whether the IBM cloud provider teams (e.g. BlueMix) will be interested with an anonymization service.

7.3.5. FCSR

No updates to the plan stated in the DoA have been necessary.

7.3.6. LISPA

No updates to the plan stated in the DoA have been necessary.

7.3.7. MPL

MikroPlan is one of the leading IT Consulting and Outsourcing providers in the Rhein Main region for small enterprise customers.

MikroPlan provides solutions for all business needs for SME customers from workstations and server/storage systems to standard software and individual software Solutions.

Customers of MikroPlan are mainly from financial and insurance business sector. These customers have special requirements regarding security and privacy. By using PRISMACLOUD, MikroPlan will able to provide transparency in the cloud and guarantee the functionality of security. This is a needful base for a trustful relationship with customers from this sector.

MikroPlan is looking into using PRISMACLOUD as a framework for existing cloud solutions, including the following private services:

- Monitoring
- Backup and archiving
- Customer portals (intranet)
- Security management like Virus protection etc.

PRISMACLOUD will also help to secure public services namely eBusiness solutions like webshops and CMS (Content Management Systems). Regarding the different requirements of protecting privacy, integrity and authenticity.

7.3.8. XiTRUST

No updates to the plan stated in the DoA have been necessary.

8. List of Dissemination, Communication and Exploitation Activities Year 1

This section reports the activities carried out in the first year (Period 1) of the PRISMACLOUD project.

8.1. Scientific publications

The following list (roughly ordered by date) contains the scientific peer-reviewed publications, accepted in P1, which PRISMACLOUD used to target especially the research community:

1. Jan Camenisch, Robert R. Enderlein, Stephan Krenn, Ralf Küsters, and Daniel Rausch, "Universal Composition with Responsive Environments", IACR Cryptology ePrint Archive , 2016:034, 2016.

2. Olivier Blazy, David Derler, Daniel Slamanig, and Raphael Spreitzer. "Non-Interactive Proofs for Plaintext (In-)Equality and Group Signatures with Veriable Controllable Linkability". In Topics in Cryptology - CT-RSA 2016, The Cryptographer's Track at the RSA Conference 2016, San Francisco, CA, USA, February 29 - March 4, 2016. Proceedings, 2016.

3. David Derler, Christian Hanser, and Daniel Slamanig. "A New Approach To Efficient Revocable Attribute-Based Anonymous Credentials". In Cryptography and Coding - 15th IMA International Conference, IMACC 2015, Oxford, UK, December 15-17, 2015. Proceedings.

4. Thomas Lorünser, Thomas Länger, and Daniel Slamanig. "Cloud Security and Privacy by Design". In 6th International Conference on E-Democracy, Athens, Greece, 10th - 11th December, 2015. Proceedings.

5. Hannes Groß, Marko Hölbl, Daniel Slamanig, Raphael Spreitzer. "Privacy-Aware Authentication in the Internet of Things". In Cryptology and Network Security, 14th International Conference, CANS 2015, Marrakesh, Morocco, December 8-12. 2015.

6. Sören Bleikertz, Carsten Vogel, Thomas Groß, Sebastian Mödersheim. "Proactive Security Analysis of Changes in Virtualized Infrastructures". 2015 Annual Computer Security Applications Conference, ACSAC 31, Los Angeles, California, USA, December 5-9 December, 2015.

7. Thomas Lorünser, Andreas Happe, and Daniel Slamanig. "ARCHISTAR: Towards Secure and Robust Cloud Based Data Sharing". In IEEE 7th International Conference on Cloud Computing Technology and Science, CloudCom 2015, Vancouver, Canada, November 30 - December 3, 2015.

8. F.W.J. van Geelkerken, H. Pöhls, and S. Fischer-Hübner. “The legal status of malleable- and functional signatures in light of Regulation (EU) No 910/2014”. In Proceedings of the 1st International Conference of Young Scientists LPS-2015, L'viv:L'viv Polytechnic Publishing House, 2015.

9. David Derler, Henrich C. Pöhls, Kai Samelin, Daniel Slamanig. "A General Framework for Redactable Signatures and New Constructions", Information Security and Cryptology - ICISC 2015 - 18th International Conference, Seoul, Korea, November 25-27, 2015.

10. David Derler and Daniel Slamanig. "Rethinking Privacy for Extended Sanitizable Signatures and a Black-Box Construction for Strongly Private Schemes". In Provable Security - 9th International Conference, ProvSec 2015. Kanazawa, Japan, November 24-26, 2015

11. Stephan Krenn, Kai Samelin, and Dieter Sommer. "Stronger Security Definition for Sanitizable Signatures", In Data Privacy Management, DPM 2015, Vienna, Austria, September 21–22, 2015.

12. Jan Camenisch, Stephan Krenn, Anja Lehmann, Gert L. Mikkelsen, Gregory Neven, and Michael Ø. Pedersen. "Formal Treatment of Privacy-Enhancing Credential Systems". In Selected Areas in Cryptography, SAC 2015, Sackville, New Brunswick, Canada, August 12–14, 2015.

13. Christian Hanser, Max Rabkin and Dominique Schröder. "Verifiably Encrypted Signatures: Security Revisited and a New Construction.". In 20th European Symposium on Research in Computer Security, Computer Security, ESORICS 2015, volume 5922 of LNCS, Springer-Verlag, Vienna, Austria, September 21-25, 2015.

14. Henrich C. Pöhls and Kai Samelin. "Accountable Redactable Signatures". In 10th International Conference on Availability, Reliability and Security, ARES 2015, IEEE, Toulouse, France, August 24–28, 2015.

15. Elias Z. Tragos, Henrich C. Pöhls, Ralf C. Staudemeyer, Daniel Slamanig, Adam Kapovits, Santiago Suppan, Alexandros Fragkiadakis, Gianmarco Baldini, Ricardo Neisse, Peter Langendörfer, Zoya Dyka and Christian Wittke. Book chapter „ Securing the Internet of Things – Security and Privacy in a Hyperconnected World” in the IERC cluster book “Building the Hyperconnected Society” edited by O. Vermesan and P. Friess. https://ec.europa.eu/digital-agenda/en/news/building-hyperconnected-society-iot-research-innovation-value-chains-ecosystems-and-markets, River Publishers, June, 2015.

16. Thomas Lorünser, Charles Bastos Rodriguez, Denise Demirel, Simone Fischer-Hübner, Thomas Groß, Thomas Länger, Mathieu des Noes, Henrich C. Pöhls, Boris Rozenberg, and Daniel Slamanig. "Towards a New Paradigm for Privacy and Security in Cloud Services". In New LEIT projects on Security-by-Design - 4th Cyber Security and Privacy EU Forum, CSP Forum 2015, Brussels, Belgium, April 28th - 29th, 2015.

17. Thomas Gross. “Signatures and Efficient Proofs on Committed Graphs and NP-Statements”. In 19th International Conference Financial Crypto 2015, Puerto Rico, January 26-30, 2015.

This gives a total of 17 scientific publications, six of them jointly done by two or more partners.

In addition to the scientific publications in conferences and journals, within PRISMACLOUD the following technical deliverables, which are intended to be released to the public, have been produced.

D2.1 Legal, social and HCI requirements

D2.2 Domain independent generic security models

D4.4 Overview of functional and malleable signature schemes

D4.9 Analysis of the State of the Art of FPE, OPE and Tokenization schemes

D5.8 Overview of verifiable computing techniques providing private and public verification

The above deliverables have been or will get published on the PRISMACLOUD webpage in the section Deliverables: https://prismacloud.eu/index.php/deliverables/. In order to widely disseminate them they are also published on some of the academic partner’s webpages as TechReports.

8.2. Dissemination, exploitation and communication activities

The following list contains the activities of PRISMACLOUD partners in year 1.

No	Category	Main Leader	Title	Date	Place	Audience/ Target Group	Size of Audience	Countries Addressed
1	Website	AIT	PRISMACLOUD website	23.02.2015	https://prismacloud.eu/	All[2]		International
2	Social media	AIT	PRISMACLOUD Twitter account PRISMACLOUD Project	17.02.2015	https://twitter.com/prismacloud	All		International
3	Social media	AIT	PRISMACLOUD LinkedIn account PRISMACLOUD Project	17.02.2015	https://at.linkedin.com/in/prismacloud	All		International
4	Social media	AIT	PRISMACLOUD LinkedIn Group EU H2020 - PRISMACLOUD (Privacy and Security Maintaining Services in the Cloud)	17.02.2015	https://www.linkedin.com/groups/6931773	All		International
5	Flyers	AIT	PRISMACLOUD Poster	24.04.2015	https://prismacloud.eu/wp-content/uploads/2015/10/Poster-A0_v2_small.pdf	All		International

[2] “All” here means this applies to the scientific community, industry, civil society, general public, policy makers, medias, investors, customers, and other

6	Flyers	AIT	PRISMACLOUD Folder / Flyer	24.04.2015	https://prismacloud.eu/wp-content/uploads/2015/10/Folder-A4_04.pdf	All		International
7	Press releases	AIT	Press Release-Project Start	27.05.2015	https://prismacloud.eu/index.php/2015/06/03/project-start/	All		
8	Participation in activities organised jointly with other H2020 project(s)	AIT, TU Graz, UNI PASSAU	ICT 2015 Innovate, Connect, Transform. Networking session on “Key challenges in end-to-end privacy/security in untrusted environments” together with H2020 projects WITDOM and TREDISEC;	20-22.10.2015	Lisbon, Portugal	All	5000	Europe

9	Participation in activities organised jointly with other H2020 project(s)	AIT	DPSP Cluster Collaboration	07.09.2015		All		Europe
10	Exhibitions	AIT	Cyber Security and Privacy (CSP) Innovation Forum 2015	28-29.04. 2015	Brussel, Belgium	All		Europe
11	Participation to a conference	UNIL	e-Democracy 2015: 6th International Conference on e-Democracy - Citizen Rights in the World of the New Computing Paradigms	10-11.12.2015	Athens, Greece	All		International
12	Participation to a conference	AIT	CloudCom 2015: 7th IEEE International Conference on Cloud Computing Technology and Science	30.11-3.12.2015	Vancouver, Canada	All		International
13	Participation to a conference	TU Graz	ICISC 2015: 18th Annual International Conference on Information Security and Cryptology	25-27.11.2015	Seoul, Korea	Research Community		International
14	Participation to a conference	TU Graz	ProvSec 2015: 9th International Conference on Provable Security	24-26.11.2015	Kanazawa, Japan	Research Community		International
15	Participation to a conference	AIT, TU Graz	ESORICS 2015: 20th European Symposium on Research in Computer Security	21-25.09.2015	Vienna, Austria	Research Community	150	Europe

16	Participation to a conference	UNI PASSAU	ARES 2015: 11th International Conference on Availability, Reliability and Security	24-28.08.2015	Toulouse, France	Research Community		International
17	Participation to a conference	TU Graz	CECC 2015: 15th Central European Conference in Cryptography	8-10.06.2015	Klagenfurt, Austria	Research Community		Central Europe
18	Participation to a conference	TU Graz	CANS 2015: 14th International Conference on Cryptology and Network Security	10-12.12.2015	Marrakesh, Marocco	Research Community		International
19	Participation to a workshop	TU Graz, AIT, KAU, UNEW	IFIP Summer School 2015: Privacy and Identity Management-Time for revolution?	16-21.08.2015	Edinburg, Scotland	Research Community; Students		International
20	Participation to an event other than a conference or workshop	AIT	Sourcing & Vendor Relationship Management	17.10.2015	Vienna, Austria	Industry		Austria
21	Participation to an event other than a conference or workshop	AIT	Bits That Byte	29.10.2015	Burgenland, Austria	Research Community; Students; Industry		Austria
22	Participation to an event other than a conference or workshop	AIT	The Future of Cloud	17.06.2015	Vienna, Austria	Industry		Europe

23	Participation to an event other than a conference or workshop	AIT	M2M Forum CEE	09.06.2015	Vienna, Austria	Industry		Austria
24	Participation to an event other than a conference or workshop	UNIL	WSIS Forum 2015: World Summit on the Information Society Forum 2015	25-29.05.2015	Geneva, Switzerland	Industry; Policy makers; Intl. Organisations; Research Community		International
25	Publication	TUDA	Cryptology ePrint Archive: Homomorphic Signature Schemes - A survey	26.06.2015	https://eprint.iacr.org/2015/653	Research Community		International
26	Website	ETRA	PRISMACLOUD in ETRA Corporate Web page		http://www.etra.es/en/grupo-etra/idi-projects/prismacloud-%E2%80%93-privacy-and-security-maintaining-services-in-the-cloud.aspx	All		International

27	Participation to an event other than a conference or workshop	ETRA	CAMINO panel session at Mobile World Congress http://www.fp7-camino.eu/	03.03.2015	Barcelona, Spain	Industry Policy Makers;	Around 80 participants	International
28	Participation to an event other than a conference or workshop	ETRA	CYSM Project Final Conference / "Security challenges for Critical Information Infrastructures in the logistic chain" http://www.cysm.eu/index.php/es/related-events/17-cysm-project-final-conference/event_details	31.03.2015	Valencia, Spain	Industry; Policy Makers	Around 40 participants	International
29	Participation to a conference	AIT	FICloud Conference	24-26.08. 2015	Rome, Italy	Research Community		International
30	Participation to a conference	KAU, UNI PASSAU	1st International Conference of Young Scientists LPS-2015 http://www.ukrscience.org/lps	26.11.2015	L'viv, Ukraine	Research Community (with legal focus)	Around 120	International
31	Publication	AIT, TU Graz	ERCIM News Magazine Number 104 January 2016	January 2016	https://prismacloud.eu/wp-content/uploads/2016/01/ERCIM-104-January-2016.pdf	Research Community		

32	Participation to an event other than a conference or workshop	ATOS	Presentation of PRISMACLOUD project to Canopy, company owned by Atos, that is providing a wide range of cloud solutions and services.	18.11.2015	Barcelona, Spain	Industry		
33	Social media	AIT	SlideShare PRISMACLOUD Project	18.06.2015	http://slideshare.net/PRISMACLOUDProject	Scientific community, industry, general public		
34	Presentation to Industry	AIT	The future of cloud security, IKARUS Security Software	23.11.2015	Vienna, Austria	Industry		Austria
35	Presentation to Industry	AIT	Securing data at rest with Archistar, Ericsson	14.12.2015	Vienna, Austria	Industry		Austria
36	Presentation to Industry	AIT	Secure cloud storage and identity management, Huemer IT	04.12.2015	Vienna, Austria	Industry		Austria
37	Presentation to a research organisation	AIT	Impact in H2020 projects, FFG Austrian Research Promotion Agency		Vienna, Austria	Scientific community		Austria
38	Newsletter	AIT	Mention of PRISMACLOUD project in FP7 SECCRIT Newsletter 6 – November 2015	November 2015	https://www.seccrit.eu/upload/upload/SECCRIT-Newsletter-NOVEMBER-2015.pdf	Research community, general public		International
39	Newsletter	AIT	Mention of PRISMACLOUD project in CSP Forum Newsletter 5 – July 2015	July 2015	https://www.cspforum.eu/CSPNewsletter/files/CSPForum_Newsletter_July_Edition_No5.html	Research community, general public		International

40	Participation to a conference	UNEW	Mention of PRISMACLOUD project in Financial Cryptography 2015	January 2015	Santa Cruz, Puerto Rico	Research community	150	International
41	Presentation to Government	UNEW	Presentation to UK Cyber Security Technical Authority	May 2015	UK	Cyber security community	40-50	UK
42	Meeting with Industry	UNEW	Meeting on cloud security assurance with IBM Research - Zurich	June 2015	Switzerland	Research community, cloud provider		International
43	Presentation to Academia	UNEW	Mention of PRISMACLOUD project in invited talk at University of Edinburgh	October 2014	UK	Research community	40	UK

Table 2: List of dissemination, exploitation and communication activities in 1st year

8.3. Lectures within PRISMACLOUD

As an exploitation of results for the academic partners the plan was to use PRISMACLOUD results, findings and examples in academic lectures and other courses. The following list shows the activities in P1 targeting the group of (PhD/M.Sc./B.Sc./other) Students.

No	Name	Organisation	Title	University	Date
1	Daniel Slamanig, Christian Hanser	TU-Graz	Security and Privacy in the Cloud	TU Graz, Master course	Summer Term 2015
2	Daniel Slamanig, Christian Hanser, David Derler	TU-Graz	Modern Public Key Cryptography	TU Graz, Master course	Summer Term 2015
3	Denise Demirel, Lucas Schabhüser, Giulia Traverso	TUDA	Long-term Security	TU Darmstadt, Seminar	Summer Term 2015
4	Denise Demirel, Lucas Schabhüser, Giulia Traverso	TUDA	Long-term Security	TU Darmstadt, Lab	Winter Term 2015/2016
5	Denise Demirel, Lucas Schabhüser	TUDA	Post-Quantum Kryptographie II - Fully Homomorphic Encryption	TU Darmstadt, Master course	Winter Term 2015/2016

Table 3: List of exploitation activity in the form of academic lectures in 1st year

8.4. PhD, Master and Bachelor thesis within PRISMACLOUD

No	Name	Title	Type	Supervisor	Organization	Status
1	Jakob Stangl	Hardware acceleration and trust anchors for distributed storage systems	Master Thesis	Thomas Lorünser	AIT	Running
2	Ersi Hodo	Efficient auditing of distributed cloud storage networks	Master Thesis	Thomas Lorünser	AIT	Running
3	Marku Enio	Privacy preserving of cloud based data sharing	Master Thesis	Thomas Lorünser	AIT	Running
4	Stefan Bäuchl	Symmetric Searchable Encryption	Master Thesis	Daniel Slamanig	TU Graz	Running
5	Michael Stradner	Anonymous Authentication for Android Devices	Master Project	Christian Hanser	TU Graz	Running
6	Sebastian Ramacher	Bilinear Pairings on Elliptic Curves	Master Thesis	Christian Hanser	TU Graz	Completed (11/2015)
7	Christian Hanser	Signatures on Equivalence Classes: A New Tool for Privacy-Enhancing Cryptography	PhD Thesis	Christian Rechberger	TU Graz	Running
8	David Derler	Protocols for Privacy and Authenticity in Future Computing Scenarios	PhD Thesis	Christian Rechberger	TU Graz	Running
9	Sebastian Ramacher	TBD	PhD Thesis	Christian Rechberger	TU Graz	Running
10	Nabil Alkeilani Alkadri	Post-Quantum Commitment Schemes	Master Thesis	Denise Demirel	TUDA	Completed (05/2015)
11	Jacqueline Brendel	Efficient Proactive Secret Sharing (working title)	Master Thesis	Denise Demirel	TUDA	Running
12	Christian Weinert	Building a Modular Long-term Archiving System	Master Thesis	Denise Demirel	TUDA	Running

13	Thomas Klir	Archiving scheme providing long-term integrity and unconditional confidentiality (working title)	Master Thesis	Denise Demirel	TUDA	Running
14	Martín Augusto Gagliotti Vigil	Trustworthy and Efficient Protection Schemes for Digital Archiving	PhD Thesis	Johannes Buchmann	TUDA	Completed (07/2015)
15	Lucas Schabhüser	Verifiable Computing (working title)	PhD Thesis	Johannes Buchmann	TUDA	Running
16	Giulia Traverso	Long-term security (working title)	PhD Thesis	Johannes Buchmann	TUDA	Running
17	Henrich C. Pöhls	Increasing the Legal Evidentiary Value of Private Malleable Signatures	PhD-Thesis	Joachim Posegga	UNI PASSAU	Running
18	Katrin Riemer	Digital signature service in the cloud	Master Thesis	Helmut Aschbacher, Stefan Vorbach	XT, TU Graz	Running
19	Jack Arnstein	Implementation of cryptographic library for graph signatures	Master Thesis	Thomas Gross	UNEW	Completed
20	Soeren Bleikertz	Automated Security Analysis of Virtualized Infrastructures	PhD Thesis	Thomas Gross	UNEW	Running
21	Ioannis Sfyriakis	Secure and Dependable Virtual Components for Cloud Infrastructures	PhD Thesis	Thomas Gross	UNEW	Running
22	Michael Edwards	Zero-knowledge reachability in graphs	Bachelor Thesis	Thomas Gross	UNEW	Running
23	Shing F.J. Law	Causality in Cloud Events	Bachelor Thesis	Thomas Gross	UNEW	Running
24	Luke Whiteley	Privacy-preserving digital geo-cache system	Bachelor Thesis	Thomas Gross	UNEW	Running

Table 4: List of exploitation activity in the form of academic training

8.5. Videos and Newsletters

PRISMACLOUD has started the preparation of videos that shall explain key technologies and concepts of PRISMACLOUD to a wider audience, e.g. the general public, in a still scientifically correct way. PRISMACLOUD has started with the preparation of two videos describing verifiability of data and secure data at rest. However, currently they are still in preparation face. The plan is to disseminate this via the website, social media, and other channels – like in presentations on events – to all relevant communities to ensure maximum impact of the PRISMACLOUD concepts.

PRISMACLOUD sent out its first Newsletter at the end of January 2016. PRISMACLOUD as a project was already mentioned twice in other newsletters, namely in the August 2015 and November 2015 newsletter of the FP7 European project SECCRIT.

PRISMACLOUD

PRIvacy and Security MAIntaining Services in the CLOUD

NEWSLETTER January 2016

This is the first PRISMACLOUD newsletter from a series that will keep you updated about our research activities, project results and events. It is being sent out to members of the "User and Advisory Board" (UAB) directly as well as interested people who registered for it on our homepage where it is also available for download. This first issue contains a short overview of the project, a summary of first achievements as well as highlights from our participation in events and networking activities with other projects.

Call: H2020-ICT-2014-1
Topic: ICT-32-2014
Type of Action: RIA
Partners: 16
Duration: 42 months
Start Date: 01.02.2015
Estimated Project Cost: ~8.5 M
Requested EU Contribution: ~8.0 M
Grant Agreement No: 644962
Coordinator: AIT Austrian Institute of Technology GmbH

The Project

The EU Horizon 2020 PRISMACLOUD research project is dedicated to enabling secure and trustworthy cloud-based services by improving and adopting novel tools from cryptographic research.

The need to protect the security and privacy of the data in the cloud is a critical issue for society and the strongest level of protection can be achieved through cryptography, although technologically extremely challenging. PRISMACLOUD is contributing to this area by developing tools that allow the next generation of cryptographically secured cloud services to be built with security and privacy incorporated by design and from end to end.

A very short overview of the project goals is given in recent ECRCIM News 104 and a more in depth article was published in Cyber Security and Privacy, which can also be found in Arxiv.

Figure 10: PRISMACLOUD Newsletter - January 2016

8.6. User Advisory Board

A User Advisory Board consisting of several experts that are interested in the research results of the projects is established. Detailed information about the UAB can be found on PRISMACLOUD D9.8 User Advisory Board Communication Summary 1.

8.7. Liaison with Other Projects

PRISMACLOUD has established liaison activities with other research projects conducting research in a similar area, which are listed below:

SECCRIT: The SECCRIT project (SEcure Cloud computing for CRitical infrastructure IT) is a multidisciplinary research project with the mission to analyse and evaluate cloud computing technologies with respect to security risks in sensitive environments.

TREDISEC: The project TREDISEC (Trust-aware, REliable and Distributed Information SEcurity in the Cloud) leverages cryptographic protocols and security mechanisms, which offer strong data confidentiality, integrity and availability.

WITDOM: WITDOM (empoWering prIvacy and securiTy in non-trusteD envirOnMents) is a project to produce a framework for end-to-end (E2E) protection of data in untrusted and fast evolving ICT-based environments.

CREDENTIAL: CREDENTIAL project (Secure Cloud Identity Wallet) is a EU funded research project developing, testing and showcasing innovative cloud-based services for storing, managing, and sharing digital identity information and other highly critical personal data with a demonstrably higher level of security than other current solutions.

ECRIME: ECRIME (the economic impacts of cyber crime) aims to reconstruct the spread and development of cyber crime in non-information and communications technology (non-ICT) sectors.

ECRYPT-CSA: ECRYPT-SA is trying to strengthen European excellence in the area of cryptology and to build on the Network of Excellence ECRYPT and ECRYPT II.

Additionally, PRISMACLOUD is also part of the DPSP Cluster dedicated to Data Protection, Security and Privacy (DPSP) in the Cloud. This cluster is part of the Clusters of European Projects on Cloud supportive action seeking synergies between cloud related EU funded research projects and to join efforts towards greater impact. The cluster seeks synergies among projects focused on diverse solutions for ensuring data protection, security and privacy in the cloud. In the first period, PRISMACLOUD was involved in the following cluster activities:

1) Whitepaper focused on Initiative #14 of DSM: Initiatives on data ownership, free flow of data (e.g. between cloud providers) and on a European Cloud.
2) Map of synergies and challenges

8.8. Joint Events with Other Projects

ICT 2015 Innovate, Connect, Transform, 22 October 2015, Lisbon, Portugal

PRISMACLOUD has participated in a session at the ICT 2015 event in Lisbon on “Key challenges in end-to-end privacy/security in untrusted environments”. The session was organized together with H2020 projects WITDOM and TREDISEC. The networking session included presentations from PRISMACLOUD (represented by UNI PASSAU), Ghassan Karame (from TREDISEC) and Nicolas McDonnel (from WITDOM) and was moderated by Silvana Muscella (from WISER). From the presentations and the following panel discussion it became clear that the cryptographic tools are ripe to be used and applied. WITDOM made clear that we need to measure the need for privacy to select and adequate crypto. Also TREDISEC's presentation highlighted various cryptographic techniques, like secure multi party computation, and pointed out that these shall be applied to remove the need to trust the cloud. The panel and the audience, which actively participated, gained the consensus that privacy and security must be considered to increase the trust in cloud services. Of course this requires that standardisation and legal frameworks would harmonize the domain of cloud computing’s requirements towards security and privacy across the EU. A further remark was that the EU shall foster the development of trustworthy hardware components, as even with soundly implemented cryptographic primitives in place there is always a component that you need to trust, e.g. to generate or store your keys securely. PRISMACLOUD was very happy about the enlightening discussions and plans to collaborate and exchange ideas and solutions with TREDISEC and WITDOM in the future.

The Future of Cloud, 17 June 2015, Vienna, Austria

PRISMACLOUD together with CREDENTIAL H2020, SECCRIT FP7 and Trust in Cloud organized the Future of Cloud event and brought together researchers from the cloud industry and the scientific community, market researchers and HR specialists as well as startups. This event took a look at the next three years of cloud development from different perspectives, bringing the latest findings and information from the research labs to Vienna. The objectives of the event were:

- Getting a clearer picture of how the cloud will develop over the next few years: Cloud 2.0
- Taking a look at the future from different perspectives to be able to form one’s own opinion and make one’s own decisions.
- Presenting complex research topics in an innovative and exciting manner in an overall context

8.9. Standardisation Activities

An important planned impact of the PRISMACLOUD project is to guide standardisation in the right direction following PRISMACLOUD results. In order to use standardisation as a vehicle to ensure long-term sustainability and the widest possible dissemination of PRISMACLOUD’s results the right strategy is required. Therefore, PRISMACLOUD has planned standardisation activities as a separate task with an individual set of deliverables and the results of the work done there is not listed here. Please find the details on the project’s strategy for the dissemination of project results by standardisation and the proposals for targets in the Deliverable D9.5 Initial assessment of current cloud standardization efforts, that is also submitted at the end of period 1 (1st year).

9. Conclusion and Future Activities

The intention of this document was to present the communication, dissemination and exploitation strategy of the PRISMACLOUD project as well as to report all the communication, dissemination and exploitation activities have been accomplished during the first year of the project. At the closing of the first year partners have showed a good understanding on how to disseminate and exploit project's results. At the time being more dissemination and exploitation activities are examined.

During project's lifetime revisions to the strategy and possible updates will be done, which will be reported in the following deliverables, alongside with the progress made in the future:

- D9.3: Dissemination and Exploitation Report 2
- D9.4: Dissemination and Exploitation Report 3

Moreover, communication strategy and actions to the User Advisory Board will be reported through:

- D9.8: User Advisory Board communication Summary 1
- D9.9: User Advisory Board Communication Summary 2

PRISMACLOUD also produced a first newsletter containing summaries of the project's achievements. This will become a series of newsletters. Printed versions of the latest newsletter is planned to be distributed by any of the consortium members participating at European or national events dealing with related subjects. It will also be distributed electronically to the members of the User and Advisory board members and also to other relevant bodies.

Additionally, future standardisation actions are currently being assessed and the plans in that respect and the progress made in the remaining lifetime of the project will be reported in the deliverables:

- D9.5: Initial assessment of current cloud standardisation efforts
- D9.6: Standards Activity Report 1
- D9.7: Standards Activity Report 2

Finally, a large number of publications in conferences and scientific magazines are expected to be generated during the next reporting period, as well as participation in workshops and European Commission's events, and further cooperation with other EC projects.