D4.1.3

Final Dissemination, Training, Standardisation and Exploitation Report

Project number:	257243
Project acronym:	TClouds
Project title:	Trustworthy Clouds - Privacy and Resilience for Internet-scale Critical Infrastructure
Start date of the project:	1st October, 2010
Duration:	36 months
Programme:	FP7 IP

Deliverable type:	Report
Deliverable reference number:	ICT-257243 / D4.1.3 / 1.0
Activity and Work package contributing to the deliverable:	Activity 4 / WP 4.1
Due date:	30th September 2013 – M36
Actual submission date:	1st October 2013

Responsible organisation:	TUDA
Editor:	Mihai Bucicoiu
Dissemination level:	Public
Revision:	1.0

Abstract:	This deliverable reports on the final state of the dissemination, standardisation, exploitation and project internal/external education and training activities, including project year 3.
Keywords:	Dissemination, Training, Standardisation, Exploitation

Editor

Mihai Bucicoiu (TUDA)

Contributors

Imad Abbadi (OXFD)

Elmar Husmann, Christian Cachin (IBM)

Norbert Schirmer (SRX)

Martina Truskaller, Patricia Rio Branco (TEC)

with contributions from TClouds partners

Disclaimer

The information in this document is provided as is, and no warranty is given or implied that the information is fit for any particular purpose.

The user thereof uses the information at its sole risk and liability. The opinions expressed in this deliverable are those of the authors. They do not necessarily represent the views of all TClouds partners.

Executive Summary

This deliverable reports on the outcomes of the project partners regarding the implementation of dissemination activities, standardisation and exploitation efforts within the TClouds project. Moreover, project's internal/external training and teaching activities during the third year of the project are presented.

Notably, this deliverable addresses the exploitation and standardisation efforts of the partners in the last year of the project.

- An update of the exploitation efforts and the responses of each partner are presented in order to help identifying new opportunities.

- Standardisation opportunities identified in year one have been assessed by the project partners and potential contributions to those standards been identified.

The following falls under the achievements and work towards the project goals of the last project year for dissemination:

- With at least 32 peer-reviewed scientific publications, including publication at renowned international conferences and workshops such as ACM CCS and NDSS, the project partners continued a successful scientific dissemination in the last year.

- In the last year of the project, an update of the flyer (TClouds Leaflet) and a new poster were also used to disseminate project activities.

- An introductory video presenting the main features of the TPaaS Healthcare Platform was posted on YouTube and disseminated in meetings.

- A series of 15 factsheets containing high-level descriptions of technology components, prototypes, and use cases developed within the TClouds project were prepared and posted on the TClouds website.

- Project partners were involved in and responsible for the organisation of some academic and industrial flagship events including ESORICS Trustworthy Clouds Workshop and IFIP Summer School on Privacy and Identity Management for Emerging Services and Technologies.

- Several project partners represented the TClouds project at nearly 70 different occasions at academic and industrial events during Y3.

Contents

List of Figures

List of Tables

Chapter 1   Introduction

1.1 TClouds - Trustworthy Clouds

Cloud-computing technologies are one of the most fast growing technologies that empower the fast evolvement of business ranging from public lightning to health care. Existing cloud computing services provide computing, network and storage resources for a low cost. One major challenge for the providers of such services is to offer a trusted infrastructure for critical services that require security and privacy. In the TClouds project partners deal with this challenge and provide different solution, integrated to work as one, in order to create a trustworthy Internet-scale cloud service that will allow more grown of cloud computing technologies. In the two scenarios purpose in TClouds, power grids and electricity management and patient-centric health-care, the purposed solutions are evaluated in terms of security offerings.

Moreover, TClouds project also deals with legal implications and business opportunities of using such a trusted infrastructure. The project, focusing on security, privacy and resilience aspects of cloud computing, contributes to building a framework that enables such characteristics on commodity clouds.

The main contribution of TClouds is defining an architecture and prototypes for secure clouds. One of the prototypes is built on top of OpenStack, the main open-source infrastructure for administrating cloud environments. Furthermore, the cloud-of-clouds proposed-solution builds on the existing infrastructures to enhance their services by providing security, privacy and resilient middleware for adaptive security. This solution is not dependent on any single cloud provider. This feature of the TClouds platform will provide tolerance and adaptability to mitigate security incidents and unstable operating conditions for a range of applications running on a cloud-of-clouds.

To sum up, the project results show promising security, privacy and resilience enhancement that can be adopted (some are already products) to improve different business that could benefit from such features.

1.2 Activity 4 – Programme Management and Dissemination

The goal of Activity 4 is to develop and implement plans for dissemination and standardisation activities as well as to implement operational management and secure technical vitality of the TClouds project. The project itself aims at influencing the development of relevant standards in the areas of cloud infrastructure, trustworthy infrastructure, middleware, as well as existing and novel (Cloud-) applications.

Activity 4 is structured into two main work packages that focus on different aspects of standardisation, dissemination, and management activities relevant in the context of TClouds.

1.3 Work package 4.1 - Standardisation and Dissemination

WP4.1's first objective is to foster the close cooperation with relevant standardisation bodies, in order to provide input to and influence (new) standards. In particular, the TClouds project aims to influence or/and initiate the development of relevant standards in the areas of Cloud infrastructure and trustworthy infrastructure (e.g., platforms, protocols, and interfaces), resilient middleware (e.g., resilient protocols and systems), and existing as well as novel (Cloud-) applications (e.g., related to eHealth, power grid, smart metering).

Moreover, the aim is to develop and implement exploitation plans on consortium and partner level, as well as to develop strategies to create revenue of the project results and maximise the benefit for the project participants. In particular, TClouds aims to establish a European approach to trustworthy and privacy-preserving cloud computing and foster a strong European research community in the area of resilient, privacy-preserving cloud computing as a leading group within international research in this area.

WP4.1's second objective is wide dissemination to drive thought leadership in industry and academia. The dissemination of the main project results and raising public awareness through various dissemination channels like conferences and trade shows, articles in technical and academic publications or technical workshops is one of our major goals. Furthermore, the knowledge transfer to users and achieving broad acceptance for the new technologies is a focus our project, as well as the development of training concepts and material to ensure knowledge and innovation transfers.

1.4 Deliverable 4.1.3 - Final dissemination, training, standardisation and exploitation

Overview. This deliverable reports on the final status of the project partners in terms of implementing the strategy for dissemination of the project, the standardisation and exploitation efforts of project results, and project internal/external training and teaching during the third year of the TClouds project. In particular, this deliverable reports on the progress of the standardisation and updates exploitation efforts.

Structure. The remainder of this deliverable is organised as follows. Chapter 2 presents the dissemination activities of year 2. Chapter 3 summarizes the assessment results for the potential contributions of the TClouds project to various standards. In Chapter 4 the results of a project internal questionnaire regarding exploitation at partner level and the consequence for exploitation at consortium level are presented. Chapter 5 lists the ongoing efforts for education and training.

Deviation from Workplan. This deliverable conforms to the DoW/Annex I, Version 4.

Target Audience. The present deliverable aims at providing an overview of the dissemination, standardisation, and exploitation efforts of the TClouds project to all interested parties. The deliverables of WP4.1, including the present deliverable D4.1.3, relate to most other deliverables and work packages by receiving the achieved results (deliverables, presentations, and scientific publications) as input. This deliverable summarizes the dissemination activities leveraging the achieved results, elaborates on the progress of devising exploitation plans at partner and consortium level from these results as well as assessing the potential contribution of these results to standards. Moreover, the progress on transferring the acquired knowledge and technology to training and education is presented.

Chapter 2

Dissemination

Chapter Authors:

Mihai Bucicoiu (TUDA), Martina Truskaller and Patricia Rio Branco (TEC)

2.1 Introduction

Dissemination activities are provided to ensure the visibility and awareness of the project and to support the widest adoption of its results in industry and research. The strategy for the dissemination of TClouds has aimed at creating this awareness, raising the public interest in the project, and promoting project results to potentially interested parties.

2.2 Dissemination Strategy

No update to the dissemination strategy was deemed necessary due to the successful dissemination in periods 1 and 2, and recent dissemination activities in period 3.

2.3 Dissemination Activities

We present below the dissemination activities executed in period 3 of TClouds.

2.3.1 Organized conferences and events

The following conferences/workshops and events have been (co-)organized by project partners. Additional information related to the type and goal of each event as well as the nature of audiences is provided.

Type of activities	Main leader	Title	Date	Place	Size of audience	Type and goal of the event	Countries addressed
Workshop	ULD, TEC	CPDP (Computers, Privacy & Data Protection) 2013 "Reloading Data Protection"	23-25.01.2013	Brussels, Belgium,	150	CPDP 2013, Moderator of Panel "10.30 Cloud, Trust and Privacy: Towards The InterCloud" at CPDP (Computers, Privacy & Data Protection) 2013 "Reloading Data Protection", http://www.cpdpconferences.org/friday25january2013.html#top	International
Workshop	ULD	Meeting with research project CloudCycle	24.04.2013	Kiel, Germany	10	Cloud project cooperation meeting	National
Conference	ULD	8th International IFIP Summer School on Privacy and Identity Management for Emerging Services and Technologies http://pilab.nl/ifip-summerschool-2013/program.html	16.-21.06.2013	Nijmegen, Netherlands	70	Chairing of the event, introducing TClouds Results	International
Conference	ULD	ULD Summer School ("Sommerakademie") "Big Data - Informationelle Fremd- oder Selbstbestimmung?!"	26.08.2013	Kiel, Germany	400	Chairing of the event, Relation Cloud Computing and Big Data	National
Workshop	IBM, TUBS	Workshop on Trustworthy Clouds (co-located with ESORICS 2013)	12.-13.09.2013	Royal Holloway, University of London (UK)	30	The workshop aims at bringing together researchers and practitioners working in cryptography, security, and distributed systems, from academia and industry, who are interested in the security and resilience of cloud computing.	International
Presentation	FFCUL	1st Workshop on Trustworthy Clouds (together with ESORICS'13, supported by TClouds)	13.09.2013	London, UK	40	Presentation "Cloud-of-Clouds Computing for supporting Public Utilities - A Case Study" in a TClouds session attended	International

Type of activities	Main leader	Title	Date	Place	Size of audience	Type and goal of the event	Countries addressed
						also by the TClouds advisory board	
Workshop	TUBS, ULD	Gesellschaft für Informatik "Systemsoftware für Cloud Computing"	25.-26.04.2013	Braun-schweig, Germany	50	Talk by Ninja Marnau on contractual and organisational cloud computing security measures	National

Table 1: List of organized conferences/workshops

2.3.2 List of scientific (peer-reviewed) publications

The following list provides an overview of the scientific publications and articles by partners of the TClouds project, which have been peer-reviewed and accepted. This list comprises publications of Period 3 *only.* For an overview of the overall publication record of the project partners, please refer to the *Publication* section on the project website (https://www.tclouds-project.eu/index.php?option=com_jumi&fileid=3).

Title	Main author	Title of the periodical or the series	Number, date or frequency	Publisher	Place of publication	Year of publication	Relevant pages	Permanent identifiers (if available)	Is/Will open access provided to this publication?
CheapBFT: Resource-efficient Byzantine Fault Tolerance	Kapitza, R.; Behl, J.; Cachin, C.; Distler, T.; Kuhnle, S.; Mohammadi, S. V.; Schröder-Preikschat, W. & Stengel, K.	7th ACM European Conference on Computer Systems (EuroSys '12)	ISBN: 978-1-4503-1223-3	ACM	Bern, Switzerland	2012	295-308	http://dx.doi.org/10.1145/2168836.2168866	yes
Secure Cloud Maintenance - Protecting workloads against insider attacks	Sören Bleikertz and Anil Kurmus and Zoltan A. Nagy and Matthias Schunter	7th ACM Symposium on Information, Computer and Communications Security (ASIACCS'12)	ISBN: 978-1-4503-1648-4	ACM	New York, USA	2012	83-84	http://dx.doi.org/10.1145/2414456.2414505	yes
The TClouds Architecture: Open and Resilient Cloud-of-Clouds Computing.	P. Verissimo, A. Bessani, M. Pasin	2nd International Workshop on Dependability of Clouds, Data Centers and Virtual Computing Environments (DCDV'12)	ISBN: 978-1-4673-2264-5	IEEE	Boston, USA	2012	1-6	http://dx.doi.org/10.1109/DSNW.2012.6264686	yes
From Byzantine Consensus to BFT State Machine Replication: A Latency-optimal transformation.	J. Sousa, A. Bessani	9th European Conference on Dependable Computing (EDCC'12)	ISBN:978-1-4673-0938-7	Conference Publishing Services (CPS)	Sibiu, Romania	2012	37-48	http://dx.doi.org/10.1109/EDCC.2012.32	yes

Title	Main author	Title of the periodical or the series	Number, date or frequency	Publisher	Place of publication	Year of publication	Relevant pages	Permanent identifiers (if available)	Is/Will open access provided to this publication?
Clouds Trust Anchors	I. M. Abbadi	11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom'12)	ISBN: 978-1-4673-2172-3	IEEE	Liverpool, UK	2012	127-136	http://doi.ieeecomputersociety.org/10.1109/TrustCom.2012.107	yes
DQMP: A Decentralized Protocol to Enforce Global Quotas in Cloud Environments	J. Behl, T. Distler, R. Kapitza	14th International Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS '12)	Vol. 7596	Springer-Verlag	Toronto, Canada	2012	217-231	http://dx.doi.org/10.1007/978-3-642-33536-5_21	yes
On Limitations of Using Cloud Storage for Data Replication	C. Cachin, B. Junker, A. Sorniotti	6th Workshop on Recent Advances in Intrusion Tolerance and reSilience (WRAITS 2012), DSN 2012 Workshops	ISBN: 978-1-4673-2264-5	IEEE	Boston, USA	2012	1-6	http://dx.doi.org/10.1109/DSNW.2012.6264683	yes
Robust Data Sharing with Key-Value Stores	C. Cachin, B. Junker, A. Sorniotti	International Conference on Dependable Systems and Networks (DSN'12)	ISBN: 978-1-4673-1624-8	IEEE	Boston, USA	2012	1-12	http://dx.doi.org/10.1109/DSN.2012.6263920	yes

Title	Main author	Title of the periodical or the series	Number, date or frequency	Publisher	Place of publication	Year of publication	Relevant pages	Permanent identifiers (if available)	Is/Will open access provided to this publication?
Privacy and Resilience for Internet-scale Critical Infrastructures	Alysson Bessani and Imad M. Abbadi and Sven Bugiel and Emanuele Cesena and Mina Deng and Michael Grone and Ninja Marnau and Stefan Nürnberger and Marcelo Pasin and Norbert Schirmer	European Research Activities in Cloud Computing	ISBN: 978-1-4438-3507-7	Cambridge Scholars Publishing	N/A	2012	151-175	N/A	yes
A look to the old-world sky: EU-funded dependability cloud computing research	Bessani, A.; Kapitza, R.; Petcu, D.; Romano, P. Gogouvitis, S.V.; Kyriazis, D. and Cascella, R.G.	In ACM SIGOPS Operating Systems Review	Volume 46, Issue 2	ACM	New York, USA	2012	43-56	http://dx.doi.org/10.1145/2331576.2331584	no
Security and Privacy Enhancing Multi-Cloud Architectures	Jens-Matthias Bohli and Nils Gruschka and Meiko Jensen and Luigi Lo Iacono and Ninja Marnau	IEEE Transactions on Dependable and Secure Computing	Volume 99; ISSN: 1545-5971	IEEE Computer Society	IEEE computer Society Digital Library	2013	1	http://doi.ieeecomputersociety.org/10.1109/TDSC.2013.6	no
Policy-based Secure Deletion	Christian Cachin and Kristiyan Haralambiev and Hsu-Chun Hsiao and Alessandro	IBM Research Report	RZ 3843	IBM Research	Zurich, Switzerland	2013	N/A	http://eprint.iacr.org/2013/152	yes

Title	Main author	Title of the periodical or the series	Number, date or frequency	Publisher	Place of publication	Year of publication	Relevant pages	Permanent identifiers (if available)	Is/Will open access provided to this publication?
	Sorniotti								
On Verifying the Consistency of Remote Untrusted Services	Christian Cachin and Olga Ohrimenko	CoRR - ACM Computing Research Repository	Volume: abs/1302.4808; RZ 3841	IBM Research	Zurich, Switzerland	2013	N/A	http://arxiv.org/abs/1302.4808	yes
Client-controlled Cryptography-as-a-Service in the Cloud	Bleikertz, S.; Bugiel, S.; Ideler, H.; Nürnberger, S. and Sadeghi, A-R.	11th International Conference on Applied Cryptography and Network Security (ACNS'13)	ISBN: 978-3-642-38979-5	Springer-Verlag	Berlin, Germany	2013	N/A	http://openfoo.org/research/acns2013.pdf	yes
FITCH: Supporting Adaptive Replicated Services in the Cloud	Vinicius Vielmo Cogo and Andre Nogueira and Joao Sousa and Marcelo Pasin and Hans P. Reiser and Alysson Bessani	Proc. of the 13th IFIP International Conference on Distributed Applications and Interoperable Systems -- DAIS'13	ISBN: 978-3-642-38540-7	Springer-Verlag	Heidelberg, Germany	2013	15-28	http://www.navigators.di.fc.ul.pt/wiki/Publication:Cogo13fitch	yes
On the Efficiency of Durable State Machine Replication	Alysson Bessani and Marcel Santos and João Felix and Nuno Neves and Miguel Correia	Proc. of the USENIX Annual Technical Conference -- USENIX ATC 2013	ISBN 978-1-931971-01-0	USENIX Association	USA	2013	169-180	https://www.usenix.org/conference/atc13/efﬁciency-durable-state-machine-replication	yes
Efficient Byzantine Fault-Tolerance	Giuliana Santos Veronese and Miguel Correia and Alysson Bessani and Lau Cheuk Lung and Paulo Verissimo	IEEE Transactions on Computers	vol. 62 no. 1	IEEE (Institute of Electrical and Electronics Engineers)	USA	January 2013	1-62	http://doi.ieeecomputersociety.org/10.1109/TC.2011.221	yes

Title	Main author	Title of the periodical or the series	Number, date or frequency	Publisher	Place of publication	Year of publication	Relevant pages	Permanent identifiers (if available)	Is/Will open access provided to this publication?
On the Performance of Byzantine Fault-Tolerant MapReduce	Pedro Costa and Marcelo Pasin and Alysson Bessani and Miguel Correia	IEEE Transactions on Dependable and Secure Computing	vol. 10 no.5	IEEE Computer Society	IEEE computer Society Digital Library	2013	N/A	http://doi.ieeecomputersociety.org/10.1109/TDSC.2013.7	yes
DepSky: Dependable and Secure Storage in Cloud-of-Clouds	Alysson Bessani and Miguel Correia and Bruno Quaresma and Fernando Andre and Paulo Sousa	To Appear in ACM Transaction on Storage	N/A	N/A	N/A	2013	N/A	http://www.di.fc.ul.pt/~bessani/publications/tos13-depsky.pdf	yes
Secure Combination of XML Signature Application with Message Aggregation in Multicast Settings	Andreas Becker and Meiko Jensen	Proceedings of the IEEE 20th International Conference on Web Services	ISBN: 978-0-7695-5025-1	IEEE CPS	Washington DC, USA	2013	531-538	N/A	no
Challenges of Privacy Protection in Big Data Analytics	Meiko Jensen	Proceedings of the 2013 IEEE International Congress on Big Data	ISBN 978-0-7685-5006-0	IEEE CPS	USA	2013	242-245	http://doi.ieeecomputersociety.org/10.1109/BigData.Congress.2013.39	no
Privacy-by-Design Cloud Computing Through Decentralization and Real Life Trust.	Cutillo, L. A. and Lioy, A.	In 13th Int. Conf. on Peer-to-Peer Computing, 2013.	N/A	N/A	N/A	2013	N/A	N/A	no
Towards Privacy-by-Design Peer-to-Peer Cloud Computing	Cutillo, L. A. and Lioy, A.	In 10th Int. Conf. on Trust, Privacy and Security in Digital Business, 2013.	ISBN 978-3-642-40342-2	Springer Berlin Heidelberg	Springer Berlin Heidelberg	2013	85-96	http://doi.ieeecomputersociety.org/10.1007/978-3-642-40343-9_8	no

Title	Main author	Title of the periodical or the series	Number, date or frequency	Publisher	Place of publication	Year of publication	Relevant pages	Permanent identifiers (if available)	Is/Will open access provided to this publication?
Attack Surface Metrics and Automated Compile-Time OS Kernel Tailoring	Kurmus, A.; Tartler, R.; Dorneanu, D.; Heinloth, B.; Rothberg, V.; Ruprecht, A.; Schröder-Preikschat, W.; Lohmann, D. and Kapitza, R.	In Proceedings of the 20th Network and Distributed System Security Symposium (NDSS '13)	N/A	N/A	San Diego, CA United States	2013	N/A	http://www.ibr.cs.tu-bs.de/users/kurmus/papers/kurmus-ndss13.pdf	yes
Enhancing Coordination in Cloud Infrastructures with an Extendable Coordination Service	Distler, T.; Fischer, F.; Kapitza, R. and Ling, S.	Proceedings of the 1st Workshop on Secure and Dependable Middleware for Cloud Monitoring and Management (SDMCMM '12)	ISBN: 978-1-4503-1615-6	ACM	Montreal, Quebec, Canada	2012	1-6	http://dx.doi.org/10.1145/2405186.2405187	no
Automatic OS Kernel TCB Reduction by Leveraging Compile-Time Configurability	Tartler, R.; Kurmus, A.; Ruprecht, A.; Heinloth, B.; Rothberg, V.; Dorneanu, D.; Kapitza, R.; Schröder-Preikschat, W. and Lohmann, D.	In Proceedings of the 8th Workshop on Hot Topics in System Dependability (HotDep '12)	N/A	USENIX Association	Hollywood, CA, USA	2012	3	http://www4.cs.fau.de/Publications/2012/tartler_12_hotdep.pdf	yes
The TClouds Platform - Concept, architecture and instantiations	Bessani, A; Cutillo, L. A.; Ramunno, G.; Schirmer, N.; and Smiraglia, P.	to appear in Proceedings of DISCCO '13	ISBN: 978-1-4503-2248-5	ACM (Association for Computing Machinery)	New York, USA	2013	N/A	http://dx.doi.org/10.1145/2506155.2506156	no

Title	Main author	Title of the periodical or the series	Number, date or frequency	Publisher	Place of publication	Year of publication	Relevant pages	Permanent identifiers (if available)	Is/Will open access provided to this publication?
BFT Storage with 2t+1 Data Replicas	Christian Cachin; Dan Dobre; and Marko Vukolic	Proc. International Symposium on Distributed Computing (DISC 2013)	N/A	N/A	N/A	2013	N/A	http://arxiv.org/abs/1305.4868	yes
On the Feasibility of Byzantine Fault-Tolerant MapReduce in Clouds-of-Clouds	Correia, M.; Costa, P.; Pasin, M.; Bessani, A.; Ramos, F.; and Verissimo, P.	Proceedings of the 1st International Workshop on Dependability Issues in Cloud Computing (DISCCO'12, together IEEE SRDS'12)	ISBN 978-1-4673-2397-0	IEEE Computer Society	Irvine, CA, USA	2012	448-453	http://dx.doi.org/10.1109/SRDS.2012.46	no
Policy-based Secure Deletion	Christian Cachin; Kristiyan Haralambiev; Hsu-Chun Hsiao; and Alessandro Sorniotti	Proc. 20th ACM Conference on Computer and Communications Security (CCS)	Research Report IBM RZ 3843	IBM Research	N/A	2013	N/A	http://eprint.iacr.org/2013/152	yes
Hemmnisse für Privacy by Design und Privacy Technologies	Marit Hansen	Geschichte und Theorie des Datenschutzes, Proceedings, to be published	N/A	Fundationes: Geschichte und Theorie des Datenschutzes	Berlin, Germany	2013	N/A	http://www.fundationes.de/datenschutz.html	In the near future

Title	Main author	Title of the periodical or the series	Number, date or frequency	Publisher	Place of publication	Year of publication	Relevant pages	Permanent identifiers (if available)	Is/Will open access provided to this publication?
Data Protection by Default in Identity-Related Applications	Marit Hansen	Proceedings of the IFIP IDMAN 2013, the 3rd IFIP WG 11.6 Working Conference on Policies & Research in Identity Management	ISBN: 978-3-642-37282-7	IFIP International Federation for Information Processing, 1868-4238, Springer	Berlin, Heidelberg	2013	4-17	http://dx.doi.org/10.1007/978-3-642-37282-7_2	no

Table 2: List of scientific peer-reviewed publications

2.3.3 List of non-peer reviewed publications

The following table supplements the list from Section 1.1.1 with publications that were not peer-reviewed but contributed to the dissemination activities of the project in Y3.

Title	Main author	Title of the periodical or the series	Number, date or frequency	Publisher	Place of publication	Year of publication	Relevant pages	Permanent identifiers (if available)	Is/Will open access provided to this publication?
Datenschutz im Cloud Computing	Marit Hansen	Daten- und Identitätsschutz in Cloud Computing, E-Government und E-Commerce	ISBN 978-3-642-30101-8	Springer-Verlag Berlin Heidelberg	Berlin, Heidelberg	2012	79-95	http://dx.doi.org/10.1007/978-3-642-30102-5_4	No

Table 3: List of non-peer reviewed publications

2.3.4 Further Dissemination Activities

According to the *Guidance Notes on Project Reporting (version 2012)* of the European Commission, the following table lists all dissemination activities from Period 3 (M25-M36).

Type of activities	Main leader	Title	Date	Place	Size of audience	Type and goal of the event	Countries addressed
Presentation	FFCUL	eChallenges 2012 workshop on Storage Clouds for the Future Internet	October, 2012	Lisbon, Portugal	40	Invited presentation "Abstractions for Trusted Cloud Computing: The TClouds Approach"	International
Presentation	ULD	University Ostfalia, Cloud summit "Erosion von Informationssicherheit in Unternehmen – Smartphone, Cloud & Co." (Erosion of information security in enterprises - smart phone, cloud & co.)	12.10.2012	Wolfenbüttel, Germany	60	Information event for Industry - Invited keynote (Marit Hansen)	National
Conference	ULD	34th International Conference of Data Protection and Privacy Commissioners	22.-24.10.2012	Punta del Este, Uruguay	150	Participation in discussions on future cloud computing and data transfer politics	International
Other	TUBS	Technical discussions	22.10.2012	Zurich, Switzerland	5	Technical discussions with IBM in preparation of publications and further research	International
Conference	TEC	ERIC Conference	22-25.10.2012	Barcelona, Spain	400	Representing TClouds at Securing Clouds and Mobility workshop	International
Flyer	TEC	TClouds Leaflet Update	24.10.2012	Online	/	The TClouds Leaflet has been updated due to Amendment No. 1. It can be downloaded via the TClouds project website.	International
Other	ULD	Stiftung Warentest Expert Meeting on Cloud Computing	30.10.2012	Berlin, Germany	15	Evaluation of security in commodity cloud services	National
Presentation	ULD	Fraunhofer FOKUS, eIDEE – Wettbewerb zum digitalen Handschlag - Talk: "Mit Sicherheit E-Commerce" (Secure e-commerce) http://www.fokus.fraunhofer.de/de/fokus_events/elan/ecommerce/	31.10.2012	Berlin, Germany	100	Fraunhofer Event for scientists and industry - Invited Talk (Marit Hansen)	National
Workshop	SRX	IT Security Association working group	16.11.2012	Berlin, Germany	10	Smart Grid and Cloud Computing	National
Conference	SRX	thinksmart conference	20.11.2012	Düsseldorf, Germany	40	Conference on Smart Grid security	National

Type of activities	Main leader	Title	Date	Place	Size of audience	Type and goal of the event	Countries addressed
Presentation	ULD	Workshops "Biometrische Identitäten und ihre Rolle in den Diskursen um Sicherheit und Grenzen" des Berliner Stiftungsverbundkollegs der Alcatel-Lucent Stiftung für Kommunikationsforschung unter Mitarbeit der LFE »Informatik in Bildung und Gesellschaft« der Humboldt-Universität zu Berlin, Talk: "Biometrie in Zeiten von eIDs, Social Networks und Cloud Computing – die Datenschutzsicht" (Biometry and Cloud from the privacy point of view) http://waste.informatik.hu-berlin.de/tagungen/digiID/	30.11.2012	Berlin, Germany	70	Interdisciplinary Workshop on Biometrics and the information society, Invited talk (Marit Hansen)	National
Presentation	IBM	Bretagne-Networking Workshop on Storage	Nov. 2012	Rennes, France	100	Invited talk	International
Presentation	IBM	Computer & Electronics Security Applications Rendez-vous (C&ESAR)	Nov. 2012	Rennes, France	250	Keynote talk	International
Presentation	TUBS	1st Workshop on Secure and Dependable Middleware for Cloud Monitoring and Management (SDMCMM '12)	04.12.2012	Montréal, Canada	30	Presentation of "Enhancing Coordination in Cloud Infrastructures with an Extendable Coordination Service"	International
Workshop	ULD	Dagstuhl Seminar "Organizational Processes for Supporting Sustainable Security", Talk ""Insider Threats" and "Supporting Sustainable Security" – Adding the Dimension of Privacy and Data Protection"	09.12.2012-12.12.2012	Dagstuhl, Germany	15	Dagstuhl seminar	International
Presentation	FFCUL	63rd Meeting of the IFIP 10.4 Working Group on Dependable Computing and Fault Tolerance	January, 2013	Tavira, Portugal	30	Invited presentation "Recent Advances in Cloud Computing Dependability"	International

Type of activities	Main leader	Title	Date	Place	Size of audience	Type and goal of the event	Countries addressed
Interview	ULD	Interview for http://cloud.irights.info/	12.01.2013	Germany		Interview with Marit Hansen and Ninja Marnau on Cloud Security Risks http://cloud.irights.info/uld-ein-gewisses-misstrauen-ist-berechtigt	National
Conference	ULD, TEC	CPDP 2013, Moderator of Panel "10.30 Cloud, Trust and Privacy: Towards The InterCloud" at CPDP (Computers, Privacy & Data Protection) 2013 "Reloading Data Protection", http://www.cpdpconferences.org/friday25january2013.html#top	23-25.01.2013	Brussels, Belgium,	150	CPDP (Computers, Privacy & Data Protection) 2013 "Reloading Data Protection"	International
Conference	INNOVA, IBM	CPDP 2013	25.01.2013	Brussels, Belgium	500	Conference on Computers, Privacy, Data Protection	International
Other	ULD	Working Group on legal policies for cloud of the German Federal Ministry of Economics and Technology	28.01.2013	Köln Germany	30	Standardisation and policy work	National
Other	TUBS	Practical course: Practical Cloud Computing	01.02.2013	Braunschweig, Germany	10	Practical experiences with infrastructure cloud systems	National
Conference	TEC	ICT Trust & Security Project Clustering Open Communications Event	07.02.2013	Brussels, Belgium	150	Introducing TClouds	International
Presentation	TUBS	20th Annual Network & Distributed System Security Symposium	24.-27.02.2013	San Diego, USA	100	Presentation of "Attack Surface Metrics and Automated Compile-Time OS Kernel Tailoring"	International
Workshop	INNOVA, IBM	Oxford Workshop, Technical TClouds Platform Presentation	25.02.2013	Oxford, UK	15	Technical TClouds Platform Presentation; Diffusion of TClouds Modules and Technology	International
Conference	ULD	CeBIT 2013	07.03.2013	Hannover, Germany	100	Talk by Meiko Jensen "Cloud Computing Attacks And Appropriate Security Measures"	International

Type of activities	Main leader	Title	Date	Place	Size of audience	Type and goal of the event	Countries addressed
Presentation	FFCUL	Invited presentation at University of Neuchatel	23.03.2013	Neuchatel, Switzerland	30	Presentation "Cloud-of-Clouds Storage: from a Register to a File System"	International
Conference	FFCUL	13th International IFIP Conference on Distributed Applications and Interoperable Systems (DAIS'13)	06.04.2013	Rome, Italy	150	Presented the paper "FITCH: Supporting Adaptive Replicated Services in the Cloud" in the joint DISCOTEC session	International
Presentation	ULD	IFIP IDMAN 2013: Policies & Research in Identity Management, Talk: "Data Protection by Default in Identity-Related Applications" http://www.idman2013.com/programme.html	08.04.2013-09.04.2013	London, UK		IFIP IDMAN 2013: Policies & Research in Identity Management, invited talk (Marit Hansen)	International
Presentation	IBM	IDC Cloud Computing Forum Austria	09.04.2013	Vienna, Austria	100	Presentation on "Trustworthy Cloud Computing"	International
Presentation	TUBS	International Workshop on Cloud Data and Platforms (CloudDP'13)	14.04.2013	Prague, Czech Republic	30	Presentation of the CheapBFT demonstrator	International
Presentation	FFCUL	3rd Workshop on Cloud Data and Platforms (together with ACM EuroSys'13, supported by TClouds)	14.04.2013	Prague, Czech Republic	30	Presentation "Cloud-of-Clouds Storage: from a Register to a File System" in the TClouds-sponsored session of the workshop	International
Presentation	FFCUL	DoCEIS'13 - 4th Doctoral Conference on Computing, Electrical and Industrial Systems	15.04.2013	Almada, Portugal	150	Keynote speech "Security and Dependability of Cloud Computing: Where is my data?!"	National
Presentation	ULD	Forum für Datenschutz: Datenschutztage 2013, talk: "Vertrauenswürdiges Cloud Computing" (Trustworthy cloud computing)	16.04.2013	Wiesbaden, Germany	60	Symposium for data protection, Invited talk (Marit Hansen)	National
Workshop	INNOVA, IBM	Cambridge Workshop Trinity College	16.04.2013	Cambridge, UK	15	Technical TClouds Platform Presentation to Venture Capital and Startup; Diffusion of TClouds Modules and Technology into Venture Capital	International

Type of activities	Main leader	Title	Date	Place	Size of audience	Type and goal of the event	Countries addressed
Presentation	ULD	a-i3/BSI-Symposium "Dezentral und mobil: die Zukunft der Datenverarbeitung", Ruhr-Universität Bochum, Talk: "Cloud-Zertifizierung aus Sicht des Datenschutzes" (Cloud certificates from a data protection point of view)	17.04.2013	Bochum, Germany	100	National summit on the future of data processing, Invited talk (Thilo Weichert)	National
Conference	ULD	Law firm Bird&Bird's IT Law Conference	20.04.2013	Frankfurt, Germany	150	IT Law conference	National
Presentation	TUBS	Presented Tailored Memcached at the "Fachgruppentreffen Betriebssysteme"	26.04.2013	Braunschweig, Germany	50	The "Fachgruppentreffen Betriebssysteme" is a national meeting for researchers in the field of operating systems and distributed systems. It takes place two times a year at changing locations.	National
Presentation	SRX	TClouds presentation and advisory board work on SECCRIT workshop	06.05.2013	Vienna, Austria	30	Workshop of EU project SECCRIT	International
Conference	ULD	re:publica 2013	08.05.2013	Berlin, Germany	300	Panel discussion on the new EU data protection regulation with Ninja Marnau (ULD), Jan Philipp Albrecht (Member of the European Parliament), Paul Nemitz (European Commission), Susanne Dehmel (Bitkom)	International
Conference	ULD	acatech privacy forum. Panel Participation at acatech "Forum Internet Privacy"	15.05.2013	Berlin, Germany	80	acatech privacy forum, panel discussion participation (Marit Hansen)	National
Other	ULD	Cloud Accountability Project (A4Cloud - http://www.a4cloud.eu/) Advisory Board	10.06.2013	London, UK	20	A4Cloud Advisory Board	International
Workshop	TEC	First Plenary Meeting of the NIS Public-Private Platform	17.06.2013	Brussels, Belgium	300	Represented TClouds consortium in discussion	International
Conference	FFCUL	USENIX Annual Technical Conference (USENIX'13)	27.06.2013	San Jose, CA, USA	250	Presented the paper "On the Efficiency of Durable State Machine Replication"	International
Workshop	ULD	CAST Workshop on SOA- and Cloud-Security http://www.cast-forum.de/workshops/infos/176	27.06.2013	Darmstadt, Germany	50	Talk by Ninja Marnau "Secure is not enough"	National

Type of activities	Main leader	Title	Date	Place	Size of audience	Type and goal of the event	Countries addressed
Workshop	ULD	IEEE 2013 Third International Workshop on Security and Privacy Engineering (SPE2013)	27.06.-02.07.2013	Santa Clara, CA, USA	50	workshop organized by Meiko Jensen as part of the IEEE 2013 World Congress on SERVICES, which also hosts some of the most relevant scientific events in the areas of Cloud Computing (IEEE CLOUD), Web Services (ICWS), and Big Data (IEEE BigData Congress)	International
Conference	ULD	IEEE COMPSAC 2013	22.07.-27.07.2013	Kyoto, Japan	150	Paper: Jensen, M. Towards Privacy-Friendly Transparency Services in Inter-Organizational Business Processes. In Proceedings of the 2013 IEEE COMPSAC Workshops, 2013	International
Presentation	POL	10th Int. Conf. on Trust, Privacy and Security in Digital Business, 2013.	28.08.2013	Prague, Czech Republic	20	Presentation of "Towards Privacy-by-Design Peer-to-Peer Cloud Computing"	International
Presentation	POL	13th Int. Conf. on Peer-to-Peer Computing, 2013.	09.09.2013	Trento, Italy	30	Presentation of "Privacy-by-Design Cloud Computing Through Decentralization and Real Life Trust."	International
Conference	ULD	Datenschutztag 2013	24.09.2013	Köln Germany	expected 60-100	Talk by Marit Hansen "Cloud Computing und Datenschutz"	National
Presentation	FFCUL	2nd Int Workshop on Dependability Issues in Cloud Computing (DISCCO 2013)	30.09.2013	Braga, Portugal	30	Presentation of "The TClouds Platform - Concept, Architecture and Instantiations" paper & Keynote talk entitled "On the Role of State Machine Replication in Cloud Infrastructures"	International
Presentation	FFCUL	1st Workshop on Planetary-Scale Distributed Systems (together with IEEE SRDS'13)	30.09.2013	Braga, Portugal	30	Presentation "Evaluating State Machine Replication Over a WAN"	International
Other	TEC	TClouds Factsheets	02.04.2013	Online	/	15 fact sheets containing high-level descriptions of technology components, prototypes, and use cases developed within the TClouds project.	International

Type of activities	Main leader	Title	Date	Place	Size of audience	Type and goal of the event	Countries addressed
Flyer	TEC	TClouds Leaflet Update	26.08.2013	Online	/	Content update	International
Poster	TEC	TClouds Final Project Poster	27.08.2013	Online	/	Poster outlining project information and final results. To be used for future promotion of TClouds results.	International
Web	TUBS	http://www.ibr.cs.tu-bs.de/projects/tclouds/download/	23.09.2013	Online	/	Open source release of RBPEL and Tailored Memcached subsystems	International
Workshop	TEC	First Meeting of WG3 on Secure ICT research and innovation - NIS Public-Private Platform	27.09.2013	Brussels, Belgium	200	Represented TClouds consortium in discussion	International
Other	FCSR	Production of video presenting TPaaS healthcare platform and TClouds infrastructure	September, 2013	London, UK	50	Dissemination/AB	International
Press release	TEC	TClouds Final Press Release	September, 2013	Online	/	Final press release announcing end of TClouds project and its main results	International

Table 4: List of further dissemination activities

2.3.5 New Websites

Websites related to the project, which have been launched in Y3.

Website	Description of the main TClouds related information
http://workshop13.tclouds-project.eu	Workshop collocated with ESORICS 2013 where TClouds-related topics were discussed within a broader audience.

Table 5: Project related websites launched in P3

2.3.6 TClouds project website statistics

In the following we present statistics generated from the TClouds project website (http://www.tclouds-project.eu) to underline the successful dissemination activities of P1 – P3 of TClouds.

2.3.6.1 Website visitors

Figure 2 presents the visitor statistics for the project website for the entire duration of the project. The figures clearly show a dramatic increase in the number of visits and unique visitors in 2013 compared to the previous two years, thus highlighting the success of the consortium's dissemination efforts.
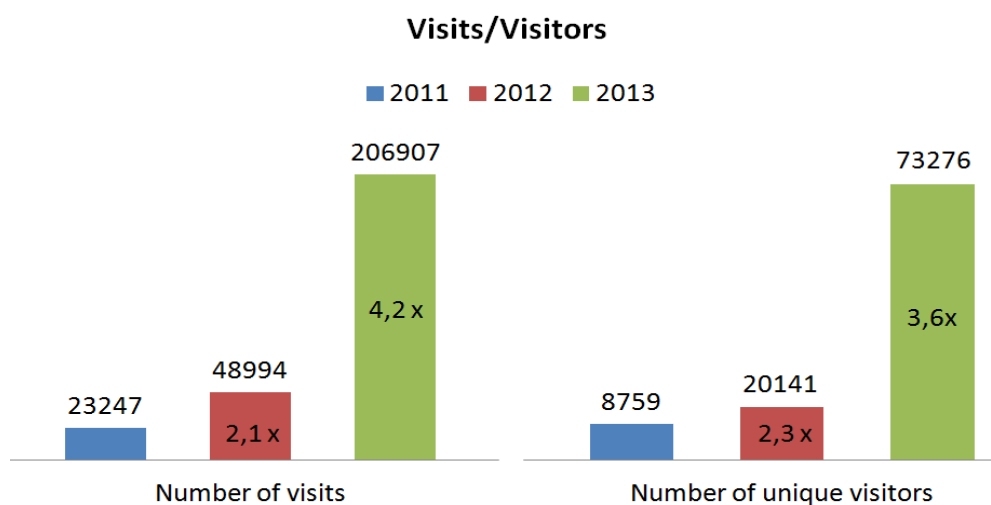
Figure 1: Visitor website statistics for TClouds project

Finally, the pie chart below illustrates the range of visitor nationalities to the TClouds website. The majority originates from European countries, but also includes visitors from India, China and the USA.

Country
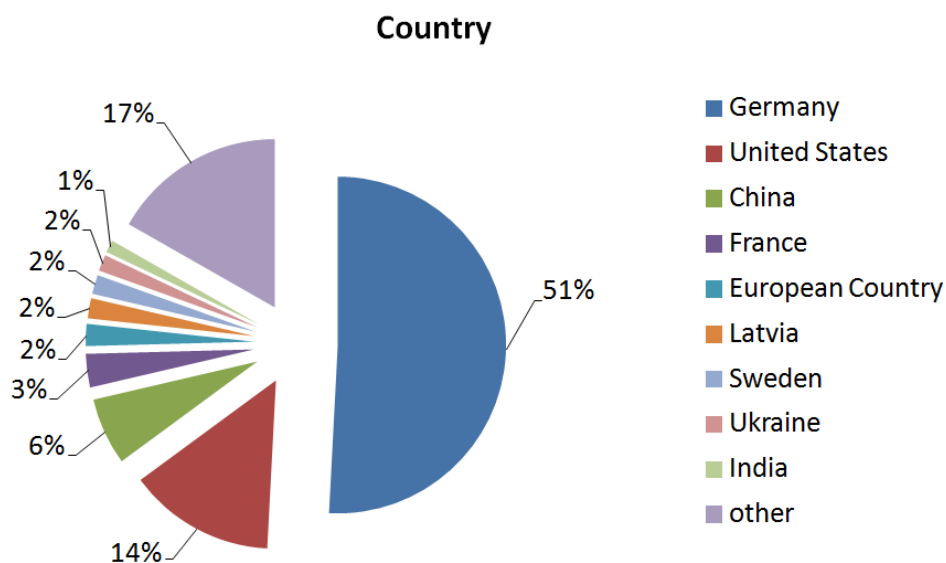
Figure 2: Visitor nationalities for TClouds website

2.3.6.2 Top downloads

The following table presents statistics on the top downloaded content in the last project year.[1] A high demand for published deliverables was observed.

Rank	Name	Downloads
1	Annual Privacy Forum 2012	1052
2	Cloud-Computing: Business Requirements Analysis	940
3	Technical Requirements and Architecture for Privacy-enhanced and Resilient Trusted Clouds	680
4	TClouds Prototype Architecture, Quality Assurance Guidelines, Test Methodology and Draft API	651
5	Cloud Computing: Legal Analysis	595
6	Preliminary Architecture of Middleware for Adaptive Resilience	547
7	Trust Model for cloud applications and first Application Architecture	546
8	Cloud Computing: Business Impact Analysis	427
9	Cloud Computing - Solutions and Enablers	413
10	Components and Architecture of Security Configuration and Privacy Management	378

Table 6: Top downloaded content from project website in the 3rd project period

---

[1] Statistic created on 12th September 2013.

2.3.6.3 Search engine queries

Analysis of the search engine queries, which redirect visitors to the project website, shows that search engines connect the TClouds project with the term *"trustworthy cloud(s)"* and the paper titles / author names of the published scientific papers listed on the website.

2.3.7 Updated TClouds Project Leaflet

The official TClouds leaflet is a four page informative and graphically appealing A4 flyer, highlighting the objectives and the work programme of TClouds. It is used for distribution at conferences or certain other events in order to provide further visibility to the TClouds project. An electronic version of the leaflet is available on the TClouds website.

TEC has been responsible for a recent leaflet update. The leaflet was under revision due to a project amendment and some content update (consortium changes). The new version of the leaflet has been published on our official project website at:

http://www.tclouds-project.eu/downloads/TClouds_Leaflet-Update-20130826-web.pdf
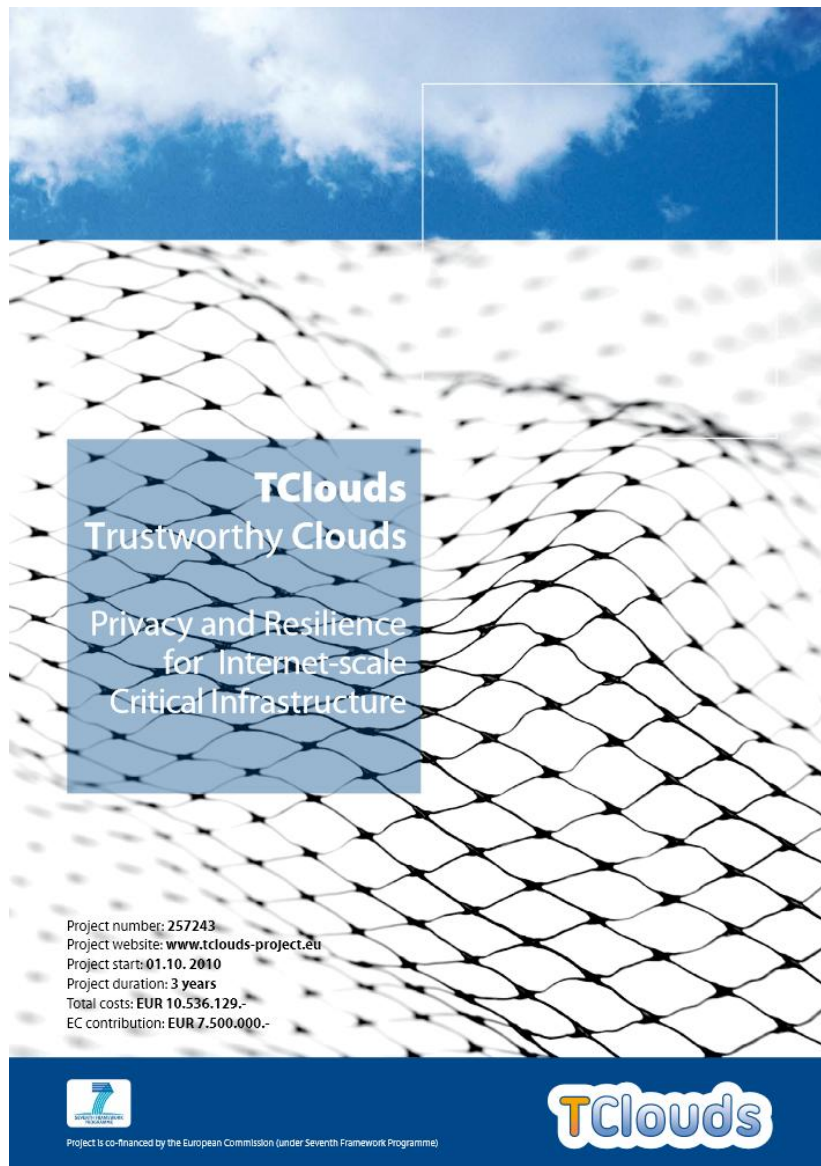
2.3.8 TClouds Factsheets ("TCloudlets")

TClouds fact sheets (or "TCloudlets") contain high-level descriptions of some of the components, prototypes, and use cases developed within the TClouds project. These fact sheets explain the advantages of TClouds technology in an easily accessible way and thus greatly help in disseminating the project results to the industrial and academic communities. Each topic is illustrated on a printable 2-page document in PDF format available for free download from the TClouds project website under **About TClouds → Fact Sheets** or the URL http://www.tclouds-project.eu/index.php/about-tc/factsheets. Figure 4 and Figure 4 present the front-page and back-page of a TClouds Fact Sheet example.

Figure 3: TClouds Facts Sheet example (Front-page)

Figure 4: TClouds Fact Sheet example (Back-page)

2.3.9 TClouds Poster

A TClouds Summary Poster containing essential information about the project and summarising its main results was created in August 2013. Its main purpose will be to disseminate the project results beyond the TClouds official end date.

Figure 5: TClouds poster

2.3.10 TPaaS Healthcare Platform video

TPaaS is a safe place where one can store, use and share personal health information. One can connect devices and third party apps to analyze their data and discover more about themselves, or simply track their health status.

An introductory video presenting its features was created and posted on YouTube at:

http://www.youtube.com/watch?v=Ulr9XRiwfwY

The video has been published on 12th September and currently[2] YouTube lists around 95 views.

---

[2] Checked YouTube on 25th September 2013.

2.4 Updated cooperation with external organisations or other projects/programmes

Place	Type, content of the cooperation	Cooperation partners	Countries addressed (international/ national – which country)
Cooperation with the NESSOS project (www.nessos-project.eu), Cooperation meeting on security challenges of ULD and University Duisburg-Essen, ULD participants: Marit Hansen, Meiko Jensen	Communication/knowledge transfer	NESSOS	International
Cooperation meeting with German research project CloudCycle (http://www.cloudcycle.org/)	Communication/knowledge transfer	CloudCycle	National
Cloud Accountability Project www.a4cloud.eu	Communication/knowledge transfer	TEC	International
Advanced Security Service cERTificate for SOA http://assert4soa.eu/	Communication/knowledge transfer	TEC	International
Certification, InteRnationalisation and standaRdization in cloUd Security http://www.cirrus-project.eu/	Communication/knowledge transfer	TEC	International
CloudScale http://www.cloudscale-project.eu/	Communication/knowledge transfer	TEC	International
CloudSpaces http://www.cloudspaces.eu/	Communication/knowledge transfer	TEC	International
Certification infrastructure for MUlti-Layer cloUd Services http://www.cumulus-project.eu/	Communication/knowledge transfer	TEC	International
FI-WARE http://www.fi-ware.eu/	Communication/knowledge transfer	TEC	International
Aniketos http://www.aniketos.eu/	Communication/knowledge transfer	TEC	International
MAnagement of Security information and events in Service Infrastructures http://www.massif-project.eu/	Communication/knowledge transfer	TEC	International
Mobile Cloud Networking http://www.mobile-cloud-networking.eu/site/	Communication/knowledge transfer	TEC	International
PoSecCo http://www.posecco.eu/	Communication/knowledge transfer	TEC	International
Trustworthy Embedded Systems for Secure Cloud Computing Applications	Communication/knowledge transfer	TEC	International

Place	Type, content of the cooperation	Cooperation partners	Countries addressed (international/ national – which country)
http://www.trescca.eu/			
BiobankCloud project (www.http://biobankcloud.eu)	Communication/knowledge transfer	FFCUL	International
SEGrid	Communication/knowledge transfer	FFCUL	International
BMBF Statusmeeting IT-Sicherheitsforschung, Meeting of the German Ministry for Education and Research for IT Security Projects	Communication/knowledge transfer	German IT Security Projects	National
Cloud Accountability Project (A4Cloud - http://www.a4cloud.eu/) Advisory Board	Communication/knowledge transfer	A4Cloud	International
W3C Tracking Protection Working Group Meetings	Communication/knowledge transfer	W3C	International
Contribution to Trusted Cloud Initiative of the BMWi Kompetenzzentrum Trusted Cloud	Communication/knowledge transfer	BMWi Trusted Cloud Projects	National

Table 7: List of cooperation with external organisations or other projects/programmes

Chapter 3

Standardisation

Chapter Authors:

Christian Cachin, Elmar Husmann (IBM)

3.1 Introduction

A detailed account of the standardisation landscape related to secure and trustworthy cloud computing has been included in D4.1.2, which was written in early 2013. This also included an individual validation of each standard in the context of the TClouds architecture and components. Therefore, this chapter focuses only differences that have arisen in the last months of the project. For complete reference, please refer to D4.1.2.

During the last part of the third year of TClouds, several technology components developed by TClouds partners have been refined; many have been more tightly integrated with the OpenStack platform, in particular those that are part of TClouds' Trustworthy OpenStack prototype.

In the following, we first review the TClouds map of cloud standards and describe related dissemination activities and linkage into the CEN work on aligning European cloud standards.

A second line of activities has been towards DIN and ISO/IETF – notably by ULD and a third activity line towards the W3C Tracking Protection Working Group.

In addition to this direct work with standards bodies, TClouds has done a substantial work on improving OpenStack components from the perspective of trustworthy cloud computing.

It should be noted in this context, that the linkage between OpenStack and standards in the TClouds map is close. Several of the recommended standards are already implemented in OpenStack (e.g. OVF) while further standards implementation projects are underway (e.g. OCCI). Hence, OpenStack can be regarded as an environment that is already partially compliant with the TClouds standards map.

This means that using TClouds enhanced OpenStack components already partially allows to use TClouds recommended open cloud standards at the same time.

A general concern is that the work with standards has its own – usually long - time cycles and while TClouds can demonstrate involvement and first contributions, the further impact and uptake will depend on the exploitation time after the finish of the project. This also means a continuous support by partners such as IBM or ULD that have been directly interfacing for TClouds with standards bodies. This is linked to the exploitation plans that are described in the later part of this document.

In addition to introducing the TClouds Map of Standards to the cloud standards community, a detailed description of the map is also included in the TClouds Whitepaper "Cloud, Trust, Privacy". The paper also highlights TClouds stakeholder survey results and the Cambridge and Oxford workshop discussions – that all included debates on the role of cloud standards. Our stakeholder survey has particularly supported the need for open cloud standards and highlighted the insufficiencies of the landscape of currently adopted de-facto cloud industry standards.
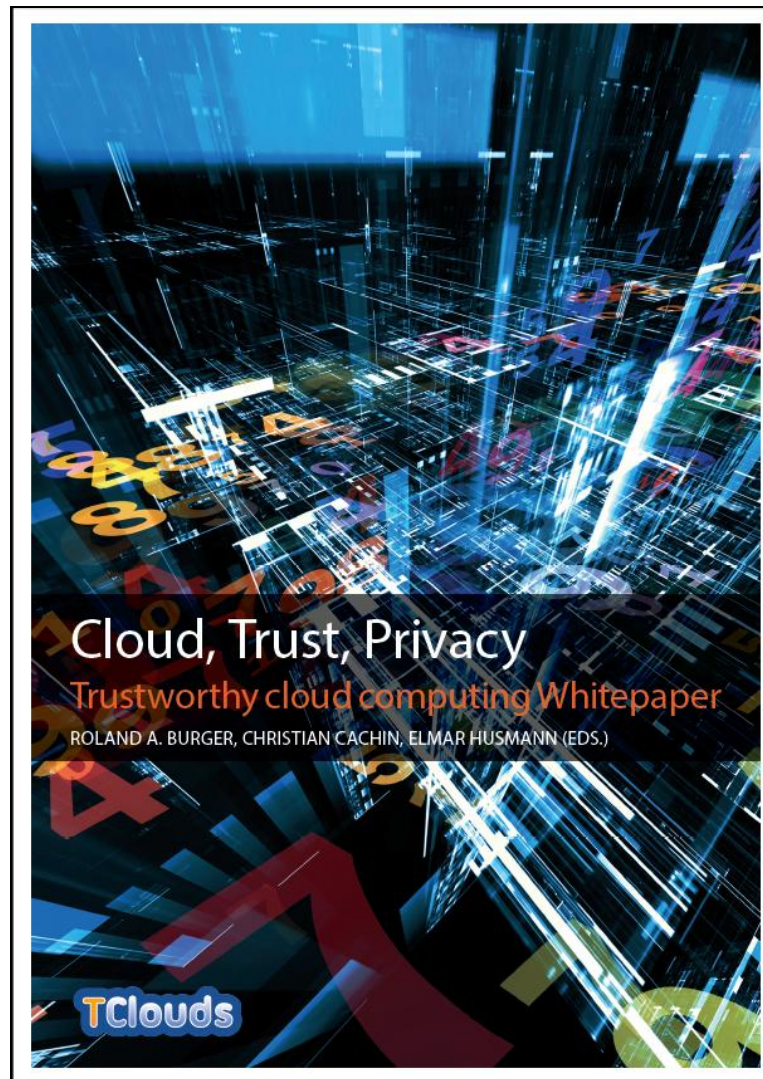
Figure 6: TClouds Whitepaper

3.2 TClouds Map of Cloud Standards and contribution to CEN/CENELEC

The refined TClouds Map of Cloud Standards for secure, privacy protective and trustworthy infrastructure clouds has first appeared in D4.1.2. It is included again in the next figure. The detailed analysis of the standards map and its relation to the technology in the TClouds platform are included in D4.1.2, chapter 3. Almost all components integrated in the TClouds platform are exhibited there; as the TClouds platform's composition has not changed in the last months of the project, these relations are static and not repeated here.

IBM has already been invited and agreed to present the TClouds map of cloud standards on November 19th in the 3d Cirrus Workshop hosted by the Austrian Institute of Standards and the CEN/CENELEC BT (Technical Board) Working Group 6 "ICT Standardization Policy" with the aim of preparing a CEN Workshop Agreement (CWE) on standards for secure cloud computing.

The workshop is supported by Eurocloud and the Cloud Security Alliance as well as industrial partners such as SAP and EMC. It is planned in this CEN Workshop Agreement to suggest aligning European cloud standardization efforts in the following areas that directly correspond to the TClouds map:

- Provider certification (Organization Level Cloud Standards)

- SLA (Service & Application Level)

- Testing, validation and continuous monitoring (Infrastructure Topology & Validation Level)

- Security (Infrastructure Level)

It should be noted that a CEN Workshop Agreement is, while being a formal contribution to the CEN standardization process, still far from being a European standard and involves no obligation as a normative document at European or national level.

This indicates the early state of the CEN debate around standards for secure cloud computing. The mapping analysis done in the TClouds project therefore provides a good support of crystallizing out the interplay of different security relevant elements and complementary standards in cloud computing.

This also goes along with the fact that the standards named in the TClouds map are only partially implemented yet in commercial cloud services and products. So, standardisation in clouds will still demand significant research and commercial engagements in the upcoming years – and we are just standing at the beginning.

Organization-Level	ISO/IEC 27001 – **Information Security Management** Data Protection and Cloud Computing WG *ISO*
Semantic-Level	**Cloud Computing Definition**, Security, Portability, & Interoperability Use Cases *NIST*
Service & Application Level	Cloud Toplogy and Orchestration Specification **(TOSCA)** Web Services Business Process Execution Language **(WS-BPEL)** OASIS
Infrastructure & Topology Validation Level	Security Goal Language for Virtualized Environments (**VALID, IF/ASLan**) IBM & EU Proiect AVANTSSAR

Infrastructure Level

VM Management Open Virtualization Format (OVF) *DMTF*	**Cloud Storage** Cloud Data Management Interface (CDMI) *SNIA*	**Infrastructure Management** SimpleCloud API DMTF CIMI *OGF Open Cloud Computing Interface (OCCI)*	**Authentication & Key Mgt.** Key Managament Interoperability Protocol (KMIP), *OASIS Open Authorization Framework OAuth 2.0 (IETF)*	**Remote Attestation** Infrastructure Work Group Core Integrity Schema (Trusted Computing Group)	**Hypervisor Configuration** libvirt XML Format *Linux*

Figure 7: TClouds Map of Cloud Standards

3.3 "Do not track" and contribution to W3C

TClouds members IBM and ULD have been closely involved in the W3C Tracking Protection Working Group. As Matthias Schunter – former TClouds scientific coordinator and chair of the group – transferred in Y2 from IBM to Intel, this work has been partially transferred as well. Ninja Marnau (ULD) continued to be involved as a link to TClouds and invited expert to the group. ULD contributed in particular the results of the TClouds legal analysis (Wp1.2) of complex internet-based architectures and Privacy Enhancing Technologies.

A first standard that has been issued by the group is the Tracking Preference Expression (DNT) that already has been adopted – e.g. by the Mozilla Foundation for the Firefox Web Browser.

Still debates are ongoing with providers to adopt DNT and customize services accordingly.

3.4 Contribution to DIN and ISO/IETF

ULD hosted a workshop with several stakeholders and members of the German DIN institute to discuss and contribute to several ISO/IETF standard drafts such as the draft 27018 "Code of practice for data protection controls for public cloud computing services" and draft 29102 "Privacy Architecture Framework".

3.5 Standardisation of TClouds Technology via OpenStack

TClouds has proposed several security enhancements to OpenStack. To integrate these into the OpenStack platform distribution, TClouds has already adapted several OpenStack APIs. Some OpenStack interfaces were extended by TClouds in order to implement the desired functionality in the trustworthy cloud infrastructure.

The next table lists those components that have been identified as directly integrateable with OpenStack, the corresponding changes, and the status of this work.

Most components demonstrated with the Trustworthy OpenStack distribution are ready or nearly ready for being integrated in the OpenStack platform through the OpenStack community process. As this requires effort of a different nature than pursued by TClouds, the corresponding work is left for the future.

	TClouds Enhancements	Relation to Open Stack	Status
Access Control as a service	Trustworthy Cloud Scheduler. Matching User security & privacy requirements to cloud virtual resource allocation. Cloud security policy enforcement.	ACaaS is implemented as a scheduler filter in NOVA. It is invoked by the scheduler. To support ACaaS's operations, the central database has been updated, to incorporate necessary fields. Correspondingly, APIs related to database manipulations are added. For invoking ACaaS services,	Technology is ready, contribution to OpenStack in form of technology blueprint is planned.

	TClouds Enhancements	Relation to Open Stack	Status
		both of the CLI (python-nova-client) and web-based interfaces (Dashboard) are modified.	
Cryptography as a service	Protection and user empowerment while deploying high value cryptographic credentials to the cloud.	CaaS is integrated at the level of the hypervisor, where multiple options exist for OpenStack. The prototypes work with Xen. Integration of KMIP for key management in connection with remote key servers is possible from the hosted VMs.	Technology is ready, but needs first to be integrated in hypervisor (most likely, Xen); then it will work with OpenStack after modifications to the NOVA interfaces. Integration is planned with a future release of OpenStack.
Security Assurance in Virtualized Environments (SAVE)	Verify isolation among different tenants in platform	New REST endpoint to obtain libvirt data directly in SAVE; then SAVE can be integrated.	REST endpoint developed; presenting to OpenStack at next summit (Nov. 2013).
Remote Attestation Service	Assess the integrity of nodes in the Cloud infrastructure.	Integration into OpenStack by adapting the existing code of Nova Scheduler (more precisely, the TrustedFilter) to support new integrity verification results (integrity levels) that may be assigned to a host depending on the checks defined on integrity measurements taken by the cloud nodes.	Integration depends on modifications made to the OpenAttestation framework. Due to the extent of the changes, it will take some time before the component can be absorbed by OpenStack. This is planned for after the end of TClouds.
Secure Log Service	Support different secure logging schemes. Guarantee log integrity and authenticity in monitoring the cloud.	Needs extension of the internal logging mechanism and addition of an administration panel within the OpenStack dashboard, with LogService management panel.	Technology is ready, integration and writing of blueprint is planned.

	TClouds Enhancements	Relation to Open Stack	Status
Ontology based reasoner	Management of trusted virtual domains in the cloud	This subsystem has been integrated into Trustworty OpenStack as an enhancement of the Quantum OpenvSwitch plugin. Basically, a new Quantum agent (to create through an extended Libvirt the new virtual network types), and the extension of the Libvirt driver of Nova (to plug virtual machines' network interfaces into the correct TVD network).	Technology is currently integrated in an older snapshot of Libvirt and OpenStack. After processing upstream patches, this subsystem will be ready for integration with the community edition of OpenStack.

Chapter 4   Exploitation

Chapter Authors:

Norbert Schirmer (SRX), Martina Truskaller and Patricia Rio Branco (TEC), TClouds partner responses to questionnaire

4.1 Introduction

This chapter refines the exploitation efforts and plans of the partners as defined in the work plan and reported in deliverable D4.1.2. As D4.1.2 was revised and updated in M30 (March 2013) of the project, the results presented here are only a minor update of the corresponding chapter in D4.1.2 V02.

4.2 Questionnaire

The goal of exploitation is to ensure the sustainability of the projects results beyond the project end and to demonstrate how the project has influenced the EU landscape.

Exploitation includes:

- Financial exploitation, e.g. by building products, projects or services based on the project results

- Research & Development, by engaging new projects (EU funded or other) based on the experiences gained in the project

- Education, e.g. courses, master / PhD students, etc.

- Community building around the topics of the project

- Knowledge transfer from academia to industry, by collaboration or via employees

- Contributions to open source projects, standardization efforts (this overlaps with "Standardization and Dissemination).

We have created a questionnaire as a guideline in order for each partner to act as the basis for a few self-contained paragraphs which loosely answer those questions. We have grouped the questions into two categories, one biased towards the industry partners, one biased towards academic partners. These categories act as a guideline only and questions can be taken as a basis from both if need be.

4.2.1 Questions biased towards industry partners

General Questions

1. What are the main results you expect from the project and how are they exploited commercially (products, services, …)

2. Which business and operating models are possible after the end of the project to bring the project results to customers? How do effort flow and cash flow look like? Which role do you see for 3rd parties (not participating in the project) in this scenario?

3. Drivers and Obstacles: Which obstacles for a successful exploitation do you see from today's perspective? How can these obstacles be tackled? Which drivers for a successful exploitation do you see from today's perspective? How can those drivers be harnessed and strengthened?

4. How do European stakeholders (cloud providers and customers) profit from the exploitation of the results (business perspective)? What does this mean for the European economy?

5. What is the timeline for the exploitation? In which phases can the exploitation be structured? What is the prospective time frame after the end of the project to bring the results to the market?

6. Which concrete customer needs do you address with your solution / product? How can you quantitatively measure the success?

7. In which way are marketing / product-management / sales departments already involved during the project?

8. How does the consortium see the kick-off for exploitation (at the end of the project) with respect to demonstration of the results, inclusion of multiplicators and publicity. Is it may be possible to start exploitation of intermediate results already during the project.

9. Are there synergies for exploitation with other projects, possibly also funded ones? If yes, which?

Economic Prospects of Success

1. How can a quick market access be guaranteed? Is it necessary to create new markets for a successful exploitation?

2. How does the market for exploitation look like today (market analysis, prognoses, technical developments).

3. How is the competition for the developed results, in Europe / worldwide?

4. What is the innovation in project results, what are the advantages compared to competitors?

Scientific / Technical Prospect of Success

1. Which impact does the general technological progress have on the exploitation scenarios?

2. Which role do non-technical developments have (legal aspects, privacy aspects,…) on the exploitation phase?

Inventions / Patents

1. Are there (plans for) patents?

4.2.2 Questions biased towards academic partners

General Questions

1. Drivers and Obstacles: Which obstacles for a successful exploitation do you see from today's perspective? How can these obstacles be tackled? Which drivers for a successful exploitation do you see from today's perspective? How can those drivers be harnessed and strengthened?

2. How do European stakeholders (providers and customers) profit from the exploitation of the results (business perspective)? What does this mean for the European economy?

3. What is the timeline for the exploitation? In which phases can the exploitation be structured?

4. Which concrete customer needs do you address with your solution / product? How can you quantitatively measure the success?

5. How does the consortium see the kick-off for exploitation (at the end of the project) with respect to demonstration of the results, inclusion of multiplicators and publicity? Is it possible to start exploitation of intermediate results already during the project?

6. Are there synergies for exploitation with other projects, possibly also funded ones? If yes, which?

Scientific / Technical Prospect of Success

1. Which impact does the general technological progress have on the exploitation scenarios?

2. Which role do non-technical developments have (legal aspects, privacy aspects …) on the exploitation phase?

3. How is the competition for the developed results in Europe / worldwide?

4. What is the innovation in project results, what are the advantages compared to competitors?

Inventions / Patents

1. Are there (plans for) patents?

Scientific Impact & Education

1. Do you (plan to) offer seminars, lectures, lab-courses and the-like with topics related to TClouds? Or in which way did the TClouds results influence / improve your education and training?

2. How did your TClouds work influence / improve your contribution to the European research in Cloud Security, like building scientific communities, organizing or participating in workshops etc.?

3. Did the TClouds work help you to attract new researchers / students?

4. Did your TClouds work results improve / foster the dissemination of your work in conferences (Industrial / Academic), journals, etc?

5. How did (or will) the project help you to build scientific communities, or help you get into communities?

Sustainability (How will the project results sustain after the end of the project?)

1. To which Open-source projects do you (plan to) contribute?

2. Are your results made available to the public domain (e.g., open-source, websites)?

3. What activities will ensure the maintenance of the project results after the project ended?

4. Have you planned follow up projects or are you already involved in other projects.

5. How did the projects influence your work in other projects? Are there synergies or follow-up work?

6. Did new partners come up during the duration of the TClouds project with which you will continue to cooperate?

7. Did the TClouds work help you to acquire new projects and / or third party funding.

Technology transfer

1. Could you awake interest in the industry for your project results?

2. Did students gain valuable knowledge by their work in the project that makes them more attractive for industry or (industrial) research?

4.3 Partner responses

This section provides the detailed responses by the project partners to the questionnaire. This is a revised version of the partners' responses presented in D4.1.2 V02 submitted in March 2013.

4.3.1.1 EDP

At the end of the project, we expect to know if it is technically possible to host Smart Grid components in a cloud computing environment while complying with a specified set of functional and security requirements. Today, smart grid related systems are hosted in the private network of a utility which fulfills a number of requirements. It is not known if these requirements are met in a cloud environment. TClouds' technological progress will tell us if it is technologically feasible.

Smart Lighting System is one of the two use cases of TClouds. It is a Smart Grid public lighting management system using cloud technology and it is thought to be able to replace the application that we currently use to manage the Portuguese public lighting infrastructure. The main difference between the two is the move to a cloud environment and also the new features and services which become possible. The decision to use Smart Lighting instead of the current application will be left until after the end of the project and it will take into consideration TClouds' results.

Data integrity and data availability are the two main security aspects to be considered. TClouds' security components will provide resilience to Smart Lighting.

- Data integrity – we need to ensure that all the communication between the client and the Smart Lighting system is completely secure, e.g. there is no possibility to corrupt data.

- Data availability – smart lighting is a near real-time system; therefore, data must be available when needed in the overall system.

In Smart Lighting there are no legal or privacy concerns because public lighting schedules are public information.

We also expect to know what is the effort required to make the switch. It is not known what effort is required to move a smart grid functionality to a cloud. This approach may be better or worse, cheaper or more expensive. This doubt acts simultaneously as an obstacle and as a driver to the adoption of a cloud computing approach in a smart grid.

We are also exploring the possibility of expanding this approach to other Smart Grid components. A possible solution would be to use a private cloud connected to a public cloud (see Figure 8).
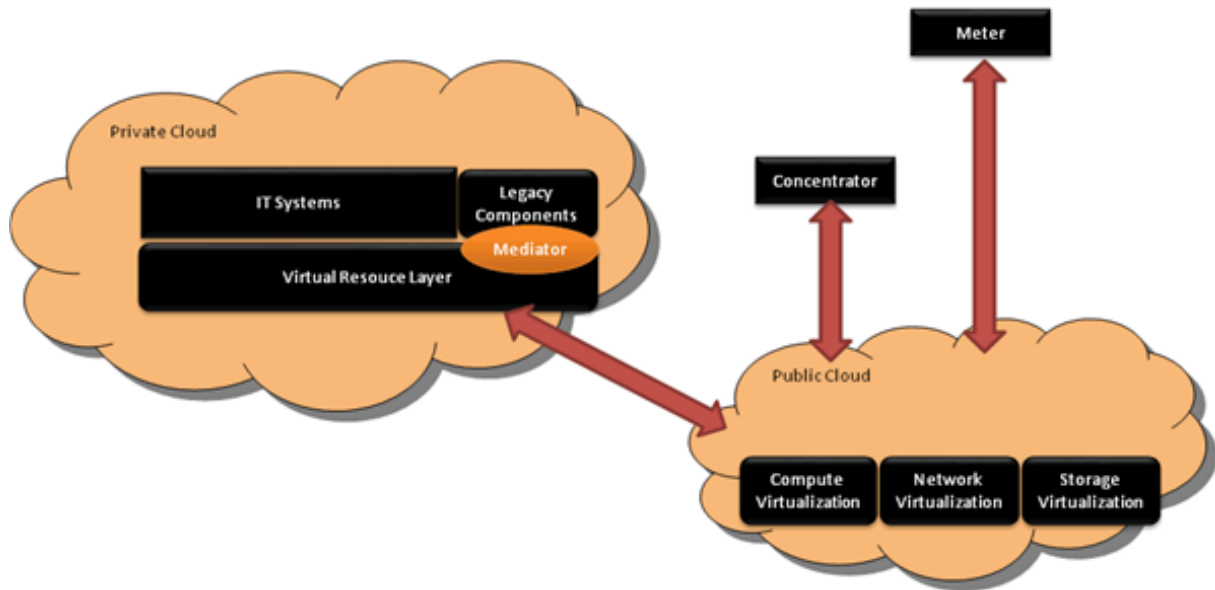
Figure 8: Smart Grid using private and public clouds

The private cloud is a more controlled environment in terms of security when compared to a public cloud. It would enable integration with legacy equipments, including those that cannot communicate through Ethernet. The public cloud would allow us to communicate with remote equipment such as the ones used in Smart Lighting, including different geographies. This solution would allow us to benefit from the characteristics of the two types of clouds. Although security aspects would be the same as in Smart Lighting, Smart Grid components such as Smart Meters bring privacy issues into discussion. TClouds will also give us a better insight into this matter.

If we prove it is feasible to host smart grid related systems in a cloud computing environment, a number of new solutions using cloud computing in smart grids may arise in the following years. Utilities get improved smart grids, and customers get better services. This can contribute to diminishing outage times and increase energy usage efficiency, which is in line with the 20-20-20 targets established by the European Commission. Moreover, vendors can increase their solution portfolio. All this can contribute to the growth of European economy.

We have been participating as speakers in several cyber security related conferences where we disseminate TClouds' intermediate results and explain our expectations for the end results and what these can enable. The project has been well accepted by other participants who show interest in our approach.

4.3.1.2 EFACEC ENG

The Smart Lighting System is a sample application from a broader Smart Grid Architecture, proposed in partnership by EDP and EFACEC, to serve as a test bed for TClouds demonstration. Aiming to first evaluate the cost-benefits of moving such an application to a cloud environment, and ultimately how it may benefit from TClouds security components.

In this sense, at the end of the project EFACEC expects to have a reasonable technical evaluation of public cloud environments, the required effort to migrate traditional solutions into the cloud, and gather enough awareness and expertise of their security and reliability flaws as well as how TClouds may help overcome those deficits.

A commercial exploitation of cloud computing solutions, and services based on TClouds or integrating parts of TClouds technology, will be timely assessed by EFACEC once the technical feasibility analysis is complete by the end of the project. A consolidated decision shall then depend on multiple other factors, namely the market trends, cost benefit analysis, customer requirements and customer willingness to embrace cloud computing solutions, all

taking into consideration the profile of the products / solutions provided by EFACEC within the Power System Automation business unit. However, given the technical complexity involved, an eventual time to market would expectedly take at least 2 to 3 years after TClouds project conclusion.

Currently, EFACEC Power System Automation business unit market demands streamlined solutions accessible from multiple devices with an extremely high level of availability and resiliency, all with reduced deployment and maintenance costs, without compromising performance, security and confidentiality levels usually encountered in their data centers.

It is a fact cloud environments are a growing trend amongst IT companies, and even though the power utilities market usually has their own infrastructures and data centers, it is a matter of time until they are open to their benefits, particularly given TClouds security enhancements. Therefore, being part of this technological evolution provides EFACEC with a valuable advantage over competitors, and improved knowledge to answer future market demand.

Particularly the Smart Lighting System is a demonstration of such market interest, driven by the Portuguese main utility company EDP, concerning a new approach to public light management, with a close involvement of Municipalities and hosted in a cloud environment. Future commercial exploitation and business model of the Smart Lighting System previewed within TClouds, and other Smart Grid functions, may undergo a joint (EFACEC and EDP) and more thorough evaluation upon the project conclusion.

4.3.1.3 FFCUL

Most of the TClouds' work by FFCUL is on the development of the cloud-of-clouds (CoC) model and its application to cloud storage services. The overall idea is to use a set of commercial cloud providers instead of just one, avoiding any internet-scale single-point of failure. Moreover, components like DepSky ensure that the data stored in the providers is kept private, and under the control of its owner. Consequently, this kind of solution addresses security concerns such as vendor lock-in, data privacy, integrity and availability.

The fact that we have several mature cloud providers around the world competing to offer better services with competitive prices opens great possibilities for implementing CoC services. However, this technology is not free from its costs. There are problems related to the latency of running the required replication protocols (they involve wide-area communication), the monetary costs (there are at least a 50% overhead due to replication) and the lack of a business model. For instance, although any individual or organization can use a system like DepSky to store data securely, it is still not clear how a company can make money from such user-centric technology. More generally, we believe CoC technology aims to empower cloud customers, not cloud providers.

In terms of scientific and technical prospects of success, FFCUL TClouds components are leading software initiatives in their area. DepSky was the first system to show that cloud-of-clouds storage is practical, and it is still the one requiring minimal assumptions from the providers. BFT-SMaRt is the only BFT state machine replication library stable enough to be used for research and development of innovative critical services. *Moreover, besides the papers and deliverables describing these components, we are making our implementations available as open-source projects: http://code.google.com/p/bft-smart/ and http://code.google.com/p/depsky/. Besides that, these components are being used in other FP7 projects: BFT-SMaRt is being used in MASSIF (http://www.massif-project.eu) while DepSky will be extended in BiobankCloud (http://www.biobankcloud.com), which started in Dec. 2012.*

In terms of scientific impact and education, our work on TClouds was subject to several talks, tutorials and lectures given by the FFCUL team both in Portugal and around the world. Moreover, at least 8 MsC theses related to TClouds were concluded in the last years, and 2 PhDs are underway.

Overall, working on TClouds was extremely beneficial for FFCUL. In particular, *the DepSky paper got a lot of citations (85, according to google scholar, in a bit more than two years), which demonstrates the interest of the community on the cloud-of-clouds concept, and we were invited to participate in two other EU project proposals. The first one was accepted and the project is underway (BiobankCloud), and the second is under evaluation (informally accepted according to insider information).*

In terms of the sustainability of the software developed in TClouds, we expect to build small developer communities around our base components, and thus we launched two open-source projects. In particular, BFT-SMaRt is already attracting some people (especially from the research community). Moreover, we expect further projects to continue providing some funding for the continuation of their development.

In terms of technology transfer, we think C2FS, the cloud-backed file system built around DepSky, attracted the attention of industry people in all talks where we described such work. We are trying to understand how we could create a startup or find other ways to do some technology transfer related to this component. Still regarding technology transfer, it is worth mentioning that all our students involved in TClouds were hired right after leaving university (in some cases before).

4.3.1.4 FCSR

Fondazione Centro San Raffaele (FCSR) is developing a healthcare secure and trustworthy platform (namely, TPaaS or Health TPaaS) that is built on top of TClouds infrastructure and leverages to it most of the privacy and security issues related to cloud computing.

TClouds is positively affecting FCSR by enhancing internal knowledge of cloud computing in general and TClouds in particular, since the platform is intended either to be used in synergy with TClouds technology and to validate the platform itself.

Exploitation activities can be seen within the platform development activities, hence the platform itself will be the starting point for new services to be delivered either into San Raffaele hospital, in order to increase quality of services and internal bureaucracy, or to the health market, providing brand new health services. In the latter case, the tight cooperation with TClouds partner (in particular with Philips) helped to get to know each other's expertise and improve network and ideas that can be useful for exploitation activities.

Thanks to effort into A1 TClouds' activity, FCSR has higher understanding of PHR/HER market needs moreover, at the end of TClouds project FCSR will continue to analyze the potential markets, the feasibility for transforming the actual Proof of Concept into a first prototype at beta stage. The strategy adopted to build the Health Platform allows FCSR to focus into privacy and security perspective (issues still delicate at PaaS/SaaS level) and the administrative functionalities platform, allowing anyway the growth of the platform under the market perspective, thanks to the App developer communities that can arise with it.

If TPaaS concepts are adopted at European level by the health compartment (either private or public) each country's government would benefit with a consistent reduction of costs of management of health data and an increased awareness of their citizens with regard to health. This, consequently, is translated into a better self-management of health status that increases life's quality. The adoption of TClouds technologies and its infrastructure is the key driver to convince industries and government to adopt systems like Health TPaaS as PHR/EHR data management into the cloud.

The main focus and philosophy behind TPaaS development is the need to increase awareness of privacy and personal data usage, combined with the search of a healthier lifestyle. Increasing privacy and security awareness means providing each user (thus, citizen) with the liberty to manage and share personal sensitive data with anyone safely.

Moreover, thanks to the adoption of TClouds technology, TPaaS exploitation can benefit from a reduced time-to-market and being able to address effectively market needs being

competitive at the same time into the young market of online PHRs and into the competitive seasoned (even though fragmented) HER market. TClouds, in fact, can be used not only as a valid tool at technology level, but also can provide valuable support to the whole marketing/branding compartments, since TClouds novelty looks very promising also under the perceived trustworthiness of final users.

In the actual PHR/HER market we can already identify important competitors either at European and international level (such as Microsoft Health Vault and Patient Know Best) and a myriad of small start-ups focused mainly in PHR services with an unsure business model. Since the market is still relatively young, new uncovered business areas can be identified. TPaaS is aimed at those areas by leveraging the tough technical part to TClouds infrastructure. Health TPaaS can identify enhancement in respect to the competitor mainly in the areas of Security, awareness of "personal data" concept, PHR/EHR sharing and interoperability, and Legal compliances EU-wide.

The exploitation phase will take into account important findings of non-technical partners. In fact FCSR will mainly benefit from the legal studies since its platform aims at solving complex legal issues such as the data storage location at European level.

4.3.1.5 IBM

As general results from TClouds, IBM Research expects further attention to the subject of cloud-computing security in the wider community. In the short term, IBM Research will focus on further expanding components developed in TClouds to actual products. In the long term, IBM Research plans to explore and research new security components based on the results from TClouds project.

The business markets and target customers of IBM Research are aligned with those of IBM and IBM's products. The focus of IBM Research will remain on SAVE and Intercloud/cloud-of-clouds storage components. The SAVE technology has already become integrated into an IBM product called TrustedSurveyor in the PowerSC line of offerings. The Intercloud storage approach is currently being evaluated for forming the basis of a cloud-gateway component for storage systems, with the emphasis on extensibility. As such, third parties may build their customizations on top of this product. Development discussions are currently underway.

Several challenges lie ahead. The main obstacle may be that users may not be interested in security and resilience-oriented technology and therefore the general public does not adopt results from TClouds. Globally, it may pose an issue, however, it is possible that, in Europe, where general population, as well as administrative bodies, are aware of (and proactive toward) security and privacy issues would help in adopting various aspects of TClouds project. Moreover, this may be the driving factor of guiding the exploitation of projects' results.

From a European perspective, the TClouds technology gives a great opportunity for EU-based cloud providers, that may (or need) to focus on security and privacy issues. This way, European providers and customers can benefit from the results in several ways. First, cloud providers and users may benefit from ability to perform compliance reporting of various components in the cloud, for example using the SAVE technology in TrustedSurveyor. Second, clients may benefit from the Intercloud storage approach as their data is not dependent on a single cloud provider anymore. As such, data resilience is increased, and, as a consequence of replication, storage clouds become commodity. Thus, we expect to gain new markets for cloud data storage.

On behalf of IBM Research, the exploitation phase is already in progress. We feel that for any successful project, like TClouds, exploitation must start before the project ends. For us, the first exploitation phase was an internal (within IBM) discussion on possible productization of components and project results. The second phase consists of turning research prototypes into product-ready solutions. The third phase is product marketing,

world-wide distribution and support through regular IBM channels. Results from TClouds are expected to take that road between now and 2015.

The above-mentioned technology resulting from TClouds addresses concrete customer needs in the domains of audits for cloud systems and data-storage on clouds. Its success can be measured financially. IBM's marketing and sales departments have already been involved in the projects descending directly from the SAVE component (TrustedSurveyor). Product management is involved in all phases of TrustedSurveyor.

Furthermore, IBM Research actively participates in the dissemination of TClouds' results. In addition to publishing scientific papers at relevant conferences and speaking at industry-leadership events, IBM Research promotes the results of TClouds to customers regularly at meetings on-site and with customers. Recently, IBM Research has also covered cloud-computing security in a broadcast on Switzerland's national TV.

Like all involved partners, IBM Research benefits from the exchange of information with partners, especially on use-case scenarios. A good cooperation with other partners forms a solid foundation for future joint ventures and projects. Moreover, received feedback from partners, as well as customers, enables (and motivates) future projects in related fields.

Regarding the time-to-market, we mention that a quick market access could be established through either seeking potential customers in domains covered by exploitation use-case in TClouds (healthcase, smart-grid), or by addressing the needs of existing IBM customers. As the security is paramount for the majority of customers, approaches like TrustedSurveyor introduce additional benefits. For storage use case, adding a well integrated solution in existing client workflows is an enabler for additional features. So far IBM's customers have shown great interest in the two technologies (SAVE and Intercloud storage).

Of course, for both technologies there exist competing products. However they are lacking specific features compared to TClouds results; for example, existing cloud-gateways for storage systems do not offer the resilience of a cloud-of-clouds storage system, they would only address one remote storage cloud. The specific innovation of TClouds resides in technical features, as described in the TClouds deliverables.

There exists a risk that other technology providers realize similar features faster, but this risk exists always. There is no specific risk that technology provided by TClouds becomes obsolete due to technological advances, however. Non-technical (legal or economic) issues appear not to block the commercialization of the technology. Recent developments rather point in the opposite direction: legal and economic motivations for protecting cloud computing applications increases. Hence they contribute to a successful commercialization of the technologies concerned.

4.3.1.6 OXFD

OXFORD contribution in TClouds project focuses on developing a trusted scheduler. The scheduler is directly beneficial for IaaS cloud providers. This covers the area of managing the allocation of virtual machines at physical machines by considering both user requirements and infrastructure properties. Currently, the main obstacles for adopting clouds by critical infrastructure and critical applications are the lack of trust in the cloud infrastructure. Our scheduler establishes one of the foundations for addressing such a key requirement. This is by considering user requirements which includes privacy and security attributes when allocating resources. Within TClouds project we focused on addressing the issues of restricting users who share physical resources with anther users. We also focused on enforcing restrictions on the geographical location where a user data could be stored and processed. In addition, we provided an implementation of the remote attestation principle at the cloud infrastructure. The remote attestation ensures that only trusted physical servers could host users' virtual machines.

In addition, to the developed scheduler we proposed a set of integrated frameworks which help in establishing trust in the cloud. The heart of the frameworks is the proposed scheduler.

Our frameworks were published on top journals in their field. We have been recently contacted by Sophos research lab, as they show an interest in these frameworks and they wanted to establish a research links to extend the work. Specifically, Sophos are currently working on developing a Cloud SaaS for their customers, and they wanted to understand how TClouds results could help them in establishing trust in their products and infrastructure.

The competition in the cloud market is enormous and competing providers fight for customers with more and more features. As of today, no cloud provider has installed similar measures to enhance the customer's trust by providing proofs of running software and isolated environments. We have contacted the executive director of OpenStack and discussed with him TClouds results. He showed an interest in this and invited us to their architecture board meeting which is held twice a year: in April and October. We plan to contribute to the October architecture board and introduce TClouds result. We decided to go for the October one as it will be held in London which would save travelling costs (the other would be held in the United States).

In addition to the above, we have developed an MSc module which partially covers TClouds result. The course is attended by industrial professionals, which would help in disseminating the TClouds project results within the industry.

4.3.1.7 PHI

The main result that Philips expects from the project is to build a trustworthy platform to host various healthcare service applications towards Philips customers. This platform will be deployed at PaaS and SaaS cloud levels, based on the TClouds IaaS clouds (or PaaS cloud-of-clouds). The results have the potential to be exploited commercially to offer health and well-being services for Philips. This platform offers accessibilities and management capabilities towards end users as well as third party application developers. Trustworthiness shall be guaranteed by integrating TClouds results of security, privacy, and resilience components. The platform also allows for sharing of users' data across different apps, or with their social contacts.

Many European stakeholders, both providers and customers, can profit from the exploitation of the TClouds results from a business perspective. Besides, the TClouds results can bring a positive impact to the European economy. Philips Research Europe is a leading research institute in healthcare and wellness technologies.. Technologies are transferred on a yearly basis from Philips Research to Philips business units, and hence European customers directly benefit from such innovation results.

The exploitation phase is already in progress on behalf of Philips Research. Exploitation of TClouds results start within Philips before the project ends. As the first exploitation phase, the TClouds results will be exploited in Philips Research to facilitate faster pilot project development and testing. At a later stage, there are potential opportunities to exploit the results into Philips Healthcare business units.

To bring the project results to customers, at the end of TClouds, we foresee that the primary beneficiaries will be within Philips Research and eventually Philips B2B or B2C customers. Possible operating models can allow faster development and deployment of pilot projects and product by using the security and resilient features offered by the TClouds healthcare platform and the cloud infrastructure. As stated above, there will be no direct commercial solution to our business units at the end of the project.

From today's perspective, potential obstacles for a successful exploitation mainly lie in the mistrust in the public cloud, as well as the cross border legislation compliance. Healthcare systems are mostly hosted in private legacy networks. The use of cloud computing, especially public cloud, is still in its experimental phase. Finding the most suitable business models for companies to exploit the TClouds results is a challenge.

The above-mentioned technology resulting from TClouds addresses concrete customer needs to provide various healthcare services to our customers, either being healthcare

institutes or end customers. Its success can be measured financially. IBM's marketing and sales departments have already been involved in the projects descending directly from the Healthcare TPaaS solution. Product management is involved in all phases of exploiting Healthcare TPaaS.

Furthermore, Philips Research actively participates in the dissemination of TClouds' results. In addition to publishing scientific papers at relevant conferences and speaking at industry-leadership events, Philips Research promotes the results of TClouds to our business units and customers at meetings and internal or external exhibitions.

Philips Research benefits from the exchange of information with other TClouds partners, especially on legislative analysis and cloud infrastructure development. Philips Research has been involved in many EU projects and benefited from collaboration of such projects in similar domains. An incomplete list, covering past and future EU-funded projects includes: FP7-ENSURE, FP7-UNIVERsal, FP7-CO-LIVING, FP6-ANGEL, FP6-SPEED, etc. A good cooperation and interaction with other partners forms a solid foundation for future collaborations and projects in related fields.

From the scientific and technical prospect of success, general technological progress has positive impacts on the exploitation scenarios. Our results from TClouds, in particular the trustworthy cloud based healthcare platform, will have an impact on improved healthcare services delivery and quality. Our TClouds medical platform will bring benefits to both end users and healthcare service providers.

Our results provide solutions to enhance global coverage and ubiquitous access in such a way that the health platform makes it easy for end users to share data with other service providers and access various applications deployed on the platform on the Internet scale. Compared with the current market offerings for cloud based healthcare solutions, the platform enforces security, privacy and resilience, and facilitates a trustworthy environment to allow end users to access the 3rd party healthcare applications. End users' personal data and their privacy rights are protected in compliance with the EU data protection legislation. Users are able to modify their security and privacy policies to permit particular service providers to access the whole or part of their data.

Our results also bring benefits for service providers such that compared to traditional healthcare IT services, the cloud based health platform brings advantages at lower infrastructure investment cost, and lower hardware and software maintenance cost. It also minimizes revenue loss from data center outage and network intrusion/failure with a reduced recovery time by making a resilient workflow execution and data storage affordable and easy to use. It offers reduced provisioning time and higher productivity, and allows for dynamic healthcare service composition, flexible business model and marketing strategy. This makes it easier for a provider to change the commercial partner if needed, without impacting the development process.

Besides the technical developments, non-technical developments such as legal and privacy aspects also impact the exploitation phase greatly. We consider EU legislation on data protection and privacy of utmost importance to provide a legal guideline to the technical development in TClouds. Regarding the healthcare use case, protection of users' privacy and personal data should be ensured at various levels of the developed cloud-based healthcare system, ranging from the IaaS, to PaaS and SaaS applications. Besides, cross-border transfer of cloud-based personal data is one of the main challenges to be identified. Our aim is to be compliant with EU legislation and to allow for cross border data exchange. We are working closely with legal experts in the TClouds consortium, and will continue the cooperation throughout the duration of project.

4.3.1.8 POL

We do not see any obstacle for the dissemination of research results: we think that European stakeholders can profit from research results through commercial products that incorporate

developed technologies, even though this is not the main focus of POL. Demonstration of research results could help Cloud Providers in finding potential security solutions for their infrastructures and improve their existing products.

Furthermore we think that our public contributions to the prototype Trustworthy OpenStack and in particular the contribution returned to the OSS communities of OpenStack and Libvirt can be of interest for the industry. The source code of the developed subsystems is available on POL's web site starting from the page: *http://security.polito.it/tclouds/*.

Research results are and will be exploited only in the education area. Indeed an important outcome of this research work is to allow students to acquire a more precise knowledge of security aspects of the Cloud Computing technology.

Moreover, in the education area, training material for students will be continuously updated by taking into account the most recent technologies, in particular the course in Computer Security. The main role of non-technical developments in education is that it will help students understand legal and business implications in the software design.

We have evidence that TClouds attracted both researchers and master students working on the topic security of Cloud Computing for the MSc program. However, we do not have yet evidence that the knowledge acquired by the students makes them more attractive for industry, whereas we expect that this will happen.

Commercial exploitation of these results, instead, has not been planned.

In terms of dissemination, we attended some workshops specifically focused on the security of Cloud Computing. For the moment TClouds has not increased so much our scientific production, since the major effort was spent on development and integration, but such an improvement is expected soon at the end of the project as we are working on papers that will be submitted at the end of the project.

As follow-up, we are investigating the possibility to cooperate with the partners beyond the end of the project and we and other partners have submitted a proposal for an EU-funded project that partially builds on the subsystems we developed in TClouds, that we hope will be positively evaluated..

4.3.1.9 SRX

As part of the TClouds project Sirrix AG will consolidate and expand its expertise in the field of cloud computing and in particular in the area of Infrastructure as a Service (IaaS). In the short term, Sirrix after a target group analysis and a demand analysis will bring components developed in TClouds into pilot phase projects at test customers and after successful evaluation into German/EU market. In the medium to long term, Sirrix will bring the project results into the development of new products.

In this context, our particular focus is on enhancements of the TrustedInfrastructures product line, especially by TrustedServer as an important component for the whole infrastructure. Customers have evinced first interest onto such a product.

The Sirrix TrustedObjects Manager (TOM), as the key element of TrustedInfrastructures, is extended with multi-client capabilities but is still a single point of failure because of the lack of high availability and fault tolerance, which shall be overcome with the results of the TClouds project. The high availability and fault tolerance of management components, the integration of security rules and the administration and enforcement in a distributed cloud infrastructure is in the focus of the knowledge and technology transfer between the project partners and Sirrix.

Sirrix will benefit from the exchange of information with partners from use-case scenarios about the usability of TrustedInfrastructures related components developed or enhanced in TClouds.

Exploiting the expected technology transfer, Sirrix will gain a technological advantage in the field of trusted systems and will transfer them into marketable products. In addition, strong synergistic effects on other company products are in sight. The good cooperation with partners in the project provides a solid foundation for further deeper cooperation in future projects. In addition, there is an intense cooperation with companies and research institutions in the EU and thus a lot of new opportunities and promising feedback from partners and customers which enable a seamless continuation of the project results in further projects.

After the end of the project, Sirrix will market the enhanced TOM, TrustedChannel components and the new TrustedServer component to existing customers of TrustedInfrastructures product line. Also Sirrix will have a Private Cloud business model that may be sold to a customer or operated by Sirrix. The S3 proxy component will be available as an optional security service for the TrustedServer and as a separate appliance for customers that do not need a full blown TrustedInfrastructure. 3rd parties (not participating in the project) may sell our TrustedInfrastructures as resellers or use technology to build secure Software as a Service products upon it or even sell it as Security as a Service.

From today's perspective the main obstacle is whether "Trusted Clouds" will be adopted by major public Cloud providers today and what the diversification between Trusted Clouds and commodity clouds will be like. However, as the TrustedInfrastructure technology can also be used for Private or Community Cloud infrastructure solutions for security sensitive customers we do not depend on the established Cloud providers to adapt such a trusted solution to their Cloud infrastructure. We see as a major driver of "Trusted Clouds", that the alertness of customers (SMEs) for security and privacy is significantly higher in the EU/Germany compared to the US where the major Cloud providers are located today. This gives a great opportunity for EU-based cloud providers offering TClouds technology. European providers and customers can profit from the results by enhancements to the Cloud infrastructures in data centers that now can be fully remote attestable when using Sirrix TrustedInfrastructures technology as developed during the project. Sirrix is addressing customer needs for controlling integrity of Cloud infrastructure components and also the information flow between such components.

The exploitation begins even before the end of the project. The first phase of the exploitation is a target group and demand analysis which is engaged by continuous feedback from our customers that we gain by elaborating the TClouds ideas in meetings and workshops. The second phase will be the marketing of new important components/features and enhancements of the TrustedInfrastructures series and to find potential pilot (test) customers. In the third phase one or more successful pilot projects have to be undertaken. In the last phase a diversified marketing is done and resellers have to be found to help to sell the products to customers in Germany and the EU.

Our product-management will be directly involved in the last phase of the project; marketing and sales departments have been involved since the second phase of the project (e.g. CeBIT 2012, CeBIT 2013, it-sa 2013), where we explain how the TrustedInfrastruce Cloud can extend our TrustedInfrastructure product line. Exploitation of intermediate results is already done during the project. Some results are adopted by the product teams to improve the Sirrix management component TOM, moreover we are in contact with potential pilot customers for TrustedServer

Sirrix have been participating as speakers in European (cyber) security related conferences (e.g. ISSE 2011 and European Smart Grid Cyber Security Conference 2012) where we disseminate TClouds' intermediate results and explain our expectations for the end results and what these can enable. The TClouds project has been well accepted by other participants who showed interest in our approach, especially in TrustedInfrastructures and TVDs.

Economical prospects of success

From Sirrix's point of view a quick market access can be guaranteed for TrustedInfrastructure Cloud by searching potential pilot customers in the area of the use-cases addressed in TClouds (smart grid and heath care) and get evaluation deployments ready in an early stage of the product already in prototype phase.

The development of cross-industry use-cases and the generalization of results are paramount to full exploitation of project results. In this regard, there is the need for further research funding to take adequate measures here.

Sirrix provides a trusted computing based infrastructure, so called TrustedInfrastructures, for cloud computing, consisting of the management component TOM, server component TrustedServer, a secure communication & management channel TrustedChannel and a cloud storage component, the S3 proxy. The infrastructure is filling the following security gaps of today's infrastructures:

I. Integrity of the infrastructure is ensured by Trusted Computing and attestable by remote attestation.

II. The infrastructure enforces the concept of Trusted Virtual Domains (TVDs) on the infrastructure to provide separation of tenants, transparent labeling and secure encryption of data, including legacy cloud services, e.g. cloud storage via the S3 proxy.

III. New trust model: The customer does not have to fully trust the cloud provider as this is the case today. The management is completely controlled by the trusted infrastructure via secure communication & management channels and there is no root account for cloud administrators on the servers.

The competitive projects and products worldwide that are comparable to Sirrix's solutions developed or enhanced in TClouds from a technically perspective are Cloud management frameworks like OpenStack, OpenNebula, Eucalyptus and Citrix OpenCloud Framework. From a commercial perspective these are infrastructure Cloud providers like Amazon Web Services or RackSpace and from a product's perspective there are competitive products to build-up a Private Cloud, such as VMware vCloud and Citrix CloudStack.

The Sirrix TrustedInfrastructure related components developed within TClouds cover all the major parts of an infrastructure cloud: management, servers (computing) and storage (via S3 proxy) and secure communication channels. The interplay and seamless integration of all these components is crucial to provide a high level of security throughout the whole infrastructure.

The main novelty of the TrustedInfrastructure based cloud compared to today's offerings, such as Amazon Web Services, is the fundamental switch in the trust model. In today's offerings you need to completely trust the provider and its employees, especially the administrators to preserve confidentiality of your data. In a TrustedInfrastructure Cloud we established technical means to enforce this. Trusted Computing technology is employed to build up and manage a public key infrastructure to secure confidentiality and integrity of the infrastructure and provide means to attest this between communicating components of the infrastructure (e.g. management component and servers) and to the customers. All interfaces for remote management are controlled by the TrustedInfrastructure which replaces the practically almighty 'root' accounts for administrative tasks on today's cloud deployments.

The existing management frameworks (OpenStack, OpenNebula, Eucalyptus) focus on the infrastructure management. The management component TOM however, focuses on security management of the cloud infrastructure, e.g. providing and deploying a trusted computing based public key infrastructure into the cloud infrastructure. This is orthogonal to the features of existing frameworks. Within the project we aim to take the best of both worlds and combine the security management features of TOM with the infrastructure management capabilities of OpenStack.

Available products to build-up a Private Cloud, such as VMware vCloud, which build up trust on VMware vSphere software solution as the foundation of its infrastructure, are not able to implement Trusted Virtual Domains (TVDs) in an a consistently proactive approach, which is addressing threats by design and an adequate security architecture. TOM, TrustedChannel and TrustedServer focuses on a consistently proactive approach implementing TVDs, which means a proper isolation of virtual infrastructures (computing, networking and storage) by virtualization, encryption and VPN technology, all founded on trusted hardware anchors, such as TPM.

Scientific / technical prospect of success

In the fast moving Cloud market, technological-innovation is largely driven by the existing industrial players as well as some start-ups. In that context, general technological progress is often done through the successful introduction of a new service, a new product or a new technology.

In the advanced phase of a market development – such as the current stage of the Cloud market – this leads to a range of competing vendor or provider specific solutions.

The impact of this general technological progress on the one hand is minor, with respect to the technological development within TClouds, since there are unique features and novelty of the TrustedInfrastructure based cloud compared to today's offerings. On the other hand, the actual phase of market development is helping Cloud infrastructure services market penetration especially for Sirrix's main target group for Cloud Computing: SMEs.

Sirrix also sees the need for further research and is already engaging into the participation within follow-up R&D projects with EU and national funding. One major aspect is the integration of mobile devices into the TrustedInfrastructure Cloud to provide end-to-end security for the upcoming trend towards mobile devices and "Bring your own device" scenarios. Moreover, novel use cases scenarios for the general TrustedInfrastructure Cloud technology should be elaborated in further projects and our activities within the German Software Cluster.

4.3.1.10 TEC

The TCLOUDS project will reinforce and extend Technikon's knowledge in value co-creation with regard to secure Web services in a Cloud by extending the state-of-the-art in the field of collaboration software, defining the user requirements and projecting expectations to ensure high impact of future realization. Experience gained with service modelling will be funnelled into our industrial security services on requirement engineering. As an emerging SME, the reputation gained from the project is positively influencing our acquisition activities.

TEC will implement the TCLOUDS security concepts within its own infrastructure to run its Web-based collaboration tools and to deploy a private cloud scenario within its IT services. These will security harden and leverage our trusted server infrastructure (based on fully XEN virtualized TPM secured Linux SUSE instances) and create new business opportunities currently not being covered. Starting from the TPM checked Virtual machines we will extend our IT services by the cloud-of-cloud concept and further improve the security and availability of its running secure web services.

The TCLOUDS security concepts will be integrated into our infrastructure. Currently the majority of our trusted server customers are Industry. We plan to launch a new business line for providing our services to a larger number of SME costumers. The raised security, trustworthiness and higher reliability, justified by the outcome of the TCLOUDS project, are the essential pillars to establish this new service line. These three aspects are the main needs of any customer besides 24/7 support and regular maintenance.

Currently we provide our trusted server services as a package within our industrial services. The new scalability, raised security and reliability founded on the integration of the TClouds outcomes, allow us to think of additional models. Our focus is to charge a monthly flat rate for

the usage of our cloud services including some hours per month for support and to provide dedicated solutions for different business sectors. Lawyers and charted civil engineers are our first step focus. The success of our solution can then be measured by calculating the number of customers (companies or individuals), which are willing to work with and pay regularly (more than one year) for our service.

All current and future users of our IT services (currently more than 3.000 individuals) will benefit from the increased availability and security. Our business model depended heavily on our Internet connectivity. An Internet failure in southern Austria (9.5.2012 8:45-11:45 am local time) showed how vulnerable our services are. Our key selling point is the highly security hardened services we provide.

We implement the full chain of trusted computing developed together with HP and IBM in the Open Trusted Computing project. Combining both the TPM hardened services and the secure Cloud-of-Clouds concept of TCLOUDS, enable us to provide convincing arguments to sell and use our industrial collaboration services. These services are in prototyping phase and being tested. We believe that within one or two years of the project end we can go to full production phase.

The scientific prospects of success of TCLOUDS are not essentially relevant for TEC as a service SME. We are an early adopter of novel technologies and have benefited from integrating new security measures before they become common knowledge. We are using mainly open source modules and we do not have plans within TCLOUDS for a patent application.

In summary it can be said that we gained a lot of business momentum from our technical work within TClouds project. We are involved in several follow up projects dealing with the concept of securing cloud infrastructures and providing secure services. In the course of the TClouds project we hired 2 additional students and plan to sustainably bind them to the company. The strong collaboration with universities but also industry partners within the TClouds consortium was beneficial for our development in this field and yielded close cooperations beyond the TClouds project.

4.3.1.11   TUBS

As an academic partner, TU Braunschweig is mainly interested in research and teaching. Regarding both fields, the project TClouds was and is an invaluable opportunity for TU Braunschweig in general and the Distributed Systems working group of the IBR in particular to get closer to its ambitious goals, that is, pursuing cutting-edge research and provide students with the skills necessary for coping with present problems as well as with future ones.

Research

Publications at selected conferences and workshops shall raise the awareness not only about TU Braunschweig and the TClouds project but also about how tremendously important it is to solve dependability, security, and privacy issues in order to bring cloud computing to its full potential.

Two publications at and around the EuroSys 2012 conference, for instance, allowed us to be present at this distinguished event. It is one of the leading conferences in the field of operating systems and distributed systems, and cloud computing has been a major focus of it in recent years. Besides the presentation of results from the TClouds project, attending conferences like the EuroSys 2012 and workshops like the SDMCMM 2012 also gives the opportunity to meet other researchers as well as industrial representatives, and to discuss with them risks and potentials, problems and solutions arising around and within cloud computing. This way, we are able to get feedback on our current research, to draw inspiration for new research, and to explore possible co-operations, resulting perhaps in future projects.

Although conferences like the EuroSys are important to get in touch with the community around cloud computing, a diversified project like TClouds enables its partners to reach also a broader spectrum of communities. For example, TU Braunschweig had the pleasure to present some of its work carried out in the context of TClouds and TClouds itself at the SSS 2012. Despite being a conference about distributed systems in general and their more theoretical foundations, the project TClouds was already known by some of the attendees of the SSS. The dialogue with researchers who are not directly connected to cloud computing is almost as invaluable as the dialogue with people involved in more or less the same field of research. Discussions across boundaries help to change perspectives and thereby to obtain unforeseen ideas and solutions.

Even after the official end of the TClouds, TU Braunschweig will benefit from the knowhow and knowledge gained during the course of the project. For example, we submitted papers for workshops around the 2013 edition of the SOSP, one of the top conferences in the field of system software.

Publications are indispensable for an academic institution like TU Braunschweig to document achievements in ongoing research. However, the sustainability of developed approaches, concepts, and solutions can only be ensured if they are taken up, continued, and enhanced by follow-up projects. Therefore, research started with TClouds will not end with TClouds. Most of the subsystems developed in this project will be extended or at least further exploited in the future, for instance in form of dissertation of PhD students. Additionally, TU Braunschweig has been making huge efforts to participate in and/or even organize potential future projects. Up to now, two new project proposals directly connected to TClouds have been submitted. Among others, partners from TClouds are involved in both proposals. That way, the experience in organizing and running collaborative projects gained during the TClouds project can be optimally utilized. Further, started collaboration in terms of research can be deepened.

Teaching

No less important for the sustainable success of cloud computing is the introduction of students and beginner researchers to this relatively young technology. Therefore, TU Braunschweig places great emphasis on teaching and plans to integrate the research conducted in the context of TClouds into lectures, seminars, and offered theses.

In fact, we developed a course that comprises a lecture and associated exercises and covers general topics about cloud computing as well as techniques, algorithms, and tools employed in this field. In practical exercises, students are taught how to use existing cloud services and how to develop their own ones. Some exercises are dedicated to dependability issues. Here, students learn techniques, among others, that are used in subsystems devised by TU Braunschweig within TClouds. Connecting general topics with current ongoing research belongs to the concept of this course. That way, interested students acquire the means necessary or at least helpful for preparing a thesis on a subject that belongs to these subsystems. This course has been offered three times so far and was overwhelmingly received by the students. Thus, we intend to continue and enhance it even beyond the end of TClouds.

Moreover, in the winter term of 2012, we developed and offered a practical course in which students could learn more about OpenStack, the default infrastructure platform chosen by the TClouds consortium. Besides getting a deeper insight into the existing components of OpenStack and their interaction, the participating students were assigned to implement some smaller extensions to the OpenStack platform, thereby improving their programming skills and enhancing the platform at the same time. As in the case of the more general lecture course, we will offer this practical course at regular intervals, although the specific subject may be changed. Due to the great reception of this practical course, it is planned to conduct it also in the winter term 2013.

Not least due to the offered courses regarding cloud computing, several students could be won over to conduct their thesis about one or the other subsystem developed in the context of TClouds. As a consequence, results obtained in TClouds inure to the benefit of the project itself as well as following projects.

4.3.1.12   TUDA

TUDA's work in the TClouds project focuses mainly on solutions to the problems of secure key-management and key-usage in IaaS clouds. This includes establishing trust in cloud infrastructures and VM images deployed thereon. Currently, there still is a large demand from a cloud customer's perspective as the contemporary cloud providers do not allow any insight in their infrastructure which hinders an establishment of trust. Our solutions allows the customer to gain certain trust in the infrastructure by knowing exactly that the hypervisor is a trusted and known version, that his VM images were not tampered with and that his keys are deployed and handled in a secure environment. Unfortunately, as of now the migration to a public cloud service provider would have meant to blindly trust its infrastructure to be secure and employees not to be malicious. CaaS is a step forward in that direction as it brings a transition from on-premise servers to public cloud service providers into reasonable and prospective light.

We focused on building the architecture that makes this transition possible and, being a research institution, our main goal is to disseminate the results among the research community in the form of scientific publications and the advancement of education. Potential financial exploitation is most likely expected through application of these results for improved consulting of and collaboration with industrial partners in the context of the Center for Advanced Security Research Darmstadt (CASED). Results of our research target foremost the cloud provider and aim at improving the trustworthiness of clouds and thus benefiting the cloud customers to use cloud infrastructure more securely. Moreover, based on these results we developed collaboration with Amazon Web Services LLC that will allow us to further investigate adoption of such a system in public clouds. The research results of CaaS are publicly available to everyone. Not only did we publish scientific papers in international renowned, peer-reviewed proceedings of security conferences but we also made the source code publicly available for everybody to assess the progress and contribution. This puts European and world-wide stakeholders in the position to use our prototype for evaluation or even build upon our code base which drastically minimizes set-up costs as we have made the technology readily available. We foresee a future in which CaaS has laid the ground for building advanced infrastructures or even commercial products based on a secure VM and key deployment which customers can trust.

The positive influence of the project on education can help preparing students for industrial work in the area of cloud computing and thus indirectly benefit the stakeholders. Courses are promoted to students at the Technical University of Darmstadt and in the context of CASED also to students at the University of Applied Sciences Darmstadt. Results are already incorporated in education in the form of lecture content, labs, seminars and summer schools. The success can already be measured by the increasing interest in the topic and subsequent theses. Moreover, one of our scientific publications was covered by many press releases, giving us the opportunity to further increase the interest in the topic.

To sum up, we can state that TClouds had provided us with a lot of both technical knowledge and community opportunities. We have extended our research in cloud security aspects by being part of a new, already approved, EU project, called PRACTICE, that aims at establishing a secure cloud framework that allows advanced and practical cryptographic and security technologies to provide privacy guarantees for all parties involved in cloud-computing scenarios. The collaboration within TClouds with other universities and industry partners has been helpful in providing different perspectives that enriches our own.

4.3.1.13 ULD

ULD is the public authority competent for data protection in the German federal state Schleswig-Holstein. Our task in the TClouds project is the analysis of the legal foundation for cloud computing with focus on data protection and IT security laws.

The main results we expect from our work in the TClouds project are:

- A comprehensive legal analysis of cloud computing (EU-level);

- Identification of gaps and frictions in the current legal framework and specific suggestions to address these;

- Guidelines for a lawful cloud computing contract/SLA;

- Methodology for a future Data Protection Impact Assessment of cloud computing services.

We plan on using these results in our future research and policy work as well as influencing and fuelling our tasks of public authority such as consulting and enforcement.

1. *Policy and regulatory work*

   ULD actively takes part in policy and regulatory discussions at state, federal and European level. We contributed our findings of gaps in the current legal framework in the discussion of the future Data Protection Regulation at EU level. We also take part in the policy Working Group "Trusted Cloud" of the German Federal Ministry of Economics and Technology. The results of the legal research of TClouds have also contributed to the writing of regulatory guideline documents: the Article 29 Working Party Opinion on cloud computing and the German Orientierungshilfe Cloud Computing of the German Data Protection Agencies.

2. *Standardization*

   The research in the TClouds project enables us to take part in global standardization efforts. ULD hosted a workshop with several stakeholders and members of the German DIN institute to discuss and contribute to several ISO/IETF standard drafts such as the draft 27018 "Code of practice for data protection controls for public cloud computing services" and draft 29102 "Privacy Architecture Framework". Furthermore, we contribute the results of our legal analysis of complex internet-based architectures and Privacy Enhancing Technologies to the W3C Tracking Protection Working Group.

3. *Research*

   We already used and will further use the findings of the TClouds project for synergies with other internal and external research projects. Being part of the Advisory Board of the parallel EU project A4Cloud (Accountability For Cloud and Other Future Internet Services) we are able to pass on relevant results of the TClouds project to support further cloud research of the EU. Based on results of the TClouds project we also applied for the funding of a research project that enables an EU-wide cloud CERT (Computer Emergency Response Team).

4. *Consulting*

   The work of the TClouds research team provides synergies with the consulting departments of ULD. The basis for the work of ULD is laid down in the State Data Protection Act Schleswig-Holstein. This act is one of the most progressive ones worldwide and includes among others provisions on a seal of privacy for IT products and on privacy protection audits for public authorities. In addition to the privacy seal based on German national and regional law, ULD is coordinating the European Privacy Seal initiative EuroPriSe which grants privacy seals on the European level in case of a successful evaluation of compliance to European regulation. The results of

the legal analysis influence future audits of cloud services and architectures and the requirements for the EuroPriSe certification of cloud services.

5. *Enforcement*

   The results of the TClouds research will also be used to assess and evaluate the lawfulness of existing cloud solutions within the scope of our competences.

Apart from this very specific exploitation of the legal results we expect the technological progress of the TClouds project to enhance the state of the art in cloud security in the long term. To provide state-of-the-art IT security will be highly relevant to comply with Article 17 of 95/46/EC and future cyber security regulation.

4.3.1.14   INNOVA

INNOVA expects a rising market opportunity from commercial and public administration customers after the successful end of the project. As the various stakeholder questionnaires have shown, there is considerable interest in a Trustworthy Cloud offering. The market potential is growing further due to a generally raised awareness as a consequence of the revelations after June 2013 around secret service spy efforts in the U.S. and Europe. The market however demands clear and modular solutions. The user community established during our work for the D1.1.5 deliverable, constitutes a valuable user group, that we shall seek to actively engage further. To this respect INNOVA is considering further engaging the user community, for example with a specific panel and discussion group towards CPDP 2014 in Brussels. The conference organizers have already confirmed and reserved a slot for a re-edition of last year's successful TClouds panel. Details of this are being negotiated as of the time of this writing (beginning of Sep.2013). The panel will resemble the 2013 TClouds panel and represents thus as such a direct continuation of the TClouds efforts.

Also a more systematic user engagement is planned with the launch of a thematic social network empowered portal, that will constitute a venue for actively continuing the discussions and enable a continuous user feedback. For this the expertise of INNOVA in setting up such portal systems for instance for SME communities will be a valuable asset.

A specific section of the user portal will also host a series of multimedia items such as videos, webinars, and leaflets around TClouds topics for business scenarios.

Also the contacts with the Business/Venture capital community that have arisen after the successful TClouds workshops held in Spring 2013 at Oxford and Cambridge University represent a valuable chunk of the targeted user community. The following groups/institutions have shown interest so far in such a stakeholder platform:

- Amadeus Capital Partners Cambridge, founder Hermann Hauser
- Oxford Said Business school Professor Marc Ventresca
- INSME (Int. Association of SMEs)
- Forum-PA (largest special fair in Italy around Public Administration)
- Springboard Cambridge ideaAccelerator
- Stockholm University/DSV Security Lab
- Int. Entrepreneurship Academy
- Cambridge Computer Lab/Prof. Jon Crowcroft
- Peter Drucker Forum Vienna

As a follow-up we are also actively staying in touch with several partners for specific customer-initiated consulting and/or contracting work that is being requested by INNOVA

clients for the Italian market. The partners present in TClouds constitute a formidable partner network to tailor services and efforts, specifically tailored for different client scenarios.

 INNOVA is also working on the planning for a specific spin-off startup company to target the Trustworthy Cloud market in Italy and beyond.

Finally INNOVA is actively working on a publication that presents TClouds results in a whitepaper kind of form, to be distributed widely and also to be inserted into the CPDP 2014 conference participants' bag, thus ensuring wide dissemination of TClouds results and technologies.

4.4 Joint exploitation effort

With respect to exploitation at consortium level, the updated versions of D4.1.1 and D4.1.2 presented a joint exploitation plan that is based on 1) the modularity of the TClouds platform and 2) the "consumer versus (technology) provider" relationship between the project partners. Its goal is to integrate the TClouds technology into the selected use-cases of Activity3:

- **Modularity:** Different orthogonal subsystems, such as secure storage or resilience, have been identified and project partners work on different aspects of each subsystem. The technical deliverables resulting from Activity 2 of TClouds (D2.*.*) present the results. A declared goal for joint exploitation is to demonstrate how these subsystems fit together into an overall cloud infrastructure and we refer to deliverable D2.4.3 for information about the TClouds platform.

- **Integration into use-cases:** As stated above, different types of partners are involved in the project. As stated in D4.1.1 and in D4.1.2, a goal of joint exploitation is to show how the technologies developed in the TClouds project can be leveraged and integrated into applications – here Smart Lighting and Home Healthcare. In this sense, the industrial and academic partners take the role of technology providers for the SMEs. The final demonstrators of the project exhibit the demonstration applications running on the TClouds platform.

To this end, it was decided at consortium level (and with respect to the particular exploitation plans of each partner, see Section 4.3) that the best strategy for a joint exploitation is to ensure the sustainability of the jointly developed integrated Trustworthy OpenStack prototype beyond the end of the project. In particular in light of recent developments in the cloud market, where known international companies such as Intel[3], IBM[4], and PayPal[5] announced their support and choice of OpenStack, continuous integration of the TClouds components into a trustworthy cloud platform based on a widely used platform is expected to be the right choice for joint exploitation and to receive public attention.

Figure 9 illustrates the general idea of this approach. As stated above, the modularity of the TClouds Trustworthy OpenStack platform allows each partner to individually exploit his results and continue development of his components. However, as demonstrated by the TClouds integrated prototype at the end of the third project year, these single components are assembled into an integrated platform, which will act as a jointly exploited platform, publicly available.

---

[3] http://www.openstack.org/user-stories/intel/

[4]https://www-304.ibm.com/connections/blogs/59c1123b-0353-458e-a719-b002d84108d5/entry/ibm_announces_platinum_sponsorship_of_the_new_openstack_foundation?lang=en_us
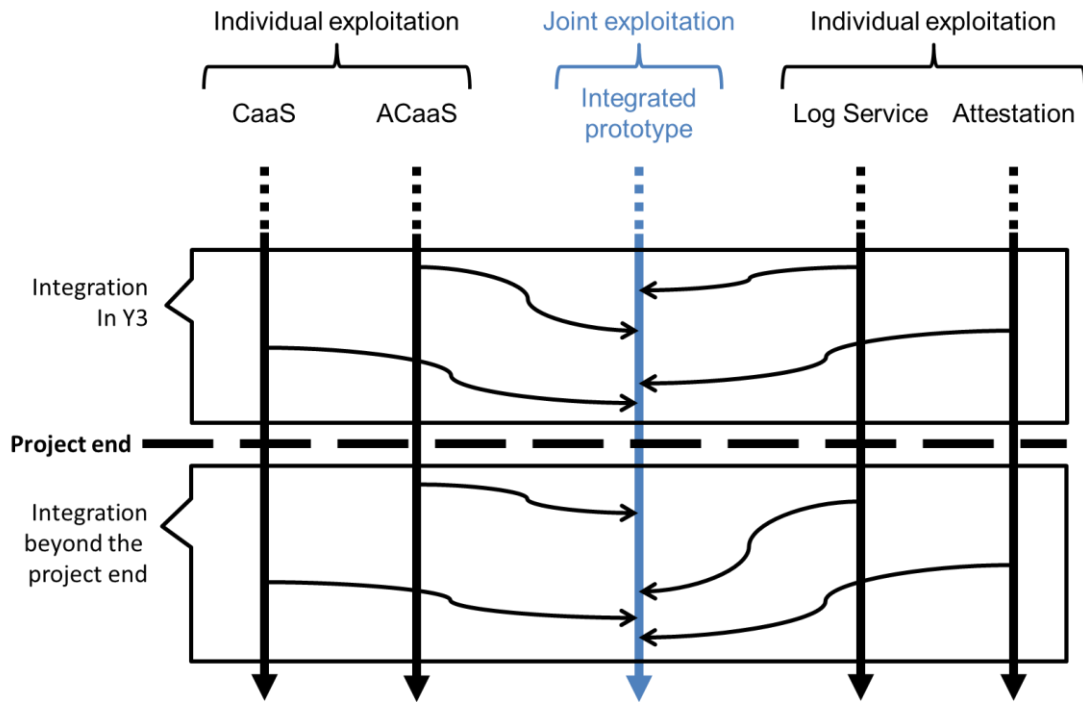
[5] http://www.openstack.org/user-stories/paypal/

Figure 9: Joint exploitation based on the Trusteworthy OpenStack components

Chapter 5

Training and Education

Chapter Authors:

Imad Abbadi (OXFD), Patricia Rio Branco (TEC)

5.1 Introduction

The aim of the education and training task in TClouds project is to support the wider cloud adoption by providing trustworthy knowledge of information in this domain. The task also aims to understand the training which was required by TClouds partners to perform their activities within the project. In the first year of the project, we started by a training and education survey amongst TClouds partners. The survey showed that good educational materials and course development would make a positive output for the TClouds project and ensure its continuity after the project lifetime.

There are a number of partner members in TClouds, which results in a possible diversification of the range of skills already acquired by the partners and those desired. In order to have a good understanding of the level of skills within the project and identify the gaps, one needs to look at every partner to identify their needs. The survey was conducted to understand partners' need. A template with sample questions was created and each partner was asked to provide answers to the questions in the survey and where necessary to indicate any gaps. The survey was also designed to collect information about the materials expected from the project and any plans of curriculum development based on the work from the project. The remaining part of this chapter covers the final outcome in the education and training task.

5.2 Training

This section summarises results from the survey regarding the amount of training that project members have received. Most training was carried along with the progress of the project. Mostly, it was in a form of self-training and learning. Project members acquired a certain level of skills with regard to the specific directions of the components they were in charge of. Listening to partners talks at project meetings helped sharing knowledge and inspiring innovation. Table 1 shows some of training topics delivered and received.

Topic	Description
OpenStack-based Clouds with KVM	Setting up the OpenStack-based Clouds with KVM
AWS	A description of Amazon Web Services and its features, architectures and interfaces.
Virtual Machine Security	A description of various aspects of Virtual Machine Security mechanisms, and urgent problems.
OpenStack	A description of OpenStack architecture and administration.

Table 8: Major training topics

5.3 Education

5.3.1 Course development

Oxford University runs an MSc in Software and Systems Security. This is a well-known and well-established program which targets part-time students. The majority of participating students comes from around the world and work in the industry. Oxford University, as a leader in the training and education task has decided to introduce a novel postgraduate module in Cloud security covering some of the outcome of TClouds project. The module was first run in Oct 2012 and then in April 2013. The student feedback was very positive and showed an interest in learning more about TClouds. In this section we briefly discuss the objectives and structure of the course.

5.3.2 Objectives

The successful participants of the Cloud security course will

- Be able to explain Cloud architecture, properties, management services, and security challenges.

- Understand security risks associated with different Clouds' deployment models, and what could be done to address such risks.

- Experience a real demonstration, provided by on building a simple Cloud using an appropriate management tool, managing it, and hosting a web-application on it.

5.3.3 Contents

The Cloud security is composed of the following main entities.

- Introduction: Cloud definition, models and types.

- Cloud Infrastructure Management: Cloud Taxonomy, Cloud management tools, and Infrastructure properties and policies.

- Secure Management of Cloud Infrastructure: virtual layer self-managed services, application layer self-managed service, and security best practices for automate Cloud infrastructure management.

- Cloud Trust Model: Cloud Dynamic Nature, Operational trust in the Cloud, Establishing trust in IaaS, PaaS, and SaaS Cloud types

- Security challenges related to data provenance: Forensic investigation in the Cloud, Fault detection and isolation in the Cloud, Billing in the Cloud

- Insider threats analysis and mitigation in the Cloud: discuss how to lessen the effects of insiders in the Cloud.

- Case Study on Home Healthcare using the above concepts

5.3.4 Requirements

Participants of the Cloud security course should have a basic understanding of computer security principles. They should also have a working knowledge of computer systems architecture and their network connectivity.

5.3.5 Educational Materials

Oxford University have prepared the education material based on various sources: industrial and academic. It also incorporates some of the TClouds project result as part of this course.

5.4 Additional educational knowledge generated within TClouds

The technical and scientific knowledge acquired during the project continued to be transferred into the education of students in Period 3. This was especially the responsibility of the academic partners in the project. In the following, we provide a brief overview of established courses (lectures, seminars, or practical courses) by the academic partners and also list currently on-going theses (B.Sc., M.Sc., PhD.) supervised by members of the project.

The following table outlines lectures, workshops, and courses organised or taught by project partners in Period 3:

Type of activities	Main leader	Title	Date	Place	Size of audience	Type and goal of the event	Countries addressed
Other	OXFD	Lecture: Cloud Security	22.10.2012	Oxford, UK	18	Part of Oxford University MSc in software and system security	International
Other	FAU	Lecture: Middleware/Cloud Computing	Ongoing, since Oct 2012	Erlangen, Germany	25	Lecture with integrated practical exercises	National
Workshop	IBM	Presentation at Workshop on Computing Systems	08.01.2013	Cambridge, UK	80	Academic workshop with prominent participants	International
Other	ULD	Lecture at privtech12, Privacy Enhancing Technologies (PET) PhD Course, "Top Mistakes in System Design from a Privacy Perspective", http://www.csc.kth.se/~buc/PPC/	29.01.2013	Gothenburg, Sweden	40	privtech12, Privacy Enhancing Technologies (PET) PhD Course, Lecture by Marit Hansen	International
Other	TUBS	Practical course: Practical Cloud Computing	01.02.2013	Braunschweig, Germany	10	Practical experiences with infrastructure cloud systems	National
Other	IBM	Lecture at ETHZ: Security and Fault-tolerance in Distributed Systems	Feb.-Jun. 2013	Zurich, Switzerland	20	Lecture	National
Other	ULD	Lecture at University of Kiel by Marit Hansen (ULD) "Datenschutz und Technik I – Datenschutzfördernde Technik" (Privacy-enhancing technology)	24.04.2013	Kiel, Germany	20	Lecture by Marit Hansen	National
Other	TUBS	Lecture: Cloud Computing	13.07.2013	Braunschweig, Germany	60	Lecture with integrated practical exercises	National
Other	TUBS	Practical course: Software Developement Practical: The VisibleCloud	13.07.2013	Braunschweig, Germany	10	Implementing a mobile cloud middleware on basis of OpenStack	National

Table 9: List of educational activities in terms of lectures, workshops and courses

Table 11 lists all academic theses started from Period 3:

Type of activities	Main leader	Title	Date	Place	Size of audience	Type and goal of the event	Countries addressed
Theses	TUBS	Development and Evaluation of a Customizeable, Memcached-Compatible Caching Service Implemented in Haskell	October, 2012	Braunschweig, Germany	/	Bachelor-Theses	International
Theses	TUBS	Transformation von Workflows zur deterministischen Ausführung am Beispiel BPEL	23.11.2012	Braunschweig, Germany	/		National
Theses	POL	The logging problem in cloud environment - Openstack Cloud Logging (M.Sc.)	30.11.2012	Torino, Italy	/	Thesis on cloud computing. The thesis started in December 2011.	National
Theses	TUBS	Entwicklung und Evaluation eines erweiterbaren Koordinierungsdienstes zur adaptiven Konfiguration von Cloud-Infrastrukturen	12.12.2012		/		National
Theses	POL	Security of virtual machines in cloud environment (M.Sc.)	29.03.2013	Torino, Italy	/	Thesis on cloud computing. The thesis started in January 2012.	National
Theses	POL	Remote attestation integration with OpenStack (M.Sc.)	29.03.2013	Torino, Italy	/	Thesis on trusted computing. The thesis started in January 2012.	National
Theses	TUBS	Entwicklung und Evaluation eines ressourceneffizienten Fehlertoleranzprotokolls mit rotierendem Anführer	April, 2013	Braunschweig, Germany	/	Bachelor-Theses	International
Theses	FFCUL	An AJAX-based Programming Framework for dealing with Untrusted Web Servers (M.Sc.)	30.07.2013	Lisbon, Portugal	/		National
Theses	POL	Attesting a complete Ubuntu distribution (M.Sc.)	30.09.2013	Torino, Italy	/	Thesis on trusted computing. The thesis started in January 2012.	National
Theses	POL	Security and Access Control in MapReduce (M.Sc.)	still ongoing	Torino, Italy	/	Thesis on cloud computing. The thesis	National

Type of activities	Main leader	Title	Date	Place	Size of audience	Type and goal of the event	Countries addressed
						started in May 2011.	
Theses	POL	Forensic analysis for cloud environments (M.Sc.)	still ongoing	Torino, Italy	/	Thesis on cloud computing. The thesis started in December 2011.	National
Theses	FFCUL	Cloud-of-Clouds State Machine Replication (Ph.D.)	still ongoing	Lisbon, Portugal	/		International
Theses	FFCUL	Secure Multi-Party Computations in the Clouds (Ph.D.)	still ongoing	Lisbon, Portugal	/		International
Theses	FFCUL	Intrusion-tolerant cloud management services (Ph.D.)	still ongoing	Lisbon, Portugal	/		International
Theses	FFCUL	Pragmatic Intrusion-Tolerant Database Replication (M.Sc.)	still ongoing	Lisbon, Portugal	/		International
Theses	FFCUL	A Fault-Tolerant SCADA Architecture (M. Sc.)	still ongoing	Lisbon, Portugal	/		International
Theses	FFCUL	Metadata and Locking Services in a Cloud-of-Clouds File System (M.Sc.)	still ongoing	Lisbon, Portugal	/		International
Theses	FFCUL	A virtual Disk Abstraction for a Cloud-of-Clouds File Syste (M.Sc.)	still ongoing	Lisbon, Portugal	/		International
Theses	FFCUL	Checkpointing and Recovery in Non-trivial BFT Services (M.Sc.)	still ongoing	Lisbon, Portugal	/		International
Theses	FFCUL	Cloud resource management for Intrusion-Tolerant service replicas (M.Sc.)	still ongoing	Lisbon, Portugal	/		International

Type of activities	Main leader	Title	Date	Place	Size of audience	Type and goal of the event	Countries addressed
Theses	FFCUL	Byzantine fault-tolerant Hadoop MadReduce (M.Sc.)	still ongoing	Lisbon, Portugal	/		International
Theses	FFCUL	Improvements on a State Machine Replication library (M.Sc.)	still ongoing	Lisbon, Portugal	/		International
Theses	FFCUL	SCADA in a Cloud-based Architecture (M.Sc.)	to be concluded in October 2013	Lisbon, Portugal	/		National
Theses	PHI	Security Solutions for Cloud-based Information Management Systems	08.10.2013	Eindhoven, The Netherlands	/		International

Table 10: List of educational activities in terms of theses