D4.1.1 – Version 2

Plan and Initial Report on Dissemination, Training, Standardisation and Exploitation

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 / D4.1.1 / 2.0
Activity and Work package contributing to the deliverable:	Activity 4 / WP 4.1
Due date:	March 2012 – M18
Actual submission date:	2nd April, 2012

Responsible organisation:	TUDA
Editor:	Sven Bugiel
Dissemination level:	Public
Revision:	2.0

Abstract:	This deliverable reports on the progress and further plans of the project partner for their dissemination activities, standardisation and exploitation of project results, and project internal/external education and training. Overall, this document updates revision 1.0 of this document as submitted in M12 of the project.
Keywords:	Dissemination, Training, Standardisation, Exploitation

Editor

Sven Bugiel (TUDA)

Contributors

Elmar Husmann (IBM)

Cornelius Namiluko, Imad Abbadi (OXFD)

Norbert Schirmer (SRX)

Patricia Rio Branco, Martina Truskaller (TEC)

Ahmad-Reza Sadeghi (TUDA)

Disclaimer

This work was partially supported by the European Commission through the FP7-ICT program under project TClouds, number 257243.

Executive Summary

This deliverable reports on the progress of the project partners in terms of dissemination of the project, standardisation and exploitation of project results, and project internal/external training during the first year of the TClouds project. It further describes the planned future activities in those areas during the remainder of the project duration.

In particular, the deliverable documents the avenues to create impact for the project in the international cloud computing research and industry community:

- Scientific publications on high-quality, international conferences and the organisation of scientific events attracted well-renowned researchers in this area and provided scientific visibility.
- TClouds has positioned itself within the cloud standards landscapes and outlines potential contributions of the diverse working packages of the project to international standardization initiatives.
- Delivered and planned training and educational measures. The training occurred on the one hand project internally and tailored for the peculiarities of Activity 2 in order to achieve a common technological knowledge base among the project partners. And on the other hand project externally, e.g. within the education at the academic partners.
- An updated overview of the project partners' plan on exploitation is presented.

To further raise the public level of awareness of the project within the scientific and industrial communities, a diversity of dissemination activities have been impelled, including a project website with blog and twitter and presentations at international road shows such as CEBIT.

The following falls under the achievements and work towards the project goals of the first project year for disseminations and standardisation:

- 25 peer-reviewed scientific publications, including publications at flagship conferences such as ACM CCS and ESORICS or workshops such as CCSW.
- 3 organized events (workshops, summer schools) with an international audience and very good feedback as well as organization (or involvement in the organisation) of high-profile international events.
- 25 invited presentations and trade fairs including a presentation at CeBIT 2011.
- A thorough survey of standardisation opportunities and first contact with the related projects and standardisation bodies.

Updated version (March 2012)

Overall, this document updates D4.1.1 as submitted in M12 of the project. In particular, Chapter 1 and Chapter 3 were updated. Chapter 1 now contains an updated list of the peer-reviewed publications by the project partners. Chapter 3 was supplemented with a joint exploitation plan of the partners in Section 3.3, which illustrates shared efforts and collaboration by the project partners towards realizing certain security services in cloud infrastructures. Additionally, Chapter 3 contains now a preliminary market analysis (Section 3.2.2) by the partners in order to provide a first evaluation of the market chances of the services and components developed within the TClouds project. A thorough market analysis will be provided in deliverable D4.1.2 at the end of the second project year.

Contents

List of Figures

List of Tables

Chapter 1

Dissemination

Chapter Authors:

Sven Bugiel (TUDA), Martina Truskaller (TEC)

1.1 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 aims at creating this awareness, raising the public interest in the project, and promoting project results to potentially interested parties.

1.2 Dissemination Strategy

The dissemination strategy comprises four different methods, which are implemented in parallel:

1. **Purely academic research**
2. **Bringing together academic and industrial parties**
3. **Promoting results and ideas at EU level**
4. **Education**

These methods are realized through publications, cloud related events, and public relations.

1.2.1 Publications

To implement this strategy, the project and its results are disseminated by invited talks at conferences, by publications at renowned scientific and industry oriented conferences (such as ACM CCS, IEEE Security and Privacy, ESORICS, ISSE, or RSA) and in academic journals (e.g., IEEE Transactions), and by organising technical workshops within the project. In general, this establishes and fosters a strong European research community in which TClouds is positioned as a leading group in the relevant research areas. The industrial partners focus primarily on trade shows, commercial conferences and customer-oriented literature, thus fostering the cooperation between the TClouds project and industry.

1.2.2 Cloud related events

Workshops, seminars and summer schools, such as at Schloss Dagstuhl, are organized, where crucial issues may be scrutinised and investigated, the latest scientific and technological advances are discussed, and project results presented. Moreover, these workshops bring together interested parties from different areas such as practitioners,

cryptographers, and security experts and provide ideal points of collaboration with other European projects (e.g., ECRYPT II and CSC'11 Workshop in Zurich). Furthermore, summer schools and seminars provide training and education for PhD students as well as industry and help spreading the goals and ideas of the TClouds project.

1.2.3 Public relations

Additionally, a web server and a web-site has been installed, where the consortium members supply information to external stakeholders. Partners with access to special on-line forums post articles, news, and other information about TClouds there. A Blog on the project website and an additional Twitter account, which automatically announces new Blog posts, provide the means to better disseminate new results and news. Setting up a common project design, such as a TClouds logo, templates for documents and presentations further improves the dissemination. Designing the project information material (such as a leaflet and an introductory off-the-shelf presentation), which can be distributed later on without greater effort being invested.

Other suitable means for online dissemination will be examined, and the necessary infrastructure will be set-up and maintained during the project and beyond. This activity may include web forums, blogs, newsletters or news feeds, etc.

1.3 Dissemination Activities

We now present our dissemination activities in order to document the extent to which we have executed our strategy documented in Section 1.2.

1.3.1 Upcoming and planned activities

Name/Kind	Data & place (if available)	Remark
CCSW 2011 - ACM Cloud Computing Security Work-shop	21.10.2011, Chicago USA	Most prestigious scientific venue for cloud-security research, co-organized by ACM and TClouds members
Summer School on Wireless and Mobile Security	31.10.2011 – 05.11.2011, Bertinoro, Italy	Summer school co-organized by TUDA, including invited lectures on "mobile cloud security"
IBM Cloud Computing Symposium	28.11.2011-30.11.2011, Darmstadt, Germany	Co-organized and invited talk by partner TUDA
Dagstuhl Seminar 11491: Secure Computing in the Cloud	04.-09.12.2011, Schloss Dagstuhl, Germany	Seminar for academic and industrial interested

Name/Kind	Data & place (if available)	Remark
CSA[1] Cloud Symposium	16.-17.11.2011, Orlando, USA	Invited talk by partner TUDA
Dagstuhl Seminar 11511: Privacy and Security in Smart Energy Grids	18.-21.12.2011, Schloss Dagstuhl, Germany	Seminar for academic and industrial interested
Cloud Security Conference	April 2011	Workshop with industrial partners, project partners, and invited experts; other co-organizers are ENISA[2] and CSA
Dagstuhl Seminar 12-0111: Security and Dependability for Federated Cloud Infrastructures	9.-13.7.2012, Schloss Dagstuhl, Germany	Seminar for academic and industrial interested

Table 1: List of upcoming and planned dissemination activities

1.3.2 Past Activities

A number of dissemination activities already took place and are listed in the chapters below.

1.3.2.1 Organized conferences

Name	Date & place	Remarks
Workshop on Cryptography and Security in Clouds (CSC'11)	15.-16.3.2011, Zurich, Switzerland	Organized in cooperation with EC-funded NoE ECRYPT II
5th Workshop on Recent Advances in Intrusion-Tolerant Systems – WRAITS 2011	27.6.2011, Hong Kong, China	Organized in cooperation with BBN Technologies, USA
ETISS'11 - European Trusted Infrastructure Summer School	19.-24.09.2011, Darmstadt, Germany	Summer school organized by partner TUDA; includes lectures and classes on security in Cloud computing

Table 2: List of organized conferences/workshops

[1] CSA: Cloud Security Alliance (https://cloudsecurityalliance.org)

[2] ENISA: European Network and Information Security Agency (http://www.enisa.europa.eu)

1.3.2.2 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.

Publication title	Conference/Workshop/Journal	Authors
The Trusted Platform Agent	IEEE Software (Special issue on Software Protection), 8 (2): 35-41, 2011	Giovanni Cabiddu, Emanuele Cesena, Roberto Sassu, Davide Vernizzi, Gianluca Ramunno, Antonio Lioy
Trustworthy Clouds underpinning the Future Internet	Future Internet Assembly, pages 209-221, Springer-Verlag, Lecture Notes on Computer Science (LNCS) 6656, 2011	Rüdiger Glott, Elmar Husmann, Ahmad-Reza Sadeghi, Matthias Schunter
TClouds – Privacy meets Innovation	Journal Symposia, 1/2011: 39-42, 2011	Marit Hansen, Eva Schlehahn, March 2011
Cloud Computing und Safe Harbor	Datenschutz und Datensicherheit, 05/2011: 311-316, 2011	Ninja Marnau, Eva Schlehahn
TClouds – Heraus-forderungen und erste Schritte zur sicheren und datenschutzkonformen Cloud	Datenschutz und Datensicherheit, 05/2011: 333-337, 2011	Ninja Marnau, Norbert Schirmer, Eva Schlehahn, Matthias Schunter
A Virtualization Assurance Language for Isolation and Deployment	2011 IEEE International Symposium on Policies for Distributed Systems and Networks (POLICY'11), IEEE Press, 2011	T. Gross, S. Bleikertz
Robust data sharing with key-value stores, in	30th ACM Symposium on Principles of Distributed Computing (PODC), ACM, 2011	C. Basescu, C. Cachin, I. Eyal, R. Haas, and M. Vukolic:
DepSky: Dependable and Secure Storage in a Cloud-of-Clouds	6th ACM SIGOPS/EuroSys European Systems Conference (EuroSys'11), ACM, 2011	Alysson Bessani, Miguel Correia, Bruno Quaresma, Fernando André, Paulo Sousa
Recursive Virtual Machines for Advanced Security Mechanisms	1st International Workshop on Dependability of Clouds, Data Centers and Virtual Computing Environments (DCDV'11), together with IEEE/IFIP DSN'11, IEEE, 2011	Bernhard Kauer, Paulo Verissimo, Alysson Bessani.

Publication title	Conference/Workshop/Journal	Authors
Verifying Trustworthiness of Virtual Appliances in Collaborative Environments	TRUST 2011 International Conference on Trust and Trustworthy Computing	Cornelius Namiluko, Jun Ho Huh and Andrew Martin
Toward Trustworthy Clouds' Internet Scale Critical Infrastructure	7th Information Security Practice and Experience Conference (ISPEC'11), Springer-Verlag, Berlin, Lecture Notes in Computer Science , 2011	Imad M. Abbadi
Challenges for Provenance in Cloud Computing	3rd USENIX Workshop on the Theory and Practice of Provenance (TaPP '11), USENIX Association, 2011	Imad Abbadi and John Lyle
Lucy in the Sky without Diamonds: Stealing Confidential Data in the Cloud	1st International Workshop on Dependability of Clouds, Data Centers and Virtual Computing Environments	M. Correia, F. Rocha
A home healthcare system in the cloud – addressing security and privacy challenges	IEEE International Conference on Cloud Computing (CLOUD'11), IEEE, 2011	I. Baroni, M. Deng, M. Nalin, M. Petkovic
Operational Trust in Clouds' Environment	Workshop on Management of Cloud Systems (MoCS'11), IEEE Computer Society, 2011	Imad Abbadi
Middleware Services at Cloud Application Layer	Second International Workshop on Trust Management in P2P Systems (IWTMP2PS'11), 2011	Imad Abbadi
Clouds' Infrastructure Taxonomy, Properties, and Management Services	International workshop on Cloud Computing: Architecture, Algorithms and Applications (CloudComp'11), Springer-Verlag, LNCS , 2011	Imad Abbadi
Middleware Services at Cloud Virtual Layer	2nd International Workshop on Dependable Service-Oriented and Cloud computing (DSOC'11), IEEE, 2011	Imad Abbadi
Confidentiality and Privacy in the Final Frontier: Inside the Clouds	IEEE Computer , vol.44, no.9, pp.44-50, Sept. 2011	Francisco Rocha, Miguel Correia, Salvador Abreu
EBAWA: Efficient Byzantine Agreement for	12th IEEE International High Assurance Systems Engineering	Giuliana Santos Veronese, Miguel Correia, Alysson

Publication title	Conference/Workshop/Journal	Authors
Wide-Area Networks	Symposium (HASE'10), IEEE, 2010	Neves Bessani, Lau Cheuk Lung
Trustworthy Middleware Services in the Cloud	Third International Workshop on Cloud Data Management (CloudDB'11), ACM Press, 2011	Imad M. Abbadi, Mina Deng, Marco Nalin, Andrew Martin, Milan Petkovic, Ilaria Baroni, Alberto Sanna
AmazonIA: When Elasticity Snaps Back	18th ACM Conference on Computer and Communications Security (CCS'11), ACM, 2011	Sven Bugiel, Stefan Nürnberger, Thomas Pöppelmann, Ahmad-Reza Sadeghi, Thomas Schneider
TwinClouds: Secure Computation with Low Latency	Communications and Multimedia Security Conference (CMS'11), Springer, 2011	Sven Bugiel, Stefan Nürnberger, Ahmad-Reza Sadeghi, Thomas Schneider
On Scalability of Remote Attestation	6th ACM Workshop on Scalable Trusted Computing (STC'11), ACM, 2011	Emanuele Cesena, Gianluca Ramunno, Roberto Sassu, Davide Vernizzi, Antonio Lioy
A unified ontology for the Virtualization domain	1st International Symposium on Secure Virtual Infrastructures (DOA-SVI'11), Springer, 2011	Jacopo Silvestro, Daniele Canavese, Emanuele Cesena, Paolo Smiraglia
Secure Virtual Layer Management of the Clouds	10th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom-11), IEEE, 2011	Imad Abbadi, Muntaha Alawneh, Andrew Martin

Table 3: List of scientific peer-reviewed publications

1.3.2.3 List of non-peer-reviewed publications

The following table supplements the list from Section 1.3.2.2 with publications that were not peer-reviewed but contributed to the dissemination of the project.

Publication title	Conference/Workshop/Journal	Authors
Robust data sharing with key-value stores	Proceedings of the 30th ACM Symposium on Principles of Distributed Computing (PODC), ACM, June 2011.	C. Basescu, C. Cachin, I. Eyal, R. Haas, and M. Vukolic, June 2011

Publication title	Conference/Workshop/Journal	Authors
SMART GRID CYBER SECURITY ROADMAP	The 21st International Conference and Exhibition on Electricity Distribution (CIRED'11)	Miguel Areias
A home healthcare system in the cloud – addressing security and privacy challenges	Proceedings of the 4th International Conference on Cloud Computing (IEEE CLOUD'11)	Partners HSR and PHI
From Trusted Cloud Infrastructures to Trustworthy Cloud Services	Information Security Solutions Europe (ISSE 2011)	Norbert Schirmer and Michael Gröne
Typing a core binary field arithmetic in a light logic	Foundational and Practical Aspects of Resource Analysis (FOPARA'11)	Emanuele Cesena, Marco Pedicini, Luca Roversi
Trust in Clouds	Elsevier Information Security Technical Report	Imad Abbadi and Andrew Martin
Smart Power Metering in the Clouds	Smart Metering Industry Journal	Miguel Areias

Table 4: List of non-peer reviewed publications

1.3.2.4 Participated conferences

The following list provides an overview of talks and presentations given by partners at conferences and workshops, which contributed to the dissemination of the TClouds project. It does **not** include the mandatory presentations given by the authors of accepted (peer-reviewed) papers that were documented in Section 1.3.2.3.

Conference name	Date & place	Dissemination activity
ICT 2010	27.-29. 09.2010, Brussels, Belgium	Presentation of TClouds in the 2nd EffectsPlus Clustering Session (partner IBM)
Cloud Computing Forum 2010	21.-26.11.2010, Lisbon, Portugal	Dissemination of the project goals and approaches
1st ACM International Health Informatics Symposium – IHI 2010	11.-12.11.2010, Arlington, VA, USA	Propagated TClouds as possible solution to implement a secure e-Health Cloud infrastructure
Future Internet Assembly 2010	16.-17.12.2010, Ghent, Belgium	Presentation of TClouds at a cloud security workshop (partner IBM)

Conference name	Date & place	Dissemination activity
IBWAS'10 – 2nd OWASP Ibero-American Web Application Security conference	16.-17.12.2010, Lisbon, Portugal	Dissemination of the project goals and approaches
37th Conference on Current Trends in Theory and Practice of Computer Science (SOFSEM 2011)	24.01.2011, Novy Smokovec, Slovakia	Invited talk on "Integrity and Consistency for Untrusted Services"
CeBIT 2011	03.03.2011, Hannover, Germany	Talk by partner ULD
European American Business Council – Cloud Panel	08.-09.02.2011, Brussels, Belgium	Representing TClouds in a dialogue on EU-US cloud policy collaboration (partner IBM)
Cloudscape III	15.-16.03.2011, Brussels, Belgium	Panel Participation and TClouds Presentation in a workshop on cloud standardisation (partner IBM)
IBM Technical Expert Council – Technologieforum 2011	29.03.2011, Zurich, Switzerland	Presentation of Cloud security and the TClouds project to IBM customers
EffectPlus – 1st technical cluster meeting	29.-30.03.2011, Brussels, Belgium	Presentation of the TClouds project (partner TEC)
Workshop on Security and Privacy in Implantable Medical Devices	01.04.02011, Lausanne, Switzerland	Talk "From IMD to Cloud" by partners TUDA and PHI
Bird&Bird LawCamp	02.04.2011, Frankfurt, Germany	Talk by partner ULD on legal issues regarding the Cloud computing
II Fórum de Sistemas de Informação do Grupo José de Mello (2nd Workshop on Information Systems of José de Mello Corporation)	08.04.2011, Lisbon, Portugal	Partner EFACEC presented TClouds project and the Smart Lighting application; Partner FCUL gave a talk on Security in Clouds
EuroCloud Switzerland	13.04.2011, Zurich, Switzerland	Presentation of the TClouds project (partner IBM)
Workshop of German Data Protection Authorities on Cloud Computing	19.05.2011, Hannover, Germany	Talk by partner ULD

Conference name	Date & place	Dissemination activity
2nd Workshop on Software Services: Cloud Computing and Applications based on Software Services	6-9.06.2011, Timisoara, Romania	Presentation of TClouds
ASUT Seminar 2011 – Main event of Swiss Telco Association	09.06.2011, Bern, Switzerland	Presentation about Cloud security and the TClouds project (partner IBM)
CAST Workshop on SOA- and Cloud-Security	16.06.2011, Darmstadt, Germany	Talks by partners ULD and TUDA on technical and legal issues of Cloud computing security
Workshop on current and emerging challenges of eHealth	16.-17.06.2011, London, UK	Talks by partners PHI and ULD
EC workshop "Socio-economics in trustworthy ICT"	22.06.2011, Brussels, Belgium	Dissemination of the TClouds project by partner POL
conhIT (eHealth Congress)	04.07.2011, Berlin, Germany	Dissemination of the TClouds project by partner ULD
ULD Summer School	29.08.2011, Kiel, Germany	Talk by partner ULD on "Trustworthy Cloud Computing"

Table 5: List of participated conferences

1.3.2.5 Websites

The following table provides an overview of websites, established by the project partners, to disseminate TClouds and to provide additional, partner-specific information about their results.

Web-site	Description of the main TClouds related information
http://www.tclouds-project.eu/	The official web-site of the TClouds project.
http://www4.cs.fau.de/Research/TCLOUDS/	Project announcement on FAU website and annual report in order to improve public visibility.
http://www.comlab.ox.ac.uk/projects/TClouds/index.html	Local web presence. Oxford component of TClouds has its own web page, with pointer to the main

Web-site	Description of the main TClouds related information
	TClouds page.
http://www.zurich.ibm.com/csc/security/tclouds.html	Project announcement on IBM website.
http://twitter.com/tclouds_project	Twitter account for TClouds, to announce news about TClouds results or events.
http://www.trust.informatik.tu-darmstadt.de/projects/current-projects/tclouds/	TClouds project website of TU-DA with references to partners and main TClouds page.
http://www.sirrix.com/content/pages/tclouds_en.htm	TClouds project website of SRX with references to partners and main TClouds page.
http://security.polito.it/tclouds/	TClouds project website of POL with references to partners and main TClouds page.

Table 6: List of project-related websites

1.3.2.6 Press releases and newsletters

In the following, we provide an overview of press releases and entries in various newsletters (known to us) which report about the TClouds project.

Title	Publication details (journal, newspaper, web, etc.)
IBM will die Cloud absichern	Press release (German): http://www.computerworld.ch/aktuell/news/52897/
Die “Regierungswolke" als EU-/IBM-Forschungsprojekt	Press release (German): http://www.inside-it.ch/frontend/insideit?_d=_article&site=ii&news.id=23231
IBM spearheads secure TClouds consortium	Press release (English): http://www.siliconrepublic.com/strategy/item/19164-cldctr2010/
Europäische Union startet Konsortium Advanced Cloud Computing Projekt mit Krankenhaus-und Smart-Power-Grid-Provider	Press release (English): http://technologeeko.com/de/european-union-consortium-launches-advanced-cloud-computing-project-with-hospital-and-smart-power-grid-provider/
TClouds – EU Konsortium startet zukunftsweisendes Cloud-Security-Projekt	Press release (English): http://www.pressetext.at/news/101124005/tclouds-eu-konsortium-startet-zukunftsweisendes-cloud-security-projekt/
European Union Consortium Launches Advanced Cloud Computing Project With Hospital and Smart Power Grid Provider	Press release (English): http://www.prnewswire.com/news-releases/european-union-consortium-launches-advanced-cloud-computing-project-with-hospital-and-smart-power-grid-provider-109929104.html

Title	Publication details (journal, newspaper, web, etc.)
European Union Funds Research Into Cloud Computing	Press release (English): http://www.pcworld.com/businesscenter/article/211290/eu_funds_technical_and_policy_research_into_cloud_computing.html
The TClouds project will hope to produce a highly secure cloud model	Press release (English): http://www.itpro.co.uk/628849/study-seeks-super-secure-cloud-computing-model
Ibm e San Raffaele nel progetto TClouds	Press release (Italian): http://www.lineaedp.it/articolo.php?aId=0000088218&cId=27&cpId=8&n=Ibm+e
Un nuovo consorzio dell'Unione Europea per la sicurezza del cloud	Press release (Italian): http://www.datamanager.it/news/cloud-computing/un-nuovo-consorzio-dellunione-europea-la-sicurezza-del-cloud
TClouds, la via europea alla sicurezza nella nuvola	Press release (Italian): http://www.01net.it/articoli/0,1254,3_ART_137794,00.html
Un nuovo progetto e un nuovo consorzio dell'Unione Europea per sviluppare soluzioni avanzate per la sicurezza del cloud computing	Press release (Italian): http://www.digitalnewschannel.com/comunicati-stampa/un-nuovo-progetto-e-un-nuovo-consorzio-dellunione-europea-per-sviluppare-soluzioni-avanzate-per-la-sicurezza-del-cloud-computing
Diagnosi e cloud computing al San Raffaele	Press release (Italian): http://www.businesspeople.it/Societa/Attualita/Diagnosi-e-cloud-computing-al-San-Raffaele-_12827
Un projet européen pour la sécurisation du cloud	Press release (French): http://www.lemondeinformatique.fr/actualites/lire-un-projet-europeen-pour-la-securisation-du-cloud-32213.html
Cloud: Bruxelles finance un énième projet autour de la sécurité	Press release (French): http://www.lemagit.fr/imprimer/securite-ibm-cloud-computing-bruxelles/7538/1/cloud-bruxelles-finance-enieme-projet-autour-securite/
TClouds - Projekt für datenschutzkonformes Cloud Computing gestartet	Press release (German): http://www.datenschutzzentrum.de/presse/20101129-tclouds.htm
Cloud Security: IBM and Hewlett-Packard make European moves	Press release (English): http://www.mspmentor.net/2010/11/29/cloud-security-ibm-and-hewlett-packard-make-european-moves/
EU consortium to trial health cloud	Press release (English): http://www.futuregov.asia/articles/2010/nov/29/hospital-cloud-tests-encourage-adoption/
European Union Funds Research Into Cloud Computing	Press release (English): http://www.pcworld.com/businesscenter/article/211290/eu_funds_technical_and_policy_research_into_cloud_computing.html

Title	Publication details (journal, newspaper, web, etc.)
IBM tests secure cloud on Portuguese electricity and Italian health	Press release (English): http://www.techeye.net/business/ibm-tests-secure-cloud-on-portuguese-electricity-and-italian-health
Auf dem Weg zur sichereren Cloud	Press release (German): http://www.channelpartner.de/channelcenter/cloud_computing/298540/

Table 7: List of project-related press releases and newsletters

1.3.2.7 Other dissemination activities

The following table lists dissemination activities that cannot be categorized in one of the aforementioned categories.

Category	Publication details (journal, newspaper, etc.)	Type (international/ national)
Leaflet/Logo	http://www.tclouds-project.eu/media/publications/TClouds-leaflet.pdf	International
Trade show	Represented TClouds project at CeBIT 2011 (at the CASED stand of TU-DA)	International
Industry Open Day	Poster on TClouds	National (UK)

Table 8: Other dissemination activities

1.3.2.1 Project Logo

In order to improve the visibility of the TClouds project, a logo has been designed. The logo is used on all internal templates as well as on all kinds of external dissemination tools.

Figure 1: TClouds Logo

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

Figure 2: TClouds Folder

1.3.3 Project Website

1.3.3.1 Public TClouds Website http://www.tclouds-project.eu

The official project website provides an overview of the project and up-to-date information on its activities and results, as well as contact details, partner information and information on events. The website is based on the Content Management System (CMS) "Joomla!", a webserver which provides the public website of the project and additionally restricted areas for members only. The website can be viewed with a standard web browser and will be kept alive throughout the project period and at least 3 years afterwards. The project website has been designed to be easily accessible and give an introduction to the project.

The TClouds project website is available on the following link: http://www.tclouds-project.eu

The official TClouds project website was launched on the 19th of November 2010 (M02) and has been updated continuously. The structure of the official part of the TClouds website is as follows:

TClouds Blog

- *Legal notices* (Disclaimer, Privacy and Legal notices)
- *News* (Blog entries categorized under News)
- *Press* (Blog entries categorized under Press)
- *Publications* (Blog entries categorized under Publications)
- *Events* (Blog entries categorized under Events)
- *The Cloud Market* (Blog entries categorized under The Cloud Market)

About Us

- *News* (news concerning the project activities (e.g. links/sites that disseminate project results; links to TClouds related events))
- *Strategy* (detailed structure of TClouds project activities)
- *Project* (general introduction to the project (project details))
- *Partners* (the consortium – logos of the partners and links to their websites)
- *Objectives* (the goals of the TClouds project)

Published Results

- *Publications* (publications by TClouds project partners (e.g. downloads: leaflet, articles, papers))

- *Public Deliverables*

Feedback

- A template for website visitors' feedback.

Restricted Area

- Login area for project internal use.

Workshops

- Workshop booking form targeting participants outside the TClouds consortium. It provides the organiser with essential information such place availability, participants' information, and time and date of booking.

Further pages can be added to the structure upon necessity. The website is continuously updated by the project Coordinator, whereas all partners participate in the process by notifying the Coordinator of important news and developments.

Figure 3 shows the front page of the official TClouds website which is the TClouds Blog. The TClouds Blog was created with the purpose of raising awareness of the project by means of a more dynamic interface in which consortium members are encouraged to be more active within the project. Its main goal is thus to reach a wider audience and improve the website's dissemination potential. Posts by partners are made more accessible and easy to read.

Messages posted under News, Press, Publications and Events are particularly relevant to the TClouds project whereas the section entitled "The Cloud Market" contains more general topics related to Cloud Computing.

Some of the functionalities of the blog include:

- Management of all blog entries (unpublish, edit, delete)
- Management and moderation of blog comments
- Creation of team blogs (group bloggers into specific team or groups)
- Creation of ACL (access control lists) which defines what a blogger is allowed to do in the system
- Creation and management of categories and tags

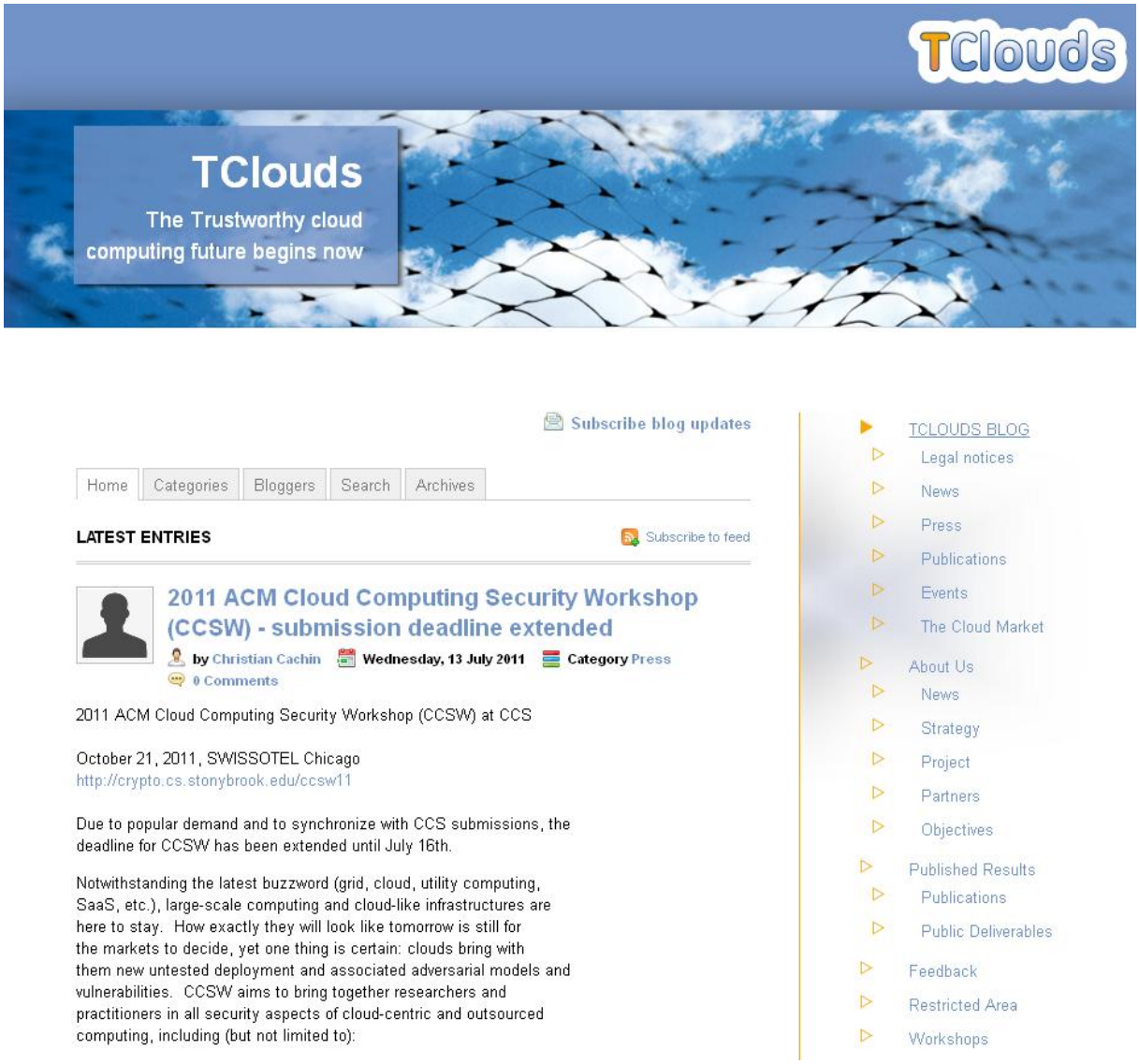

Figure 3: Front page of the TClouds website

The following illustration shows the “About Us” page of the TClouds website. The right side has a navigation slot, while on the left side the content of the respective section is given. The website can be best viewed with a standard web browser. The website will be kept alive throughout the project period and a few years afterwards.

Figure 4: Welcome page of the TClouds website

The project website serves as the most versatile information and communication tool because on the one hand it provides the opportunity to make information available for a worldwide audience and on the other hand it enables a comprehensive provision of information as well as a platform for the project team. So the website's structure aims to

provide both easily accessible basic information for external visitors and special information in more detail for registered users.
As mentioned above, the webpage provides the users with general information about the TClouds project, its activities and its achievements as well as background information, contact details and events. It informs the visitor about the project partners and by clicking on the name/logo of a partner the user can access the adequate homepage of the company. Furthermore, publications can be downloaded and useful links are given, which is illustrated in the following figure. Additional publications can be found in the blog category "Publications".

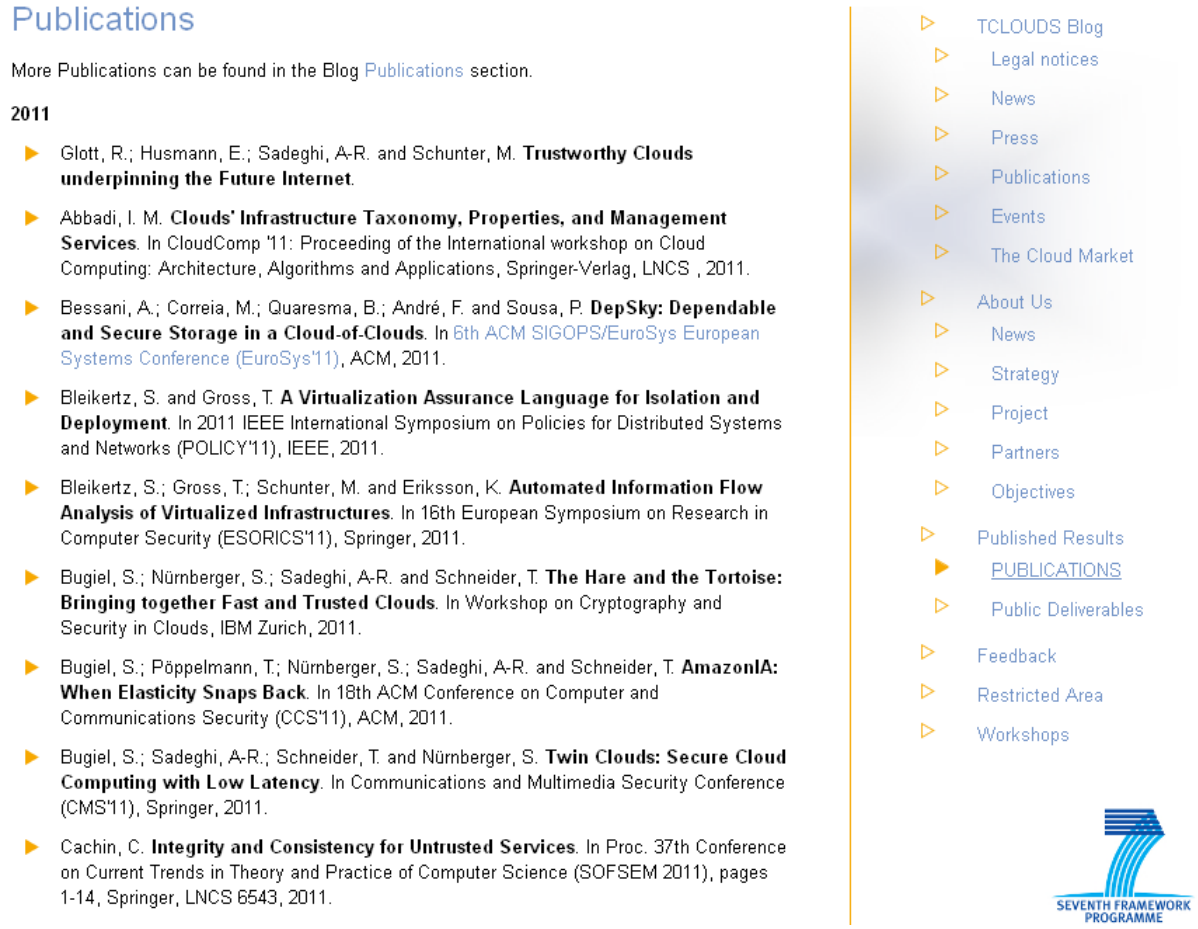

Figure 5: Publications page of the TClouds website

1.3.3.2 Restricted Area of TClouds Website

Parallel to the general accessible area there is a special domain on the TClouds website with password protected pages and thus made accessible to selected individuals and/or groups. In this way the website also serves as a platform of the project and may be used by the TClouds members for internal communication. Registered TClouds partners can use this special user menu and can benefit from the options offered there, e.g.:

- Calendar for appointments and meetings (mirrored from SVN),
- Forum for information exchange concerning special topics,
- Wiki function to post and to deal with some articles,
- Mailing lists for managing our project-internal mailing groups

Figure 6 illustrates the content of the restricted area.

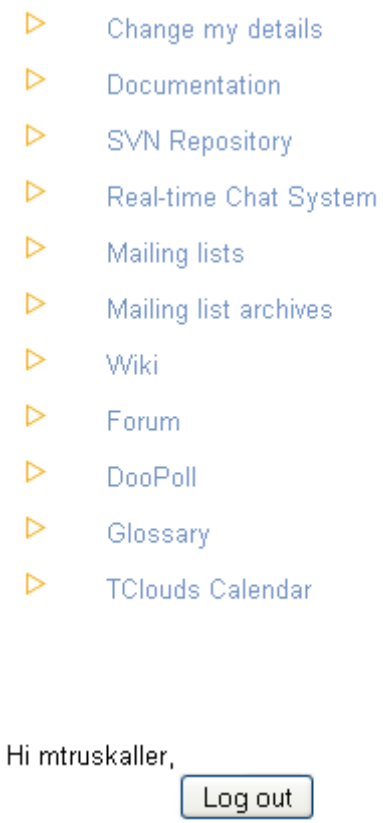

Figure 6: Content of restricted area

1.4 Cooperation with external organisations or other projects/programmes

Place	Type, content of the cooperation	Cooperation partners	Countries addressed (international/ national – which country)
Posecco EU contract IST-257129 www.posecco.eu	"Loose collaboration" with Posecco for the definition of an ontology for the virtualization domain	POL	International
Fraunhofer SIT, Darmstadt, Germany	Collaboration on security of Cloud storage	TUDA	National

Table 9: List of cooperation with external organisations or other projects/programmes

Chapter 2

Standardisation

Chapter Authors:

Elmar Husmann (IBM)

2.1 Introduction

This chapter provides an overview of the TClouds position and first activities in the area of standardization. Cloud computing aims at the industrialization of IT. As a consequence, standardization and interoperability in cloud computing are strategic topics for the industry. Several initiatives have started on this as well as relevant work from standardization organizations.

This chapter starts with an assessment of three different levels of cloud standards – technical, semantic and organizational – and then works out TClouds positions with regards to proprietary vendor solutions, emerging de-facto industry standards and open standards in the cloud space. In this context, the specific characteristics of open cloud standards are worked out as the primary target of TClouds participation.

Whereas the cloud standards landscape has already been well mapped by e.g. the http://cloud-standards.org, two standardization initiatives are highlighted here in particular – the US National Institute of Technology's "Standards Acceleration to Jumpstart Adoption of Cloud Computing" (SAJACC) and the "European Roadmap on Grid and Cloud Standards" (SIENA). TClouds is already in contact with both and has contributed to the SIENA roadmap.

The NIST initiative is particularly known for its working definition of cloud computing and taxonomy work (effectively being the first to formalize notions such as IaaS, PaaS and SaaS). In this context, a 1st area of TClouds standards contributions is suggested: a contribution to a refined taxonomy on security and privacy concerns in cloud computing. Further collaboration with Industry Alliances – such as the Open Data Center Alliance or the Cloud Security Alliance – is suggested in this context.

SIENA puts a specific emphasis on three cloud management standards – namely: the DMTF Open Virtualization Format (OVF), the SNIA Cloud Data Management Interface (CDMI) and the OGF Open Cloud Computing Interface (OCCI). A 2nd area of TClouds standards contribution is suggested towards adding security and privacy parameters to these standards.

Only to a limited degree assessed is a third area that relates directly to security standards rather than cloud management standards and their potential adaptation to the specific of cloud computing. One first relation has been established to the W3C in the area of user tracking protection.

Finally the document gives an overview on TClouds collaboration with Initiatives, Standards Organizations and other EU research projects that are relevant in the area of standardization.

This document is based on working sessions that have been conducted in the TClouds kick-off meeting (October 2010) and the TClouds technical workshops in Lisbon (January 2011) and Turin (May 2011) as well as on the described collaboration sessions and meetings with other initiatives, standards organizations and projects.

2.2 Cloud Standards categories – by interoperability level

The NESSI European Technology Platform on Software and Services has suggested the following categories of standards[3]. These apply well to the domain of cloud computing.

2.2.1 Technical Cloud Standards

Technical standards address interoperability at the technical level e.g. via specifying interfaces. Typical examples in cloud computing are APIs[4] that allow the automated access to specific service management capabilities of the cloud – such as e.g. for the launching of a virtual machine in an Infrastructure-as-a-Service (IaaS cloud).

Another example for a technical standard is a data format such as e.g. a virtual machine image format or a deployment description format.

Furthermore, important for TClouds are also technical cloud standards that allow propagating of monitoring information from a cloud provider as well as the selection of monitoring parameters and sources.

The application of technical standards may be described in *an architectural pattern* of a limited scale. In that context, the architecture pattern shows the prototypical interplay of technical standards, generic functional components and services.

A complementary way to describe the application of technical standards is via *use cases*. Here, the use case describes the application of one or multiple standards in the context of a typical service, a cloud user- or provider driven activity – e.g. the deployment of an enterprise application on an IaaS cloud.

A consistent technical standards contribution from TClouds would therefore need to include

- the reference to use case(s) and addressed requirements by the contribution,
- the architecture pattern(s) for the assumed implementation scenario and probably a description of a corresponding demonstration / reference testing implementation and
- the actual specification contribution to the standard.

2.2.2 Semantic Cloud Standards

Semantic standards provide a further level of abstraction. Typically they define relations and basic concepts in one domain (ontology). So they may actually be matched to different technical standards in order to implement the same concepts and relations. Semantic standards typically imply, apart from the ontology definition, a taxonomy definition – which is an agreed description of the terms that are used in the ontology.

[3] NESSI Position Paper on Standards, published by the NESSI Standardization Committee, 2010

[4] Application Programming Interfaces

A well-known example from the cloud domain is the NIST taxonomy of cloud services (that has coined the accepted notions of IaaS, PaaS, SaaS)[5] or the OpenCrowd Cloud Taxonomy[6].

Some work on cloud ontology has been suggested by researchers – such as in the UCSB/IBM "Toward a Unified Ontology of Cloud Computing" paper. Also relevant to this area is the work on *cloud reference architectures* as e.g. *by NIST*[7].

A consistent contribution from TClouds to the semantic standardization in cloud computing should concentrate on a taxonomy contribution in the domain of cloud security and privacy.

In return it is currently not suggested that TCloud would engage in the cloud reference architecture or cloud ontology discussion. Defining cloud reference architecture is a complex and multifaceted topic[8]. So this may better be addressed in dedicated architecture-oriented projects like in the Future Internet Core Platform Project (FI-Ware) that is starting in 2011.

As currently discussed in TClouds Activity 2, the architecture of the TClouds platform should rather allow to work with different cloud architectures and not impose too many requirements on the architectural side of the cloud providers, so that it may also more easily lead to exploitation in external cloud security and privacy services, software tools or hardware appliances.

2.2.3 Organizational Level Cloud Standards

Organizational level standards refer to management principles, organizational roles, processes and procedures. Typically the implementation of organizational level standards is linked to a process of certifying compliance to the particular standard.

As cloud computing is not only about specific technologies, but to a large extent about new service and business models, organizational level standards and certification will play a particularly important role. The adherence to technical standards – in particular the support of open standards – could become an element of the certification.

Certification may relate to the organization or services of a cloud provider. In that case, compliance to organization-level standards is either certified by an independent auditor or may also in some cases be self assessed and documented.

In addition to this, cloud providers may offer certification of their business partners and customers – e.g. consultants, administrators, solution architects or third party solution providers – to ensure adherence to organizational level standards across their business ecosystem.

It is questionable if TClouds can make a contribution on organization level cloud standards. An example of a related issue that is currently debated in the TClouds project is the risk of cloud insider fraud and the potential restriction mechanisms for access rights of cloud administrators. This of course has also an organizational dimension.

If TClouds would make a contribution on organizational level cloud standards, this is most likely to be expected by highlighting deficits in an existing organizational standard (such as a cloud or data-center administrative process) and by describing an alternative as a delta to an

[5] NIST Cloud Computing Taxonomy, Preliminary Draft, NIST CCRATWG - 007

[6] see http://cloudtaxonomy.opencrowd.com/

[7] http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/ReferenceArchitectureTaxonomy

[8] Already the previous attempts on defining reference architectures in SOA (service oriented architecture) are only partially been considered successful (such as e.g. the web services reference architecture)

established standard (e.g. in reference to well-accepted data-center management processes such as from the ITIL).

2.3 Cloud standards categories – by market position

2.3.1 Vendor or provider specific solutions (non standards)

In the fast moving ICT market, technological-, organizational- and service-innovation is largely driven by the existing industrial players as well as via entrepreneurial activities and start-up creation. In that context, standardization is often rather an afterthought after the successful introduction of a new service, product or technology.

In the early phase of a market development – such as the current stage of the cloud market – this is a typical phenomenon and leads to a range of competing vendor or provider specific solutions.

A solution that is specific to a single vendor or cloud provider and that has not been developed in a transparent process by a wider stakeholder group may hardly be regarded as a standard or a candidate for a standard as long as it has not been widely adopted within the market - regardless of the potential open access of the specification. In TClouds, these will be considered as vendor or provider specific solutions but not as standards. Contributions from the projects to such solutions will not fall under the category of standards contributions but would be considered as exploitation. The complexity of specific solutions by large providers can be seen at the example of the Google API and developer products overview table (http://code.google.com/intl/de/more/table/) that lists just the different families of APIs associated with the services of one provider (Google).

2.3.2 De-facto industry standards

The de-facto standards are a particular sub-type of the previous one. What separates a vendor or provider-specific solution from a de-facto standard is primarily the wider adoption by the market and the support from other providers and third party solutions. The process of creating de-facto standards by successful market players has always been important in the ICT domain.

A well-known example of an emerging de-facto standard in the IaaS cloud market is the set of Amazon Elastic Compute Cloud APIs. (http://docs.amazonwebservices.com/AWSEC2/latest/APIReference/). Still the cloud market is in an early stage of development – therefore it could be argued that it is not yet largely determined by de-facto standards.

It has been attempted several times in the past to turn a de-facto standard into an open standard (e.g. Microsoft has done so for their office documents de-facto standards with the Office Open XML specification[9]). However, this has mostly turned out to be a tricky process, in particular as the original vendor typically is continuing to dominate the further development of the standard and it is difficult to motivate additional parties to start contributing to it.

So it is clearly preferable to support in the emerging market of cloud computing – with its particular strong interoperability requirements – the current multi-vendor and multi stakeholder collaboration on open cloud standards instead of already supporting a particular vendor-specific standard.

[9] Office Open XML (http://en.wikipedia.org/wiki/Office_Open_XML) has been initially standardized in a fast-rack process by ECMA and was later accepted as an ISO standard

Nevertheless the support of de-facto standards may greatly enhance the practical applicability and exploitation of TClouds components. It is suggested that in the cases where the TClouds Activity 2 implements selected emerging de-facto standards (such as Amazon EC2 APIs) as part of the demonstrators or for testing purposes, these are first of all out of scope for TClouds standards contributions. Secondly, TClouds should ensure the parallel and alternative application of open standards for the same functionalities. This should be a general principle.

2.3.3 Open cloud standards

It is also important to agree on a definition of *open* cloud standards. The European Interoperability Framework has defined in 2004 open standards in the following way[10]. This is now a widely accepted definition in Europe[11]:

- The standard is adopted and will be maintained by a not-for-profit organisation, and its ongoing development occurs on the basis of an open decision-making procedure available to all interested parties (consensus or majority decision etc.).
- The standard has been published and the standard specification document is available either freely or at a nominal charge. It must be permissible to all to copy, distribute and use it for no fee or at a nominal fee.
- The intellectual property - i.e. patents possibly present - of (parts of) the standard is made irrevocably available on a royalty-free basis.
- There are no constraints on the re-use of the standard.

For cloud computing many providers have signed in early 2009 the Open Cloud Manifesto[12]. In the manifesto, several principles of *open clouds* are defined. The manifesto was drafted in view of the expected strong growth and competing technological developments in the cloud market. In particular, the manifesto is concerned with the questions on how to avoid vendor control or lock-in in the cloud market on the one hand while on the other hand ensuring that standards will “promote innovation and not inhibit it”. The following suggestions were made with regard to open cloud standards:

Close collaboration of standards organizations, advocacy groups, cloud providers and related communities – in particular to ensure that cloud standardization efforts:

- do not overlap
- do not “reinvent the wheel” but build instead on existing, industry accepted standards wherever possible. This also includes adjustments of existing ICT standards to the specifics of cloud computing
- “be judicious and pragmatic to avoid creating too many standards”
- be driven by and be verified against real customer requirements and not be merely developed by technical needs

These pragmatic goals imply the understanding that cloud computing is largely building on existing technologies and only add new technologies and functionalities in very specific parts.

[10] European Interoperability Framework for pan-European eGovernment Services, Version 1.0 (2004) ISBN 92-894-8389-X page 9

[11] Other definitions see: http://en.wikipedia.org/wiki/Open_standard

[12] *www.**opencloudmanifesto**.org*

For TClouds this further implies that useful standards contributions should be seen as contributions to the ongoing open cloud standardization development and not as “green field” developments. Hence, early alignment with organizations that are driving TClouds relevant open standards developments is essential.

In the following sections it will be described how we have approached this in the first 12 months of the TClouds project.

2.4 The role and process of standards organizations

Standards organizations are important in the development and maintenance of open standards – in particular as they are not-for-profit organizations and not linked to particular commercial interests. Therefore they can take a neutral role in moderating the contributions to specifying and maintaining a standard.

From a practical perspective, standards organizations are of course supported by specific industrial players and these also exert influence e.g. via roles they fulfil in workgroups or committees.

Hence it is important to assess how broad the industry support is behind a particular standards organization and which industry partners as well as other stakeholders would support a TClouds -contribution.

From a process perspective, standards organizations typically start with a formal definition of requirements and use cases and then apply several stages of creating a specification that include also phases of public validation and approving of the specification.

For that reason it is of particular importance to assess not only which standards and which related standards organizations are of interest for a contribution from TClouds, but also in which stage the particular standardization process is and what would be the most optimal timing for this alongside the project runtime.

2.5 Open cloud industry alliances

Open industry alliances play a complementary role to standard setting organizations. They usually do not engage in the development of standards but rather endorse and promote standards. They may also define more complex compliance requirements or quality standards. These typically imply multiple of the standards as discussed before.

The following organizations are of interest for cooperation with TClouds. Partially contacts have already been established:

The Open Data Center Alliance (ODCA)[13]

The ODCA was created in 2010 as an alliance to represent the IT customer side – in particular representing large-scale organizations such as BMW, Deutsche Bank or JPMorgan. A central output of the ODCA are cloud usage models in areas such as secure federation. ODCA usage models are vendor agnostic but provide requirements and recommend standards for purchasing decisions. It is of interest to match these against the requirements gathered through the TClouds Activity 1 process (such as focus groups and expert interviews).

[13] http://www.opendatacenteralliance.org/

The Cloud Security Alliance (CSA)[14]

The CSA is an alliance of cloud service and technology providers with a specific focus on security and privacy. The CSA is concerned with cloud security compliance audit standards (organization-level), certification and related training but also conducts further research on specific security, privacy and transparency aspects of cloud computing. In a similar way as the ODCA results this can be used to map against the TClouds Activity 1 requirements.

TClouds has met with the new EMEA Director of the CSA and is planning a workshop in May 2012 (co-organized with Activity 1) in the context of the "Cloud Security 2012" conference that the CSA is organizing in Frankfurt. Other partners in this event are Fraunhofer and ENISA.

As the Open Data Center Alliance has a preferred link to the CSA – TClouds is also planning to approach ODCA in the same context.

2.6 Cloud policy oriented initiatives

To make the picture complete, there are also cloud policy-oriented initiatives and organizations – with which TClouds is in contact.

NESSI, the Future Internet PPP and the xETP Group

The European Technology Platforms are representing the research agendas and research policy interests of the ICT industry. The Networked European Software and Services Initiative (NESSI) is in particular concerned with cloud computing. Several ICT Technology Platforms – including NESSI – have joined together in the xETP Group. This group is jointly promoting a research agenda on new Internet technologies. This includes also a support for related open standards. xETP can be important organizations to strategically promote TClouds research topics and standards for further development. The xETP Group has been at the origin of a wide research program called the Future Internet Public Private Partnership.

IBM is involved in the FI-Ware core platform project of the Future Internet PPP as leader of the IaaS domain and co-leader on security and privacy. This would allow potential collaboration with TClouds. But this will probably apply in a later stage of the project.

European American Business Council (EABC) – EU-US Cloud Computing Working group

The EABC has established a working-group that deals with issues such as cloud data governance and data privacy regulation. In particular they address the collaboration between the US and the EU. This also includes a collaboration with the US National Institute of Standards and Technologies (NIST) and the US Federal Government. TClouds has been invited to a cloud computing panel organized by the EABC that included US Industry players operating in Europe such as Microsoft and Verizon.

[14] https://cloudsecurityalliance.org/

European Cloud Strategy - Expert Group

This group focuses on a research roadmap for cloud computing and has published this in 2010 in "The Future of Cloud Computing" report[15]. TClouds has been invited to present the project in a workshop of the cloud expert group (28th September 2011)[16]. TClouds is further aiming to contribute to the update version of the report (planned for 2012).

ENISA – The European Network and Information Security Agency

ENISA published in 2009 their report: "Cloud Computing Risk Assessment"[17]. It is planned to release a second version of this report by 2012. TClouds is evaluating a contribution to this second report.

2.7 Potential standard contribution areas in TClouds

Cloud standardization is an emerging domain. A good overview on recent efforts is given e.g. by the Cloud Standards Wiki (http://cloud-standards.org/wiki/index.php?title=Main_Page). Also the NIST initiative SAJACC (Standards Acceleration to Jumpstart Adoption of Cloud Computing) should be mentioned in this context (http://www.nist.gov/itl/cloud/sajacc.cfm). In Europe, the SIENA initiative (www.sienainitiative.eu) is active in fostering cloud standards.

From what has been said before, it can be concluded that TClouds is addressing semantic standardization – primarily via the results of activity 1 and 3 and technical standardization via the related results of activity 2.

2.7.1 TClouds contribution area (out of Activity 1 and Activity 3): towards a refined taxonomy of security and privacy concerns in cloud computing

NIST is leading an already well-accepted effort on cloud taxonomy and has systematically defined many terms from the cloud-computing domain. Currently the NIST taxonomy (referred Version 1/10/2011) lists the following categories for cloud security services:

- Identity management
- Security policy management
- Authentication and Authorization
- Confidentiality and Privacy
- Security monitoring
- Auditing

From a first analysis of cloud security and privacy concerns that TClouds has submitted for publication to the European Future Internet Assembly Book 2011[18], it is already obvious that – whereas the above given categories are broad and not specific to clouds – in each of them specific cloud security and privacy challenges will apply. For example "multi-tenant isolation"

[15] http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf

[16] http://ec.europa.eu/information_society/events/ssai/ios2011/index_en.htm

[17] http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

[18] Glott R., Husmann E., Sadeghi A.-R., Schunter M., "Trustworthy Clouds Underpinning the Future Internet", to appear in: FIA Book 2011, Springer Publishing, 2011

is a sub concern of authentication and authorization that is of particular importance for IaaS cloud compute resource providers serving multiple customers from virtual machines running on the same shared physical hardware. “Data integrity” is another example of an important sub-category of “security monitoring” when it comes to cloud storage providers.

In other words a refined taxonomy of security and privacy concerns in cloud computing would help to map the cloud security and privacy problem space and assess technical solutions and use cases against it. In the Siena Cloudscape III workshop[19] on cloud standardization (March 2011) where TClouds presented its project goals and NIST as well as other standards organizations were present, particular interest was expressed in this area.

TClouds is applying a parallel deep investigation of two realistic industrial use cases (via Activity 3) as well as an investigation based on focus-groups and cloud-expert interviews (via Activity 1). The rigour of this methodology would provide a TClouds taxonomy contribution on cloud security and privacy concerns the necessary validity. From the initial discussion it seems that timing of this contribution will be a particularly critical issue.

Apart from a potential contribution to taxonomy standards, TClouds is also active in this context (as stated before) in the contribution to EU level reports on cloud computing – in particular:

- The 2nd version of the Cloud Expert Group Report
- The 2nd version of the ENISA Cloud Risk Assessment

2.7.2 TClouds contribution area (out of Activity 2): Including security and privacy relevant elements in technical cloud standards

At the early stage of the TClouds project it is still difficult to assess in which specific areas TClouds will be able to make contributions to technical standards at the level of cloud-providers. From the initial architectural discussion in Activity 2, two initial directions can be concluded:

- TClouds is interested to one extent in technologies that may add additional security and privacy protection in between the user and multiple IaaS cloud providers and that are controlled and applied by the user (or its intermediate security service provider) rather than the cloud provider. One example for this is data or computation integrity verification in combination with duplication to multiple cloud providers at the same time. This addresses e.g. issues of data restoration and business continuity after accidental corruption or external attack of a single cloud provider.
- TClouds is further interested in the mechanisms of trusted cloud federations (or cloud-of-clouds) of IaaS clouds. This would imply to propagate security relevant information in between cloud providers – e.g. information about geographical location constraints of data. Also, it would demand to propagate security relevant monitoring information in between providers at run-time and probably allow enforcement or remedial actions.

The first direction of research may relate to security standards (e.g. ANSI’s T10 DIF on data integrity) rather than to specific cloud standards. However in some of these, cloud services may pose new and currently not addressed challenges. A first contact has been established with the W3C working group on Web Tracking Protection.

In the TClouds Technical Workshop in Darmstadt (September 2011) it was agreed with the Activity 2 partners, that A2 will investigate the following standards with respect to their

[19] http://www.sienainitiative.eu/StaticPage/Cloudscape.aspx

application in the TClouds architecture. This will also include a gap analysis between the capabilities of the standard as-is and potential extensions that would be needed to cover functionality needed by TClouds.

An example for such an extension is the configuration of Trusted Virtual Domains in a deployment description standard like the OVF.

2.7.2.1 W3C – Web Tracking Protection

Tracking user behaviour through different means such as cookies, web beacons, ad-networks and specific tracking service providers has become a usual practice on the Internet. These practices constitute a substantial privacy concern for individual end-users. .

W3C has accepted in early 2011 a proposal to establish a tracking protection standard based on the technology that Microsoft uses for Internet Explorer 9. Protection from tracking of customer activity in the cloud or in federated clouds is a next evolutionary step. Requirements and technologies for such tracking protection for cloud services need to be discussed. Three key questions will be examined in this area:

(a) What protocols are used to opt out of tracking.

(b) What data are web-sites allowed to collect, store, process, and disclose once an individual has opted out of tracking.

(c) How can one ensure compliance by all sites.

The second direction relates directly to cloud management standards that enable cloud federation and external access to cloud management services.

In this context, the following technical standards are of interest to TClouds – corresponding also to the recommendations of the SIENA “Roadmap on Grid and Cloud Standards for e-Science and beyond” to which TClouds contributed a first view on its use cases.

2.7.2.2 SNIA – Cloud Data Management Interface (CDMI)

CDMI (http://cdmi.sniacloud.com/) is a SNIA architecture standard that was developed in the context of SNIA’s Cloud Storage Initiative (http://www.snia.org/forums/csi). CDMI allows tagging of data with specific metadata that may trigger automated services of the cloud provider (e.g. encryption).

CDMI introduces the notion of a container to allow access to and control of aggregated data. Services can then be specified for these data aggregates.

A joint white paper of SNIA and the Open Grid Forum (OGF)[20] explores how CDMI containers may be used as virtual disks attached to virtual machines in an IaaS cloud scenario. So effectively CDMI describes a mechanism to control virtual storage entities complementary to virtual machines.

2.7.2.3 DMTF – Open Virtualization Format (OVF)

OVF (http://www.dmtf.org/standards/ovf) is the core technical DMTF standard in the domain of virtualization management (VMAN). OVF allows the portability and deployment of virtual

[20] OGF and SNIA, “Cloud Storage for Cloud Computing”, Whitepaper, September 2009

appliances across multiple virtualization platforms. Virtual appliances may include multiple related virtual images. So it can be used to describe complex deployments. Other DMTF VMAN standards address complementary aspects of the management lifecycle of a virtualized environment – e.g. monitoring at run-time.

OVF provides an open standard alternative and additional functionalities beyond proprietary virtual machine image formats such as Amazon's AMI. OVF is supported by vendors such as VMware, Microsoft or Citrix. The EU project RESERVOIR has suggested a number of extensions to OVF to integrate IaaS cloud specific parameters – such as parameters on scalability or elasticity rules into the OVF deployment description.

2.7.2.4 OGF – Open Cloud Computing Interface (OCCI)

OCCI (http://occi-wg.org/) is an emerging standard by the OGF that has attracted a lot of interest by the cloud research community – also it is not yet widely commercially implemented. The open source cloud platform Open Nebula – that will be investigated in TClouds – also supports OCCI.

OCCI is a REST based interface standard and protocol for IaaS cloud management including deployment, scaling and monitoring. OCCI allows the execution of fundamental actions (such as create or delete) on entities (defined by linked resources) in an IaaS cloud. OCCI may be combined with OVF and CDMI as description standards for specific cloud entities. The OCCI interface specification has also largely been influenced from the RESERVOIR project.

2.7.3 TClouds contribution area (out of Activity 2): Contribution of security relevant additions to the Open Stack Open Source Cloud Framework.

Activity 2 has conducted in year 1 a detailed security analysis of Open Stack (D2.1.1). This has included the following parts of Open Stack (sub projects):

- NOVA – the basic cloud management components (similar to Amazon EC2)
- Swift – the cloud storage components (similar to Amazon EC3)
- Glance – the object storage for virtual machine images

TClouds has conducted an analysis against the following requirements: confidentiality, integrity, availability, authenticity, accountability and authorization. This has revealed a number of security shortcomings (see D2.1.1 for details).

It is planned to communicate these to the Open Stack project management and to start further to discuss potential contribution areas from TClouds. This shall happen already at the beginning of Year 2 – even though actual technical contributions are primarily expected by Year 3.

2.8 TClouds – initial collaborations on standards

Collaboration with the following organizations, initiatives and projects has been determined to be relevant in the context of the preliminary standardization plan of TClouds. Partially, these collaborations have already started. Relevant activities up to M12 are included in the overview below.

2.8.1 Collaborations with Standards Organizations

SNIA – Cloud Storage Initiative (http://www.snia.org/cloud)

DMTF – Cloud Standards Incubator (http://www.dmtf.org/standards/cloud)

NIST – Cloud Computing Program (http://www.nist.gov/itl/cloud/)

OGF – Open Cloud Computing Interface WG (www.occi-wg.org)

*OASIS – Identity in the Cloud (www.**oasis**-open.org/committees/**id-cloud**/)*

W3C – User Tracking Protection WG (http://www.w3.org/2011/tracking-protection/charter-draft.html)

ETSI – Standards in the Cloud (see http://www.etsi.org/WebSite/NewsandEvents/2011_09_STANDARDSINTHECLOUD.aspx)

Except for W3C. all these organizations were involved in the Cloudscape III workshop (March 2011)– TClouds was a sponsor of the workshop and represented on the cloud security panel.

NIST was also on the cloud panel of the EABC Workshop and W3C represented in the discussion with TClouds at the Cloud Expert Group.

With the OGF, TClouds is planning a presentation in an upcoming meeting of the ISOD-RG (Infrastructure Services) working group – at one of the next two OGF conferences in 2012.

IBM is also engaged – via the IBM Technical Relations Group – in the ETSI "Standards in the Cloud: a transatlantic mindshare" event (jointly conducted by ETSI and NIST). It is probable that ETSI will get a mandate from the European Commission to take the lead on European cloud standards collaboration. The contribution of TClouds in this context is yet to be explored.

2.8.2 Collaboration with Coordinating Initiatives

We now list coordinating activities and how TClouds contributed to each of them.

SIENA (http://www.sienainitiative.eu/)

European coordination initiative on cloud standards

TClouds panel participation in the Cloudscape III workshop (March 2011)

EFFECTSPLUS (http://www.effectsplus.eu/)

European coordination initiative on EU security and privacy research projects

TClouds panel participation in the 2nd Effectsplus Clustering Session at the ICT Conference (September 2010)

NESSI (http://www.nessi-europe.eu)

European Technology Platform on software and services – important industrial community

TClouds presented in the NESSI Steering Committee, current discussion about affiliation of TClouds as a strategic NESSI project

EUROPEAN FUTURE INTERNET INITIATIVE (http://www.future-internet.eu/)

European initiative on Internet related research

TClouds panel participation in the Future Internet Assembly in Ghent (December 2010)

IBM is a partner in the FI-WARE core platform project (*www.**fi**-ppp.eu/projects/**fi**-**ware**/*) leading the IaaS domain and co-leading on security.

EUROPEAN AMERICAN BUSINESS COUNCIL – EU-US Cloud Collaboration (http://www.eabc.org/)

TClouds represented in the cloud panel – at the EU-US Digital Economy Workshop (February 2011)

TClouds represented in the committee to draft a position paper on EU-US cloud collaboration

Open Grid Forum

Invitation to present TClouds in the OGF Infrastructure as a Service Workshop (September 2011, Lyon)

2.8.3 Collaboration with other Research Projects

RESERVOIR (www.reservoir-fp7.eu/)

A relevant – although finished – EU project that has pioneered a European cloud federation architecture (for IaaS clouds) and had an impact on the OVF as well as the OCCI standards.

TClouds contact via IBM

VISION (www.visioncloud.eu/)

An EU project with several consortium members of RESERVOIR that is extending the RESERVOIR architecture to cloud storage. The cloud standards organization SNIA is a consortium member.

TClouds contact via IBM

ENSURE

An EU project on long-term data preservation, archiving and long-term meeting of regulatory requirements – in particular for data stored in clouds. ENSURE also has a medical use case with Philips.

A first collaboration call has taken place, a further telephone meeting between TClouds and ENSURE is planned to assess mutual requirements of the medical use case.

TClouds contact via IBM

FI-WARE

The core platform project of the Future Internet PPP.

TClouds contact via IBM

SAIL (http://www.sail-project.eu/)

An EU project on network virtualization and the network part of IaaS clouds.

Chapter 3

Exploitation

Chapter Authors:

Norbert Schirmer (SRX), Patricia Rio Branco, Martina Truskaller (TEC)

3.1 Introduction

Exploitation is recognised as the key enabler for the success of the TClouds project. Hence all TClouds partners are aware of and committed to the exploitation of the project results. It is the principle of all exploitation activities to use research results to create value within all participating organisations and thus to improve their competitive advantage. Only by scaling up the results into commercial offerings, can all European constituents be reached while ensuring profitability through economies of scale.

Wherever possible, research results will be used for the creation and support of new products and services. These products and services will lead to a competitive advantage of the participating organisations and will substantially contribute to the benefit of the targeted constituents. In order for the exploitation to be effective, an integrated approach will be necessary, combining experience and expertise from the development department and solution management, and the involvement of a user base represented by the consortium partners and the user council.

In Section 3.2 we now present the preliminary individual exploitation plans of the partners. Section 3.4 elaborates on the Intellectual Property issues that were collected by questioning the partners via individual questionnaires. In Section 3.5 the status quo of the project regarding exploitation is summarized and Section 3.6 elaborates on the agreed procedure for delivering project results. Finally Section 3.7 concludes with the IPR issues after the project.

3.2 Exploitation Plans of the Partners

3.2.1 Changes to Exploitation Plans

This preliminary exploitation plan is based on the plan presented in Annex I – Description of Work. We surveyed the partners for changes. No changes were deemed necessary.

IBM: IBM is a major provider of middleware and computing infrastructure. Cloud Computing is the emerging new delivery model for large-scale services for IBM. IBM will enhance consulting practice and spread overall cloud security expertise. We expect that TClouds will provide a security model and mechanisms to our emerging cloud computing products and offerings. Important examples are the current cloud-computing offerings (such as IBM WebSphere CloudBurst and IBM Smart Business Services) as well as IBM's initiative to design and build a next-generation data center An important path of exploitation for IBM will be standardisation that enables interoperable cloud offerings from competing vendors.

SRX: Sirrix is highly interested in commercially exploiting the results of the TClouds project and expects strong opportunities in getting the results to the market in the medium term. Sirrix markets secure IT infrastructures and plans to integrate TClouds components, such as the TrustedServer, into their products and commercial applications portfolio and extend components, such as the TrustedObjects Manager, towards Cloud Management

TUDA: TU Darmstadt's main interest, as a research institution, is the dissemination of the TClouds results among the scientific community. Moreover, through its role in the Center for Advanced Security Research Darmstadt (CASED) and the consequent cooperation with the University of Applied Sciences Hessen and the Fraunhofer Institute for Secure Information Technology, the project results will be exploited for improved consulting of and collaboration with industrial partners, e.g., IT enterprises in Darmstadt.

FFCUL: FFCUL is an educational and research institution, which is indirectly involved in the commercial exploitation of information technology products or services. Therefore, its main role will be in disseminating the TClouds results among the scientific community and industry, the latter mostly through students involved in Masters programmes in the areas of security and dependability, and the other degrees in computer science provided by the University (two bachelors, several masters and PhDs).

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

TEC will implement security measures and concepts developed within its own infrastructure to deploy a private cloud scenario within its IT services. Furthermore it will use the cloud-of-cloud concept to improve the security and availability of its running secure web services. All current and future users of our IT services (currently more than 3.000 persons) will benefit from the increased flexibility and security. We trust that the introduction of TClouds security measures will keep us on the leading edge of high secure web services for the research community served by us.

ULD: ULD will improve its ability to consult governmental organisations and companies in state-of-the-art technology. ULD will make use of the legal analysis conducted in the project when cloud computing is concerned. ULD will bring in this expertise in privacy commissioner working groups on the national and European level.

POL: POL will re-use TClouds results for its industrial cooperations in the cloud computing field. The proof of concepts and the components developed within TClouds will be valuable tools for training labs, during both Masters courses and summer schools like ETISS.

FAU: FAU is an educational and research institution and therefore results will mainly be disseminated amongst cooperating industry partners (e.g., Siemens and local SMEs such as Method Park Software AG). From an educational point of view bachelor, Masters and PhD students will greatly benefit from the results of TClouds.

PHI: Philips is a leading supplier of healthcare infrastructure, devices, and services; the movement of healthcare into the consumers’ home is a large driver for the future growth in the healthcare arena. Philips is also a leading contributor towards standards for medical connectivity, e.g., through ZigBee and the Continua Alliance. Philips will leverage the TClouds results through both of these channels, integrating them into future home healthcare devices, and by putting the ability to cloudsource computation on the agenda for future standardisation efforts.

HSR: HSR is interested in exploring the potentiality of the TClouds platform for enabling the creation of innovative services that the Hospital can provide to its patients, enhancing the

quality of care. With the TClouds project San Raffaele can investigate the opportunities and enhancements offered by the Cloud Computing in the healthcare domain, both traditional and innovative (eHealth). HSR will also use the TClouds project for the individuation of business connections, industrial collaborations, academic collaborations, and relationships with institutional stakeholders, access to venture capitals and evaluation of ad hoc spin-off.

EDP: EDP is interested in assessing the results of the Smart Lighting system using a cloud like infra-structure and, afterwards, evaluates the possibility of integrating other parts of the Smart Grid architecture in the same infra-structure. The decision will depend on the degree of privacy, security, and resilience that is achieved by the components that are being developed in TClouds, at the end of the project. The main concern of EDP is the safety of client data, the safety of the energy grid, and the real time information required to command and control the electrical network.

EFACEC ENG: EFACEC ENG is a company active in the areas of power system management, automation and protection. Although it is based in Portugal, EFACEC ENG has activities all over the world, with main focus in Northern and Southern Africa, Latin America and Eastern Europe. In the Electric Power Distribution area, EFACEC ENG supplies SCADA/DMS systems and Substation Automation and Protection Systems. The TClouds project addresses technological topics such as system availability, data integrity and security targeted to critical infrastructures, that are also relevant for EFACEC ENG solutions and products. Therefore the TClouds project, from an industrial point of view, is a great opportunity to widen our knowledge and awareness of cutting-edge technology, providing an insight of future trends in this area. Commercial exploitation of cloud computing solutions and services based on TClouds or integrating parts of TClouds technology, will be timely assessed by EFACEC ENG and the expectations are high. However a consolidated decision shall depend on multiple factors, namely the market trends, customer requirements and customer willingness to embrace cloud computing solutions, taking in consideration the profile of the products / solutions provided by EFACEC ENG within the Power System Automation business unit.

3.2.2 Preliminary Market Overview

In order to give a first overview of the market chances of the solutions developed within the TClouds project, all partners involved in Activity 2 filled in a short questionnaire regarding existing competitors to their specific TClouds components (we refer to deliverables D2.1.1, D2.2.1, D2.3.1, and D2.4.1 for details of the TClouds architecture and its components). The future Deliverable D4.1.2 (due end of the second project period) will evaluate in more detail the specifics of the exploitation of each subsystem, based on the technical particularities and dependencies derived from the second year prototype implementations. Please note, that the list of components evaluated in the following is not as detailed as the corresponding components' list in the Activity 2 deliverables, because some partners aggregated their components in context of this evaluation. This is motivated by the fact, that their components form an overall infrastructure, which shall be exploited.

3.2.2.1 Ontology-based Reasoning for Cloud Infrastructures (POL)

1. **Relating to your component(s)/research, which demand for such a solution exists for practical or existing cloud infrastructures or which security gap does it fill?**

   Our ontology allows describing a complete virtualized environment at different levels of granularity in a centralized way. It can be used to depict the virtual network infrastructures, the virtualized hardware used and the relationships amongst the virtual machines and the physical hardware. Furthermore it allows performing inferences, logical deductions and subsumptions over the virtual and physical hardware, thus giving

administrators a powerful tool which can be used to perform advanced security analysis and assessments through the powerful classification capabilities of the ontologies.

2. **Which (most related) competitive projects / products do exist, that are comparable to your solution or that might render your component superfluous?** Apparently no known comparable project exists.
3. **How is your solution different and better than the competitive solution(s)?** There are several languages such as OVF (http://www.dmtf.org/standards/ovf), the libvirt XML format (http://libvirt.org/format.html) and also partially CIM (http://www.dmtf.org/standards/cim), which can be used to describe a virtualized environment but they completely lack inferential capabilities. These languages are purely declarative and cannot be directly used to infer additional information, while our solution can both describe a virtualized infrastructure and perform logical deductions over it.

3.2.2.2 Log Service (POL)

1. **Relating to your component(s)/research, which demand for such a solution exists for practical or existing cloud infrastructures or which security gap does it fill?**

   The goal of the log-service is to create a write-only logging service which is protected against attacks using cryptography. This allows a user to immediately detect tampering of log entries. Moreover, a Log Service will create log entries with privacy enforced by design using mechanisms for ensuring per log entry access control. A Log Service will interact with other TClouds components such as Deepsky distributed storage (FFCUL) or Secure Block Storage (TUDA) in order to guarantee availability of logs and will be capable of applying policies on log entries that define their usage.

2. **Which (most related) competitive projects / products do exist, that are comparable to your solution or that might render your component superfluous?**

   Loggly (http://loggly.com)

   Papertrailapp (https://papertrailapp.com)

   RSyslog (http://www.rsyslog.com)

3. **How is your solution different and better than the competitive solution(s)?** While RSyslog make users able to setup a basic remote logging system Loggly and Papertrailapp provide in addition to the basics advanced and useful cloud oriented features like aggregation, analysis and advanced search. Despite this, such products offer no security features like log integrity verification and per log entry Access Control system.

   In order to ensure security of the log entries, a log system must provide the integrity over the stored log entries. In addition to the integrity of each log entry, it is desirable to provide the forward integrity security property of the whole log. The forward integrity implies that, if an attacker succeeds in compromising the log system, he cannot modify log entries collected before his attack without being noticed.

   Since it is not possible to guarantee that the log system will never be compromised, the Access Control must be embedded within the log entry itself, in a way that the relevant data is cryptographically protected at the creation time and only the authorized people will have access to the keys required for accessing the data.

3.2.2.3 Security Audits for Heterogeneous Virtual Infrastructures (IBM)

1. **Relating to your component(s)/research, which demand for such a solution exists for practical or existing cloud infrastructures or which security gap does it fill?**

SAVE retrieves the configuration of an infrastructure cloud and then performs security analysis on this data. The current prototype focuses on validating multi-tenant isolation. The mid-term goal of SAVE is to build a solution that provides completeprovide complete end-to-end virtual systems configuration assurance market. The customer needs are to gain assurance that the technical configuration of a range of heterogeneous virtual systems (e.g. a private cloud) satisfy given business and compliance requirements. There are two reasons why such assurance is needed. The first is compliance (PCI-DSS) the second are risk mitigation.

2. **Which (most related) competitive projects / products do exist, that are comparable to your solution or that might render your component superfluous?** *Configuresoft* (now EMC) covers the complete space of configuration management for servers. This includes discovery of systems, patch management, as well as approval and roll-out of changes. Their main product used to be the Enterprise Configuration Manager.

   Hyper9 leverages Google-like search technologies for simplifying the management of virtual servers. It uses a range of 'agent-less' collectors to collect data from multiple sources such as the vCenter API of VMware.

   Tripwire provides products for operating system configuration assurance. This information is then used to establish a baseline configuration for each component, against which it runs a configuration.

3. **How is your solution different and better than the competitive solution(s)?** *Configuresoft's* configuration audit is tightly integrated with the overall configuration management product and is likely to focus on VMware as the main (maybe only) virtualization platform. Furthermore, their focus is currently on US customers. SAVE provides a solution that is independent of the virtualization platform and the configuration management product used. SAVE provides configuration audits on top of existing configuration management products. We achieve this by retrieving configuration information from multiple heterogeneous sources such as different virtualization platforms as well as different pre-existing configuration management databases.

   Hyper9 is an example of a modern configuration management systems (similar products are available from IBM, HP, BMC). These products usually do not offer configuration validations.

   Tripwire: The offerings of tripwire are rather low-level: For virtual systems, Tripwire records configurations, is able to perform local validations by executing a range of patterns against the recorded configurations. The focus is on identifying and documenting changes to the existing configurations. No higher-level validations or verification across machines are performed

3.2.2.4 Trusted-Computing-Based Cloud Computing Infrastructure and Management (SRX)

1. **Relating to your component(s)/research, which demand for such a solution exists for practical or existing cloud infrastructures or which security gap does it fill?**We provide a trusted computing based infrastructure for cloud computing, consisting of a management component (TrustedObejcts Manager (TOM)), server components (TrustedServer) a secure communication & management channel (TrustedChannel) and a cloud storage component (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 and 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.

2. **Which (most related) competitive projects / products do exist, that are comparable to your solution or that might render your component superfluous?**

   Technically: Cloud management frameworks like OpenStack, OpenNebula, Eucalyptus, Citrix OpenCloud Framework.

   Commercially:

   I. Infrastructure cloud providers like Amazon Web Services or RackSpace.

   II. Products to build-up a Private Cloud, such as VMware vCloud, Citrix CloudStack

3. **How is your solution different and better than the competitive solution(s)?** The TrustedInfrastructure components developed within TClouds cover all the major parts of an infrastructure cloud: management, servers (computing) and storage (via the S3 proxy) and a 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 like 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. TrustedComputing 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 best of both worlds and combine the security management features of TOM with the infrastructure management capabilities of OpenStack.

   Existing 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 (TVD) in an a consistently proactive approach which is addressing threats by design and an adequate security architecture. TOM, TrustedChannel and TrustedServer focuses a consistently proactive approach implementing TVDs which means a proper isolation of virtual infrastructures (computing, networking and storage) by means of virtualization, encryption and VPN technology, all founded on trusted hardware anchors.

3.2.2.5 Tailored Cloud Services / memcached (FAU)

1. **Relating to your component(s)/research, which demand for such a solution exists for practical or existing cloud infrastructures or which security gap does it fill?**

Traditional operating systems are primarily designed to run on real physical hardware and contain many functions not necessary in a cloud environment. Many of these are active by default and pose unnecessary security risks if not deactivated by a manual process.

2. **Which (most related) competitive projects / products do exist, that are comparable to your solution or that might render your component superfluous?**

   I. HalVM, Open-source project by Galois Inc.

   I. (Light-)House, Research, Oregon Health&Science University / Portland State University

   II. Mirage, Research, University of Cambridge

3. **How is your solution different and better than the competitive solution(s)?**

   FAU's work will concentrate on improving the automated adaption and verification aspects of such platforms. As developing an entire operating system from scratch is out of scope for this project, HalVM and the House operating systems provide a good starting point for our own research. Mirage uses a programing language with side-effects (namely "OCaml"), which isn't particularly well-suited for verification purposes. Current research regarding the Mirage system also seems to be more directed towards implementing models for concurrent execution.

3.2.2.6 RBPEL: Providing Fault-tolerant Execution of Web-service-based Workflows within Clouds (FAU)

1. **Relating to your component(s)/research, which demand for such a solution exists for practical or existing cloud infrastructures or which security gap does it fill?**

   With a variety of services rapidly evolving at all architectural levels of cloud computing, there is an increasing demand for a standardized way to coordinate their interactions. Business process management, that is, more general, the management of Web-service-based workflows, could satisfy this demand and, indeed, first corresponding offerings have gained instant popularity. While from a functional perspective, these Platform-as-a-Service (PaaS) solutions are already quite mature, their support for fault tolerance is still very limited, making them inapplicable for critical tasks.

2. **Which (most related) competitive projects / products do exist, that are comparable to your solution or that might render your component superfluous?**

   Standard BPEL engines like Apache ODE

3. **How is your solution different and better than the competitive solution(s)?**

   Standard BPEL engines log state changes to persistent storage to enable recovery of active workflows after a reboot or crash. This approach has two disadvantages: first, the need for synchronous logging slows down the execution speed during normal operation; second, the reliability of this mechanism depends on the reliability of the storage. In addition, BPEL provides only limited means to handle failures of the Web services the workflows are based on. Making these Web services fault tolerant is not supported at all by standard BPEL infrastructures.

   Besides achieving a higher performance than a standard unreplicated BPEL implementation, our fault-tolerant BPEL infrastructure, called RBPEL, has additional advantages: First, it does not depend on reliable storage. Second, it also provides improved fault tolerance as the services offered by a replicated business process remain available even in the presence of a limited number of crashes. Third, in our holistic approach, fault tolerance is achieved by actively replicating not only the workflows, but

also the Web services on which they are based and dependent. Fourth, using active replication gives the opportunity to tolerate arbitrary faults in a next step.

3.2.2.7 CheapBFT: Resource-efficient Byzantine Fault Tolerance

1. **Relating to your component(s)/research, which demand for such a solution exists for practical or existing cloud infrastructures or which security gap does it fill?**

   One of the main reasons why system that are able to tolerate arbitrary faults, so-called Byzantine fault-tolerant (BFT) systems, are not widely used lies in their high resource consumption: 3f +1 replicas are necessary to tolerate only f faults. Recent works have been able to reduce the minimum number of replicas to 2f +1 by relying on a trusted subsystem that prevents a replica from making conflicting statements to other replicas without being detected. Nevertheless, having been designed with the focus on fault handling, these systems still employ a majority of replicas during normal case operation for seemingly redundant work. Furthermore, the trusted subsystems available trade off performance for security; that is, they either achieve high throughput or they come with a large trusted computing base.

2. **Which (most related) competitive projects / products do exist, that are comparable to your solution or that might render your component superfluous?**

   I. PBFT, BFT-SMaRt (see also note in the next section): Require 3f + 1 replicas

   II. MinPBFT: Requires 2f + 1 replicas and a trusted subsystem (TPM or hypervisor-based)

3. **How is your solution different and better than the competitive solution(s)?**

   CheapBFT is the first BFT system that limits the execution and agreement components for all requests to only f + 1 replicas, whereas only f passive replicas witness progress during normal-case operation. Furthermore, it relies only on a lightweight trusted counter abstraction, increasing dependability by decreasing the trusted computing base.

   The trusted counter of CheapBFT is realized as a FPGA module, improving resilience as well as performance. This module can be easily deployed on machines of a trusted cloud as developed in Work Package 2.1. Therefore, CheapBFT is especially beneficially within such environments. BFT-SMaRt, another BFT system researched in the context of the TClouds project, is more suitable for cloud-of-clouds scenarios as they are subject of Work Package 2.2. It requires more resources but does not depend on a trusted subsystem and is more insensitive to different timing behaviors of its components.

3.2.2.8 High-Performance BFT State Machine Replication Library (FFCUL)

1. **Relating to your component(s)/research, which demand for such a solution exists for practical or existing cloud infrastructures or which security gap does it fill?**

   BFT-SMaRt (http://code.google.com/p/bft-smart/) is a complete implementation of a Byzantine Fault-Tolerant state machine replication protocol in Java, enforcing modularity and maintainability of the (complex) protocols required. The main innovation this library brings is the possibility of implementing real world intrusion-tolerant services in which the system keep working correctly if less than a third of the replicas of the system are corrupted with minimum assumptions about the underlying environment. This kind of technique is fundamental for implementing cloud-of-clouds services in which non-passive replicas are deployed in different clouds.

2. **Which (most related) competitive projects / products do exist, that are comparable to your solution or that might render your component superfluous?**

   Most competitive solutions were academic prototypes that offer almost no guarantees in terms of performance or fault tolerance, e.g., PBFT

(http://www.pmg.csail.mit.edu/bft/#sw) and UpRight (http://code.google.com/p/upright/). Coordination systems like Apache ZooKeeper (http://zookeeper.apache.org/) can also be used to solve similar problems.

3. **How is your solution different and better than the competitive solution(s)?**

   There are two important differences between BFT-SMaRt and similar systems like PBFT and UpRight. First, these libraries never become mature enough to implement real systems or convincible demonstrations of dependable services under attacks, faults and intrusions. Second, these projects appear to be abandoned (last modification on their webpages in 2010).

   Moreover, BFT-SMaRt focus on modularity and maintainability makes its code much smaller and simpler, without sacrificing performance or resilience.

   ZooKeeper implements a service for process coordination (e.g., leader election), and does not provide any general support for services replication. BFT-SMaRt, on the other hand, is a replication library. Moreover, ZooKeeper tolerates only crash faults (that can't model intrusions), on the contrary of BFT-SMaRt, that can be used to build services tolerating arbitrary faults.

   Note: ChepBFT is a similar solution in the TCLOUDS project, but it targets a different environment: resource constrained systems in which the replicas have access to a secure co-processor (e.g., TPM). CheapBFT is more useful in a single-cloud environment (Workpackage 2.1).

3.2.2.9 Cloud-of-Clouds Storage IBM / FFCUL)

1. **Relating to your component(s)/research, which demand for such a solution exists for practical or existing cloud infrastructures or which security gap does it fill?**

   Current cloud storage solutions providing encryption already exist. The IBM and FFCUL-provided system that builds reliable and secure storage through a federation of object storage services from multiple providers. Many clients may concurrently access the same remote storage provider and operate on the same objects without trusted gateway. The software is a library run by each client before it accesses cloud storage.

   Customers are interested in client-side encryption, integrity protection, and added resilience for their data for enhanced security and for compliance with regulations.

2. **Which (most related) competitive projects / products do exist, that are comparable to your solution or that might render your component superfluous?**

   There are various libraries and proxy-based solutions available to encrypt data when it leaves a company perimeter. The challenge is managing keys. The Storage component uses inherent key-management, there is no need for maintaining encryption keys at the clients. Clients only need the authentication keys for accessing the cloud resources.

   No commercial product currently offers seamless data replication across multiple different clouds.

   Cleversafe Inc. offers a cloud storage solution based on generalized erasure codes but has no capability to defend against attacks by the storage providers.

3. **How is your solution different and better than the competitive solution(s)?**

   See answer to question 2.

3.2.2.10 Access Control as a Service (OXFD)

1. **Relating to your component(s)/research, which demand for such a solution exists for practical or existing cloud infrastructures or which security gap does it fill?**

The core of AcaaS manages the hosting decisions of virtual resources over physical resources based on both user requirements and infrastructure properties. This component helps addressing different security and application requirements as in case of controlling the hosting of mutually exclusive VMs on different physical hosts.

2. **Which (most related) competitive projects / products do exist, that are comparable to your solution or that might render your component superfluous?**

   Currently OpenStack proposes nova-schedual which is still immature (as explicitly indicated by Openstack nova-schedual still require lots of work). Other industrial (e.g. Amazon web services, RackSpace), as in the case of OpenStack, are still immature in this direction.

3. **How is your solution different and better than the competitive solution(s)?**

   AcaaS is planned to integrate and improve OpenStack nova-schedual in such a way the scheduling algorithm will consider the overall infrastructure proprieties and then decide on the allocation of virtual resources over appropriate physical resources that best matches user requirements.

3.2.2.11 Smart Lighting Management System (EDP / EFACEC ENG)

1. **Relating to your component(s)/research, which demand for such a solution exists for practical or existing cloud infrastructures or which security gap does it fill?**

   The Smart lightning management system (SLMS) is an application and not a security component. Thus in this context the question does not apply.

   SLMS uses the cloud to be able to scale and serve its users, as the database and the number of requests to the server grows. It uses the cloud's computing power to execute the application also in a growing perspective.

   The application uses TClouds security components to gain resilience and security features.

2. **Which (most related) competitive projects / products do exist, that are comparable to your solution or that might render your component superfluous?**

   Capgemini's smart public lighting system for the city of Texel

   Capgemini provides a smart public lighting system based on the Windows Azure cloud environment in the Dutch city of Texel allowing its employees to control public lighting wirelessly, enabling city employees to manage public lighting from any location with an Internet connection. This is the first pilot worldwide involving wirelessly controlled public lighting by Capgemini. This technology uses Microsoft's Bing Maps API to provide an interactive dynamic map of Texel with additional functionality and communication services provided by ASP.NET, Microsoft SQL Azure and the Azure AppFabric service bus to enable connectivity between data services.

   Its comparable benefits to TClouds Smart lightning management system are:

   I. Helping reducing energy usage and lowering carbon emissions

   II. The possibility to gather data provided by the Smart Lighting system trough an information hub

   III. The usage of cloud computing

   Petra Solar's IllumniWave

   IllumniWave is a solution that combines smart grid communications and intelligence for remote monitoring, command and control of streetlights to promote energy efficiency and savings worldwide for municipalities and other street lighting providers. Its street light control system is equipped with two-way smart grid wireless communications, enabling

remote control and management of distributed street lights from a central location. Users can remotely schedule street lights to turn off or dim at predetermined times for energy conservation savings. Alerts on outages, energy consumption data and reports are managed through the IntelliView Lighting Control System (LCS).

Its comparable benefits to TClouds Smart lightning management system are:

I. Allowing governments, municipalities and utilities to reduce energy consumption.

II. Enables environmental benefits associated with energy efficiency

III. Reduces operational and capital expenses

IV. Leverages Petra the smart grid technology deployment.

V. Accurately reports alerts on bulb outages and energy consumption data

3. **How is your solution different and better than the competitive solution(s)?**

The Smart Lighting solution will be a web application that will let authorized users to interact with the underlying smart grid infrastructure in order to operate and/or extract information from the public lighting sub-system, thus enabling a more efficient management over the public lighting service. It´ll include a set of management capabilities like on/off commands, real time status, energy consumption and schedules update. The other similar public lighting solutions offer some of these benefits but not such in an efficient and elaborate way as offering the possibility to schedule lighting management.

In comparison with the The IllumniWave solution, Smart lighting doesn't oblige the implementation of on-location intelligent devices in order to operate its solution.

As it's described, the IllumniWave solution's technology transfers communication data from each unit back to a secure data centre and via the IntelliView portal, users are able to remotely command and control all smart energy applications on the smart grid network, whereas with Smart Lighting , a cloud computing environment is used providing access to the operation through various means. So it is plausible to extrapolate that Smart Lighting's cloud computing oriented solution is innovative in the public lighting area. Capgemini's solution is relatively similar but it provides a smart public lighting system based on the Windows Azure cloud environment. This technology uses Microsoft's Bing Maps API to provide an interactive dynamic map of the covered location to operate in and communication services are provided by ASP.NET, Microsoft SQL Azure and the Azure AppFabric service bus to enable connectivity between data services. EDP Distribuição and EFACEC already have great experience and the right technology in telecom and electricity distribution which brings trustworthy confidence in the implementation of the Smart Lighting Solution.

Smart Lighting is also highlighted through the fact that it does not have critical data related with customers' consumptions, making data confidentiality as part of the information security issues. It´s main benefits include:

Monitoring consumptions; Monitoring state and anomaly events (alarms); Managing lighting Services and Schedules; Managing public lighting settings; Actuate over control circuits; Managing settings of public lighting intelligent devices (DTC & EB).

3.3 Joint Exploitation Plan

Figure 7 illustrates the joint design and development architecture and subsystems developed by different partners of TClouds that are grouped together. Each of those subsystems foresees a joint exploitation.

At the application level the two uses-cases for Smart Public Lightening and Home Healthcare using the secure cloud services that are provided by the TClouds Security Platform. In this context the security platform is an enabler technology for these uses cases as well many other cloud related application. For instance Philips Medicare is collaboration with TUDA to deploy smart devices connected to the cloud and the medical devices of Philips for secure and remote diagnose.

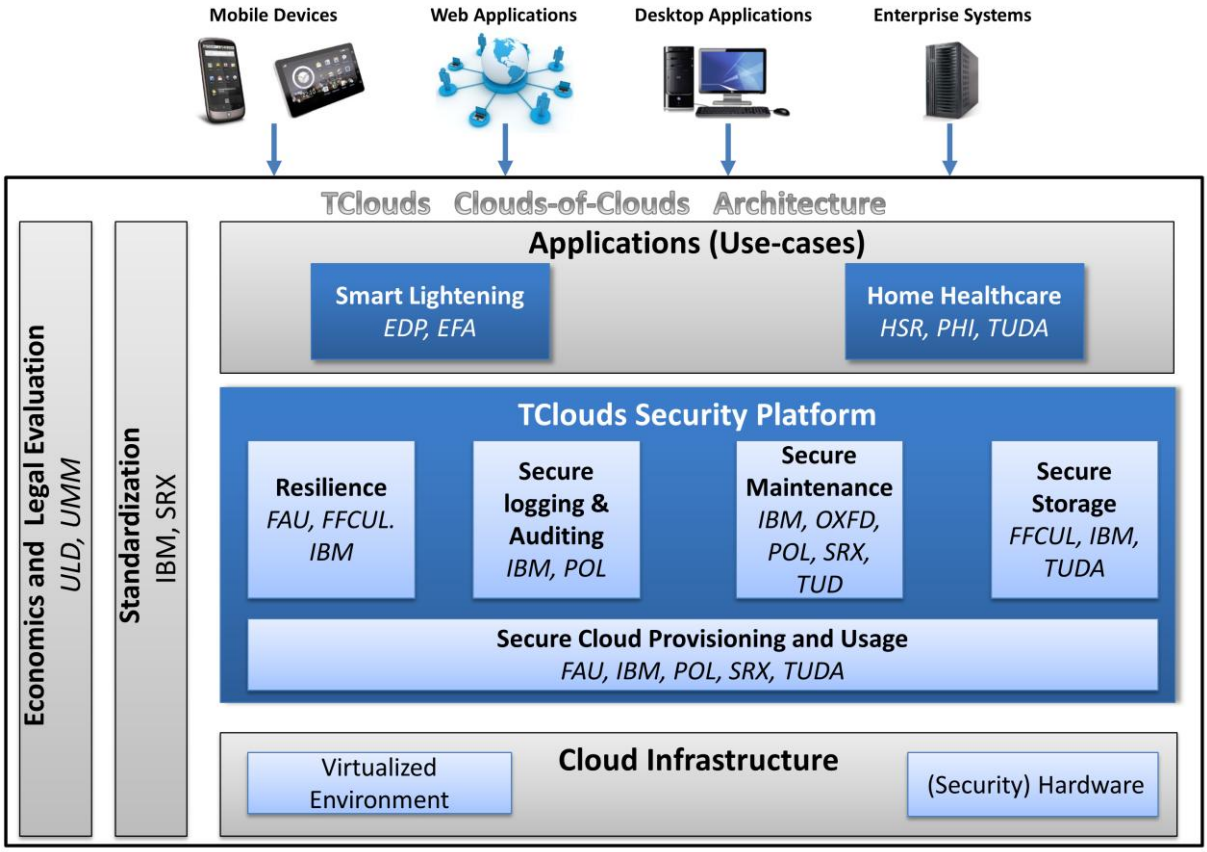

Figure 7: Subsystems (abstractly) for joint exploitation

The joint exploitation plan aims to provide “security as a service” to cloud providers and allows the design of secure cloud applications and their secure usage.

At this abstraction layer, there are various services that guarantee security and resilience targets of TClouds project as we explore in the following. We only give a brief explanation of the individual services and refer to the corresponding deliverables for more details. Each of these services is expected to be proto-typed and evaluated in accordance to the methodology described in D2.4.1.

Secure Logging and Auditing (IBM, POL):

Deliverable reference: D2.1.1, D2.2.1

Description: Allows to verify security properties like information flows and domain isolation and provides a secure logging demon which can be used by customers or auditors.

Secure Maintenance (IBM, OXF, TUDA, SRX):

Deliverable reference: D2.1.1, D2.3.1

Description: Constitutes Access control mechanisms (IBM) and secure migration of resources (OXF, SRX) within and across clouds, and key management aspects (TUDA, IBM) under various trust assumptions.

Secure Storage (FFCUL, IBM, TUDA):

Deliverable reference: D2.1.1, D2.2.1, D2.3.1

Description: Provides and abstracts data confidentiality, integrity and availability for various types of cloud storage such block storage (TUDA), or object storage (FFCUL, IBM, SRX).

Resilience (FAU, FFCUL, IBM):

Deliverable reference: D2.2.1

Description: Provides availability and consistency of services and executions (e.g., whole Virtual Machines or a specific software component) in the cloud (FAU, FFCUL, IBM). This service features Byzantine Fault-Tolerance (FAU, FFCUL), State Machine Replication (FFCUL), Fault-Tolerant Workflow Execution (FAU) and Consistency for Untrusted Service Execution (IBM).

Secure Cloud Provisioning and Usage (FAU, IBM, POL, SRX, TUDA):

Deliverable reference: D2.1.1, D2.3.1

Description: Methods to increase the security of users' virtual machines by tailoring the implemented services (FAU), provide a key management framework for securely deploying credentials in cloud infrastructures (IBM, TUDA), offering Trusted Computing services by means of a trusted platform agent (POL), or implementing a trusted infrastructure (SRX).

3.4 IPR issues identified in the TClouds project

In the environment of international applied research projects with industrial partners such as TClouds, the careful handling of IPR issues is of strategic importance. Within the TClouds project, many individuals of numerous organisations cooperate across national borders. In order to develop novel technologies, concepts or processes, exchanging information with other parties is a necessity. Furthermore, jointly creating new intellectual properties is common. Therefore confidentiality is a very important issue for participants in TClouds, from the project start-up phase of joint activities to the implementation phase and further to the exploitation of results.

All efforts related to IPR issues aim to create a favourable environment for respecting intellectual property rights (IPR) because of moral and economic reasons. Without IPR protection the joint creativity of natural persons or legal bodies as well as the dissemination and exploitation of results would be highly restricted not to risk a substantial drain of knowledge. Intellectual property (IP) is an intangible asset and created as a result of intellectual creative effort of the human mind in relation to works of authorship and/or inventions. With the ownership of intangible assets certain legal exclusive property rights which are established by law or by contractual obligation are connected and maintain the control in relation to the protection of the interests of the creators by excluding these creations from public property. This means the right to permit or deny the use and exploitation of the creative work. So IPR provides a protection of the creations and inventions to the owners by preventing users from using or copying them without reservation or payment for a certain period of time.

Intellectual property can be classified into

- industrial property items like inventions which can be a product or a process providing new solutions for solving (technical) problems and which can be protected by registering a patent and
- copyright items which provide exclusive rights to the creator to prohibit the unauthorized copying, adaptation and reproduction of its intellectual work.

The nature of the intellectual property connected to TClouds will not only include traditional artifacts such as patents but also internal workflow, documentation and software. The protection of this knowledge is vital for each of the participants.

3.4.1 Prerequisites for the TClouds project

The management of intellectual property in TClouds was already important at the project proposal set-up stage where the first development of appropriate ideas for the joint research activities and the assembling of the project consortium took place.

Even at this early stage discussions and the exchange of information between different people from institutions with different knowledge, background and interests was required and IPR issues needed to be discussed and integrated into the appropriate sections within the proposal.

Later on, the grant agreement (GA) represents a contract which establishes the beneficiaries' rights and obligations towards the European Community and towards each other. It contains a specific provision on confidentiality that defines the obligation and its term. Moreover it also covers an intellectual property related section.

Furthermore, in order to guarantee a uniform approach by the TClouds participants, internal rules should be defined, including confidentiality clauses for the use of dissemination of results, which can be incorporated in the consortium agreement (CA).

In the present section, all stages and contracts, which are important IPR prerequisites for the project set-up will be briefly explained, with the focus on their implementation in the TClouds project.

3.4.2 Drafting of Proposal

In writing the project proposal for TClouds, the management of IPR was already outlined because the exchange of information between the partners in such an early stage is of certain risk. Although copyright allows some legal protection against unlawful copying of works, all parties should nevertheless only reveal any such information under terms of confidentiality in order to protect the contained ideas in a broader sense.

During the TClouds proposal drafting phase, it was laid down that the consortium agreement, as an outline contract between the partners, would define the rules and measures as well as the rights and duties for protecting the IP within the TClouds project. Through signing the consortium agreement and its confidentiality clauses the TClouds partners committed themselves to protecting the confidential information brought into or resulting from the TClouds project. Also plans for the use and protection of the results have been considered (more in “Consortium Agreement” chapter).

Additionally, the management structure has been set up with the protection of knowledge in mind, which foresees the permanent monitoring of IPR issues during the project.

3.4.3 Contracts

Within the TClouds project two agreements have been prepared, which all partners had to sign in order to participate in the project: the grant agreement and the consortium agreement. Both of these agreements include IPR regulations for the project and therefore represent the contractual basis for IPR within TClouds.

3.4.3.1 Grant agreement (GA)

The grant agreement is the contractual basis for the European Commission (EC) funded project TClouds, which is the principal agreement between the EC and the coordinator. This contract sets out in writing the key project details such as the parties involved, the scope, the duration and start date of the project, the reporting periods, the maximum financial contribution of the EC, the main contact data of the contracting parties as well as some specific issues.

It was clear to the project partners from the beginning that due diligence would be required with regard to confidentiality. Therefore they determined the level of confidentiality of information that would be provided in deliverables throughout the TClouds project when the work to be done in the project was defined and stated in Annex I to the GA. For selected deliverables, where the dissemination level is “public” the consortium decided to include a confidential report and therefore some deliverables will be divided into two parts – containing a public and a confidential part.

3.4.3.2 Consortium agreement (CA)

The consortium agreement is signed between the project participants of the consortium and implements the grant agreement, establishing provisions related mainly to consortium management, the distribution of the Community financial contribution and IP. The CA is a negotiated and agreed mandatory contract between the project partners, which has to be signed by all partners before the entry into force of the Grant Agreement. The legal requirements are singled out in the Grant Agreement but the details regarding the cooperation are given in a specific Consortium Agreement. The TClouds Consortium Agreement was signed by all partners in October 2010 and it sets out the internal management guidelines for the consortium including established rules, structures and processes for handling IPR.

The CA includes guidelines for the project internal management of the cooperation by providing rules for the following issues:

- the parties' obligations for the implementation of the GA
- project internal organisation and project structure (project bodies and their functions, rights and duties, voting regulations)
- handling of commission payments (distribution of the funding by the coordinator)
- provisions about the ownership and licensing of intellectual property (e.g. foreground, publications, access rights, dissemination of results)
- handling of matters of liability and confidentiality
- procedures for settling internal disputes
- handling of defaults and remedies (exclusion/withdrawing)

Knowledge, or foreground[21], generated within the project will be protected by patent filing or publication in accordance with the consortium agreement that also represents an outline contract between the partners. The status of background[22] and sideground[23] brought in or developed in parallel is also covered by the CA. Amendments to the CA can be done on a per partner basis as the needs for knowledge and protection varies between the partners.

In TClouds some partners specified which know-how would be made available for the project and/or of excluding specific background from their obligation to grant access rights in order to delimitate the background they were willing to share. With the signature of the CA by all partners, they agreed to the restriction of access rights.

Besides the general principles relating to access rights, the TClouds CA deals with clauses concerning access rights for affiliates, for the execution of the project, for use, to third parties as well as the inability to grant access rights due to third party rights, special provisions concerning access rights to software, have made rights, standards and access rights for parties joining or leaving the project. Furthermore the CA covers rules regarding the confidentiality period, exceptions, disclosure of confidential information in compliance with a court order and to the Commission as well as disclosure of confidential information to

[21] **Foreground** is understood to be tangible and intangible project results in terms of information, materials and knowledge generated inside the project. Foreground is principally owned by the partner who generated it; when the generation of the foreground is a joint process, it is - unless the partners do not agree on another solution - jointly owned by the participants.

[22] **Background** is understood to be information, knowledge and any IPR relevant to the project already held by the project partner before the accession to the EC Grant Agreement.

[23] **Sideground** is intellectual property created during a contract but which is not considered to be part of the contract.

affiliates and to other third parties and it covers regulations regarding the disclosure of results to the public as well as the provided information to the EC.

3.5 Status quo of the project

On the basis of the above-mentioned contractual framework defined and agreed in the run-up to the project the relevant intellectual property rights must be maintained during the project. Therefore the management structure, workflows and tools are designed with the protection of knowledge in mind. The project management is responsible for the monitoring of IPR issues. All partners are obligated to report any protection of intellectual property to the project management.

New knowledge produced during the project belongs to the supplying partner and any commercial exploitation or public disclosure of new knowledge can only be done after the owner gives his consent. The decisions to patent any results belong to the owner; the other partners must not interfere in this process. In case of jointly developed new knowledge the ownership needs to be agreed upon before any dissemination and/or exploitation.

The protection of knowledge, or Foreground generated within the project, is vital for each of the TClouds participants and is mainly realised by patent filing and/or publications.

The following subchapters should provide an insight regarding the current situation concerning different IPR issues within the TClouds project.

3.5.1 Licences

Until now the cloud platform (OpenStack + KVM) is developed as open source and the code we produce falls under this license. Additional comments from some partners can be found in the following:

IBM: Within the pre-project phase the work was partially based on IBM background and no licensing was needed for project use. For auditing and replicated storage components, IBM does not include code from other participants. Therefore for use by IBM no licensing is needed.

POL: The code developed under the former Open_TC project was released with dual GPLv2 and LGPLv2 licences. POL expects to use only free software (GPL/LGPL/Apache/OpenSSL licences) and they plan to release all their code with GPLv2 and/or LGPLv2 licences.

PHI: For the proof of concept, PHI is using the license of Actiware from Philips Respironics.

EFACEC ENG: The partner EFACEC ENG mentioned that if a Smart Lighting solution happens to go commercial, it will then be licensed.

Other TClouds partners at the moment do not intend to use or do not expect to need any other licences but parts of the developed code may stay proprietary to a single partner and may not be disclosed.

Regarding SW used or developed within the TClouds project the following public licences are relevant:

BSD-style Open Source Licences:

These kinds of licences are relevant for the OpenSSL which is used in TClouds. The OpenSSL toolkit is licensed under an Apache-style licence, which basically means that you are free to get and use it for commercial and non-commercial purposes subject to some simple license conditions. The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit.

Actually both licences are BSD-style Open Source licences. (BSD licences represent a family of permissive free software licences. The original was used for the Berkeley Software Distribution (BSD), a Unix-like operating system after which the license is named.)

GNU General Public License:

GPL is a widely used license for most of command-line tools in a GNU/Linux system. The GPL has “strong copyleft”, which means software under GPL is free to use; any modifications to the software for external use, have to be made available in source code for everyone and have to be put under the GPL or a compatible license.[24]

Lesser General Public License:

Lesser or formerly called library General Public License is mostly used, as the old name indicates, for libraries. If the libraries were used as e.g. DLL the software that uses the library does not have to be put under the LGPL. This license has in comparison to the GPL so called "weaker copyleft". But of course one is free to distribute the software that uses the library under LGPL.

Commercial Licences:

Commercial licensing is for use in commercial, government and non-profit organizations. Typically, the users are free from the restrictions of using the software output for commercial uses, such as distributing, selling and other options to generate revenues directly with the software output. Any duplication and modification to the software are prohibited.

Freeware:

A proprietary software which is available for use at no cost or for an optional fee is called freeware. Unlike common belief freeware is not free software, it is usually restricted to one or more rights to copy, distribute, and make derivative works of it.

3.5.2 Patents

Patents are officially granted rights to an inventor, to exclude to a certain extent anyone from commercially exploiting the invention for a limited time. In return for the patent-inherent exclusive rights, the inventor has to disclose the innovation adequate for the dissemination of knowledge for further developments. A patent can be obtained by submitting an application with a detailed description of the invention as well as demonstration of its novelty compared to already existing technologies to a patent office. In the evaluation process experts check the fulfilment of certain conditions and balance the interests of the patentee as well as those of the general public in order to decide over the issuing of the patent. Once a patent has been granted for a certain extension, for any further commercial exploitation of the patented product or process invention an authorization of the patent holder in the form of a permission or a licence must be obtained. With the expiry of the patent after a limited period, the protection ends and everybody is allowed to use the innovation for commercial exploitation without acting illegally.

Until now no patents were applied in reference to work generated within TClouds. However it is very likely that patents will emerge from results obtained in the TClouds project.

[24] detailed information can be found at http://www.gnu.org

3.5.3 Copyrights

In general, there were no copyright issues taken into the TClouds project. Therefore, it was not necessary to take this into account.

Future material developed within the project will automatically be copyrighted, e.g. Smart Lighting Specification, Design, Source Code, course materials, and so on.

By default, everything developed by a partner is copyrighted by this partner, unless it is explicitly given a different status.

3.5.4 White Papers

TClouds Consortium internal rules prevent project members from publishing public deliverables before they have been accepted by the reviewers in the annual review meeting. If a partner wants to disseminate certain information which is contained in a public deliverable early, this is possible through the creation of a white paper, but this is rather unlikely as most results are and will be published as scientific papers.

3.5.5 Violations

During the preparation phase of this document all TClouds partners were asked whether they noticed any violations concerning IPR issues inside or outside of the project and none of them reported anything in this regard.

3.5.6 Partnerships with other projects/partners outside TClouds dealing with a related topic

Also in partnerships with other projects or partners it is necessary to adhere to the IPR regulations and to share only ‘public’ TClouds-related information.

There have been some partnerships with other projects or partners dealing with a topic related to TClouds which were for example:

During the pre-project phase FFCUL concurrently wrote other project proposals related to, but not competing with, TClouds. ULD participated in the projects “Prime” and “Prime Life”, PHI in Trust in digital life, for its strategic research agenda that includes cloud computing. POL, TEC and IBM have collaborated in the project Open_TC (EU contract IUST-027635). There the software related to Trusted Computing has been developed, which is used and extended in TClouds

Currently the partner FFCUL participates in MASSIF & SECFUNET EC projects, and half a dozen national projects. ULD participates in the ABC4Trust project and POL in the Posecco project, where they are developing an ontology for the virtualization domain that shall be used in Posecco and in TClouds. Furthermore, the partner SRX is working in a project with the German BMBF “Software Cluster”.

With respect to partnerships with other partners outside TClouds dealing with a related topic, the partner TU-DA has a partnership with Fraunhofer SIT, Darmstadt.

Moreover, ULD mentioned that the participation in several possible future projects with related topics underlies non-disclosure agreements.

3.6 Project Results

The following subchapter describes the development of project results (deliverables, reports and scientific publications) as well as the regulations of such results within the TClouds project.

3.6.1 Deliverables, Reports and Scientific publications

All project participants are obliged to take care that the information provided in the deliverables and reports corresponds to the IPR regulations, especially when compiling public deliverables and reports.

In order to ensure that only public content is contained in public deliverables and that IPR rules have been considered the TClouds consortium defined an internal review process for publications and deliverables.

This process requires the approval of both the Project Management, and a reviewer external to the work package, before a publication or deliverable is released. This ensures that the qualitative targets are reached with regards to technical content, the objectives of the project and adherence to formal requirements established in the GAs and CAs.

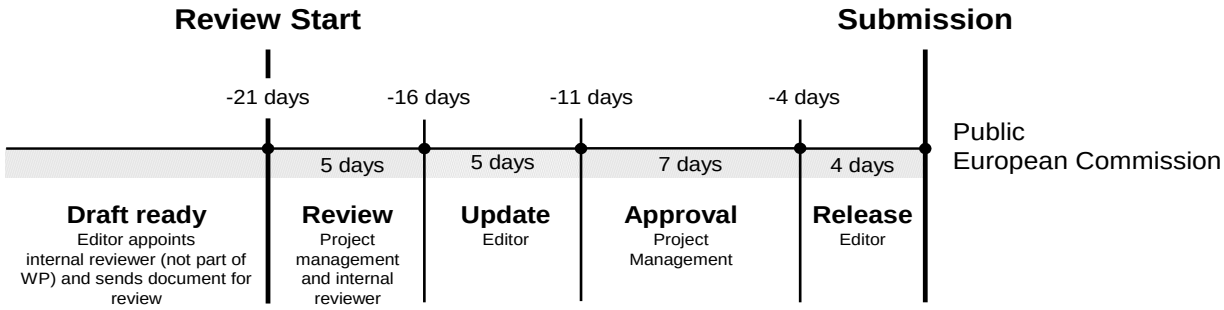

Figure 8: Deliverables and Publications Process

The editor is responsible for appointing an external reviewer and sending a draft to the Project Management at least 21 days before the planned publication or delivery. This draft is also sent to the internal reviewer. A copy is similarly sent to owners of Intellectual Property related to the content. The reviewer and the Project Management shall send their comments back to the editor within 5 days. The editor updates the deliverable within 5 days and sends it back to the Project Management for final approval.

Once approved, the editor prepares the publication for release and submits it to the publisher with a copy sent to the Project Management. If the publication is a deliverable it will be forwarded to the Coordinator who submits it to the Commission. The editor for any deliverable is by default the work package leader. It is the responsibility of the work package leader to ensure that the review form (see Figure 9) has been filled out correctly.

	PM: Technikon			Internal Reviewer		
	Answer	Comments	Type*	Answer	Comments	Type*
1. Is the deliverable in accordance with						
(i) the Description of Work	☐ Yes ☐ No		☐ M ☐ m ☐ a	☐ Yes ☐ No		☐ M ☐ m ☐ a
(ii) The international State-of-the-Art	☐ Yes ☐ No		☐ M ☐ m ☐ a	☐ Yes ☐ No		☐ M ☐ m ☐ a
2. Is the quality of the deliverable such						
(i) that it can be sent to the EC?	☐ Yes ☐ No		☐ M ☐ m ☐ a	☐ Yes ☐ No		☐ M ☐ m ☐ a
(ii) that it needs further editing	☐ Yes ☐ No		☐ M ☐ m ☐ a	☐ Yes ☐ No		☐ M ☐ m ☐ a
(iii) that the content needs to be improved	☐ Yes ☐ No		☐ M ☐ m ☐ a	☐ Yes ☐ No		☐ M ☐ m ☐ a

* Type of comments: M = Major comment, m = minor comments, a = advice

Figure 9: Deliverable Review Form

All in all, in the first project year 15 deliverables and 25 peer-reviewed publications have been compiled in the TClouds project according to these rules. All of them have been of public nature, which (as already stated above) requires special precautions since it implies the disclosure of results to the public.

A complementary process is valid for scientific publications. This means that we use a publication mailinglist to notify all partners about any paper submissions in order to prevent possible IPR conflicts (or establish collaboration on short notice). The basic rules are that the notification should be sent ideally 3 weeks before the submission, however the Consortium has agreed that it can be sent at least 1 one week before and it should contain an abstract of the content. An attached full paper (draft) is not necessary, but if available of course welcome. So far, several scientific publications related to work performed within TClouds have been cleared and submitted for publication.

3.7 IPR issues after the project – Conclusion

In a nutshell, each partner will productise IP that has been solely created by him. The TClouds prototypes will be open source and can therefore be freely reused by the partners and outside parties as well.

The exploitation chapter of this report defines the first iteration of the report on IPR and other issues within the TClouds project, which includes TClouds relevant information on IPR.

The chapters presented are the ones which the partners viewed as the most important ones. In the beginning the prerequisites for the regulatory framework in the TClouds project were introduced. Then the current status concerning different IPR relevant issues in the TClouds project was presented. This effort aims to reduce negative impacts from IPR obstacles in the most professional way.

Chapter 4

Training and Education

Chapter Authors:

Cornelius Namiluko, Imad Abbadi (OXFD)

4.1 Introduction

Training and education is an important aspect of every successful project. It provides an opportunity to (i) *improve the skills of project members* – leading to a better understanding of the problem domain among members and thus a greater chance of producing better results, (ii) *enable knowledge sharing* – leading to better collaboration relationships and (iii) *disseminate project results* – enabling transparency of project activities and greater awareness of the problem domain and thus fostering further research.

Within the TClouds project, training and education will be offered to project members on the topics that relate to the activities of the project. To enable appreciation of the problems addressed within the project, the problems being addressed and the results obtained will be distributed in various forms, including articles, tutorials and demos, to a wider audience. Such education sessions have become an introductory block in our technical workshops.

It is our belief that good educational materials can make a positive output from the project. It is for this reason that some effort has been dedicated towards planning for training and education. Therefore, this report draws out a plan for the training and education that the TClouds project will provide to members and non-members alike. The report has been prepared as part of Task 4.1.4. It outlines the topics that will be covered in training and education, the necessary delivery time frame, the form (tutorial, demos, etc.) the materials will take and the mode of delivery (courses, online resources, etc.)

The report continues with a short description of the method used to come up with the plan before providing details of the plan.

4.2 Methodology

There are a number of partners on the project and each partner has a number of members, resulting in a possible diversification of the range of skills already acquired 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 to every partner to identify their needs. For this reason, this report is based on a survey of the training and education requirements of each partner. 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.

4.3 Training already delivered and received

At this point, the project has been running for over a quarter and results have already started being produced. This means that project members must have already acquired some level of skills. It would be impossible to identify the gaps in skills without understanding the current level of skills within the project. For this reason, this section summarises results from the survey regarding the amount of training that project members have already received.

4.3.1 At project meetings

Project meetings enable members to meet face-to-face. This provides an opportunity for members to share their work, knowledge and skills, and therefore a means of providing training. The Lisbon meeting provided such an opportunity, covering the topics as shown in Table 1. Also, IBM (TClouds partner) organized a workshop at Zurich which covers presentations of scientific papers from well recognized individuals around the world.

Topic	Description
OpenNebula	Covered an introduction of OpenNebula together with a demonstration of its features and how to use it
Introduction to Cloud	This session introduced members to definitions and concepts within cloud computing. This was a good opportunity to get some consensus on some of the conceptualisation of cloud and how that relates to TClouds
OpenStack Introduction	A description of OpenStack and its features
Scientific Presentations	Presenting of published papers to TClouds' partners

Table 10: Topics covered at the Lisbon workshop

4.3.2 Training provided elsewhere

In addition to the training shared at project meetings, some of the partners have had internal training and discussions about security and privacy issues in cloud computing. Some partners have also looked at other cloud related solutions, such as Amazon EC2, as part of their internal activities. In addition the related materials that have been shared (via subversion) by various members have provided insights into cloud computing issues and a starting point for work on TClouds.

4.4 Training needed and planned

A number of members still need some training in the topics surrounding cloud computing. These are discussed in the context of immediate to short-term requirements and long-term plans.

4.4.1 Year 1 requirements

For those members that are involved in the development of the prototype, it is apparent that skills specific to the selected platform (OpenStack) will be needed. More specifically, training in OpenStack-related topics will be needed as members need to understand all aspects of its design in order to extend or modify it. These requirements, together with the necessary time frame, and other topics that should be covered in the first year are indicated in Table 2.

Topic	Description	Time frame	Possible delivery mode
Cloud computing	More training covering general issues with cloud computing. This would serve both as a refresher to those who already know about cloud computing and a primer for those new to cloud computing. In addition, this should provide a clear distinction between the various cloud computing models and how to host services in the cloud	Immediately, and through the length of the project and beyond.	This could be delivered as an always-available resource, e.g. using the e-learning platform from UMM.
TClouds platform properties	This would cover the properties that are expected from a TCloud platform/infrastructure. It would include definitions of the properties such as resilience, reliability etc. as envisaged by the project. It will also provide a means of reaching consensus on the definitions and qualities of a trusted cloud	Immediately, preferably before the design of the TClouds architecture is complete	Again the e-learning platform from UMM could be utilised, in addition a taxonomy can be developed and made available to the appropriate audience
OpenStack	More detailed explanation of the features of OpenStack including administration aspects, development and management. Currently, some of this information is available in fragmented form, but having them in one place and in a consistent structure would be beneficial for the project.	Immediately, preferably before the design of the TClouds architecture is complete	Could be delivered in the form of tutorials or “how tos”

Table 11: Year 1 training requirements

4.4.2 Later requirements and external training opportunities

At this point in time, most of the partners cannot identify any further training that they will require. Nevertheless, there is need to have an idea of these requirements and also to identify possible opportunities that could be used to offer training to non-members. Table 3, therefore lists some of these requirements and opportunities together with a rough idea of the topics that should be included.

Requirement/Event	Description	Possible topics
Application architectures for TClouds	This would cover mechanisms of how to maximise benefits from a TClouds system	What kinds of application architectures can maximise the benefits coming from TClouds How can existing applications be adapted to make use of TClouds
ETISS 2012	The European trusted infrastructure summer school is a yearly event that provides an opportunity for new researchers in the area of trusted computing to get to know about ins and outs of trusted computing. This event could be a good venue to include some TClouds results/challenges. Further discussions are underway to arrange for some sessions on TClouds.	What are the challenges a trusted cloud should offer From non-trusted to trusted cloud: discussion of how the project enhanced an existing cloud Usage of trusted computing within TClouds

Table 12: Training delivery for the future

4.5 Education

The technical and scientific knowledge acquired during the project should be transferred into the education of students. This is 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.

Name	Kind/Description	Partner
Security and Fault-tolerance in Distributed Systems	Course at ETH Zurich	IBM
Protocols for secure cloud computing	Tutorial, presented at METIS-CTDS 2011, International Spring School on Distributed Systems, Marrakech, Apr. 2011	IBM

Name	Kind/Description	Partner
From reliable to secure distributed programming	Tutorial, presented at the 25th International Symposium on Distributed Computing (DISC), Sept. 2011	IBM
Cloud Security Lab	Lab session, given at ETISS 2011, Sept. 2011	TUDA
Cloud Security and Management	Lecture	OXFD
Byzantine Fault-Tolerance	Lecture	FFCUL
Cloud Computing	Debate session, part of a Parallel Computing lecture	FFCUL
Middleware/Cloud Computing	Lecture with integrated practical exercises	FAU
Ausgewählte Kapitel der Systemsoftware: Cloud Computing (Selected topics of system software: Cloud Computing)	Seminar	FAU

Table 13: List of courses taught by project partners

Title/Topic	Kind	Partner
Security and Access Control in MapReduce	M.Sc.	POL
Applications of Trusted Computing on Cloud Architectures - Trusted Cloud Logging	M.Sc.	POL
Cloud-of-Clouds State Machine Replication	Ph.D.	FFCUL
Secure Multi-Party Computations in the Clouds	Ph.D.	FFCUL
Intrusion-tolerant cloud management services	Ph.D.	FFCUL
Pragmatic Intrusion-Tolerant Database Replication	M.Sc.	FFCUL
A Fault-Tolerant SCADA Architecture	M.Sc.	FFCUL
Metadata and Locking Services in a Cloud-of-Clouds File System	M.Sc.	FFCUL
A Virtual Disk Abstraction for a Cloud-of-Clouds File System	M.Sc.	FFCUL

Title/Topic	Kind	Partner
Checkpointing and Recovery in Non-trivial BFT Services	M.Sc.	FFCUL
Cloud resource management for Intrusion-Tolerant service replicas	M.Sc.	FFCUL
Byzantine fault-tolerant Hadoop MapReduce	M.Sc.	FFCUL
Improvements on a State Machine Replication library	M.Sc.	FFCUL
Flexible Replikation von Geschäftsprozessen (Flexible replication of business processes)	M.Sc.	FAU
Entwurf und Implementierung einer sicheren Nachrichtensignatur für verteilte Systeme (Design and implementation of a secure message signature for distributed systems)	B.Sc.	FAU
Minimizing Human Administrator Interventions in Infrastructure Clouds	M.Sc.	IBM

Table 14: List of theses supervised by project partners

Chapter 5

List of Abbreviations

Acronym	Meaning
BSD	Berkeley Software Distribution
CA	Consortium Agreement
CDA	Confidential Disclosure Agreement
EC	European Commission
EP	European Patent
GA	Grant Agreement
GNU	Gnu's not Unix
GPL	General Public Licence
IP	Intellectual Property
IPR	Intellectual Property Rights
KVM	Kernel-based Virtual Machine
LGPL	Lesser General Public License
NDA	Non-Disclosure Agreement
CMS	Content Management System