D4.1.2

Updated Dissemination, Training, Standardisation and Exploitation Report

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

Deliverable type:	Report
Deliverable reference number:	ICT-257243 / D4.1.2 / 2.0
Activity and Work package contributing to the deliverable:	Activity 4 / WP 4.1
Due date:	March 2013 – M30
Actual submission date:	2nd April, 2013

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

Abstract:	This deliverable reports on the progress of the dissemination, standardisation, exploitation and project internal/external education and training activities during project year 2.
Keywords:	Dissemination, Training, Standardisation, Exploitation

Editor

Sven Bugiel (TUDA)

Contributors

Imad Abbadi (OXFD)

Stefan Nürnberger (TUDA)

Elmar Husmann (IBM)

Norbert Schirmer (SRX)

Martina Truskaller, Patricia Rio Branco (TEC)

with contributions from TClouds partners

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 implementing the strategy for dissemination of the project, the standardisation and exploitation efforts of project results, and project internal/external training and teaching during the second year of the TClouds project.

In particular, this deliverable reports on the progress of the standardisation and exploitation efforts.

- A project internal survey at consortium level refines the exploitation efforts of each project partner and helps identifying potential joint exploitation opportunities.
- Standardisation opportunities identified in year one have been assessed by the project partners and potential contributions to those standards been identified.

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

- With 12 peer-reviewed scientific publications, including publication at renowned international conferences and workshops such as ACM EuroSys and ACM ASIACCS, the project partners continued the successful scientific dissemination of the first year.
- Several project partners jointly authored and contributed a chapter to the book “European Research Activities in Cloud Computing”
- Project partner were involved in and responsible for the organisation of some academic and industrial flagship events including Dagstuhl Seminars, CSA SecureCloud, or ACM CCSW.
- Several project partners represented the TClouds project at more than 60 different occasions at academic and industrial events during Y2.

Updated version 2.0 (2nd April 2013)

Overall, this document updates D4.1.2 as submitted in M24 of the project. In particular, Chapter 3 and Chapter 4 were updated according to the reviewers' and project officer's recommendations. Chapter 3 now contains in Section 3.5 explicit plans for standardization efforts in year 3 of the project. The exploitation plans presented in Chapter 4 extend the original exploitation questionnaire introduced in the first version of this deliverable and now also address non-commercial exploitation aspects and hence take into consideration the plans of the academic partners. Moreover, more concrete plans for joint exploitation efforts are presented in Section 4.4. In addition to these major points, the TClouds project partners created *TClouds Facts Sheets* (Section 2.4), which contain high-level descriptions of some components, prototypes, and use cases developed within the TClouds project and which are expected to greatly enhance the dissemination of the project results as well as to help initiating exploitation of these results.

Contents

List of Figures

List of Tables

Chapter 1 Introduction

1.1 TClouds - Trustworthy Clouds

TClouds aims to develop trustworthy Internet-scale cloud services, providing computing, network, and storage resources over the Internet. Existing cloud computing services are today generally not trusted for running critical infrastructure, which may range from business-critical tasks of large companies to mission-critical tasks for the society as a whole. The latter includes water, electricity, fuel, and food supply chains. TClouds focuses on power grids and electricity management and on patient-centric health-care systems as its main applications.

The TClouds project identifies and addresses legal implications and business opportunities of using infrastructure clouds, assesses security, privacy, and resilience aspects of cloud computing and contributes to building a regulatory framework enabling resilient and privacy-enhanced cloud infrastructure.

The main body of work in TClouds defines an architecture and prototype systems for securing infrastructure clouds, by providing security enhancements that can be deployed on top of commodity infrastructure clouds (as a cloud-of-clouds) and by assessing the resilience, privacy, and security extensions of existing clouds.

Furthermore, TClouds provides resilient middleware for adaptive security using a cloud-of-clouds, which is not dependent on any single cloud provider. This feature of the TClouds platform will provide tolerance and adaptability to mitigate security incidents and unstable operating conditions for a range of applications running on a cloud-of-clouds.

1.2 Activity 4 – Programme Management and Dissemination

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

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

1.3 Workpackage 4.1 - Standardisation and Dissemination

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

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

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

1.4 Deliverable 4.1.2 - Updated Report on Dissemination, Training, Standardisation and Exploitation

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

Structure. The remainder of this deliverable is organised as follows. Chapter 2 presents the dissemination activities of year 2. Chapter 3 summarizes the assessment results for the potential contributions of the TClouds project to various standards. In Chapter 4 the results of a project internal questionnaire regarding exploitation at partner level and the consequence for exploitation at consortium level are presented. Chapter 5 lists the ongoing efforts for education and training. Chapter 6 is the appendix, containing the detailed standards assessments.

Deviation from Workplan. This deliverable conforms to the DoW/Annex I, Version 2.

Target Audience. The present deliverable aims at providing an overview of the dissemination, standardisation, and exploitation efforts of the TClouds project to all interested parties.

Relation to other Deliverables. Figure 1 illustrates the structure of WP4.1 and its relation to other work packages according to the DoW/Annex I.

The deliverables of WP4.1, including the present deliverable D4.1.2, relate to most other deliverables and work packages by receiving the achieved results (deliverables, presentations, scientific publications) as input. This deliverable summarizes the dissemination activities leveraging the achieved results, elaborates on the progress of devising exploitation plans at partner and consortium level from these results as well as assessing the potential contribution of these results to standards. Moreover, the progress on transferring the acquired knowledge and technology to training and education is presented.

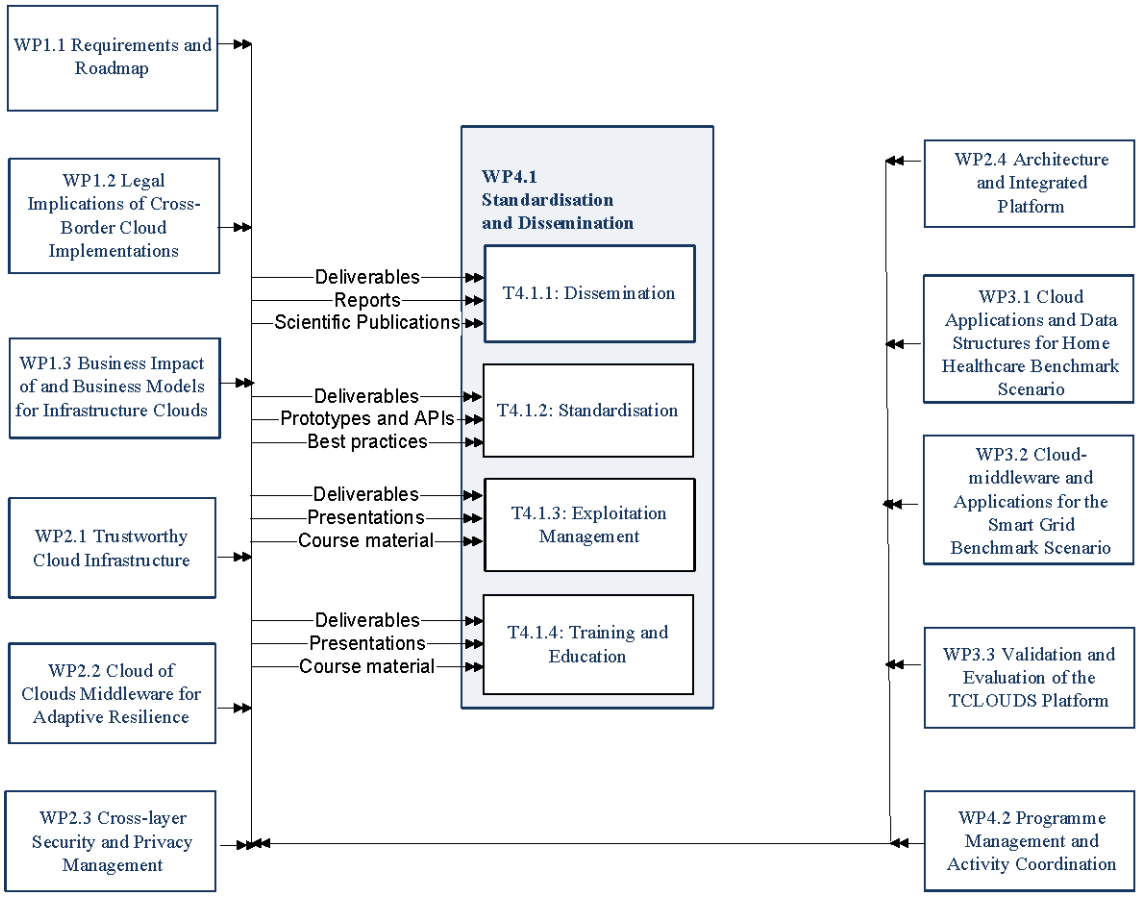


Figure 1: Graphical structure of WP4.1 and relations to other workpackages.

Chapter 2

Dissemination

Chapter Authors:

Sven Bugiel (TUDA), Martina Truskaller (TEC)

2.1 Introduction

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

2.2 Dissemination Strategy

No update to the dissemination strategy was deemed necessary due to the successful dissemination in year 1 and on-going dissemination activities in year 2.

2.3 Dissemination Activities

We now present the dissemination activities executed since the activities reported in deliverable D4.1.1 in M18 of the project.

2.3.1 Organized conferences and events

The following conferences/workshops and events have been (co-)organized by project partners. Additional information is remarked.

Name	Date & place	Remarks
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 by and invited talk by partner TUDA
Dagstuhl Seminar 11491: Secure Computing in the	04.-09.12.2011, Schloss Dagstuhl, Germany	Seminar for academic and industrial interested

Name	Date & place	Remarks
Cloud		
CSA 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
CSA SecureCloud	9.-10.05.2011, Frankfurt, Germany	Workshop with industrial partners, project partners, and invited experts; Organized by TUDA, Fraunhofer SIT, ENISA and CSA
1st European Workshop on Dependable Cloud Computing (together with EDCC'12)	8.5.2012, Sibiu, Romania	Open workshop in conjunction with EDCC'12 and with participation from several other EU-funded projects addressing cloud dependability & security. See http://ewdcc12.di.fc.ul.pt.
Dagstuhl Seminar 12-0111: Security and Dependability for Federated Cloud Infrastructures	9.-13.7.2012, Schloss Dagstuhl, Germany	Seminar for academic and industrial interested
Birds of a Feather session at the DSN 2012 conference: "Cloud Computing Resilience in practice: harder than it looks"	July 2012, Boston, USA	Organized by FFCUL, for academic and industrial interested
CPDP conference	25.01.2013, Brussels	"Panel on Cloud, Trust and Privacy: Towards the InterCloud" organized by partners ULD, INNOVA and others.

Table 1: List of organized conferences/workshops

2.3.2 List of scientific (peer-reviewed) publications

The following list provides an overview of the scientific publications and articles by partners of the TClouds project, which have been peer-reviewed and accepted. This list comprises publications of Y2 *only.* For an overview of the overall publication record of the project partners, please refer to the *Publication* section on the project website (https://www.tclouds-project.eu/index.php?option=com_jumi&fileid=3).

Publication title	Conference/Workshop/Journal	Authors
Automated Information Flow Analysis of Virtualized Infrastructures	14th European Symposium on Research in Computer Security (ESORICS'11), Springer-Verlag, LNCS 6879, 2011	S. Bleikertz, K. Eriksson, T. Groß, M. Schunter
A comparison of secure multi-tenancy	12th ACM/IFIP/USENIX international conference on	C. Cachin, M. Gupta, R. Haas, A. Kurmus, R.

Publication title	Conference/Workshop/Journal	Authors
architectures for filesystem storage clouds	Middleware (Middleware'11), Springer-Verlage, 2011	Pletka
A cloud you can trust	IEEE Spectrum, vol. 48, no. 12, pp 28-51, Dec 2011	C. Cachin, M. Schunter
Insiders Analysis in Cloud Computing Focusing on Home Healthcare System	International Conference for Internet Technology and Secured Transactions (ICITST), IEEE, 2011	I. Abbadi, C. Namiluko, A. Martin
Dynamics of Trust in Clouds	International Conference for Internet Technology and Secured Transactions (ICITST), IEEE, 2011	I. Abbadi, C. Namiluko
A framework for establishing trust in the Cloud	Computers and Electrical Engineering Journal, ELSEVIER, Sep 2012	I. Abbadi, M. Alawneh
Byzantine Fault-Tolerant MapReduce: Faults are Not Just Crashes	3rd International Conference on Cloud Computing Technology and Science (CLOUDCOM '11), IEEE, 2011	A. Bessani, M. Correia, P. Costa, M. Pasin
Automated Verification of Virtualized Infrastructures	ACM Cloud Computing Security Workshop (CCSW'11), ACM, 2011	S. Bleikertz, T. Groß, S. Mödersheim
Challenges for Provenance in Cloud Computing	3rd USENIX Workshop on Theory and Practice of Provenance (TaPP'11), USENIX, 2011	I. M. Abbadi, J. Lyle
Integrity and Consistency for Untrusted Services	37th Conference on Current Trends in Theory and Practice of Computer Science (SOFSEM 2011), Springer-Verlag, 2011	C. Cachin
Providing Fault-tolerant Execution of Web-service-based Workflows within Clouds	2nd International Workshop on Cloud Computing Platforms (CloudCP '12), ACM, 2012	J. Behl, T. Distler, F. Heisig R. Kapitza, M. Schunter
Secure Cloud Maintenance - Protecting workloads against insider attacks	7th ACM Symposium on Information, Computer and Communications Security (ASIACCS'12), ACM, 2012	S. Bleikertz, A. Kurmus, Z. A. Nagy, M. Schunter
CheapBFT: Resource-efficient Byzantine Fault Tolerance	7th ACM European Conference on Computer Systems (EuroSys '12), ACM, 2012	R. Kapitza, J. Behl; C. Cachin, T. Distler, S. Kuhnle, S. V. Mohammadi, W. Schröder-Preikschat, K. Stengel
Efficient Byzantine Fault Tolerance	IEEE Transactions on Computers. Published online (10.1109/TC.2011.221), to appear on a future issue of the	G. Santos Veronese, M. Correia, A. Bessani, L. C. Lung, P. Verissimo

Publication title	Conference/Workshop/Journal	Authors
	journal	
Privacy and Resilience for Internet-scale Critical Infrastructures	Chapter of the book “European Research Activities in Cloud Computing”, edited by Dana Petcu and José Vásquez-Poletti. Cambridge SP. March 2012.	A. Bessani, I. M. Abbadi, S. Bugiel, E. Cesena, M. Deng, M. Grone, N. Marnau, S. Nürnberger, M. Pasin, N. Schirmer
The TClouds Architecture: Open and Resilient Cloud-of-Clouds Computing.	2nd International Workshop on Dependability of Clouds, Data Centers and Virtual Computing Environments (DCDV’12), together with IEEE/IFIP DSN'12	P. Verissimo, A. Bessani, M. Pasin
From Byzantine Consensus to BFT State Machine Replication: A Latency-optimal transformation.	9th European Conference on Dependable Computing (EDCC’12)	J. Sousa, A. Bessani
Clouds Trust Anchors	11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom’12), IEEE, 2012	I. M. Abbadi
DQMP: A Decentralized Protocol to Enforce Global Quotas in Cloud Environments	14th International Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS '12), Springer-Verlag, 2012	J. Behl, T. Distler, R. Kapitza
On Limitations of Using Cloud Storage for Data Replication	6th Workshop on Recent Advances in Intrusion Tolerance and reSilience (WRAITS 2012), DSN 2012 Workshops, IEEE, 2012	C. Cachin, B. Junker, A. Sorniotti
Robust Data Sharing with Key-Value Stores	International Conference on Dependable Systems and Networks (DSN’12), IEEE, 2012	C. Basescu, C. Cachin, I. Eyal, R. Haas, M. Vukolic
A look to the old-world sky: EU-funded dependability cloud computing research.	ACM SIGOPS Operating Systems Review. Volume 46, Number 3, pp. 43-56. July 2012.	A. Bessani, R. Kapitza, D. Petcu, P. Romano, S. V. Gogouvitis, D. Kyriazis, and R. G. Cascella
Security and Privacy Enhancing Multi-Cloud Architectures	IEEE Transactions on Dependable and Secure Computing. Voulume 99, 2013	J.-M. Bohli, N. Gruschka, M. Jensen, L. Iacono, N. Marnau

Table 2: List of scientific peer-reviewed publications

2.3.3 List of non-peer reviewed publications

The following table supplements the list from Section 0 with publications that were not peer-reviewed but contributed to the dissemination activities of the project in Y2.

Publication title	Conference/Workshop/Journal	Authors
From Trusted Cloud Infrastructures to Trustworthy Cloud Services	13th Information Security Solutions Europe Conference (ISSE'11). November 2011	M. Gröne, N. Schirmer
Vertraulichkeit und Integrität von Daten und IT-Systemen im Cloud-Zeitalter (Data confidentiality and integrity of IT systems in the cloud era)	Datenschutz und Datensicherheit (DuD), Springer-Verlag, Vol. 36, No. 6, 2012	M. Hansen

Table 3: List of non-peer reviewed publications

2.3.4 List of legal policy papers and standards

The following table supplements the list from Section 0 with contributions to legal policy papers and relevant standards. These publications are drafted by working groups, committees and advisory boards involving TClouds partners. Results of the TClouds research have a relevant impact on the content.

Publication title	Published by	Contributing Partner
Orientierungshilfe – Cloud Computing **(Guidelines for Cloud Computing)**	Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (Working Groups Technology and Media of the Conference of German DPAs), published September/October 2011 http://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf	ULD
Opinion on Cloud Computing	Article 29 Data Protection Working Party, 01037/12/EN, WP 196, published July 2012 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf	ULD

Table 4: List of legal policy papers and standards to which TClouds contributed

2.3.5 Further Dissemination Activities

The following table supplements the list from Section 0 according to the *Guidance Notes on Project Reporting (version 2012)* of the European Commission with further dissemination activities in Y2.[1]

Type of activity[2]	Title	Partners
Workshop	International Workshop on Cloud Computing: Architecture, Algorithms and Applications. July 2011	OXFD
Workshop	Second International Workshop on Trust Management in P2P Systems. July 2011	OXFD
Other	Customer Meeting August 2011 (Requirements Analysis)	SRX
Other	Customer Meeting September 2011 (Requirements Analysis)	SRX
Workshop	8th VLDB Workshop on Secure Data Management (SDM'11). September 2011	PHI
Conference	7. Fachtagung IT-Beschaffung. September 2011	ULD
Other	Second Customer Meeting September 2011 (Requirements Analysis)	SRX
Workshop	IT Security Association working group of TeleTrust AG. September 2011	SRX
Other	W3C Tracking Protection Working Group Meeting, Santa Clara, October 2011	ULD
Other	Customer Meeting October 2011 (Requirements Analysis)	SRX
Conference	ACM Cloud Computing Security Workshop (ACM CCSW) 2011 http://crypto.cs.stonybrook.edu/ccsw11/	IBM
Workshop	CloudDB´11 http://www.clouddb.org/CloudDB11	OXFD, PHI, HSR
Presentation	23rd ACM Symposium on Operating Systems Principles	FFCUL
Workshop	The Sixth ACM Workshop on Scalable Trusted Computing (ACM STC 2011)	POL
Conference	10th IEEE International Conference on Trust, Security, and Privacy http://trust.csu.edu.cn/conference/trustcom2011/	OXFD
Conference	Communications and Multimedia Security - CMS 2011 http://www.cms2011.net/	TUDA
Conference	13th Information Security Solutions Europe Conference (ISSE)	SRX

[1] Including some Y1 events which have not been reported in the first year.

[2] Type of activity: conferences, workshops, press releases, flyers, articles published in popular press, videos, media briefing, presentations, exhibitions, interviews, films, TV clips, posters, others.
Type *publication* is listed separately in Sections 0 and 2.3.3. Type *web* is listed in Section 2.3.6.Type *thesis* is reported in Chapter 5 Training and Education.

Type of activity[2]	Title	Partners
Presentation	IBM Cloud Computing Symposium	TUDA, IBM
Conference	A smart grid in TClouds. SMI European Smart Grid Cyber Security and Privacy. November 2011	EDP
Presentation	Messekongress IT. November 2011	ULD
Workshop	SecTXL 2011 Re-experience Security: From Technology to Law. November 2011	ULD
Workshop	IT Security Association working group of TeleTrust AG. November 2011	SRX
Other	Customer Meeting November 2011 (Requirements Analysis)	SRX
Workshop	2nd International Workshop on Cloud Applications and Security (CAS'11). December 2011	OXFD
Conference	Association Meeting of Security on Smart Grid Solutions (German Federal Ministry of Economics and Technology). December 2011	SRX
Presentation	Dagstuhl Seminar 11491: Secure Computing in the Cloud	TUDA
Conference	Association meeting	SRX
Conference	6th International Conference for Internet Technology and Secured Transactions (ICITST)	OXFD
Other	Customer Workshop December 2011 (Requirements Analysis)	SRX
Workshop	IT Security Association working group of TeleTrust AG. January 2012	SRX
Presentation	OMNICARD 2012, Cloud Computing – Privacy Requirements, Berlin, January 2012	ULD
Presentation	Can security- and privacy-critical applications be housed in the clouds? TClouds says yes! 61st IFIP WG 10.4 Meeting. January 2012. Sainte-Luce – France.	FFCUL
Other	W3C Tracking Protection Working Group Meeting, Brussels, January 2012	ULD
Conference	5th International Conference Computers, Privacy & Data Protection (CPDP), Brussels, January 2012	ULD
Other	Customer Meeting February 2012 (Requirements Analysis)	SRX
Conference	EFA Academy Smart Grids II. February 2012	EDP, EFA, FFCUL
Presentation	3. NetUSE AG Salon "information technology insight banquet", Security and Cloud Computing, Kiel, February 2012	ULD
Presentation	TÜV NORD Akademie, Privacy Conference (Fachtagung Datenschutz), Hamburg, March 2012	ULD
Presentation	CeBIT 2012, March 2012	ULD
Conference	RSA. February 2012.	SRX

Type of activity[2]	Title	Partners
Summit	A Smart Grid in TClouds. SCADA and Smart Grid Cyber Security Summit. April 2012	EDP
Forum	TClouds – Building a Trusted Cloud. SMI European Smart Grid Cyber Security Forum. March 2012	EDP, SRX
Presentation	(BFT) State Machine Replication: Hype and Virtue... and even some Practice. Tutorial presented at ACM EuroSys'12 Conference.	FFCUL
Presentation	… And State Machine replication for all with BFT-SMaRt. Poster presented at ACM EuroSys'12 Conference.	FFCUL
Presentation	Replication in the Cloud-of-Clouds. Invited talk at the "13th Brazilian Workshop on Tests and Fault Tolerance, together with SBRC'12"	FFCUL
Presentation	Wirtschaftskammer Österreich e-day 2012, Sicherheit für Social Media im Unternehmen	IBM
Other	Customer Meeting March 2012 (Requirements Analysis)	SRX
Presentation	Law firm Bird&Bird's IT Law Conference, Frankfurt, March 2012	ULD
Conference	Microsoft Roundtable – Cloud, Privacy & Standardisation, Brussels, March 2012	ULD
Other	W3C Tracking Protection Working Group Meeting, Washington DC, April 2012	ULD
Conference	Trusted Cloud Conference of German Federal Ministry of Economics and Technology, Berlin, April 2012	ULD
Conference	Secure Cloud 2012. May 2012	FFCUL, TUDA
Workshop	IT Security Association working group of TeleTrust AG. May 2012	SRX
Other	Partner Meeting May 2012 (follow-up Projects)	SRX
Other	Customer Meeting May 2012 (Requirements Analysis)	SRX
Other	IT Security Association meeting of TeleTrust AG. May 2012	SRX
Other	Second Customer Meeting May 2012 (Requirements Analysis)	SRX
Other	Third Customer Meeting May 2012 (Requirements Analysis)	SRX
Seminar	Using Cloud Computing in Smart Grids – Experiences from the EU FP7 TClouds Project. Ensuring IT Security for Energy Infrastructures. May 2012	EDP
Presentation	Conference on Geographic Information Systems and Cloud Computing, Munich, May 2012	ULD
Presentation	Architectural resilience in cloud computing. SecureCloud 2012. May 2012. Frankfurt, Germany	FFCUL
Presentation	Can security- and privacy-critical applications be housed in the clouds? TClouds says yes! Schloss Dagsthul Seminar *on Security and Privacy in*	FFCUL

Type of activity[2]	Title	Partners
	Smart Energy Grids. December 2011. Schloss Dagsthul-Germany.	
Other	TUBS.City 2012. June 2012	TUBS
Workshop	IT Security Association working group of TeleTrust AG. June 2012	SRX
Other	Information Day for followup projects. June 2012	SRX
Presentation	Workshop on Cloud Security, University Paderborn, June 2012	ULD
Other	Customer Meeting July 2012 (Requirements Analysis)	SRX
Presentation	Towards a Cloud-of-Clouds File System. Dagstuhl Seminar on *Security and Dependability for Federated Cloud Infrastructures*. July 2012. Schloss Dagsthul-Germany.	FFCUL
Workshop	IT Security EU. July 2012	SRX
Conference	Birds of a Feather session at the DSN 2012 conference: "Cloud Computing Resilience in practice: harder than it looks"	FFCUL
Presentation	AT&T Reunion	FFCUL
Other	IT Security Association working group	SRX
Conference	PET (Privacy Enhancing Technologies) Symposium 2012, Vigo (Spain), July 2012	ULD
Other	Customer Meeting August 2012 (Requirements Analysis)	SRX
Workshop	CloudIDEAS for eGovernment, Bremen, August 2012	ULD
Other	Working Group on legal policies for cloud of the German Federal Ministry of Economics and Technology, Berlin, August 2012	ULD
Presentation	Workshop: Development of Privacy legal policies in ISO/IEC standards, Working Draft 27018 "Data Protection Controls For Public Clouds", Berlin, August 2012	ULD
Presentation	Workshop for admitted experts of the Schleswig-Holstein Privacy Seal, Kiel, August 2012	ULD
Presentation	Cloud Security Alliance EMEA Congress 2012, Amsterdam, September 2012	ULD
Other	Working Group on legal policies for cloud of the German Federal Ministry of Economics and Technology, Bonn, September 2012	ULD
Other	Working Group on legal policies for cloud of the German Federal Ministry of Economics and Technology, Düsseldorf, September 2012	ULD
Other	Customer Meeting September 2012 (Requirements Analysis)	SRX
Conference	OECD conference, Tokyo (Japan). September 2012	FSR
Conference	ITU conference, m-health. September 2012	FSR

Type of activity[2]	Title	Partners
Conference	D-A-CH Security, September 2012	SRX
Conference	Security Couds & Mobility ERIC conference, 23.-24.10.2012, Barcelona, Spain	TEC
Conference	Effectplus: ICT Trust & Security	TEC
Other	Debate session: Cloud Computing, since 2011 ongoing	FFCUL
Workshop	Cloud Security Alliance EMEA Congress 2012	ULD
Other	Working Group on legal policies for cloud of the German Federal Ministry of Economics and Technology	ULD
Workshop	Securing Clouds and Mobility	TEC
Flyer	TClouds Leaflet Update	TEC
Workshop	IT Security Association working group	SRX
Conference	thinksmart conference - Conference on Smart Grid security	SRX
Presentation	European Symposium on Research in Com-puter Security (ESORICS)	IBM
Presentation	Bretagne-Networking Workshop on Storage	IBM
Presentation	Computer & Electronics Security Applications Rendez-vous (C&ESAR)	IBM
Conference	Connect 2012, 13.11.2012, 07.02.2013, Brussels	TEC

Table 5: List of further dissemination activities

2.3.6 New Websites

Websites related to the project, which have been launched in Y2.

Website	Description of the main TClouds related information
http://www.ibr.cs.tu-bs.de/projects/tclouds	Project website of partner TUBS
http://en.wikipedia.org/wiki/Cloud_computing#Research	Link to TClouds project website on Wikipedia for the article on *Cloud Computing,* section research (TUDA)

Table 6: Project related websites launched in Y2

2.3.7 TClouds project website statistics

In the following we present statistics about the TClouds project website (http://www.tclouds-project.eu) to underline the successful dissemination activities of both Y1 and Y2 of TClouds.

2.3.7.1 Website visitors

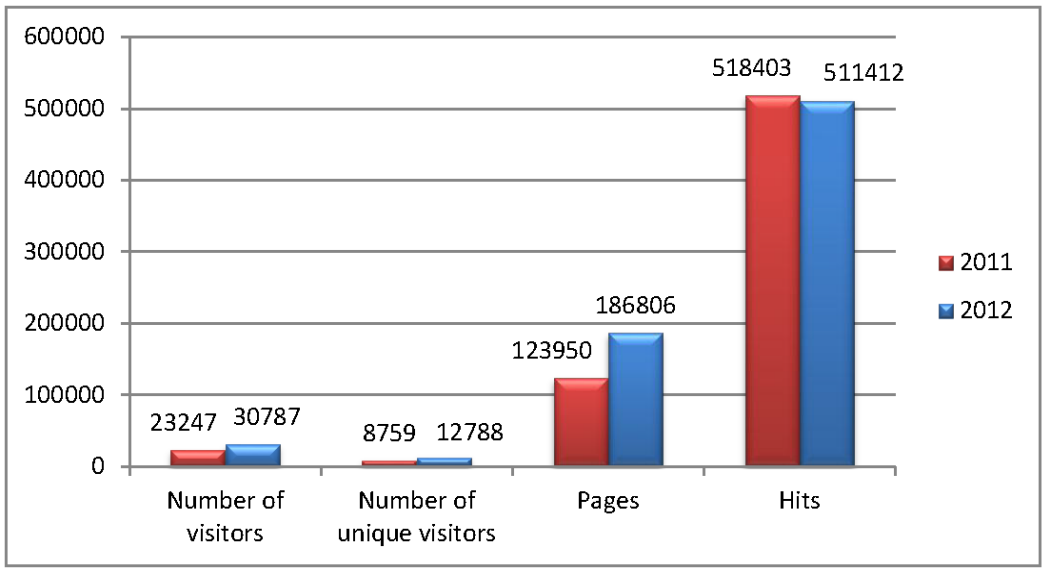


Figure 2: Visitor website statistics for TClouds project

Figure 2 presents the visitor statistics for the project website for the first and second project year. Although the number of hits slightly decreased, the overall number of pages and (unique) visitors clearly increased, thus underlining the successful dissemination efforts.

2.3.7.2 Top downloads

The following tables Table 7 and Table 8 present statistics about the top downloaded content in the first and second project year. While in 2011, for obvious reasons, promotional material clearly dominated the download list, in 2012 a high demand for the published deliverables was observed.

Position	2011	#Downloads
1	TClouds leaflet	179
2	Privacy meets innovation	71
3	Promotion video	62
4	Press release November'11	52
5	General Introduction video	24
6	Smart metering journal	19
7	N/A	N/A
8	N/A	N/A
9	N/A	N/A
10	N/A	N/A

Table 7: Top downloaded content from project website in 2011

Position	2012	#Downloads
1	TC-D1.2.2	475
2	TC-D2.1.1	458
3	TC-D1.3.1	402
4	TC-D3.1.1	358
5	TC-D2.4.1	356
6	TC-D3.2.2	295
7	TC-D1.1.1	288
8	TC-D2.3.1	269
9	TC-D2.2.1	263
10	TC-D1.1.3	236

Table 8: Top downloaded content from project website in 2012

2.3.7.3 Search engine queries

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

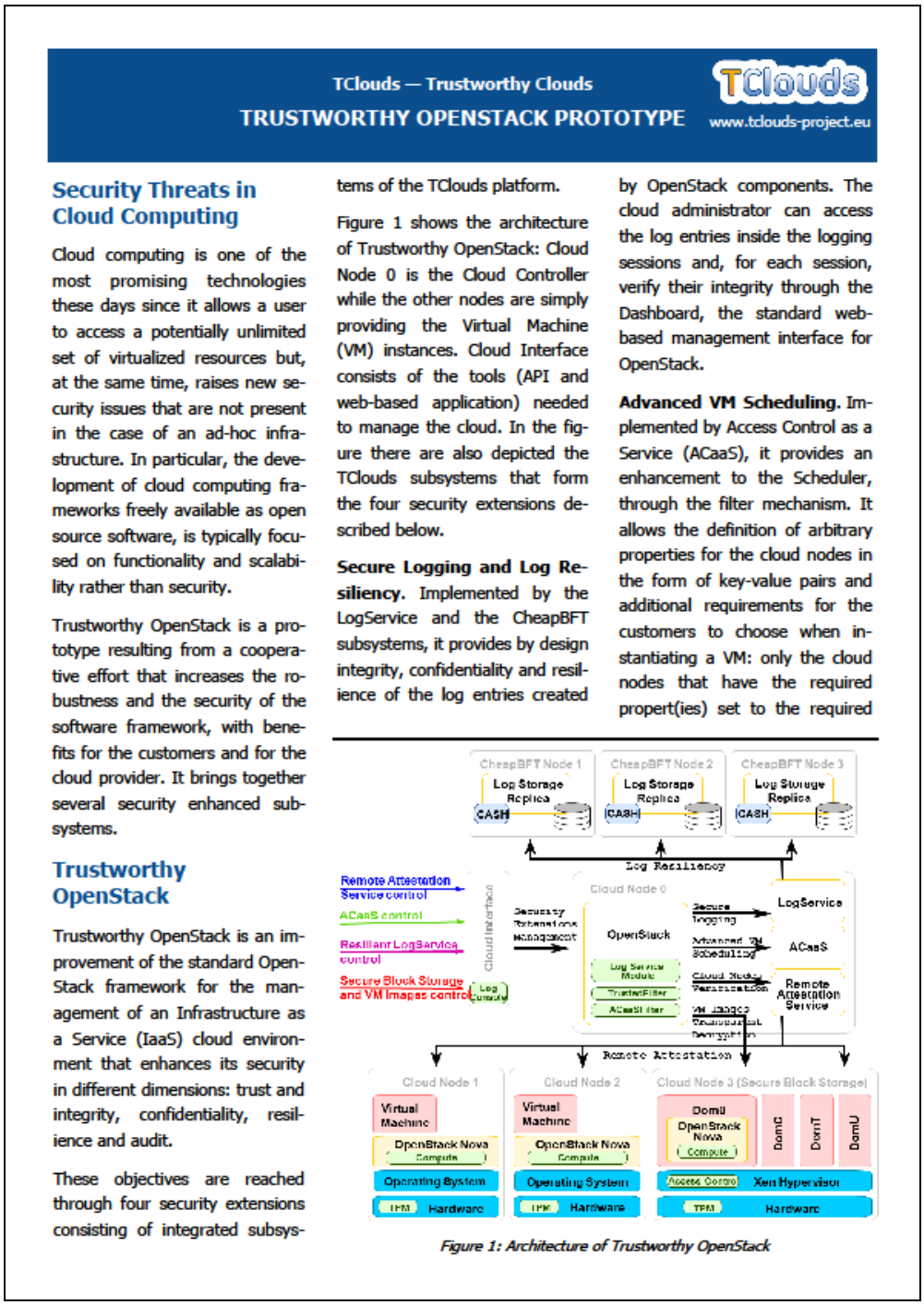
2.3.8 Updated TClouds Project Leaflet

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

Currently TEC is responsible for the leaflet update. The leaflet is under revision due to the ongoing project amendment. The new version of the leaflet will be published as soon as possible on our official project website.

2.4 TClouds Fact Sheets ("TCloudlets")

TClouds fact sheets (or "TCloudlets") contain high-level descriptions of some of the components, prototypes, and use cases developed within the TClouds project. These fact sheets explain the advantages of TClouds technology in an easily accessible way and thus greatly help in disseminating the project results to the industrial and academic communities. Each topic is illustrated on a printable 2-page document in PDF format available for free download from that TClouds project website under **About TClouds → Fact Sheets** or the URL http://www.tclouds-project.eu/index.php/about-tc/factsheets. Figure 3 and Figure 4 present the front-page and back-page of a TClouds Fact Sheet example.



TClouds — Trustworthy Clouds

TRUSTWORTHY OPENSTACK PROTOTYPE

www.tclouds-project.eu

Security Threats in Cloud Computing

Cloud computing is one of the most promising technologies these days since it allows a user to access a potentially unlimited set of virtualized resources but, at the same time, raises new security issues that are not present in the case of an ad-hoc infrastructure. In particular, the development of cloud computing frameworks freely available as open source software, is typically focused on functionality and scalability rather than security.

Trustworthy OpenStack is a prototype resulting from a cooperative effort that increases the robustness and the security of the software framework, with benefits for the customers and for the cloud provider. It brings together several security enhanced subsystems.

Trustworthy OpenStack

Trustworthy OpenStack is an improvement of the standard OpenStack framework for the management of an Infrastructure as a Service (IaaS) cloud environment that enhances its security in different dimensions: trust and integrity, confidentiality, resilience and audit.

These objectives are reached through four security extensions consisting of integrated subsystems of the TClouds platform.

Figure 1 shows the architecture of Trustworthy OpenStack: Cloud Node 0 is the Cloud Controller while the other nodes are simply providing the Virtual Machine (VM) instances. Cloud Interface consists of the tools (API and web-based application) needed to manage the cloud. In the figure there are also depicted the TClouds subsystems that form the four security extensions described below.

Secure Logging and Log Resiliency. Implemented by the LogService and the CheapBFT subsystems, it provides by design integrity, confidentiality and resilience of the log entries created by OpenStack components. The cloud administrator can access the log entries inside the logging sessions and, for each session, verify their integrity through the Dashboard, the standard web-based management interface for OpenStack.

Advanced VM Scheduling. Implemented by Access Control as a Service (ACaaS), it provides an enhancement to the Scheduler, through the filter mechanism. It allows the definition of arbitrary properties for the cloud nodes in the form of key-value pairs and additional requirements for the customers to choose when instantiating a VM: only the cloud nodes that have the required propert(ies) set to the required

Figure 1: Architecture of Trustworthy OpenStack

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

TClouds — Trustworthy Clouds

TRUSTWORTHY OPENSTACK PROTOTYPE

www.tclouds-project.eu

value(s), will be selected for the deployment of the VM.

Cloud Nodes Verification. Implemented by Remote Attestation (RA) Service subsystem, it also provides an enhancement to the Scheduler, again through the filter mechanism. It works similarly to the *Advanced VM Scheduling* extension, whereas the allowed property for the nodes (and the requirement for the VM(s) to be deployed) is the node integrity level that can assume one out of five values. The integrity level represents the summary of the integrity state of a node and may indicate that all running software is recognized as being part of a Linux distribution and all related packages are up-to-date. Or, that some packages related to the running software are not updated, because improvements or security-critical bug fixes are available. The integrity level may also indicate that not all running software is recognized as being part of the distribution. This security extension allows the customer to select the nodes for deploying a VM in a pool of Trusted Nodes - since the integrity state information of the nodes is collected through Trusted Computing technologies.

Transparent Encryption. Exploiting the cryptography-as-a-service component, the system encrypts data in VM instances and block-storage devices. It provides a secure mechanism to store the VM images encrypted and to decrypt/encrypt them on-the-fly using customer keys protected from a malicious cloud administrator by means of Trusted Computing technologies.

Upcoming Security Extension

Trusted Virtual Domains (TVDs). Implemented by Ontology-based Reasoner subsystem, it provides a way to logically group together VMs belonging to a single customer (while possibly running on different nodes) and make them communicate to each other freely and be isolated from VMs of other customers. A customer may own many TVDs. A basic support for TVDs is already present, through the Quantum component, in the Folsom release of the standard OpenStack. This TClouds extension builds on Quantum and enforces the isolation through confidentiality and integrity of the communications using secure protocols like IPsec.

Further Information

Further information about *Trustworthy OpenStack* can be found under Deliverable „D2.4.2—Initial Component Integration, Final API Specification, and First Reference Platform".

Disclaimer

The TClouds project has received funding from the European Union's Seventh Framework Programme (FP7/2007-2013) under grant agreement number ICT-257243.

TClouds at a glance

Project number:
257243

TClouds mission:
- Develop an advanced cloud infrastructure that delivers computing and storage with a new level of security, privacy, and resilience.
- Change the perceptions of cloud computing by demonstrating the prototype infrastructure in socially significant application areas.

Project start:
01.10.2010

Project duration:
3 years

Total costs:
EUR 10.536.129

EC contribution:
EUR 7.500.000

Consortium:
14 partners from 7 different countries.

Project Coordinator:
Dr. Klaus-Michael Koch
coordination@tclouds-project.eu

Technical Leader:
Dr. Christian Cachin
cca@zurich.ibm.com

Project website:
www.tclouds-project.eu

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

2.5 Updated 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 (Germany)
Amazon Web Services LLC	N/A[3]	TUDA	International
TCG Members Meeting	Sirrix is member of the Trusted Computing Group	SRX	International
CloudCycle Project sponsored by the German Federal Ministry of Economics and Technology	Liason Meeting with the German Project CloudCycle	IBM	International

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

[3] The content/type of the cooperation is confidential and cannot be disclosed.

Chapter 3

Standardisation

Chapter Authors:

Elmar Husmann (IBM)

Detailed Standards Analysis provided by all TClouds Partners (see Chapter 6 - Appendix)

3.1 Introduction

In the recently published Communication from the European Commission "Unleashing the Potential of Cloud Computing in Europe"[4], one out of the three key action lines of the European Cloud Strategy is called "Cutting through the Jungle of Standards".

The "Jungle of Standards" is certainly a valid observation for the domain of cloud computing, as indeed there is not a single set of open cloud standards. On the contrary, there are multiple parallel and competing developments as well emerging de-facto standards (such as the Amazon EC2 APIs). While this jungle is certainly difficult to navigate, it also reflects the current dynamics of the cloud computing market and technology development. It is not yet clear when and how a convergence of these different standards development directions will appear.

But it is obvious that there is a strong political support for a convergence, with the European Cloud Strategy and in the US a similar initiative under the lead of the National Institute for Standards and Technologies (NIST). Also the EU-US collaboration is particular intense on this topic. User driven initiatives like the OMG Cloud Customer Standards Council (CCSC) or the Open Data Center Alliance (ODCA) are pushing the cloud provider industry further in the direction to agree on a set of standards.

With regard to the TClouds architecture and hence the specific topic of security, trustworthiness and privacy for infrastructure clouds, we have therefore approached the cloud standardisation as a mapping exercise, whereby our map of cloud standards has become increasingly precise and validated against the TClouds architecture.

In parallel, the project has engaged in a number of European workshops on cloud standardisation and is directly contributing to the stakeholder process of refining the overall mapping of cloud standards for Europe via the following meetings (Y1 and Y2):

- EU/US Cloud Collaboration Workshop, February 2011
- SIENA Cloudscape III, March 2011
- EU Cloud Expert Group Meeting, Sept. 2011
- IBM Cloud Computing Architecture Board, January 2012
- Meeting with the Cloud Security Alliance, February 2012
- SIENA Cloudscape IV. February 2012
- NESSI Steering Committee Meeting with Ken Ducatel (new EC Head of Unit for Cloud), March 2012

[4] COM(2012)529

In this context, TClouds has contributed to:

- SIENA European Cloud Standards Roadmap
- NESSI Position Paper on Cloud Computing – Standardisation Section (with a.o. SAP, THALES, Nokia Siemens Networks)

This effort is on-going and the European Commission has provided in its Cloud Strategy a mandate to the European Telecommunication Standards Institute (ETSI) to "identify by 2013 a detailed map of the necessary standards (inter alia for security, interoperability, data portability and reversibility)".

Also the European Commission calls for technical specifications relating to "the protection of personal information in accordance with the new Regulation on European Standardisation".

TClouds has a specific focus on security, privacy and trustworthiness which are indeed crosscutting issues in infrastructure cloud computing. Hence, the project has conducted an investigation of multiple – partially interdependent - cloud standards for these specific aspects.

3.2 TClouds Map of Cloud Standards

The refined TClouds Map of Cloud Standards for secure, privacy protective and trustworthy infrastructure clouds is given by figure 3.

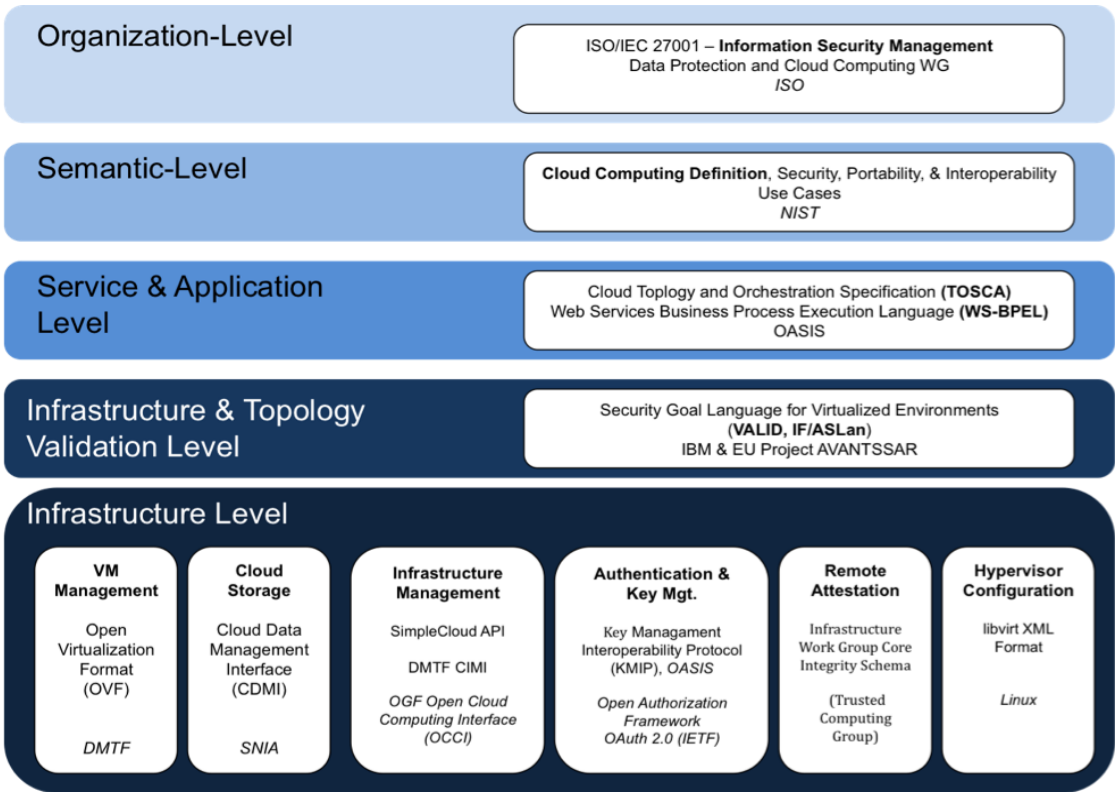


Figure 5: TClouds Map of Cloud Standards

In particular, we are distinguishing the following levels:

- **Organisation Level:** Standards concerned with management processes and organisation level security. This addresses first of all the providers of cloud services and the related operational processes in cloud data centres. It may also relate to the corresponding management processes of the user.
- **Semantic Level:** Standards concerned with the definition of entities, roles, terms and logical relations in infrastructure cloud computing – thereby supporting a semantic matching of organisation level requirements to the entities in the infrastructure.
- **Service & Application Level:** Standards concerned with the description, orchestration and deployment of applications, processes and services that build on top of infrastructure clouds.
- **Infrastructure Topology & Validation Level:** Standards concerned with the topology description of the cloud infrastructure and of the security goals as matching directly to the infrastructure. On this level, we are distinguishing between the description of the "desired" topology, the description of security goals (e.g. isolation) and the description of the "actual" live topology at it is encountered in the cloud.
- **Infrastructure Level:** Standards concerned with the technical operation of the infrastructure such as interfaces specifications or data formats. We are distinguishing in our map the following sub-areas at the infrastructure level:
    - **Infrastructure Management**: Interface standards relating to the management of the infrastructure. This includes the triggering of actions by the infrastructure (such as the deployment or migration of a VM). It also includes the access to security relevant live information from the infrastructure.
    - **VM Management**: Data standards for virtual machine images as well as meta data standards relating to the deployment and execution of the VM.
    - **Hypervisor Configuration:** This concerns the direct configuration of the virtualization software used.
    - **Cloud Storage**: Data standards for data storage in the cloud as well as related meta-data standards (e.g. for the lifecycle of data in the cloud or the type and object structure of data).
    - **Authentication:** Authentication standards are concerned with the management of secure user credentials to access the cloud and its services. Related authorization standards are concerned with the description of the access level of a user – e.g. authorized activities, access to specific secure domains etc.
    - **Key Management:** Key Management standards are concerned with the handling of encryption keys to access encrypted data or process encrypted VMIs in the cloud. Also both, the Authentication & Key Management areas, provide a link into enterprise wide infrastructures for authentication and key management.
    - **Remote Attestation:** Standards concerned with the integrity verification of components of the cloud infrastructure and the attestation of this.

A number of other standards will apply in a secure cloud scenario including e.g. standards for secure data transmission (such as HTTPS). However these are relatively unspecific for the domain of cloud computing and we have not assumed a need to adapt them to the specifics of cloud. Hence they have not been included in the map.

3.3 Detailed Analysis of Standards in the Map

The TClouds project has conducted in Y2 a detailed analysis of standards in the map. Organisation and semantic level standards have not been assessed in detail - while still, ULD is engaged in the relevant ISO 27001 Cloud working-group and WP 1.3 of A1 has taken the cloud definitions of NIST into account in the definition of requirements.

With regard to the technical standards of the other levels, these have each been investigated in detail. We have done so with the following base questions:

1) Would the standard be applicable in TClouds?

2) What would be typical uses cases in TClouds for the standard and which components of the TClouds architecture would be affected/involved?

3) Can these use cases be implemented with the actual specification of the standard – or is there a need for extending the standard to fit to the requirements of TClouds?

The detailed results of this investigation are provided in **Chapter 6** - Appendix - of this document sorted by standard and potential contributions as they appear in the map.

The results of this investigation fall into 3 categories:

1) Standards that are immediately applicable and are already or will be implemented in Y3 by TClouds. These are:
    - **WS-BPEL**: is used by the the *Fault tolerant BPEL execution engine*
    - **OVF:** will be implemented in *Trusted Object Manager* (TOM)
    - **OAuth**: is already implemented in the *TPaaS platform* of HSR and Philips (linked to the eHealth use scenario).
    - **Infrastructure WG Core Integrity Schema:** is already implemented in the *Remote Attestation Service.*
2) Standards that are applicable provided that extensions of the standard are developed by TClouds. Partially these extensions are already in work or will be developed in Y3 together with a TClouds implementation of the standard:
    - **VALID**: will be used in the *Security Assurance of Virtualized Environments* (SAVE) component. VALID is an IBM extension of the IF/ASLan language developed in the AVANTSSAR project.
    - **libVirt XML Format:** is used in the *Enforcer* component of the TClouds „Ontology-based Reasoner to Check TVD Isolation“. It has been specifically extended to describe virtual networks through VLAN tagging that can be used to group VMs in a TVD.
3) Standards that are applicable and would demand extensions in order to be implemented in TClouds. But where an implementation and the related development of extensions of the standard are currently not planned by TClouds:
    - **TOSCA**: The graph model that TOSCA uses to describe topology is similar to the one used by the TClouds *SAVE* component. However, TOSCA provides rather specifications for application and service descriptions – and not yet specifications on the matching to the infrastructure. A reasonable TOSCA extension for TClouds application would need to include the possibility to describe the „desired“ stage of the infrastructure deployment as well as to describe the „actual“ state as detected by the TClouds *SAVE* component.

- **CIMI**, **OCCI**, **Simple Cloud API**: None of the investigated cloud APIs supports currently security relevant operations, e.g. the extraction of infrastructure data by the *SAVE* component. Significant extensions would be needed for TClouds. Of course, the APIs could be applied for their standard functionalities – for CIMI and OCCI projects are underway to implement them in Open Stack.
- **KMIP:** Currently TClouds is using static keys in the crypto domain of the TClouds *Crypto-as-a -Service* Architecture. KMIP could be used to manage the cryptographic credentials in the crypto-domain and integrate this into a larger enterprise key management infrastructure. With an extension of the standard with explicit interoperability aspects for TCG TPM keys – as they are currently used by TClouds - , KMIP could further be used for bootstrapping encrypted images where the key has to be securely deployed in the cloud infrastructure.

3.4 Analysis via Architecture Areas

Further to the view from the perspective of individual standards we have also done the investigation from the view of the TClouds architecture – and general areas and component that call for the use of standards. This matches the findings stated above.

These are in particular the following components and areas of the TClouds architecture:

- **Security Assurance in Virtualized Environments (SAVE)**: using the VALID language to describe security goals and potentially using extended cloud APIs (OCCI, CIMI, Simple Cloud) for access to the security relevant information at runtime. Further potential for using an extended TOSCA to combine the description of service deployment with a desired topology of infrastructure deployment and a validation of the match/mismatch between desired and actual state.
- **Remote Attestation Service**: use of the Infrastructure WG core integrity schema.
- **Trusted Infrastructure**: use of OVF
- **Cloud File Storage**: use of CIMI
- **Ontology based Reasoner:** use of an extended libvirt XML Format
- **Cryptography-as-a-service:** use of an extended KMIP
- **Fault tolerant BPEL execution:** use of BPEL
- **General Open Stack Management Component:** potential to use OCCI, CIMI, SimpleCloud

3.5 Plan for Y3

In accordance with the exploitation plan of the project, two Y3 activity lines arising from the standards task were agreed with the TClouds A2 technical development stream.

1) The first activity line is concerned with evaluating and facilitating TClouds Open Source contributions to the Open Stack project.
2) The second activity line is concerned with the dissemination of the TClouds maps of standards

3.5.1 Evaluate and facilitate TClouds Open Source contributions to Open Stack

TClouds proposes several security enhancements to Open Stack. To integrate these in the management of Open Stack, TClouds has already adapted several Open Stack APIs.

By principle, all Open Stack APIs are REST based. Also, Open Stack already supports Open Image Formats – such as OVF images. In addition to this, several implementation projects are underway to implement further specific standards from the TClouds standards map in Open Stack. So, the TClouds standards map is fully compliant with Open Stack. Standards that are implemented in Open Stack include OCCI, CDMI and OVF.

Hence, it was decided in the project, that a promising route is to organize a concerted interaction with the Open Stack project in Y3 to discuss several TClouds enhancements while also discussing related needs to adapt APIs and potential impacts on standards implementations.

The organization of this interaction with the Open Stack project will be facilitated in Y3 through the standards task in TClouds. Also the TClouds enhancements to Open Stack will be documented in an integrated way with reference to extensions of standards and APIs.

It should be noted that Open Stack also provides support of de-facto industry standards - in particular of the Amazon EC2 APIs.

The following table provides a first overview on the enhancements that will be discussed with the Open Stack project.

	TClouds Enhancements	**Open Stack Components**	**APIs / Standards concerned**
Access Control as a service	Trustworthy Cloud Scheduler. Matching User security & privacy requirements to cloud virtual resource allocation. Cloud security policy enforcement.	NOVA/Scheduler	Several changes to NOVA API
Cryptography as a service	Protection and user empowerment while deploying high value cryptographic credentials to the cloud.	NOVA/Compute at hypervisor level	Extended KMIP
Remote Attestation Service	Assess the integrity of nodes in the Cloud infrastructure.	NOVA/Scheduler	Infrastructure WG core integrity schema
Secure Log Service	Support different secure logging schemes. Guarantee log integrity and authenticity in monitoring the cloud.	DASHBOARD	NOVA API
Ontology based reasoner	Management of trusted virtual domains in the cloud	QUANTUM/vSwitch PlugIn	Libvirt extension, Quantum API

3.5.2 Disseminate TClouds Map of Standards

Apart from a concerted discussion of TClouds enhancements with the Open Stack project, it was decided in the project to also link the dissemination of the overall set of TClouds technical components to disseminating the TClouds map of standards in a complementary TClouds “a security view on cloud standards” white paper.

The interplay of TClouds components and cloud standards will be illustrated at the example of a TClouds enhanced Open Stack and the TClouds enhanced application cases.

Also questions relating to the user requirements on cloud standards have been included in the A1 stakeholder survey and will be disseminated jointly with A1 results.

Chapter 4 Exploitation

Chapter Authors:

Norbert Schirmer (SRX), Martina Truskaller (TEC), Patricia Rio Branco (TEC), Sven Bugiel (TUDA), Stefan Nürnberger (TUDA), TClouds partner responses to questionnaire

4.1 Introduction

This chapter refines the exploitation efforts and plans of the partners as defined in the work plan and reported in deliverable D4.1.1 in M18 of the project. The refinement process is based on an internal questionnaire to the project partners.

4.2 Questionnaire

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

Exploitation includes:

- Financial exploitation, e.g. by building products, projects or services based on the project results
- Research & Development, by engaging new projects (EU funded or other) based on the experiences gained in the project
- Education, e.g. courses, master / PhD students, etc.
- Community building around the topics of the project
- Knowledge transfer from academia to industry, by collaboration or via employees
- Contributions to open source projects, standardization efforts (this overlaps with “Standardization and Dissemination).

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

4.2.1 Questions biased towards industry partners

General Questions

1. What are the main results you expect from the project and how are they exploited commercially (products, services, …)
2. Which business and operating models are possible after the end of the project to bring the project results to customers? How do effort flow and cash flow look like? Which role do you see for 3rd parties (not participating in the project) in this scenario?
3. Drivers and Obstacles: Which obstacles for a successful exploitation do you see from today’s perspective? How can these obstacles be tackled? Which drivers for a successful exploitation do you see from today’s perspective? How can those drivers be harnessed and strengthened?

4. How do European stakeholders (cloud providers and customers) profit from the exploitation of the results (business perspective)? What does this mean for the European economy?
5. What is the timeline for the exploitation? In which phases can the exploitation be structured? What is the prospective time frame after the end of the project to bring the results to the market?
6. Which concrete customer needs do you address with your solution / product? How can you quantitatively measure the success?
7. In which way are marketing / product-management / sales departments already involved during the project?
8. How does the consortium see the kick-off for exploitation (at the end of the project) with respect to demonstration of the results, inclusion of multiplicators and publicity. Is it may be possible to start exploitation of intermediate results already during the project.
9. Are there synergies for exploitation with other projects, possibly also funded ones? If yes, which?

Economic Prospects of Success

1. How can a quick market access be guaranteed? Is it necessary to create new markets for a successful exploitation?
2. How does the market for exploitation look like today (market analysis, prognoses, technical developments).
3. How is the competition for the developed results, in Europe / worldwide?
4. What is the innovation in project results, what are the advantages compared to competitors?

Scientific / Technical Prospect of Success

1. Which impact does the general technological progress have on the exploitation scenarios?
2. Which role do non-technical developments have (legal aspects, privacy aspects,…) on the exploitation phase?

Inventions / Patents

1. Are there (plans for) patents?

4.2.2 Questions biased towards academic partners

General Questions

1. Drivers and Obstacles: Which obstacles for a successful exploitation do you see from today's perspective? How can these obstacles be tackled? Which drivers for a successful exploitation do you see from today's perspective? How can those drivers be harnessed and strengthened?
2. How do European stakeholders (providers and customers) profit from the exploitation of the results (business perspective)? What does this mean for the European economy?
3. What is the timeline for the exploitation? In which phases can the exploitation be structured?

4. Which concrete customer needs do you address with your solution / product? How can you quantitatively measure the success?
5. How does the consortium see the kick-off for exploitation (at the end of the project) with respect to demonstration of the results, inclusion of multiplicators and publicity? Is it possible to start exploitation of intermediate results already during the project?
6. Are there synergies for exploitation with other projects, possibly also funded ones? If yes, which?

Scientific / Technical Prospect of Success

1. Which impact does the general technological progress have on the exploitation scenarios?
2. Which role do non-technical developments have (legal aspects, privacy aspects …) on the exploitation phase?
3. How is the competition for the developed results in Europe / worldwide?
4. What is the innovation in project results, what are the advantages compared to competitors?

Inventions / Patents

1. Are there (plans for) patents?

Scientific Impact & Education

1. Do you (plan to) offer seminars, lectures, lab-courses and the-like with topics related to TClouds? Or in which way did the TClouds results influence / improve your education and training?
2. How did your TClouds work influence / improve your contribution to the European research in Cloud Security, like building scientific communities, organizing or participating in workshops etc.?
3. Did the TClouds work help you to attract new researchers / students?
4. Did your TClouds work results improve / foster the dissemination of your work in conferences (Industrial / Academic), journals, etc?
5. How did (or will) the project help you to build scientific communities, or help you get into communities?

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

1. To which Open-source projects do you (plan to) contribute?
2. Are your results made available to the public domain (e.g., open-source, websites)?
3. What activities will ensure the maintenance of the project results after the project ended?
4. Have you planned follow up projects or are you already involved in other projects.
5. How did the projects influence your work in other projects? Are there synergies or follow-up work?
6. Did new partners come up during the duration of the TClouds project with which you will continue to cooperate?
7. Did the TClouds work help you to acquire new projects and / or third party funding.

Technology transfer

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

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

4.3 Partner responses

This section provides the detailed responses by the project partners to the questionnaire.

4.3.1.1 EDP

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

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

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

- Data integrity – we need to ensure that all the communication between the client and the Smart Lighting system is completely secure, e.g. there is no possibility to corrupt data.
- Data availability – smart lighting is a near real-time system; therefore, data must be available when needed in the overall system.

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

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

We are also exploring the possibility of expanding this approach to other Smart Grid components. A possible solution would be to use a private cloud connected to a public cloud (see Figure 6).

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

If we prove it is feasible to host smart grid related systems in a cloud computing environment, a number of new solutions using cloud computing in smart grids may arise in the following years. Utilities get improved smart grids, and customers get better services. This can contribute to diminishing outage times and increase energy usage efficiency, which is in line

with the 20-20-20 targets established by the European Commission. Moreover, vendors can increase their solution portfolio. All this can contribute to the growth of European economy.

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

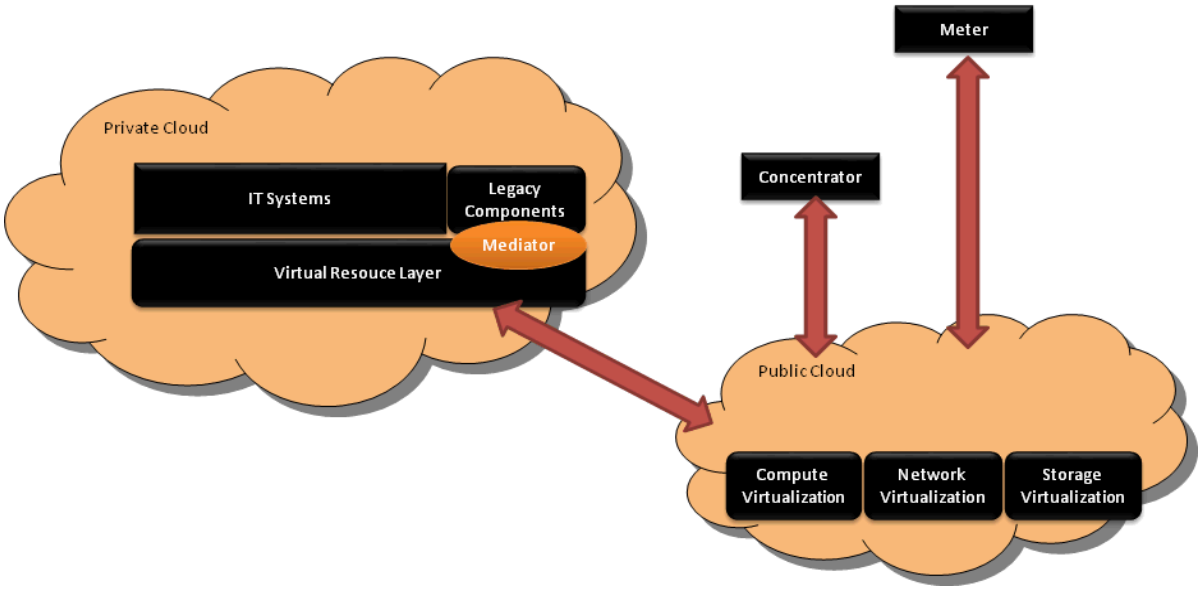


Figure 6: Smart Grid using private and public clouds

4.3.1.2 EFACEC ENG

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

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

A commercial exploitation of cloud computing solutions, and services based on TClouds or integrating parts of TClouds technology, will be timely assessed by EFACEC once the technical feasibility analysis is complete by the end of the project. A consolidated decision shall then depend on multiple other factors, namely the market trends, cost benefit analysis, customer requirements and customer willingness to embrace cloud computing solutions, all taking into consideration the profile of the products / solutions provided by EFACEC within the Power System Automation business unit. However, given the technical complexity involved, an eventual time to market would expectedly take at least 2 to 3 years after TClouds project conclusion.

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

It is a fact cloud environments are a growing trend amongst IT companies, and even though the power utilities market usually has their own infrastructures and datacentres, it is a matter

of time until they are open to their benefits, particularly given TClouds security enhancements. Therefore, being part of this technological evolution provides EFACEC with a valuable advantage over competitors, and improved knowledge to answer future market demand.

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

4.3.1.3 FFCUL

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

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

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

In terms of scientific impact and education, our work on TClouds was subject to several talks, tutorials and lectures given by the FFCUL team both in Portugal and around the world. Moreover, at least 7 MsC theses related to TClouds were concluded in the last years, and 2 PhDs are underway.

Overall, working on TClouds was extremely beneficial for FFCUL. In particular, the DepSky paper got a lot of citations (62, according to Google scholar, in less than two years), which demonstrates the interest of the community on the cloud-of-clouds concept, and we were invited to participate in two other EU project proposals. The first one was accepted and the project is underway (BiobankCloud), and the second is under evaluation (informally accepted according to insider information).

In terms of the sustainability of the software developed in TClouds, we expect to build small developer communities around our base components, and thus we launched two open-source projects. In particular, BFT-SMaRt is already attracting some people (especially from

the research community). Moreover, we expect further projects to continue providing some funding for the continuation of their development.

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

4.3.1.4 FCSR

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

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

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

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

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

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

Moreover, thanks to the adoption of TClouds technology, TPaaS exploitation can benefit from a reduced time-to-market and being able to address effectively market. TClouds, in fact, can be used not only as a valid tool at technology level, but also can provide valuable support to the whole marketing/branding compartments, since TClouds' novelty looks very promising also under the perceived trustworthiness of final users.

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

the areas of Security, awareness of “personal data” concept, PHR/EHR sharing and interoperability, and Legal compliances EU-wide.

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

4.3.1.5 IBM

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

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

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

From a European perspective, the TClouds technology gives a great opportunity for EU-based cloud providers, that may (or need) to focus on security and privacy issues. This way, European providers and customers can benefit from the results in several ways. First, cloud providers and users may benefit from ability to perform compliance reporting of various components in the cloud, for example using the SAVE technology in TrustedSurveyor. Second, clients may benefit from the Intercloud storage approach as their data is not dependent on a single cloud provider anymore. As such, data resilience is increased, and, as a consequence of replication, storage clouds become commodity. Thus, we expect to gain new markets for cloud data storage.
On behalf of IBM Research, the exploitation phase is already in progress. We feel that for any successful project, like TClouds, exploitation must start before the project ends. For us, the first exploitation phase was an internal (within IBM) discussion on possible productization of components and project results. The second phase consists of turning research prototypes into product-ready solutions. The third phase is product marketing, world-wide distribution and support through regular IBM channels. Results from TClouds are expected to take that road between now and 2015.

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

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

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

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

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

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

4.3.1.6 OXFD

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

In addition to the developed scheduler we have also proposed a set of integrated frameworks which help in establishing trust in the Cloud. The heart of the frameworks is the proposed scheduler. Our frameworks have been published in top journals in their field. We have been recently contacted by Sophos research lab, as they show an interest in these frameworks and they wanted to establish a research links to extend the work. Specifically, Sophos are currently working on developing a Cloud SaaS for their customers, and they wanted to understand better how TClouds results could help them in establishing trust in their products and infrastructure.

The competition in the cloud market is enormous and competing providers fight for customers with more and more features. As of today, no cloud provider has installed similar measures to enhance the customer's trust by providing proofs of running software and isolated environments. We have contacted the executive director of OpenStack and discussed with him TClouds results. He shows an interest in this and invited us to their architecture board meeting which is held twice a year: in April and October. We plan to contribute to the October architecture board and introduce them to TClouds result. We

decided to go for the October one as it will be held in London which would save travelling costs (the April one would be held in the United States).

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

4.3.1.7 PHI

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

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

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

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

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

The above-mentioned technology resulting from TClouds addresses concrete customer needs to provide various healthcare services to our customers, either being healthcare institutes or end customers. Its success can be measured financially. IBM's marketing and sales departments have already been involved in the projects descending directly from the Healthcare TPaaS solution. Product management is involved in all phases of exploiting Healthcare TPaaS.

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

Philips Research benefits from the exchange of information with other TClouds partners, especially on legislative analysis and cloud infrastructure development. Philips Research has been involved in many EU projects and benefited from collaboration of such projects in

similar domains. An incomplete list, covering past and future EU-funded projects includes: FP7-ENSURE, FP7-UNIVERsal, FP7-CO-LIVING, FP6-ANGEL, FP6-SPEED, etc. A good cooperation and interaction with other partners forms a solid foundation for future collaborations and projects in related fields.

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

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

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

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

4.3.1.8 POL

We do not see any obstacle for the dissemination of research results: we think that European stakeholders can profit from research results through commercial products that incorporate developed technologies, even though this is not the main focus of POL. Demonstration of research results could help Cloud Providers in finding potential security solutions for their infrastructures and improve their existing products.

Furthermore we think that our public contributions to the prototype Trustworthy OpenStack and in particular the contribution returned to the OSS communities of OpenStack and Libvirt can be of interest for the industry. Currently, apart from an older version of the LogService the subsystems developed by POL for TClouds are not yet publicly available, but they will be as Open Source Software as soon as possible and there is the plan to maintain them beyond the end of the project.

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

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

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

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

With regard to cooperation with other EU projects, at the moment we are informally evaluating if the integrated prototype Trustworthy OpenStack can be exploited within the *Contrail* project focused on federations of clouds.

In terms of dissemination, we attended some workshops specifically focused on the security of Cloud Computing. For the moment TClouds has not increased so much our scientific production, since the major effort was spent on development and integration, but such an improvement is in our plans for the remaining part of the project.

As follow-up, we are investigating the possibility to cooperate with the partners beyond the end of the project and we envision the opportunity to get funding or to participate in new projects.

4.3.1.9 SRX

General

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

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

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

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

Exploiting the expected technology transfer, Sirrix will gain a technological advantage in the field of trusted systems and will transfer them into marketable products. In addition, strong synergistic effects on other company products are in sight. The good cooperation with partners in the project provides a solid foundation for further deeper cooperation in future projects. In addition, there is an intense cooperation with companies and research institutions

in the EU and thus a lot of new opportunities and promising feedback from partners and customers which enable a seamless continuation of the project results in further projects.

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

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

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

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

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

Economic prospects of success

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

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

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

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

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

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

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

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

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

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

and combine the security management features of TOM with the infrastructure management capabilities of OpenStack.

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

Scientific / technical prospect of success

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

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

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

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

4.3.1.10 TEC

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

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

The TCLOUDS security concepts will be integrated into our infrastructure. Currently the majority of our trusted server customers are Industry. We plan to launch a new business line for providing our services to a larger number of SME costumers. The raised security, trustworthiness and higher reliability, justified by the outcome of the TCLOUDS project, are

the essential pillars to establish this new service line. These three aspects are the main needs of any customer besides 24/7 support and regular maintenance.

Currently we provide our trusted server services as a package within our industrial services. The new scalability, raised security and reliability founded on the integration of the TClouds outcomes, allow us to think of additional models. Our focus is to charge a monthly flat rate for the usage of our cloud services including some hours per month for support and to provide dedicated solutions for different business sectors. Lawyers and charted civil engineers are our first step focus. The success of our solution can then be measured by calculating the number of customers (companies or individuals), which are willing to work with and pay regularly (more than one year) for our service.

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

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

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

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

4.3.1.11 TUBS

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

Research

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

Two publications at and around the EuroSys 2012 conference, for instance, allowed us to be present at this distinguished event. It is one of the leading conferences in the field of operating systems and distributed systems, and cloud computing has been a major focus of it in recent years. Besides the presentation of results from the TClouds project, attending conferences like the EuroSys 2012 and workshops like the SDMCMM 2012 also gives the

opportunity to meet other researchers as well as industrial representatives, and to discuss with them risks and potentials, problems and solutions arising around and within cloud computing. This way, we are able to get feedback on our current research, to draw inspiration for new research, and to explore possible co-operations, resulting perhaps in future projects.

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

Publications are indispensable for an academic institution like TU Braunschweig to document achievements in ongoing research. However, the sustainability of developed approaches, concepts, and solutions can only be ensured if they are taken up, continued, and enhanced by follow-up projects. Therefore, TU Braunschweig has been making huge efforts to participate in and/or even organize potential future projects. Up to now, two new project proposals directly connected to TClouds have been submitted. Among others, partners from TClouds are involved in both proposals. That way, the experience in organizing and running collaborative projects gained during the TClouds project can be optimally utilized. Further, started collaboration in terms of research can be deepened.

Teaching

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

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

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

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

4.3.1.12 TUDA

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

We focused on building the architecture that makes this transition possible and, being a research institution, our main goal is to disseminate the results among the research community in the form of scientific publications and the advancement of education. Potential financial exploitation is most likely expected through application of these results for improved consulting of and collaboration with industrial partners in the context of the Center for Advanced Security Research Darmstadt (CASED). Results of our research target foremost the cloud provider and aim at improving the trustworthiness of clouds and thus benefiting the cloud customers to use cloud infrastructure more securely.

The competition in the cloud market is enormous and competing providers fight for customers with more and more features. As of today, no cloud provider has installed similar measures to enhance the customer's trust by providing proofs of running software and isolated environments. An obstacle in the adaptation of CaaS-like solutions could be the necessity for hardware trust anchors such as the Trusted Platform Module (TPM). Moreover, the cloud providers may fear revealing intellectual property to their competitors by indirectly disclosing information of the trusted state of their software. However, we believe that our working prototype shows that trustworthy cloud architecture is feasible and available at low additional cost. If a single cloud provider starts to implement CaaS, others are required to follow in order to keep up the level of trust and not to risk losing customers. The research results of CaaS are publicly available to everyone. Not only did we publish scientific papers in international renowned, peer-reviewed proceedings of security conferences but we will also make the source code publicly available for everybody to assess the progress and contribution. This will be done latest by the end of the TClouds project in October 2013, but maybe even earlier which enables feedback channels from users to the still ongoing development in order to enhance product features and usability. This puts European and world-wide stakeholders in the position to use our prototype for evaluation or even build upon our code base which drastically minimizes set-up costs as we have made the technology readily available. Moreover, the positive influence of the project on education can help preparing students for industrial work in the area of cloud computing and thus indirectly benefit the stakeholders. Courses are promoted to students at the Technical University of Darmstadt and in the context of CASED also to students at the University of Applied Sciences Darmstadt. Results are already incorporated in education in the form of lecture content, labs and seminars. The success can already be measured by the increasing interest in the topic and subsequent theses. We foresee a future in which CaaS has laid the ground for building advanced infrastructures or even commercial products based on a secure VM and key deployment which customers can trust.

4.3.1.13 ULD

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

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

- A comprehensive legal analysis of cloud computing (EU-level);
- Identification of gaps and frictions in the current legal framework and specific suggestions to address these;
- Guidelines for a lawful cloud computing contract/SLA;
- Methodology for a future Data Protection Impact Assessment of cloud computing services.

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

1. Policy and regulatory work

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

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

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

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

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

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

4.4 Joint exploitation efforts

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

- **Modularity:** Different orthogonal subsystems, such as secure storage or resilience, have been identified and project partners work on different aspects of each subsystem. Deliverables D2.1.2, D2.2.2, and D2.3.2 present the corresponding results. A declared goal for joint exploitation is to demonstrate how these subsystems fit together into an overall cloud infrastructure and we refer to deliverable D2.4.2 for details about the integration efforts.
- **Integration into use-cases:** As stated above, different types of partners are involved in the project. As stated in D4.1.1 (version 2), a goal of joint exploitation is to show how the technologies developed in the TClouds project can be leveraged and integrated into applications – here Smart Lighting and Home Healthcare. In this sense, the industrial and academic partners take the role of technology providers for the SMEs. The plans for this integration and its evaluation are presented in the Activity 3 deliverables and the actual integration is a particular focus of project year three.

To this end, it was decided at consortium level (and with respect to the particular exploitation plans of each partner, see Section 4.3) that the best strategy for a joint exploitation is to ensure the sustainability of the jointly developed integrated Trustworthy OpenStack prototype beyond the end of the project. In particular in light of recent developments in the cloud market, where known international companies such as Intel[5], IBM[6], and PayPal[7] announced their support and choice of OpenStack, continuous integration of the TClouds components into an OpenStack based trustworthy cloud platform is expected to be the right choice for joint exploitation and to receive public attention.

Figure 7 illustrates the general idea of this approach. As stated above, the modularity of the TClouds Trustworthy OpenStack platform allows each partner to individually exploit his results and continue development of his components. However, as demonstrated by the TClouds integrated prototype at the end of the third project year, these single components can be assembled into an integrated platform, which will act as a jointly exploited platform, publicly available. Naturally, the same platform, as will be also shown in year 3, can also be leveraged by the project partners in Activity 3 and thus forms the above mentioned "consumer versus (technology) provider" relationship between the project partners in Activity 3 versus Activity 2.

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

[6] https://www-304.ibm.com/connections/blogs/59c1123b-0353-458e-a719-b002d84108d5/entry/ibm_announces_platinum_sponsorship_of_the_new_openstack_foundation?lang=en_us

[7] http://www.openstack.org/user-stories/paypal/

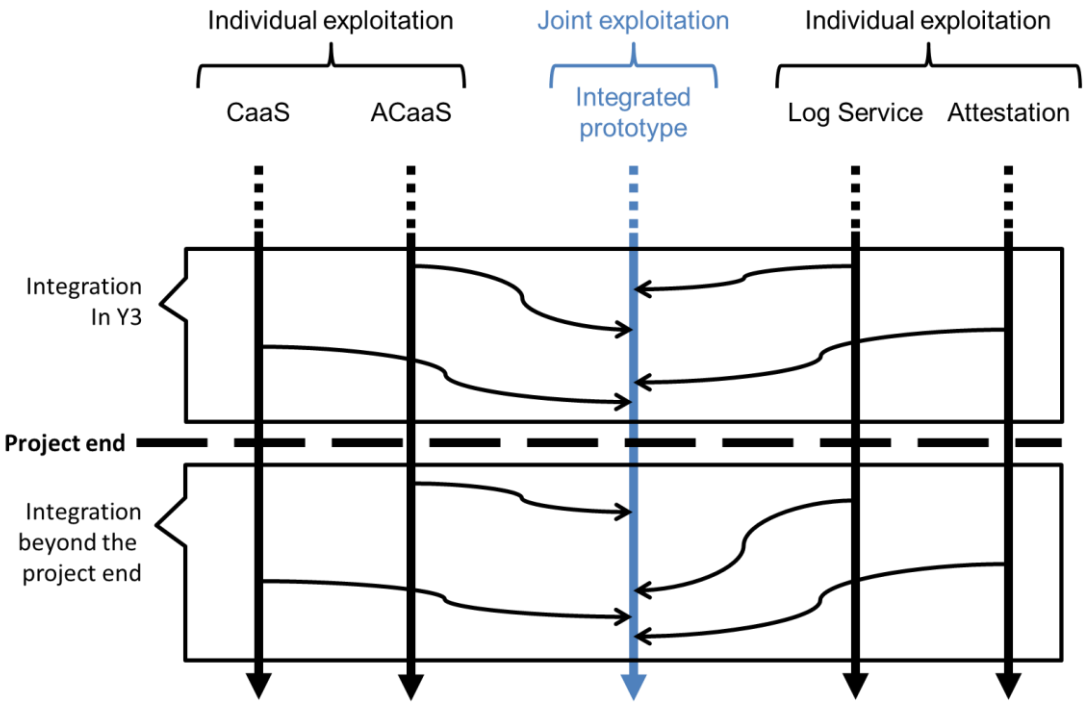


Figure 7: Joint exploitation based on Trustworthy OpenStack components

Chapter 5

Training and Education

Chapter Authors:

Cornelius Namiluko, Imad Abbadi (OXFD), Sven Bugiel (TUDA)

5.1 Introduction

Following the success of last year's training and education survey, 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.).

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

5.2 Methodology

There is a number of partners of 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.

5.3 Training

5.3.1 Training already delivered and received

At this point, the project has been running for 24 months. The architecture of the project and each component has been designed and prototypes are under development. Project members have already acquired a certain level of skills, regarding the specific directions of the components they are in charge of. This section summarises results from the survey regarding the amount of training that project members have already received.

Most training is carried along with the progress of the project. Mostly, it is in the form of self-training and learning on the job, as the detailed directions of project members have begun to divert and training on general knowledge has been carried in Year 1. Many individual and non-structured learning activities (researchers learn on-the-job) have been taken, and also the TClouds education module. Listening to partner talks at project meetings also helped sharing knowledge and inspiring innovation. Table 10 shows the major training topics already delivered and received.

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

Table 10: Major training topics

5.3.2 Training needed and planned

A number of members still need some training in the topics surrounding cloud computing. General-purpose training covering related wide topics is still needed by members, especially the cloud computing technology and security technology. 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 second year are indicated in Table 11.

Topic	Description	Time frame	Possible delivery mode
OpenStack	More explanation of the practical issues of OpenStack, including its deployment and configuration. Cloud-setup with OpenStack and Xen and low-level Cloud maintenance. VMs configurations inside the cloud infrastructures. More detailed explanation of the features of OpenStack including administration aspects, development and management.	Immediately, preferably before the development of the TClouds prototype is complete	Could be delivered in the form of tutorials or “how tos”
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	Immediately, and through the length of the project and beyond.	This could be delivered as an always-available resource.

Topic	Description	Time frame	Possible delivery mode
	cloud		
Security Technology	This would cover the security properties that are expected from a TCloud platform/infrastructure, and the security problems identified in the cloud computing community. 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, and through the length of the project and beyond.	This could be delivered as an always-available resource.

Table 11: Year 2 training requirements

5.3.3 Educational Materials

TClouds has a good number of academic partners. This provides an opportunity for the project to contribute to education of existing professionals and students in the areas covered in the project. Furthermore, non-academic partners on the project could develop professional courses to deliver to their members of staff or to other organisations. In order to achieve this, the project must create materials that are suitable for academic purposes as part of the results.

5.3.3.1 Already available from partners and other sources

A number of partners have already produced materials that could be used in education. Other organisations working in the area of cloud computing have also produced some materials that could be used as part of the TClouds training and education. Some of these include;

i) Lecture named “Middleware – Cloud Computing” together with associated exercises in winter term 2011/2012
ii) State machine replication tutorial presented to TClouds partners
iii) Course in Distributed Systems Programming with some cloud-related materials.
iv) Survey article on cloud security (C. Cachin and M. Schunter, "A cloud you can trust," IEEE Spectrum, pp. 28-32, Dec. 2011).
v) Course on security/resilience in cloud computing (ETHZ, Department of Computer Science. Security and Fault-tolerance in Distributed Systems. One-semester graduate-level course, 2011).
vi) Textbook: C. Cachin, R. Guerraoui, and L. Rodrigues, Introduction to Reliable and Secure Distributed Programming (Second Edition). Springer, 2011.
vii) Lab session for implementing different, recently published attacks on Clouds at the example of an OpenStack Cloud (taught at ETISS'11)
viii) Tutorial, slides, notes, technical documentation on Cloud setup

5.3.3.2 Curriculum development

Some of the areas covered in the project could stand as courses on their own or be incorporated into existing courses. FAU improves the cloud computing lecture every time it is held. They also offer projects and theses around cloud computing topics in general and related to TClouds subsystems in particular. FFCUL will present an improved version of the state machine tutorial on ACM EuroSys'12, together with BFT replication literature overview. The whole material used in their courses will also be updated. TUDA plans to develop new training material with the topic of Cloud Security (contemporary attacks and countermeasures of real-life clouds). It will be disseminated via teaching and provided on their webpage. It is suitable for a 4-6 ECT course. OXFD runs a number of courses for professionals in the areas of software engineering and systems security. It is expected that some of the results from the project would be incorporated as part of the MSC programmes that are delivered by OXFD. Most of the materials would be included as part of a new Course dedicated to Security in Cloud Computing.

5.3.4 Summary for Training

Members of the TCLOUDS have varying skills. For the project to be successful, some training will be required for some members of the project. In addition, the project will produce educational materials upon which academic and professional courses related to cloud computing and security can be built. This report has outlined some of the training that members have already received, areas in which further training is required as well as drawing out possible inclusion of project material into academic and professional curricula. As observed from the responses of the survey, at this point, most general-purpose training has been delivered and satisfied, self-training and learning on projects has been started on the most specific directions regarding different goals of members.

5.4 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.

The following Table 12 lists the new education activities in contrast to the ones reported in deliverable D4.1.1 in M18.

Name	Kind/Description	Partner
Cloud Computing	Lecture	TUBS
Security and Fault-tolerance in Distributed Systems	Course at ETH Zurich	IBM
Secure distributed programming	Tutorial, presented at the 18th ACM Conference on Computer and Communications Security (CCS). October 2011	IBM
From reliable to secure distributed programming.	Tutorial, presented at the 42nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), June 2012	IBM

Name	Kind/Description	Partner
Cloud Security and Management	Lecture	OXFD
Wireless and Mobile Security	Summer School, Bertinoro, Italy	TUDA
Security and Fault-tolerance in Distributed Systems	Course, Zürich, Switzerland	IBM
Byzantine Fault-Tolerance, since 2011 ongoing	Lecture, Lisbon, Portugal	FFCUL
Middleware/Cloud Computing	Lecture, Erlangen, Germany	FAU
Practical Cloud Computing	practical course, Braunschweig, Germany	TUBS

Table 12: List of courses taught by project partners

The following Table 13 lists all theses, which have started in Y2 of the project, while Table 14 lists the still on-going theses reported in deliverable D4.1.1.

Title/Topic	Kind	Partner
Implementation of a Fault-tolerant Platform for the Execution of Web-Service-Based Workflows in Cloud Computing	Lab course result	FAU
Security of virtual machines in cloud environment	M.Sc.	POL
Remote attestation integration with OpenStack	M.Sc.	POL
Attesting a complete Ubuntu distribution	M.Sc.	POL
Cryptography as a service in a cloud computing environment	M.Sc.	TUDA
Entwicklung und Evaluation eines erweiterbaren Koordinierungsdienstes zur adaptiven Konfiguration von Cloud-Infrastrukturen	M.Sc.	TUBS
Transformation von Workflows zur deterministischen Ausführung am Beispiel BPEL	M.Sc.	TUBS

Table 13: List of theses supervised by project partners (started in Y2)

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

Title/Topic	Kind	Partner
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
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 (started in Y1)

Chapter 6 Appendix

6.1 Assessment of standards and potential contributions

6.1.1 Cloud Infrastructure Management Interface (CIMI)

6.1.1.1 Details about the standards organization and the concerned standard

6.1.1.1.1 Standardisation Organization

Standards Organization:	DMTF
Receiving body of the Contribution:	Open Cloud Standards Incubator
Contact Name:	Winston Bumpus
E-mail:	wbumpus@vmware.com
Role:	Interim Co-Chair of the Incubator, DMTF President
Contact Name:	Mike Baskey
Role:	Interim Co-Chair of the Incubator
E-mail:	mbaskey@us.ibm.com

6.1.1.1.2 Standard investigated for TClouds

Standard concerned:	Cloud Infrastructure Management Interface (CIMI)
Specification concerned:	V1.0.0e
Status of the specification:	work in progress

6.1.1.1.3 Specification investigated for TClouds

Specification	Version	Date	Doc Link, Status
CIMI	1.0.0e	1 July 2012	http://dmtf.org/sites/default/files/standards/documents/DSP0263_1.0.0e.pdf

6.1.1.2 Assessment of the Standard for the TClouds Architecture

6.1.1.2.1 Relevant component(s) in the TClouds Architecture

OpenStack management component.

6.1.1.2.2 Use case example(s) to apply the standard in the TClouds Architecture

RESTful and open-standard cloud management.

6.1.1.2.3 What technology is currently used to implement this functionality in TClouds?

OpenStack implements the de-facto, but proprietary cloud management standard of Amazon EC2. Futhermore, they implement OCCI, another open standard besides CIMI.

6.1.1.2.4 How applicable is the standard in its current specification for TClouds?

The standard is not specifically applicable to TClouds, but can be applied in a more general way to OpenStack, to provide further alternatives to the existing interfaces (EC2, OCCI).

6.1.1.2.5 What are missing elements or shortcomings of this standard for TClouds?

TClouds specific, i.e., security-relevant operations, are not currently present in the standard. For example, to extract the configuration of the whole cloud infrastructure to be used in the analysis with SAVE.

Summary Recommendation	(yes/no)
Is the standard applicable in TClouds?	Yes
Is an implementation planned for Y3 of the project?	No
Are extensions to the standard necessary in this context?	Yes

6.1.1.3 Partner Contribution: IBM

6.1.1.3.1 Application context in TClouds

Use cloud management API for extracting topological and configuration information of virtualized environments and cloud infrastructures.

6.1.1.3.2 Summary of the standards contribution

A new API method that extracts the configuration and topology, and provides it to the caller.

6.1.1.3.3 Related references (e.g. TClouds Deliverables, TClouds Standards Assessments)

Type of Reference	Document / Link	Status & Distribution Level
TClouds Deliverable	D2.4.2, Chapter 8, Section 8.0.4	

6.1.2 OAuth 2.0 Authorization Framework

6.1.2.1 Details about the standards organization and the concerned standard

6.1.2.1.1 Standardisation Organization

Standards Organization: OAuth Community

Receiving body of the Contribution:

Contact Name: General Contributions Address

E-mail: spec@oauth.net

Role:

6.1.2.1.2 Standard investigated for TClouds

Standard concerned: OAuth

Specification concerned: 2.0

Status of the specification: Working Draft

6.1.2.1.3 Specification investigated for TClouds

Specification	Version	Date	Doc Link, Status
OAuth 2.0	2.0	31 July 2012	http://tools.ietf.org/html/draft-ietf-oauth-v2-31

6.1.2.2 Assessment of the Standard for the TClouds Architecture

6.1.2.2.1 Relevant component(s) in the TClouds Architecture

The TPaaS platform (built in synergy between FSR and PHI) will implement OAuth 2.0 standard. Thus it will not be a fundamental part of TClouds Infrastructure. It will be instead an important security feature on top of TPaaS to allow 3rd party apps to exchange data safely on behalf the users (data controllers).

6.1.2.2.2 Use case example(s) to apply the standard in the TClouds Architecture

App's privacy policy profile specification

A User wants a new application to access her data, while the application is not yet related with the user. After the User has authorized the application, the application can access to User's data according to the policies defined.

6.1.2.2.3 What technology is currently used to implement this functionality in TClouds?

Java programming language, Apache Amber library, and Spring MVC framework are used to implement the OAuth 2.0 protocol.

6.1.2.2.4 How applicable is the standard in its current specification for TClouds?

It is fully applicable for User's data access control in TClouds. It allows applications to access the User's data stored in TClouds without having to obtain the User's credentials.

6.1.2.2.5 What are missing elements or shortcomings of this standard for TClouds?

OAuth2.0 might be less secure than OAuth1.0 if the developers do not have a deep understanding of web security, because of unbounded tokens, bearer tokens, expiring tokens and grant types.

Summary Recommendation	(yes/no)
Is the standard applicable in TClouds?	Yes
Is an implementation planned for Y3 of the project?	Yes, already implemented in Y2
Are extensions to the standard necessary in this context?	No

6.1.3 Topology and Orchestration Specification for Cloud Applications (TOSCA)

6.1.3.1 Details about the standards organization and the concerned standard

6.1.3.1.1 Standardisation Organization

Standards Organization: OASIS

Receiving body of the Contribution: TOSCA WG

Contact Name: Paul Lipton

E-mail: paul.lipton@ca.com

Role: TOSCA WG Chair

6.1.3.1.2 Standard investigated for TClouds

Standard concerned: Topology and Orchestration Specification for Cloud Applications (TOSCA)

Specification concerned: 1.0 Draft 2.0

Status of the specification: approved

6.1.3.1.3 Specification investigated for TClouds

Specification	Version	Date	Doc Link, Status
TOSCA 1.0 Committee Specification Draft 02	1.0 Draft 2.0	5 April 2012	http://lists.oasis-open.org/archives/tosca/201205/msg00005.html

6.1.3.2 Assessment of the Standard for the TClouds Architecture

6.1.3.2.1 Relevant component(s) in the TClouds Architecture

IBM's Securit Assurance of Virtualized Environments (SAVE) component and the VALID language (based on EU Project AVANTSSAR's ASLan language).

6.1.3.2.2 Use case example(s) to apply the standard in the TClouds Architecture

Deployment and management of IT services in the form of service templates in cloud environments. Furthermore, verification that the IT service was successfully deployed and is operating according to specification.

6.1.3.2.3 What technology is currently used to implement this functionality in TClouds?

IT services are deployed manually in the form of virtual machine images. IBM's SAVE can be used to verify the isolation of virtual machines of different customers in a cloud environment, therefore insuring confidentiality of their data. Furthermore, the VALID language of IBM can be used to specify a variety of security goals for virtualized environments.

6.1.3.2.4 How applicable is the standard in its current specification for TClouds?

Similar to SAVE, the topology is represented as a graph model in the standard. However, the difference lies in the abstraction layer that is considered by SAVE and by the TOSCA standard. The former provides a view of the entire low-level cloud infrastructure, whereas TOSCA focuses on the service and application context.

In general, for verification purposes it will be challenging specifying IT services in the form of a graph model before the service is actually deployed and the cloud-specific deployment mechanisms are applied. In contrary, SAVE performs a “discovery” of the current cloud infrastructure topology, translating the discovery data into a graph model, and then performs analysis on this model. The analysis takes as one input a high-level specification of security goals.

In conclusion, the standard might be used to specify the deployment of services, but not for the verification of the infrastructure.

6.1.3.2.5 What are missing elements or shortcomings of this standard for TClouds?

The standard should provide mechanisms to specify the “desired” state of a service, i.e., how the service shall be deployed in a cloud environment, and the “actual” state, i.e., how the service is currently operated in a cloud environment. The first state covers the deployment phase, the second one the verification.

Summary Recommendation	(yes/no)
Is the standard applicable in TClouds?	yes
Is an implementation planned for Y3 of the project?	no
Are extensions to the standard necessary in this context?	yes

6.1.3.3 Partner Contribution: IBM

6.1.3.3.1 Application context in TClouds

Specification of security goals and verification of cloud infrastructure against such security policies.

6.1.3.3.2 Summary of the standards contribution

VALID is an extension of IF/ASLan for the specification of high-level, topological security goals in cloud computing and virtualized infrastructure environments. In combination with a graph-based representation of the topology (cf. TOSCA, GEXF/GraphML), the cloud infrastructure can be checked for compliance with regard to the security goals specified in VALID.

6.1.3.3.3 Related references (e.g. TClouds Deliverables, TClouds Standards Assessments)

Type of Reference	Document / Link	Status & Distribution Level
TClouds Deliverable	D2.3.2, Chapter 3, Section 3.1; Chapter 4	
TClouds Deliverable	D2.3.1, Chapter 8	

6.1.4 Simple Cloud APIs

6.1.4.1 Details about the standards organization and the concerned standard

6.1.4.1.1 Standardisation Organization

Standards Organization: Simple Cloud Org

Receiving body of the Contribution:

Contact Name: via Zend Technologies

E-mail:

Role:

6.1.4.1.2 Standard investigated for TClouds

Standard concerned: Simple Cloud APIs

Specification concerned: no version information – needs to be further checked

Status of the specification: published

6.1.4.1.3 Specification investigated for TClouds

Specification	Version	Date	Doc Link, Status
Simple Cloud API		2010	http://www.simplecloud.org/documentation
API Implementation in the ZEND Framework			https://github.com/zendframework/zf2

6.1.4.2 Assessment of the Standard for the TClouds Architecture

Assessment is analog to CIMI. Yet another cloud management interface proposal that could be implemented in OpenStack in general. SimleCloud is heavily inspired by the properitary Amazon EC2 interface. Infrastructure Work Group Core Integrity Schema.

Summary Recommendation	(yes/no)
Is the standard applicable in TClouds?	Yes
Is an implementation planned for Y3 of the project?	No
Are extensions to the standard necessary in this context?	Yes

6.1.4.3 Partner Contribution: IBM

6.1.4.3.1 Application context in TClouds

Use cloud management API for extracting topological and configuration information of virtualized environments and cloud infrastructures.

6.1.4.3.2 Summary of the standards contribution

A new API method that extracts the configuration and topology, and provides it to the caller.

6.1.4.3.3 Related references (e.g. TClouds Deliverables, TClouds Standards Assessments)

Type of Reference	Document / Link	Status & Distribution Level
TClouds Deliverable	D2.4.2, Chapter 8, Section 8.0.4	

6.1.5 Infrastructure Work Group Core Integrity Schema

6.1.5.1 Details about the standards organization and the concerned standard

6.1.5.1.1 Standardisation Organization

Standards Organization: Trusted Computing Group

Receiving body of the Contribution: Infrastructure WG

Contact Name: Ned Smith

E-mail: ned.Smith@intel.com

Role: Co Chair

6.1.5.1.2 Standard investigated for TClouds

Standard concerned: Infrastructure Work Group Core Integrity Schema Specifications

Specification concerned: V1.0.1

Status of the specification: final

6.1.5.1.3 Specification investigated for TClouds

Specification	Version	Date	Doc Link, Status
Core Integrity Schema Specification	1.0.1	17 Nov 2006	http://www.trustedcomputinggroup.org/resources/infrastructure_work_group_core_integrity_schema_specification_version_101

6.1.5.2 Assessment of the Standard for the TClouds Architecture

6.1.5.2.1 Relevant component(s) in the TClouds Architecture

Remote Attestation service, composed of OpenAttestation (from Intel) and RA Verifier (from POL).

6.1.5.2.2 Use case example(s) to apply the standard in the TClouds Architecture

Verification of the integrity level of the Cloud nodes by Cloud Controller (OpenStack).

6.1.5.2.3 What technology is currently used to implement this functionality in TClouds?

The implementation of the standard.

6.1.5.2.4 How applicable is the standard in its current specification for TClouds?

It is currently implemented and used within the Remote Attestation service.

6.1.5.2.5 What are missing elements or shortcomings of this standard for TClouds?

No missing elements or shortcomings.

Summary Recommendation	(yes/no)
Is the standard applicable in TClouds?	yes
Is an implementation planned for Y3 of the project?	already in use
Are extensions to the standard necessary in this context?	no

6.1.5.3 Partner Contribution: POL

6.1.5.3.1 Application context in TClouds

The Remote Attestation Service is a TClouds subsystem responsible to assess the integrity of the nodes in the Cloud infrastructure through techniques introduced by the Trusted Computing technology.

This service gives significant advantages in the Cloud environment. First, it allows Cloud users to deploy their virtual machines on a physical host that satisfies the desired security requirements, which are represented by five incremental integrity levels. Requiring a greater level will give to users better guarantees that the selected physical host will not misbehave and will not try to compromise their virtual machine.

Secondly, it allows Cloud Administrators to monitor the status of the nodes in an efficient way and to take appropriate countermeasures once a compromised host has been detected. For instance, they can isolate the host so that it will not attack other nodes of the infrastructure.

It is composed of two building blocks:

OpenAttestation: a framework developed by Intel, enables OpenStack Nova Scheduler to retrieve and verify the integrity of Cloud nodes so that the latter can select a host that meets the users requirements. It handles the Remote Attestation protocol.

RA Verifier: a component developed by POL to verify the measurements performed on the Cloud nodes by the Integrity Measurement Architecture (IMA) software and carried through OpenAttestation.

6.1.5.3.2 Summary of the standards contribution

No extension has been done.

The standards are used “as is” within the component OpenAttestation (to carry attestation data between the Cloud nodes and the Controller Node) and between the latter and RA Verifier.

6.1.5.3.3 Related references (e.g. TClouds Deliverables, TClouds Standards Assessments)

Type of Reference	Document / Link	Status & Distribution Level
TCG specification	TCG Infrastructure Working Group - Core Integrity Schema Specification http://www.trustedcomputinggroup.org/files/temp/641FD59B-1D09-3519-AD96998DD875FF97/IWG%20Core%20Integrity_Schema_Specification_v1.pdf	Version 1.0.1, Revision 1.0, 17 November 2006
TCG specification	TCG Infrastructure Working Group - Integrity Report Schema Specification http://www.trustedcomputinggroup.org/files/temp/6427CBE0-1D09-3519-AD519217F523C9CB/IWG%20IntegrityReport_Schema_Specification_v1.pdf	Version 1.0, Revision 1.0, 17 November 2006

6.1.6 Open Virtualization Format (OVF)

6.1.6.1 Details about the standards organization and the concerned standard

6.1.6.1.1 Standardisation Organization

Standards Organization: DMTF

Receiving body of the Contribution: Open Cloud Standards Incubator

Contact Name: Winston Bumpus

E-mail: wbumpus@vmware.com

Role: Interim Co-Chair of the Incubator, DMTF President

Contact Name: Mike Baskey

Role: Interim Co-Chair of the Incubator

E-mail: mbaskey@us.ibm.com

6.1.6.1.2 Standard investigated for TClouds

Standard concerned: Open Virtualization Format (OVF)

Specification concerned: V2.0.0c

Status of the specification: work in progress (actual specification: 1.1.0)

6.1.6.1.3 Specification investigated for TClouds

Specification	Version	Date	Doc Link, Status
Open Virtualization Format Specification	2.0.0c	11 Jun 2012	http://dmtf.org/sites/default/files/standards/documents/DSP0243_2.0.0c.pdf
Open Virtualization Format Specification	1.1.0	20 Jan 2010	http://dmtf.org/sites/default/files/standards/documents/DSP0243_1.1.0.pdf

6.1.6.2 Assessment of the Standard for the TClouds Architecture

6.1.6.2.1 Relevant component(s) in the TClouds Architecture

Partner SRX/TUDA: The standard OVF relates to the specification of Virtual Machines (VMs) for packaging and distribution of software to be run in a VM.

6.1.6.2.2 Use case example(s) to apply the standard in the TClouds Architecture

Partner SRX: A use case example is the specification of VM in the Trusted Objects Manager (TOM) which then is deployed on a TrustedServer.

Partner TUDA: A standardised format to deploy encrypted VM images with Crypto-as-a-Service component.

6.1.6.2.3 What technology is currently used to implement this functionality in TClouds?

Partner SRX: Proprietary protocol.

Partner TUDA: Raw virtual hard-disks, as used by Xen, which are encrypted. No special VM image format.

6.1.6.2.4 How applicable is the standard in its current specification for TClouds?

Partner SRX: The aim is to support interoperability of VM implementations by an abstract specification of an OVF package. An OVF package consists mainly of a descriptor for a VM and zero or more disk image and resource files together with statements on their integrity and origin. Regarding functionality, an OVF package describes the type of the virtual image by its size, installed operating system, and requirements to the virtualized hardware including network. An OVF package makes a statement of the installed applications within a VM by their EULA license. Statements on the semantics of installed applications and services of a

VM are not given. Statements on integrity and origin of a VM address security. The manifest file of an OVF package consists of the hash values of each file within an OVF package excluding the certificate file. It is digitally signed. The certificate file contains the certified public test key for verifying the digital signature of the manifest file.

Partner TUDA: The standard allows extensions and the declaration of dependencies. Thus, for Crypto-as-a-Service, an extension can be defined to indicate encrypted images and the dependency on the corresponding encryption key (potentially a Managed Key Object in the KMIP protocol).

6.1.6.2.5 What are missing elements or shortcomings of this standard for TClouds?

Partner SRX/TUDA: There are no shortcomings. For realisation within TOM we may only need certain parts of OVF.

Summary Recommendation	(yes/no)
Is the standard applicable in TClouds?	Yes
Is an implementation planned for Y3 of the project?	Yes
Are extensions to the standard necessary in this context?	No

6.1.6.3 Partner Contribution: SRX

6.1.6.3.1 Application context in TClouds

The Trusted Object Manager (TOM) configures and coordinates centralized a Trusted Virtual Domain (TVD) and its Virtual Machines (VMs) (cf. Schirmer, 2011).

6.1.6.3.2 Summary of the standards contribution

We plan to make use of (parts of) OVF to specify VMs in the TrustedInfrastructures Cloud.

There are no contributions planned in the sense of extending the standard.

6.1.6.3.3 Related references (e.g. TClouds Deliverables, TClouds Standards Assessments)

Type of Reference	Document / Link	Status & Distribution Level
Open Grid Forum, 2011a	Open Cloud Interface – Core/Infrastructure, 2011	Standard / Public, unlimited
Open Grid Forum, 2011b	Open Cloud Interface – Infrastructure, 2011	Standard / Public, unlimited
Open Grid Forum, 2011c	Open Cloud Interface – RESTful HTTP Rendering, 2011	Standard / Public, unlimited

Type of Reference	Document / Link	Status & Distribution Level
Schirmer, 2011	TClouds D2.1.1 Technical Requirements and Architecture for Privacy-enhanced and Resilient Trusted Clouds. Report ICT-257243 / D2.1.1 / 1.0	Version 1.0 / Public

6.1.7 Cloud Data Management Interface (CDMI)

6.1.7.1 Details about the standards organization and the concerned standard

6.1.7.1.1 Standardisation Organization

Standards Organization: SNIA

Receiving body of the Contribution: Cloud Storage Technical Work Group

Contact Name: Dr. Markus Pleier

E-mail:

Role: Director SNIA Europe

Contact Name: Duane Baldwin (IBM)

E-mail: Duane.Baldwin@us.ibm.com

Role: IBM contact for SNIA

6.1.7.1.2 Standard investigated for TClouds

Standard concerned: Cloud Data Management Interface (CDMI)

Specification concerned: V1.0.2

Status of the specification: published

6.1.7.1.3 Specification investigated for TClouds

Specification	Version	Date	Doc Link, Status
Open Virtualization Format Specification	1.0.2	4 Jun 2012	http://snia.org/sites/default/files/CDMI%20v1.0.2.pdf

6.1.7.2 Assessment of the Standard for the TClouds Architecture

6.1.7.2.1 Relevant component(s) in the TClouds Architecture

Cloud File Storage.

6.1.7.2.2 Use case example(s) to apply the standard in the TClouds Architecture

CDMI could serve as interface to the resilient cloud file systems developed in TClouds.

6.1.7.2.3 What technology is currently used to implement this functionality in TClouds?

Currently none.

6.1.7.2.4 How applicable is the standard in its current specification for TClouds?

CDMI defines by interfaces a virtual file system with virtual files and virtual folders for data on demand – Data storage as a Service (DaaS). It distinguishes between functional interfaces describing data traces and management interfaces describing control traces. Metadata describes enforcement of different requirements on data, e.g. how data are stored and represented.

CDMI interfaces define container for data and abstract therewith from the data's representation. A container can recursively contain containers. Operations on containers and so on data are: create, retrieve, update, and delete. They define the data path. Control path defines how data are actually accessed. Data/containers can be assigned to specific domains (Domain objects). Access on data within a domain is granted based on access control lists (ACL) and credentials for showing the authorization to access requested data. Delegation is considered. Operations on data via CDMI interface are run based on HTTP.

CDMI defines operations on data in detail by the attributes of an operation and possible values. Regarding security, CDMI requests access control on data regarding confidentiality and integrity, mechanisms for their removal, protection against malware, and communication security for data exchange. Since CDMI considers logging of data access including all security related events, this log can be used to check ex post whether rules on data access have been followed.

6.1.7.2.5 What are missing elements or shortcomings of this standard for TClouds?

See extended list in Section 6.1.1.3.1.

Summary Recommendation	**(yes/no)**
Is the standard applicable in TClouds?	Yes
Is an implementation planned for Y3 of the project?	No
Are extensions to the standard necessary in this context?	No

6.1.7.3 Partner Contribution: FCUL

6.1.7.3.1 Application context in TClouds

This specification defines the interface and features for cloud store services. This is directly related with many contributions concerning cloud-of-clouds object storage (see TClouds Deliverable 2.2.2) and is also important for satisfying the legal requirements being defined in the project (see TClouds Deliverable 1.2.2).

The main standard we are interested here is CDMI v1.0.2. Although this standard builds upon several other standards (e.g., OCCI), the main aspects related with security and metadata management of cloud object storage are defined in this standard.

From reading the standard, several advanced features that might be interesting for the TClouds call our attention. A selected subset of these features are presented below, they represent some of the most interesting features that goes beyond the basic object storage model we consider in TClouds (see D2.2.2). Note: all metadata field names referred in this and next section contains also a prefix *cdmi_*.

- Range reads and writes are supported. This feature might be important for implementing client-side caching.
- Queues support peek (reading but not consuming), enqueue and dequeue operations, which means they are not simple FIFO queues, but "augmented queues", which can be used to implement synchronization among any number of clients (i.e., it solves the consensus problem in a wait-free manner – see "Wait-free Synchronization" by M. Herlihy, ACM TOPLAS, 1991).
- Expressive access control is also available (e.g., supporting users and groups).
- The support for data_redundancy, infrastructure_redundancy and data_dispersion data system metadata allows the definition of how many copies of the data need to be stored, and if these copies need to be in different infrastructures within a certain distance one from another (in Km). This is important for supporting dependable data storage and also an initial step towards standardized cloud-of-clouds storage.
- Data location constraints are supported through the geographic_placement data system metadata, where the object creator can specify geographic locations in which the object can be stored. This feature is important since there are legal constraints related with data location.
- The system support encryption for stored data, but the key is managed by the cloud provider, which means that any privacy requirement can only be satisfied if clients encrypt their data before storing it in the clouds.
- QoS constraints might be defined by data system metadata such as latency, throughput, RPO and RTO. It is worth to mention that these constraints are specified considering the internal cloud latency, without accounting the time spent on Internet communication between the client and the cloud.
- The standard supports accountability through logging queues. This might be an important requirement for a large number of cloud-based dependable and secure applications.
- Notification queues, as defined in the standard, allows the client to monitor a given group of objects and be notified when some operation is performed on these objects. This kind of feature, if supported by providers, allows a much more efficient implementation of cloud-backed file systems, especially because cache invalidation could be pushed to the clients, instead of making them executing periodic pooling on objects state.

Unfortunately, most popular cloud storage providers (e.g., Amazon S3, Rackspace, Windows Azure, Google Storage) does not support CDMI as today, however, there are some interesting news pointing that an OpenStack Swift compliant with CDMI is under development by IBM, and will be available soon.

6.1.7.3.2 Summary of the standards contribution

Besides the interesting capabilities mentioned in previous section, we still were able to find three missing features in the CDMI standard that could be interesting for implementing dependable services in using cloud storage.

First, the data system metadata called sanitization_method allows the user to specify the method for which an object deletion should be processed. It is still not clear if this field can be used to enforce immediate deletion (with no possible recovery, even by the provider), which is sometimes required by law.

The current version of the specification defines that objects creation and updates should be atomic (which might be an abuse of language, since the specified behaviour in page 44 is similar to a regular storage, according to Lamport's definition). Although the specification support delayed completion of operations, for some applications it might be enough to have eventual consistency, and thus it might be interesting to open the possibility for users to specify that they do not need strong consistency.

The third and last thing that is missing in the specification is a conditional update of data considering the several types of metadata available. The current specification already supports the association of a large spectrum of metadata fields to each object, including some defined by the user (called User Metadata). What is missing is a way to specify some constraints on metadata values for operations to be executed in such a way that, the operation is executed only if the metadata satisfies these constraints. As an example, consider a stored object associated with a user metadata called "version" with value 5, if an update for this object with a new a value and a new "version" value is requested with a constraint like "update only if new_version > version" one will be able to implement classical quorum protocols in CDMI-based clouds.

6.1.7.3.3 Related references (e.g. TClouds Deliverables, TClouds Standards Assessments)

Type of Reference	Document / Link	Status & Distribution Level
Deliverable	TClouds Deliverable D1.2.2	Public
Deliverable	TClouds Deliverable D2.2.2	Under Review, Public
Standard	http://cdmi.sniacloud.com	Public
Article	http://www.wired.com/cloudline/2012/04/openstack/	Public

6.1.8 Web Services Business Process Execution Language (WS-BPEL)

6.1.8.1.1 Standardisation Organization

Standards Organization: OASIS

Receiving body of the Contribution: WS-BPEL TC

Contact Name: Diane Jordan

E-mail: drj@us.ibm.com

Role: Co-Chair of the TC
IBM SWG, Strategy
Program Director, Emerging Internet Standards

6.1.8.1.2 Standard investigated for TClouds

Standard concerned: Web Services Business Process Execution Language (WS-BPEL)

Specification concerned: V2.0

Status of the specification: published standard

6.1.8.1.3 Specification investigated for TClouds

Specification	Version	Date	Doc Link, Status
WS BPEL	V2.0	11 April 2007	http://docs.oasis-open.org/wsbpel/2.0/OS/wsbpel-v2.0-OS.html

6.1.8.2 Assessment of the Standard for the TClouds Architecture

6.1.8.2.1 Relevant component(s) in the TClouds Architecture

We provide a fault-tolerant BPEL execution system (FT-BPEL) as part of the TClouds project.

6.1.8.2.2 Use case example(s) to apply the standard in the TClouds Architecture

The FT-BPEL component provides a set of network proxies that coordinate multiple BPEL engines to protect against software crashes.

6.1.8.2.3 What technology is currently used to implement this functionality in TClouds?

As the fault-tolerance properties are provided on top of any regular BPEL engine, the standard can be implemented as far as the underlying engine allow for.

6.1.8.2.4 How applicable is the standard in its current specification for TClouds?

Fully, although in practice there are currently limitations imposed by the underlying BPEL engine.

6.1.8.2.5 What are missing elements or shortcomings of this standard for TClouds?

None.

Summary Recommendation	(yes/no)
Is the standard applicable in TClouds?	yes
Is an implementation planned for Y3 of the project?	yes
Are extensions to the standard necessary in this context?	no

6.1.9 Key Management Interoperability Protocol (KMIP)

6.1.9.1 Details about the standards organization and the concerned standard

6.1.9.1.1 Standardisation Organization

Standards Organization: OASIS

Receiving body of the Contribution: KMIP TC

Contact Name: Robert Griffin

E-mail: robert.griffin@rsa.com

Role: TC Chair

6.1.9.1.2 Standard investigated for TClouds

Standard concerned: Key Management Interoperability Protocol (KMIP)

Specification concerned: V1.0

Status of the specification: Committee Specification – public

6.1.9.1.3 Specification investigated for TClouds

Specification	Version	Date	Doc Link, Status
Key Management Interoperability Protocol	V1.0	15 Jun 2010	http://docs.oasis-open.org/kmip/spec/v1.0/cs01/kmip-spec-1.0-cs-01.pdf

6.1.9.2 Assessment of the Standard for the TClouds Architecture

6.1.9.2.1 Relevant component(s) in the TClouds Architecture

TUDA's Secure-Block-Storage / Crypto-as-a-Service.

6.1.9.2.2 Use case example(s) to apply the standard in the TClouds Architecture

Two explicit use-cases have been identified:

1. Integrate the crypto-domain of the Crypto-as-a-Service architecture in a larger, enterprise key management infrastructure, instead of deploying a static key with the crypto-domain. Thus, KMIP can be used to manage the cryptographic credentials deployed in the crypto-domain.
2. For bootstrapping encrypted images, the decryption key has to be securely deployed in the cloud infrastructure. While the current Crypto-as-a-Service architecture leverages TCG Trusted Computing technology, KMIP can be used to ease the deployment and management of those particular keys and could enhance the customer interfaces to the cloud (e.g., image management).

6.1.9.2.3 What technology is currently used to implement this functionality in TClouds?

Crypto-domain is deployed with a static key; no key management available. For the second use-case, TCG TPM keys are used.

6.1.9.2.4 How applicable is the standard in its current specification for TClouds?

Use-case 1: Applicable when crypto-domains are deployed with authentication credentials for the KMIP server.

Use-case2: Technically applicable, since the current KMIP specification allows for proprietary key formats.

6.1.9.2.5 What are missing elements or shortcomings of this standard for TClouds?

No obvious elements are missing. However, for the second use-case the standard could be extended with explicit interoperability aspects for TCG TPM keys.

Summary Recommendation	(yes/no)
Is the standard applicable in TClouds?	yes
Is an implementation planned for Y3 of the project?	no
Are extensions to the standard necessary in this context?	(no)*

* See Answer to Question 6.1.9.2.5.

6.1.9.3 Partner Contribution: TUDA

6.1.9.3.1 Application context in TClouds

Deploying encrypted images requires that the corresponding decryption key is securely provided to trusted hosts in the Cloud infrastructure. Currently, the Crypto-as-a-Service component of TClouds uses TCG TPM to achieve this.

6.1.9.3.2 Summary of the standards contribution

6.1.9.3.3 KMIP already allows for proprietary key formats and wrapped keys. However, to ensure interoperability when using migratable TCG TPM keys (a feature often cited for trusted Cloud infrastructures) the standard could be extended to cater for the representation of TCG TPM keys as Managed Objects.

6.1.9.3.4 Related references (e.g. TClouds Deliverables, TClouds Standards Assessments)

Type of Reference	Document / Link	Status & Distribution Level
Standards Assessment	TClouds Assessment of Cloud Standards Key Management Interoperability Protocol (KMIP)	Finished/Public (as part of D4.1.2)
Deliverable	D2.4.2 Initial Component Integration, Final API Specification, and First Reference Platform	Finished/Public
Deliverable	D2.1.2 Preliminary Description of Mechanisms and Components for Single Trusted Clouds	Finished/Public

6.1.10 Open Cloud Computing Interface (OCCI)

6.1.10.1 Details about the standards organization and the concerned standard

6.1.10.1.1 Standardisation Organization

Standards Organization: Open Grid Forum
Receiving body of the Contribution: OCCI WG

Contact Name: Workgroup Mail
E-mail: occi-wg <occi-wg@ogf.org>

Contact Name: Ignacio M. Llorente
E-mail: Ignacio Martin Llorente <llorente@dacya.ucm.es>
Role: WG Member

6.1.10.1.2 Standard investigated for TClouds

Standard concerned: Open Cloud Computing Interface (OCCI)

Specification concerned: V1.1

Status of the specification: published

6.1.10.1.3 Specification investigated for TClouds

Specification	Version	Date	Doc Link, Status
Open Cloud Computing Interface	1.1	21 Jun 2012	http://occi-wg.org/about/specification/

6.1.10.2 Assessment of the Standard for the TClouds Architecture

6.1.10.2.1 Relevant component(s) in the TClouds Architecture

Everything providing or consuming resources.

6.1.10.2.2 Use case example(s) to apply the standard in the TClouds Architecture

OCCI specifies a general framework for describing all sorts of resources. Its main purpose is to monitor and control virtual machines as well as data storage facilities on the Infrastructure as a Service (IaaS) layer.

6.1.10.2.3 What technology is currently used to implement this functionality in TClouds?

The current demonstrator is based on OpenStack, which already provides most functions using an OCCI compliant API. TClouds specific extensions (e.g. encrypted/fault-tolerance storage) aren't specified in terms of the OCCI framework, but either as extensions to the OpenStack API or other proprietary protocols.

6.1.10.2.4 How applicable is the standard in its current specification for TClouds?

The core definitions are general enough to be applicable to any type of resource.

6.1.10.2.5 What are missing elements or shortcomings of this standard for TClouds?

As OCCI itself only specifies a framework for resource management and only provides a very basic interface for cloud computing infrastructures, there is no point in extending OCCI itself. Improvements from TClouds should be incorporated into derived specifications for certain areas, like CDMI for extensions related to data storage.

Summary Recommendation	(yes/no)
Is the standard applicable in TClouds?	yes
Is an implementation planned for Y3 of the project?	no
Are extensions to the standard necessary in this context?	no

6.1.10.3 Partner Contribution: IBM

6.1.10.3.1 Application context in TClouds

Use cloud management API for extracting topological and configuration information of virtualized environments and cloud infrastructures.

6.1.10.3.2 Summary of the standards contribution

A new API method that extracts the configuration and topology, and provides it to the caller.

6.1.10.3.3 Related references (e.g. TClouds Deliverables, TClouds Standards Assessments)

Type of Reference	Document / Link	Status & Distribution Level
TClouds Deliverable	D2.4.2, Chapter 8, Section 8.0.4	

6.1.10.4 Partner Contribution: TUDA

6.1.10.4.1 Application context in TClouds

Deploying encrypted images requires that the corresponding decryption key is securely provided to trusted hosts in the Cloud infrastructure. Currently, the Crypto-as-a-Service component of TClouds uses TCG TPM to achieve this.

6.1.10.4.2 Summary of the standards contribution

6.1.10.4.3 OCCI allows the introduction of new extensions by sub-typing. To enable new interfaces for dealing with encrypted images and incorporating the necessary commands for the KMIP key deployment, new resources, links, and actions (sub-typing) should be introduced.

6.1.10.4.4 Related references (e.g. TClouds Deliverables, TClouds Standards Assessments)

Type of Reference	Document / Link	Status & Distribution Level
Standards Assessment	TClouds Assessment of Cloud Standards Key Management Interoperability Protocol (KMIP)	Finished/Public (as part of D4.1.2)
Deliverable	D2.4.2 Initial Component Integration, Final API Specification, and First Reference Platform	Finished/Public
Deliverable	D2.1.2 Preliminary Description of Mechanisms and Components for Single Trusted Clouds	Finished/Public

6.1.11 Further Contributions

6.1.11.1 Partner POL: Libvirt XML Format

libvirt XML format (http://www.libvirt.org/format.html), a de-facto standard for configuring the virtualization software, regardless of the hypervisor used.

6.1.11.1.1 Application context in TClouds

One component of the TClouds subsystem “Ontology-based Reasoner to Check TVD Isolation” is the Enforcer, and it is in charge of setting up secure tunnels by means of libvirt library (http://www.libvirt.org/).

To implement this function, libvirt has been extended to describe virtual networks isolated through VLAN tagging that can be used to group VMs in a TVD; furthermore, libvirt is now capable to connect those isolated virtual networks through different types of physical networks: for L2 networks, libvirt configures the host to send tagged Ethernet frames through the eth0 (em0) interface. For L3 networks, libvirt creates a tunnel to the another host in order to send Ethernet frames to the remote switch as they are sent locally; this is possible through encapsulation of Ethernet frames using the GRE protocol. libvirt also allows to protect data exchanged among physical hosts through a tunnel by encrypting them using IPSEC (configuration parameters are defined in the XML configuration file). Finally libvirt gives a solution to the attack model where an host is compromised and tries to send Ethernet frames with an arbitrary tag. This attack can be avoided by storing in libvirt the association between hosts and allowed TVDs, so that a benign host can discard Ethernet frames with an unexpected tag.

6.1.11.1.2 Summary of the standards contribution

XML format has been extended in the virtual network definition to support the setup of L2 frames tagging, IP tunnel definition, IPsec profile definition and simple packet filtering

6.1.11.1.3 Related references (e.g. TClouds Deliverables, TClouds Standards Assessments)

Type of Reference	Document / Link	Status & Distribution Level
TClouds Deliverable	TClouds D2.3.2 Components and Architecture of Security Configuration and Privacy Management. Report ICT-257243 / D2.3.2 / 1.0 – Section 3.2.4	Being delivered to EC
De-facto standard	libvirt XML format (http://www.libvirt.org/format.html)	

6.1.11.1.4 Status of the standards contribution

Standards Contribution Activity	Date	Status
To be submitted to libvirt community		