Publishable Summary

Project number:	257243
Project acronym:	**TClouds**
Project title:	**Trustworthy Clouds** - Privacy and Resilience for Internet-scale Critical Infrastructure
Start date of the project:	01.10.2010
Duration:	36 months
Programme:	FP7 ICT IP

Date of the reference Annex I:	06.03.2013 (Annex I – DoW Version 4.0)
Periodic report:	Publishable Summary (as part of D4.2.2 "3rd Periodic Report according to EC regulations of the model contract")
Period covered:	01.10.2012-30.09.2013 (M25-M36)
Activities contributing:	All
Due date:	30.09.2013 (M36)
Actual submission date:	19.12.2013 (V02)

Project Coordinator:	Technikon Forschungsgesellschaft mbH (TEC)
Tel.:	+43 4242 233 55
Fax:	+43 4242 233 55 77
E-mail:	coordination@tclouds-project.eu
Project website:	www.tclouds-project.eu

1 Publishable Summary

Project name: **TClouds** *Start date*: 1st October 2010
Grant Agreement: **257243** *Duration***:** 36 months
Project website: http://www.tclouds-project.eu/
Contact: coordination@TClouds-project.eu

Mission of TClouds: *To develop an advanced cloud infrastructure delivering computing, networking, and storage that achieves a new level of security, privacy, and resilience yet is cost-efficient, simple, and scalable. To change the perceptions of cloud computing by demonstrating the prototype infrastructure in socially significant application areas: energy and healthcare.*

The TClouds Project: TClouds envisioned and built a Future Internet where federations of standardized resilient and privacy-protecting global infrastructure clouds offered virtualized computing, communication, and storage resources that allowed hosting of critical and non-critical ICT systems. Particular focus was placed on privacy protection in cross-border infrastructures and on ensuring resilience against failures and attacks.

Motivation: State-of-the-art cloud computing enables seamless access to services and global availability of information, but inherent risks severely limit the application of this technology. In a cloud environment, pertinent data is accessed via information and communications technology (ICT) using remote hardware instead of being stored only on a local server or computer. The benefits of increased storage at reduced cost allow information to be made readily available. However, the cloud computing model in 2010 came with perceived risks concerning resilience and privacy. There were three fundamental trends in ICT whose risks mutually reinforced each other:

- the push towards an Internet of Services - most services were provided on the web as a platform;
- cost pressures drove a migration of ICT into so-called Infrastructure clouds;
- growing importance of ICT as the critical “nervous system” for socially relevant “smart” infrastructures – such as healthcare, energy, environmental monitoring, or mobility.

Protecting data and services in the cloud is important to governments, organizations and enterprises across all industries, including healthcare, energy utilities, and banking. Thus, the perceived security and dependability risks of cloud computing were limiting its application.

The TClouds project targeted cloud computing security and minimization of the widespread concerns about the security of personal data by putting its focus on privacy protection in cross-border infrastructures and on ensuring resilience against failures and attacks.

Objectives & Overall Strategy: Trustworthy Clouds (TClouds) aimed to build a prototype Internet-scale ICT infrastructure, which allowed virtualized computing, network, and storage resources over the Internet to provide scalability and cost-efficiency. The following objectives contributed to achieving the overall goal:

- Identifying and addressing the legal and business implications and opportunities of a widespread use of infrastructure clouds, contributing to building a regulatory framework for enabling resilient and privacy-enhanced cross-border infrastructure clouds.
- Defining an architecture and prototype for securing infrastructure clouds by providing security enhancements that can be deployed on top of commodity infrastructure clouds (as a cloud-of-clouds) and assessing the resilience and privacy benefits of security extensions of existing clouds.
- Providing resilient middleware for adaptive security on the cloud-of-clouds. The TClouds platform provided tolerance and adaptability to mitigate security incidents and unstable operating conditions for a range of applications running on such clouds-of-clouds.

To demonstrate TClouds, scientists prototyped two scenarios involving critical IT-systems including:

- A smart energy grid with Portugal’s leading energy and solution providers Energias de Portugal and EFACEC ENG: A combination of smart metering and a Web-based real-time status and energy consumption control system enabling public utility providers to monitor and

efficiently control a public lighting network. TClouds showed how such energy-preserving systems can be migrated to a cloud infrastructure while increasing their resilience, privacy protection and tolerance, from both hackers and hardware failures.

- A patient-centric home healthcare service with San Raffaele Hospital in Milano, Italy, remotely monitoring, diagnosing and assisting patients outside of a hospital setting. TClouds demonstrated how the quality of in-home healthcare can be improved cost-efficiently without reducing privacy.

The above objectives were achieved within the three main activities as displayed in Figure 1 below.

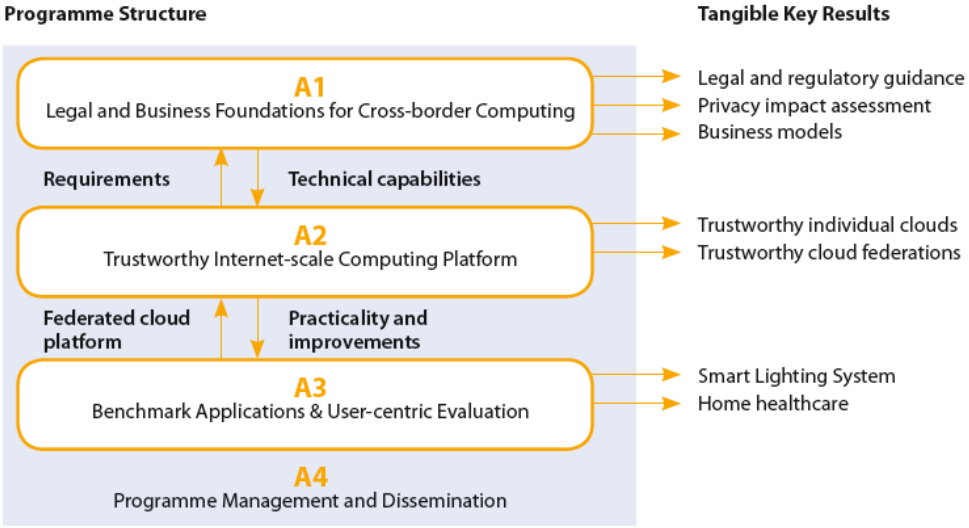

Figure 1: TClouds project activities

The work plan of TClouds encompassed four independently managed activities and twelve tightly integrated work packages.

Description of the work performed and results in the third project period

The TClouds project started in October 2010, lasted 36 months, and ended in September 2013. The consortium trusts that it has achieved all the objectives and technical goals of the project. The correspondent box was ticked on the cover page. All deliverables were submitted and all milestones reached. The progress achieved by all work packages within the 36 months project duration is in line with the initial plan and can be summarized as follows:

WP1.1 (Requirements and Roadmap) investigated the business value and market potential for specific security-enhancing and privacy-supporting technologies developed by TClouds. Furthermore, it has empirically obtained insight from market participants into the deployment of trustworthy cloud-computing technology in the online healthcare and smart-energy application domains. Multiple events were organized that placed the focus on public awareness for such technologies and that promoted their exploitation.

Within ***WP1.2 (Legal Implications and Impact of Cross-Border Cloud Implementations)*** the consortium worked towards an identification of legal implications in respect to cloud computing business and service models. A definition and analysis of the general legal framework and requirements of the European data protection law was made. Moreover, the project investigated their relevance to cloud computing scenarios and carved out different ways of achieving data protection compliance (contractual, organisational, and technical). Toward the end of the project the team conducted a Data Protection Impact Asessment of the TClouds use-case scenarios and the used components. Existing Privacy Impact Assessment Schemes were analysed, their shortcomings identified and a new universal methodology based on data protection goals was proposed. TCloudsapplied this methodology to assess the privacy impact of the TClouds use-cases and the data protection and security benefits of the TClouds components.

WP1.3 (Business Impact of and Business Models for Infrastructure Clouds) investigated requirements on security and resilience features in cloud computing from a business perspective. It provided three kinds of results. First, it summarized and analyzed the services of a representative selection of Infrastructure-as-a-Service (IaaS) cloud providers. A particular focus was put on security

features, resilience aspects, and regulatory compliance. Second, this work explored the impact of trust-related aspects on cloud-computing business models, specifically in terms of the security and resilience technology as provided in the framework of TClouds. Problems, technical approaches, and the corresponding business impact were analyzed. As a third contribution, this work package focused on the business implications for the two benchmark scenarios (Home Healthcare and Smart Lighting/Smart Energy) when supported by enhanced methods for security and resilience such as investigated by TClouds.

The objective of ***WP2.1 (Trustworthy Cloud Infrastructure)*** was to enhance the resilience and privacy-awareness of an individual cloud infrastructure. The workpackage evolved roughly in three phases, aligned with the project years. In the first year we did an intensive gap and requirement analysis to identify the major shortcomings of commodity cloud offerings. In the second year we researched into components and mechanisms to overcome these shortcomings. Finally, in the third year we integrated the technical insights into our proof-of-concept prototypes and combined them into our TClouds platform. Besides significant research papers and results the work integrated into two infrastructures, the Trusted Infrastructure Cloud and the Trustworthy OpenStack. The motivation for implementing two distinct infrastructures was as follows. TrustedInfrastructure Cloud was constructed from ground up with security and trustworthiness in mind, employing trusted computing technologies as a hardware anchor. With trusted boot and remote attestation we ensured that only untampered servers with our security kernel were started and that the sole way of administration is via the trusted channel from the management component TOM. Hence no administrator with elevated privileges was necessary and hence this functionality was completely disabled, abandoning the possibility for an administrator to corrupt the system. On the contrary, Trustworthy OpenStack was based on OpenStack which had a strong bias towards a scalable and decentralized architecture. We extended or embeded new components into the OpenStack framework to improve its security. With these two infrastructures we could cover the needs of a wide range of application scenarios. Trusted Infrastructure Cloud is especially attractive for private or community clouds with high security demands, while Trustworthy OpenStack is attractive for large-scale public clouds.

The first activity carried out in ***WP 2.2 (Cloud of Clouds Middleware for Adaptive Resilience)*** was the development of a set of architectural principles for the TClouds ecosystem for guiding the development of the technical solutions devised by TClouds. With this architecture in mind, the partners engaged in the development of several sub-systems, from which we like to highlight two. The first one was a Byzantine fault-tolerant state machine replication middleware that could be used to implement intra- and inter-cloud dependable services. Our second achievement was the development of theoretical and practical aspects of cloud-of-clouds resilient object storage. The results of this work appeared in a set of publications during the last three years (as well as in the project deliverables), open-source implementations and also in prospective products from some industrial partners. Besides these two main subsystems, there are still a set of components and ideas that different partners are developing in the context of this work-package.

The overall objective of **WP2.3** ***(Cross-layer Security and Privacy Management)*** was to provide mechanisms to manage the privacy-enhanced resilience of the TClouds platform. The work package had three phases that spanned the three years of the project. The goal during the first project year was to collect component requirements for management operations and to explore the interaction between the various technologies and the demonstration in WP2.4. Furthermore, several concepts and systems for selected management tasks were developed. In the second year, the requirements for large-scale and distributed security management were consolidated. The components and the architecture were developed further and partially finalized. These components are mostly documented in the current deliverable, and they show how the security objectives are can be implemented and managed on all different layers concerned by the TClouds platform. Finally, in the third year, this work package integrated the management functions with the TClouds platform and added automation of certain management operations. The contributions related to cloud-management systems from the TClouds project have achieved significant visibility in scientific and technical forums. Multiple papers at first-tier conferences were published, for instance, and some work has already led to concrete assets produced by the partners.

The main outcomes of the work in ***WP2.4 (Architecture and Integrated Platform)*** done during the first year were a consistent design of 15 subsystems, including secure block device, cloud-of-clouds storage, access control, secure logging, and auditing, that were developed by partners and an initial installation of the TClouds platform Version v0. This platform was an unmodified instance of OpenStack, the open-source cloud computing framework selected by TClouds for integration and

demonstration of its results. A prototype application for the benchmark applications was running on top of this. All the work for the use cases selection, design of the high-level architecture, draft API and test methodology was done by each partner on his subsystems, following the common methodology shared along the project. Each activity ended with a written report to consolidate the results, which were collected in deliverable D2.4.1. During the second year the main work consisted of an initial integration of the 15 subsystems (plus one more) into three prototypes (Trustworthy OpenStack, TrustedInfrastructure Cloud and Cloud-of-Clouds, all framed in a single scenario) that form the TClouds platform Version v1; the definition of the test plans for all subsystems and the test results for those subsystems integrated in prototypes; a consistent and automated building and testing system for developing the subsystems being part of Trustworthy OpenStack; finally, the preliminary analysis about the fulfilment of requirements from the legal perspective and the application scenarios. The work was organized in phases, where each activity ended with a written report that documented the results; this was collected in deliverable D2.4.2. During the third year, the initial concept of the TClouds platform was evolved into a comprehensive ecosystem, which includes the original subsystems, arranged in logical service layers that form the TClouds platform Version v2. Furthermore, the test plans for all subsystems were refined, the final test results for those subsystems were obtained, and the TClouds platform was provided to the two benchmark applications. For this reason the activities within this work package were carried out on two parallel tracks: refining the integration among groups of subsystems to form the infrastructures at IaaS and evolving the subsystems, where necessary, to fully support the benchmark scenarios. These activities involved a close collaboration of all partners. The results of the final TClouds platform v2 concept and implementation together with the test plans and results were collected in the deliverable D2.4.3.

WP3.1's (Cloud Applications Data Structures for Home Healthcare Benchmark Scenario) main objective was to define the cloud based Home Healthcare architecture and specification from the application point of view, to provide technical requirements for cloud computing in the healthcare sector, and to turn this analysis into an architecture, API, and protocols for the client side. This home healthcare architecture was closely linked and integrated with the TClouds platform. The WP3.1 results were validated in collaboration with the demonstrator implementation. WP3.1 started in M1, and provided its results in D3.1.1 "Trust Model for cloud applications and first Application Architecture" in M12, D3.1.2 "Application API and first specification on application side trust protocols" in M18 and D 3.1.3 "Draft proof of concept for home healthcare" in M24. In the first project year, WP3.1 delivered the cloud-based Home Healthcare use case applications, and developed the mockup based on a commodity cloud Openstack. In the second project year, WP3.1 took the effort to enhance the integration with the underlying cloud infrastructure by extending WP3.1 towards the platform layer, by developing a trusted Healthcare Platform as a Service (i.e. the Healthcare T-PaaS). The design and development Healthcare T-PaaS was reported in deliverable D3.1.2 and D3.1.3. In the third project year, WP3.1 completed the tasks to develop the application side trust protocols and the prototype of the TClouds trustworthy platform for home healthcare services. Also, WP3.1 organised and participated in several integration meetings among the involved project partners with the purpose of analysing and understanding how the technical components contribute to complying with Healthcare T-PaaS security requirements. In order to guarantee a good alignment between the participants in this work package, we organized partner-to-partner conference calls, technical meetings, and targeted teleconferences throughout the project period.

WP3.2 (Cloud-middleware and Applications for the Smart Grid Benchmark Scenario)'s main objective was to provide a sample smart grid application architecture and to validate it by means of a prototype. To do that we selected a specific use case, based on the public lighting management, to migrate to the TClouds platform while providing scalable computing and enhancing its resilience and privacy protection. WP 3.2 started with the definition of functional and technological requirements for this new application. This work was then incorporated in a smart lighting specification. After this first step, we started the reengineering process in order to adopt the TClouds middleware and TClouds platform; this resulted in a prototype solution that satisfied the requirements and architecture defined in previous tasks. Lastly we worked on the integration of the TClouds platform and assessment of results through a validation process.

The focus of ***WP3.3 (Validation and Evaluation of the TClouds Platform)*** was to validate the features of all components against the requirements defined by the demonstration scenarios. The bulk of the work was done starting from M18, and in the first months of this task FSR led the implementation of a common validation strategy both for the two application scenarios and for the whole TClouds platform. The work started from the selection of relevant requirements (collected in other WPs) on the platform, based on their relevance toward project objectives. From this

requirements selection, indicators and success criteria were identified. During the third year, WP3.3 also conducted surveys with their respective stakeholders in order to have a better understanding of the requirement's priority and importance. This validation was conducted in close cooperation with all partners.

WP4.1 (Standardisation and Dissemination) was responsible for the dissemination and exploitation of the project achievements and results. Activities done in this area were the following (M01-M36): Monitoring and update of the TClouds project website, fostering cooperation activities with related projects, publications (~74 peer-reviewed publications, 11 other publications & 21 press releases) in academic and technical magazines, 57 presentations at various academic and industrial international conferences (e.g. 13th ISSE, CPDP, Eric Conference, W3C, OECD conferences), participation in 48 workshops and publication of periodical TClouds newsletters (3 issues). Furthermore some major events were (co-)organized: Workshop Cryptography and Security in Clouds (Zurich, March 2011), Cloud Security Alliance SecureCloud conference (Frankfurt 2012), Dagstuhl Seminar Security and Dependability for Federated Cloud Platforms (July 2012), CPDP 2013 session: Cloud, trust, and privacy: Towards the Intercloud (Brussels, January 2013), Workshop on Trustworthy Clouds (London, September 2013). Within WP4.1 a roadmap of standards was laid out and concrete steps taken by the partners to contribute specific TClouds results to the identified standardisation bodies. TClouds contributed to the following cloud-computing standards initiatives: EU Art. 29 WG, Trusted Cloud Initiative, W3C Do-Not-Track. The industrial partners will individually or jointly take the newly developed technologies to the market, either in the form of concrete products, some of which are already available, or in the form of knowledge that influences future products. The partners, in particular the academic partners, transferred their acquired knowledge and results to education, which is underlined by 29 PhD, MSc and BSc theses that were or are still conducted. Furthermore several practical courses and lectures were held for students.

WP4.2 (Project Management and Activity Coordination) was responsible for the effective organisation of the project and covered all relevant management components. Some of the main achievements were: organisation of meetings and workshops (eg. GA-meetings, review and technical meetings), periodic reporting including financial reporting and distribution of tranches, biweekly EB-telcos, monitoring of the work plan (QMR-reporting), supporting partners in everyday issues (handling day2day requests), etc.

Final results and their potential impact and use

The TClouds project has improved the security and resilience of cloud computing platforms in response to widespread concerns about data privacy and robustness of services in the cloud model. It has realized a trustworthy cloud-computing platform, the TClouds platform, which integrates multiple advanced security technologies in a standard cloud distribution and in commercial cloud systems. Some of them are already being exploited commercially by the industrial partners of the project. The project has also organized many prominent and well-attended scientific workshops and technical events in Europe, which focus on the theme of cloud security. With these and through their technical contributions, the project partners have achieved global visibility for their leadership in this domain.

The TClouds Consortium

The consortium consisted of 14 partners from 7 different countries. In the third project period, partner Fondazione San Raffaele del Monte Tabor (HSR) became Fondazione Centro San Raffaele (FCSR), in addition to third party Ospedale San Raffaele (OSR). FCSR took over all rights and obligations of HSR as of 11 May 2012. Furthermore, OSR was linked to FCSR through special clause 10 within Amendment n. 3 (Annex I – version 4.0).

Figure 2: TClouds consortium

TClouds Disclaimer

All public information is marked with the following TClouds project disclaimer: “This work was partially supported by the European Commission through the FP7-ICT program under project TClouds, number 257243. The information in this document is provided as is, and no warranty is given or implied that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability. The opinions expressed in this deliverable are those of the authors. They do not necessarily represent the views of all TClouds partners."

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