Publishable Summary

Project number:	609611
Project acronym:	PRACTICE
Project title:	PRACTICE: Privacy-Preserving Computation in the Cloud
Start date of the project:	1st November 2013
Duration:	36 months
Programme:	FP7/2007-2013

Date of the reference Annex I:	05.09.2013
Periodic report:	Publishable Summary (as part of D33.2 "1st periodic report according to EC regulations of the model contract")
Period covered:	01.11.2013 – 31.10.2014
Activities contributing:	All
Due date:	October 2014 – M12
Actual submission date:	3rd February 2015, V1.2

Project Coordinator:	Dr. Klaus-Michael Koch Technikon Forschungs- und Planungsgesellschaft mbH (TEC)
Tel:	+43 4242 233 55
Fax:	+43 4242 233 55 77
E-mail:	coordination@practice-project.eu
Project website:	www.practice-project.eu

Chapter 1 Publishable Summary

Project name: **PRACTICE** *Start date*: 1st November 2013
Grant Agreement: **609611** *Duration***:** 36 months
Project website: http://www.practice-project.eu/
Contact: coordination@practice-project.eu

Mission of PRACTICE: *To design cloud computing technologies that allow computations in the cloud thus enabling new business processes while keeping the used data secret. Unlike today – where insiders can access sensitive data – PRACTICE will prevent cloud providers and other unauthorized parties from obtaining secret or sensitive information.*

The PRACTICE project aims to:

- Build a secure cloud framework that allows for the realization of advanced and practical cryptographic technologies
- Provide sophisticated security and privacy guarantees for all parties
- Offer data confidentiality and integrity, eliminating need for users to trust cloud providers
- Enable computation on encrypted data, preventing even insiders from disclosing secrets or disrupting the service

Motivation: Information processed by businesses, government organizations and individuals often comes with confidentiality and integrity requirements that the processing party must adhere to. As a result, data processors must deploy security controls for their ICT infrastructure, protecting it against external as well as internal attackers. This is relatively easy when this infrastructure is local and controlled by the processing party, but much harder when it is provided by an external service provider.
A comprehensive solution for securing the cloud computing infrastructure can be based on cryptographic mechanisms of secure computation. These mechanisms allow for distributed computation of arbitrary functions of private (secret) inputs, while hiding any information about the inputs to the functions. Put differently, these mechanisms support computation on encrypted data. We identify several settings where secure computation in the cloud is needed. PRACTICE will address all of these settings:

- Hiding user data from other users of the same cloud service.
- Hiding user data from the cloud provider.
- Securing computation between several servers.
- Securing computation between untrusting parties.

Objectives & Technical Approach: The work plan for the PRACTICE project is structured into three loosely coupled Activity lines and tightly integrated Work packages:

- **Activity 1 "Specification, Design and Implementation of Protocols"** is responsible for analysing existing techniques to build the application and protocol specifications to design the algorithms and protocols.
- **Activity 2 "Tools, Applications and Prototypes"** is concerned with the design, implementation, evaluation and demonstration of tools and applications of algorithms and protocols developed in Activity 1.
- **Activity 3 "Information Sharing and Project Organisation"** is mainly responsible for wide and effective dissemination as well as the proper programme management that ensures timely and high-quality delivery of all results while mitigating emerging conflicts and risks.

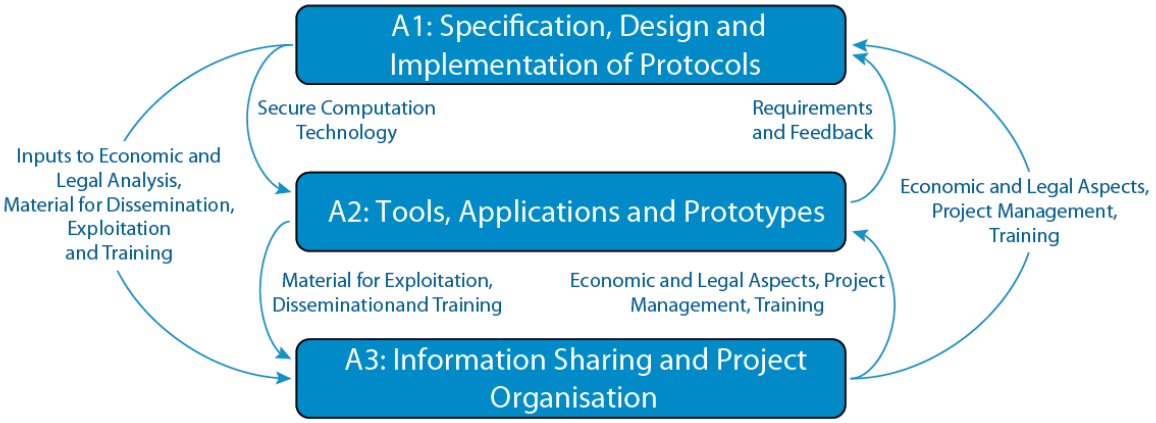

Figure 1: PRACTICE Activities overview

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

The PRACTICE project started in November 2013 and is set to run for 36 months. During the first project phase, corresponding to the first project year, the focus was placed on the analysis of existing techniques, application specifications and security requirements. All work packages initiated work and produced altogether 10 Deliverables (including this first Periodic Report) throughout the first project year.

At the beginning, major effort was put into the successful launch of the project. The major goal was to establish a sound basis for a good and fruitful cooperation of the project partners towards the research objectives. We managed to develop collaboration while creating a large number of publications and presentations documenting ideas that we can leverage and extend in subsequent years. This has been achieved by strong leadership and by optimizing the organisation and infrastructures. All relevant management components on contractual, financial, legal, technical, administrative and ethical topics were created and provided as well as catching upcoming obstacles well ahead of time. Furthermore, a public project website and the internal IT communication infrastructure were implemented. The progress achieved by all work packages within the first project year is in line with the initial plan and can be summarized as follows.

WP11 (Analysis of Existing Techniques) is responsible for a theoretical analysis of existing protocols for secure computation, in both the two-party and the multi-party settings. The analysis is with respect to generic protocols and to specialized protocols that solve specific problems with particular interest. In a later stage the WP will perform evaluation of key protocols and comparisons of their performance. Relevant key technologies are protocols for secure two-party computation based on the Yao and GMW techniques and their variants, protocols for multi-party computation based on the GMW and BGW techniques and their variants, protocols with a pre-processing step that have a very efficient online step, such as the BDOZA and SPDZ protocols, specialized protocols for specific problems such as private set intersection, and methods for ensuring universal verifiability of the protocols.

WP12 (Applications Specifications) is responsible for the specification of application scenarios that greatly benefit from secure computation technologies and provide adversary, trust, communication and system models based on those scenarios. The application scenarios were compiled in the deliverable D12.1. For each use case scenario an animation was created and published on the project website. Work on adversary, trust, communication and system models is ongoing. Another part of this WP deals with the identification and analysis of a subset of scenarios that require formal verification to establish strict correctness and security guarantees for critical components. This activity was also initiated.

WP13 (Protocol Specification and Design) is responsible for designing new protocols for secure two-party and multi-party computation, and for designing efficient verifiability solutions for secure computation. This work builds upon the analysis of the state of the art by WP12 and WP12, with the goal of designing new solutions where the existing protocols are insufficient. The tasks on this WP are ongoing and span until almost to the end project. In the first year, initial work started on the design of new protocols, with some results being published or submitted for publication.

In ***WP14 (Final Implementation)*** we are designing and developing a platform for secure computation. The platform will allow industrial and research users to quickly implement new secure computation solutions and validate the attributes of the solution. Either by benchmarking against other solutions, which are build on the platform, or by clearly seeing the value of the solution in practice. The platform will be flexible and support multiple applications and scenarios. The development of the architecture and implementation is well in progress. The architecture is being developed in coordination with WP 21 on the general architecture for secure computation applications and services. A first version of the architecture has been designed and the implementation is progressing accordingly. This has resulted in a solid foundation for the platform proper, and at least one accepted research paper. The basis for a formally verified two-party secure computation framework was launched in close connection with WP12 and WP22. The effort on verifiable secure computation in this WP is also coordinated with WP23.

WP21 (Architecture and Integration) is responsible for making sure that the secure computation technologies in PRACTICE fit together and are usable in real-world information systems. The consortium has brought together the world's leading experts in deploying real-life secure computation applications. The WP started by collecting all that knowledge and compiling an architectural analysis of current deployments. This resulted in the deliverable D21.1 – a useful document for planning future deployments in an outside of PRACTICE.

In ***WP22 (Tools)***, a set of tools shall be designed and implemented which enables practitioners to develop, test, and deploy secure computation applications. This work package started by listing the state of the art and listing the intended changes the software landscape. In the future, this work package will present prototypical implementations of the secure computation tools.

WP23 (Secure Statistics Prototype) focus on developing software for secure statistics tailored various applications such as online questionnaires (surveys), relative performance evaluation (benchmarking) and descriptive statistics in a more broad sense. The primary focus has been on developing a Survey Service where the answers are kept confidential. The secure survey will be the first deliverable in WP23 (D23.1). Surveys are widely used to evaluate almost anything, from employee satisfaction to finding the best business ideas. Our Secure Survey disrupt the traditional "supply chain" for how surveys are conducted by replacing the "trustee function" by a MPC system that keeps the answers confidential at all times. The prototype is a joint application among the three partners in the WP. There are numbers of different MPC protocols and systems and a challenging part of this prototype is to develop a system that is sufficiently flexible to run on two different MPC systems (respectively "Sharemind" and "SPDZ/Fresco"). From a customer perspective, this address a potential "vendor lock-in" and opens up for competition between MPC service providers. The prototype will be delivered in April 2015 and the development is progressing as planned. The survey system has been described and the basic software architecture is fixed. The user interface is described and currently developed alongside the backend survey system. Concerning the MPC side, the Sharemind system is made ready for the integration and the initial programming of the SPDZ/Fresco components has been initiated.

The activities related to ***WP24 (Supply Chain Prototype)*** were aimed at selecting specific industrial processes that could be improved by applying secure data sharing in a cloud system. In particular, processes involving many firms belonging to a supply chain and

constrained by the confidentiality of data, were explored. While exploring industrial practices, the general requirements of the scenarios were defined: the need of collaborative planning beyond traditional customer-supplier interactions, involvement of sensitive data, complex and joint computation to compute the plan. The selected aeronautic process is the 'fleet management': the process of maintaining efficient the engine fleet of an airline or air force. Cloud systems are already applied to standardize communication between the customer and the service provider in order to improve its own planning capabilities. An extensive usage of such systems, leading to a more efficient service planning and material flow, is constrained by the capability of cloud systems to guarantee data protection against data leakage risks. The consumer goods industry is even more complex, as OEMs apply contemporary different business models with different customers. The result is that products demand forecasts of OEMs are strongly affected by data confidentiality: customers are reluctant to provide data at all, and, in any case, they protect themselves from data leakage risks by overstating demand. For this reason, it is expected that higher security performances of a collaborative system will drive customers to provide actual demand forecasts, leading a less costly production chain. From the business model point of view, the 'vendor managed inventory' approach (the OEM manages directly the inventory of its customer – the distributor – satisfying the policy defined in the agreement) seems to be very suited for the consumer goods industry: in this case, OEM can directly plan its production and purchasing tasks. Due to the numerous customers, it is strongly required data are protected against any risk leading to data disclosing. Activities currently on going are: the development of the computational model, the definition of the specific risks associated to the data leakage events, the identification of the expected benefits of a secure cloud collaborative planning system. Results of these activities are expected in the following project period.

WP31 (Business Implications and Risks) provides a first overview of the legal issues concerning cloud computing under the current European data protection law, including a detailed discussion of the most important regulations and directives, and the analysis of some case studies useful for evaluating the techniques developed by PRACTICE under a legal perspective. On the basis of the discussion, privacy and confidentiality breaches, especially the ones involving personal data, are identified as major regulatory issues at both European and national level. Furthermore an outline of the state of the art in methodologies and techniques for assessing and managing risks for cloud-based business processes has been presented as well as a first version of a process-oriented assessment methodology, aimed to analyse risks in multi-party business processes taking place on clouds. The methodology supports the analysis and quantitative evaluation of risks related to privacy and confidentiality breaches during the execution of a multi-party business process.

For ***WP32 (Dissemination, Standardisation, Exploitation and Training)*** a robust IT infrastructure (web site, SVN repository including web access, mailing lists including mailing list archives) was established as early as M02 (D33.1; www.practice-project.eu) and regularly updated since. Hardcopies of the PRACTICE project flyers have been distributed by partners at various events. A roll-up and poster was created for several dissemination activities. The project is visible on twitter and LinkedIn. Two newsletters have been published and distributed. Dissemination activities are announced via http://practice-project.eu/news. In terms of dissemination management, to ease communication on publications, a mailing list for publication proposals has been established. A list of dissemination activities has been compiled and updated periodically. The deliverable D32.1 "Updated plan and initial report on dissemination, standardisation, exploitation and training" [D32.1] has been compiled and lists 18 peer-reviewed scientific publications, 15 organized events (workshops, summer schools) as well as organized of high-profile international events and 8 participations in conferences including party presentations.

WP33 (Project Management) was responsible for the effective organization of the project and covered all relevant management components. Some of the main achievements so far have been: the organization of meetings (e.g. Kick-Off and GA Meeting), the implementation

of monthly EB Telcos, monitoring of the work plan (Quarterly Management Reporting), supporting partners in everyday issues (handling day2day requests), etc.

Expected final results and their potential impact and use

Secure computation and secure computation services for the cloud have a potential of being a disruptive technology that will change the economics of technology development and deployment. The ability to provide cryptographic and more general secure computation services in the cloud, combined with the tools and applications that are adapted for using this secure computation framework, can bring forth new economic and technological opportunities for Europe, and new efficiencies from which multiple sectors of industry in Europe will benefit. A few improvements that could follow the development and deployment of PRACTICE technologies are listed below.

- **Harmonization** of regulatory, organizational, and user **requirements** for data access will become possible because of the unifying and verifiable framework that is provided as a set of security services. Such requirements will also be easier to formulate because it will not be necessary to adapt them to each application and each environment. Harmonized requirements greatly improve the economics of providing services.
- Organizations will have **access to** much **more information** about their business environment than ever before and will be able to make **better decisions** to drive their work forward. This will be possible without violating anyone's privacy.
- Secure computation services can increase the **openness in society**, by encouraging the **fair exchange of information** and enforcing fundamental rules of security and privacy in distributed environments under the control of multiple unconnected providers.

The PRACTICE Consortium

The PRACTICE consortium is well-positioned to achieve its objectives by bringing together a team of leading industrial and research companies, a research-oriented SME as well as well respected European universities. These 18 project partners from 11 different countries form a complete chain stretching from basic research and service design, via applied research, up to end-user oriented service providers.

Figure 2: The PRACTICE Consortium

PRACTICE Disclaimer

All public information will be marked with the following PRACTICE project disclaimer: *"The PRACTICE project has received funding from the European Union's Seventh Framework Programme (FP7/2007-2013) under grant agreement number ICT-609611."*