WITDOM: 1 year later

The WITDOM project (*empoWering prIvacy and securiTy in non-trusteD envirOnMents*) started officially on January 1st 2015 (M01). After 12 months of intense collaboration, the WITDOM consortium is proud to say that we are now a step closer towards achieving the project objectives. We look back and review the progress achieved since the beginning of the project.

1.1 *Summary of the context and overall objectives of the project.*

The advent of outsourced and distributed processing environments like cloud prompts fundamental transformations in whole ICT ecosystems, while bringing new opportunities to stakeholders in the availability and rational use of physical resources with large-scale savings in IT investments. Conversely, it also poses new security challenges especially for ensuring robust protection of privacy and integrity of personal information, which are a fundamental part of the societal acceptance of new ICT schemes, services and solutions.

In this context, the WITDOM project focuses on developing innovative solutions for truly efficient and practical privacy enhancing techniques and efficient signal and data processing in the encrypted domain for the increasingly demanded outsourced environments. Actually, the main target WITDOM pursues is to produce a framework for end-to-end protection of data in untrusted and fast evolving ICT-based environments, with a particular focus in data-outsourcing scenarios, where new threats, vulnerabilities and risks due to new uses require end-to-end security solutions that will withstand progress for the lifetime of applications they support.

This framework will be instantiated and validated in two realistic application scenarios:

- A health scenario (eHealth) based on genetic data sharing for large research data analyses and individual outsourced clinical analyses;
- A financial services scenario (FS) based on the management of both customers' data and finance data of contracts as well as providing outsourced secure financial services over private and public Cloud instances.

This framework shall use security-and-privacy-by-design (SPbD) methodologies, and advance the state of the art (SoTA) in effective protection of personal & sensitive data in the following areas:

- Privacy enhancing techniques, perturbation mechanisms and privacy metrics
- Cryptographic privacy techniques supporting encrypted processing
- Cryptographic techniques for integrity and verifiability of outsourced processes
- European legal landscape.

The WITDOM project is a Research and Innovation Action funded by the European Commision's Horizon 2020 programme and the Swiss State Secretariat for Education, Research and Innovation. This project, started in January 2015, joins together a multidisciplinary consortium comprising Universities, research centres, strong industrial stakeholders, and end-users: Atos(Spain) as the project coordinator, the University of Vigo (Spain) as the technical coordinator, Katholieke Universiteit of Leuven (Belgium), IBM Research (Switzerland), Fondazione Centro San Raffaele (Italy), BBVA (Spain), Gradiant (Spain), and the Ospedale San Raffaele (Italy).

1.2 *Project work performed from January 2015 to December 2015.*

The period covered by this management report lasts from the project start on January 1st of 2015 to 31st of December 2015, which spans from M01-M12 according to the project plan.

During this reporting period, the activities performed can be structured along the following lines of work:

- **Launching the project and setting up the different procedures** (quality, reporting, risk management, document/output storage and management, deliverable quality review, etc.), **management structure, guidelines and collaborative tools** to enable a seamless and fruitful teamwork among the consortium partners, in order to achieve the project objectives and develop the work promised in the DoA according to the schedule. This has been described in the confidential deliverables D1.1 - "WITDOM Internal website", released in M01, D1.2 - "WITDOM Internal Website and Communication Infrastructure", released in M03, D1.3 - "Quality Plan", released in M3, and D1.4 - "First Work Plan", released in M1. Updates for the second year, D1.5 - "Second Quality Plan" and D1.6 - "Second Work plan" were released in M12.
- **Clear understanding and characterization of the two project scenarios, eHealth and Financial Services,** as well as of the functionalities to be implemented and supported by the systems that will be deployed within WITDOM. The deliverable D2.1 – "Requirements analysis for un-trusted environments", released in M6, includes the description of a methodology called SPACE (Security and PrivAcy CodEsign) used for eliciting privacy and security requirements, an analysis of the two application scenarios in which the WITDOM platform will be instantiated in future stages of the project, a thorough review of the applicable security and privacy standards, a study of the scenario-specific cloud computing needs and a schematic list of the security and privacy high-level requirements for the application scenarios.

  D2.2 –"Functional analysis and use case identification", released in M12, states clearly which tasks have to be outsourced to untrusted domains, and the details of the kind of data involved. It will be exploited for the identification of suitable technological solutions for a secure and privacy-preserving outsourcing of the selected tasks.
- Analysis of the **application of the European legal framework on privacy enhancing technologies**, in particular the data protection and cybersecurity package. The deliverable D6.1 – "Legal and Ethical framework and privacy and security principles", released in M06, focuses on the extent to which data protection and cybersecurity legislation applies to the manipulation of (encrypted) personal data in untrusted environments such as the cloud, and the interaction between the basic stakeholders (data controller/processor/subject) in the context of processing personal data in these new environments.

  This deliverable also assesses ethical guidelines to support stakeholders in the advancement of central human values such as freedom, security and justice. The interaction between law, which provides formal regulatory settings, and ethical guidelines, which provide normative recourses for the interpretation of the law, is an important consideration.

  The definition of the specific legal privacy and security requirements that need to be taken into account for the development of the eHealth and Financial Services scenarios was also started during the considered period. D6.2 – "Legal requirements on privacy, data protection and security in WITDOM scenarios" is under production and will be released in M14.

- Discussions on the **formal technological security, privacy and verifiability requirements** of WITDOM platform and scenarios, taking into account the connection with user-centric requirements and European privacy and data protection legislation. These discussions are presented in the deliverable D3.1 – "WITDOM formalized technological requirements", released in M12. The requirements for the WITDOM platform and project scenarios are classified into three categories (core research requirements, demo requirements and production requirements), according to the advance in SoTA that they convey in WITDOM.

  Furthermore, the presented trust models analyzed for these scenarios identify the trusted and untrusted parties based on the definition of actors and their feared events, and determine which particular data has to be protected and from whom. The main untrusted element for these models is the Infrastructure Provider, from which WITDOM protects all the outsourced data. Additionally, the limitations for currently existing deployments are identified, identifying the most promising research approaches followed in WITDOM for addressing verifiability, security and privacy protection of outsourced process in outsourced environments.

  Finally the document presents a selection of privacy metrics that will be later on aligned to the requirements and embedded into the final privacy framework and assessment methodology. These metrics comprise information-theoretic metrics, distortion-based metrics, anonymity sets, and differential privacy, together with some scenario-specific metrics.
- **Analysis of the state-of-the art** in homomorphic encryption, secure processing, privacy enhancing techniques and integrity and consistency mechanisms. D3.3 – "WITDOM Intermediate internal cryptographic toolset", released in M12, highlights the **research challenges** posed in WITDOM for these research areas and **the main strategies** to achieve the targets of secure and privacy-preserving processing of sensitive data in outsourced untrusted environments.
- Outline a **first draft of the architectural model for the WITDOM framework** for processing data in untrusted environments (i.e: cloud), released in M12 in the deliverable D4.1 – "Preliminary specification of an end-to-end secure architecture". The architecture uses the paradigm of service orientation (and represents a service-oriented architecture, SOA), isolating the applications from the particular implementations and locations of its elements. The architecture organizes multiple components together in a comprehensive framework, providing the following protection functions:
  - Anonymization;
  - Secure signal processing;
  - Secure computation;
  - Integrity and consistency verification;
  - Data masking and desensitisation;
  - End-to-end encryption.
- Define a common **project strategy for dissemination and communication** of project advances and results, to set the base-line for individual partner's activities, in order to reach the maximum impact possible. The strategy is accompanied with a plan that establishes a series of activities to promote the project along its entire duration, as well as a complete set of graphical material that supports these activities. The graphical material entails:
  - The project branding, including a logo, colour code, templates for documents, a poster and a promotional brochure.

- A project website (www.witdom.eu) publicly accessible online since M2, as the main point of contact from externals and first means for dissemination and communication of project advances and regular achievements. The website constitutes a deliverable and is described in the accompanying document D7.1 – "Public Web Presence".
- Social media: dedicated LinkedIn group, twitter and SlideShare account.
- Press releases and campaigns, to promote the project official start and, among other events, the networking session on October 22nd at the ICT 2015 Innovate, Connect, Transform event (Lisbon, Portugal), co-organised by WITDOM in cooperation with the related H2020 projects TREDISEC and PRISMACLOUD, and where WITDOM introduced privacy challenges in the cloud and how to overcome them.

The communication and dissemination activities are grouped into four phases (Awareness, Understanding, Adoption and post-project), each one focusing on the promotion of certain aspects of the project, with customized key messages, and targeting different type of audience making use of the most appropriate channel in each case. The dissemination and communication strategy and the associated implementation plans have been defined in the deliverable documents D7.2 – "Dissemination plan", released in M6. The enforcement of these plans are reported in the deliverables D7.3 – "First dissemination Report& Material" and D7.12 – "First communication Activities Report" respectively, both released by M12.

- Set-up an **external Project Advisory Board** expected to provide WITDOM with expert advice in key relevant areas from the project such as the legal aspects and the under development research lines. D7.5 – "Report of first Advisory Board Workshop", released in M12, summarizes the initial feedback provided by this group.

1.3 *Progress beyond the state of the art and expected potential impact.*

The innovations sought in this area are three-fold: the first dimension focuses on a novel framework for a quantitative evaluation of end-to-end security and privacy, aiming at guaranteeing efficient and verifiable provision of privacy in the context of ICT services owned by third-party providers of distributed processing and storage, thereby maximizing independence from stated security and privacy commitments by respective providers, and minimizing the current need of *blind trust* from the clients, solely based on written consents. The initial contribution of this framework builds upon a requirements elicitation methodology, synergizing the results of the recently ended FP7 project PRIPARE with a co-design process to fuse privacy into the first stages of the systems design process, materializing a true Privacy-by-Design methodology.

The second dimension of innovations deals with the actual design and development of tools and technologies for efficient privacy protection of data outsourced and processed in untrusted environments. These techniques can be categorized in the four main research areas addressed in WITDOM: efficient lattice cryptosystems for homomorphic processing, allowing for faster and more resource-efficient encrypted-domain processing; accurate and effective secure signal processing to cope with the marriage between cryptography and the ubiquitous signal processing operations when dealing with sensitive signals; efficient Privacy-Enhancing Technologies for obfuscation, noise addition, anonymization and data masking, measuring and achieving quantitative guarantees for unidentifiability of the processed data and unlinkability of the produced results; and last, but not least, efficient and scalable integrity and consistency verification techniques to preserve fork-linearizability on data accessed and modified by several users on outsourced data stores. The main strength resides in that the innovations in these areas are not applied independently or autonomously, but adequately and effectively composed and in an end-to-end secure and private architecture that

defines a platform able to deploy privacy-preserving services on outsourced data with quantifiable and assessable technological guarantees. Promising initial results have already been produced within WITDOM's roadmap, which will continue to advance the state of the art in these fields during the upcoming two years.

Finally, the third dimension of WITDOM's innovations deals with the instantiation of the developed framework, platform and tools in two carefully chosen use-case scenarios, whose impact and sensitivity of the involved data make privacy a must, and where privacy and confidentiality constraints are a true barrier for profiting from the benefits of outsourced architectures and Cloud-based deployments. The first use-case scenario is a health scenario based on outsourcing genetic data processes and workflows for large research analyses and individual clinical analyses; genetic data is extremely sensitive, and genomic privacy has become a hot topic for research and innovation, to which WITDOM contributes by focusing on solutions for outsourced processing of genetic data. The second scenario deals with outsourced financial analyses based on the management of both customers' data and finance data, to enable risk calculations and fraud detection deployed as outsourced secure financial services over private and public Cloud instances.

Moreover, research and Innovation in this field cannot ignore the fundamental impact of the data protection regulations and directives on the evolution of Cloud-related environments and in the processing of personal and sensitive data. Therefore, a key aspect of WITDOM innovations is built upon a legal assessment and validation of the evolving European Data Protection Regulation, linking legal and ethical requirements with technological means to guarantee their enforcement.