Concertation Report
Data Protection, Security and Privacy (DPSP)

Think Cloud Services for Government, Business & Research

www.cloudwatchhub.eu|info@cloudwatchhub.eu |@cloudwatchhub

1 Identifying topics for the Horizon 2020 ICT Work Programme 2018 – 2020

Chaired by Francisco Medeiros, Deputy Head of Unit E2 Software, Services, Cloud computing

Presentation

Concertation meetings have been key in shaping Work Programmes for the European Commission. The CloudWATCH concertation meeting in September 2014 saw participants recommend themes for the LEIT 2016-2017 Programme. From this, two calls were closed just days before the 2016 Concertation meeting: ICT-06-2016: Cloud Computing, and ICT-10-2016: Software Technologies. Both were heavily subscribed and it is expected that over 20 new projects will be funded and commence later in 2016, including international cooperation projects.

The European Commission has initiated the preparation of the 2018-2020 Work Programme (WP) with a scoping paper to be prepared in summer 2016 with discussions with member states taking place between July and October 2016. Public consultation may occur in Q3 of 2016 while the WP will be drafted between November 2016 to June 2017. The WP is likely be adopted in 4Q 2017.

The four EC themed clusters announced at the 2015 Concertation meeting have a key role in supporting this process by providing white papers which include a set of recommendations for research challenges to be addressed by the 2018-2020 WP. These were presented and are outlined in the following sections.

1.1 Data Protection, Security and Privacy (DPSP)

Erkuden Rios Velasco, Tecnalia & Cluster Chair

[Cluster website](#) **|** [Cluster white paper](#) **|** [Presentation](#)

The DPSP Cluster deals with hot topics in Cloud research and innovation: Data Protection, Security and Privacy, which are closely related to each other. The Cluster aims at increasing the impact of the integrating projects by identifying synergies and collaboration opportunities, exchanging knowledge and carrying out technical discussions to ensure the projects advance over the state of the art and provide value added solutions to the market. The innovation in cloud security and privacy go hand in hand with the advances in cloud technologies and services themselves. The Cluster gathers 25 EU-funded research projects that work on trust and security of cloud services. We believe that by working together, the projects can make a greater difference in EU cloud security solutions.

Cluster members

APPHUB, A4CLOUD, CLARUS, CLIPS, CLOUDWATCH2, COCO CLOUD, CREDENTIAL, ESCUDO-CLOUD, MUSA, OPERANDO, PAASWORD, PRISMACLOUD, SECCORD, SERECA, SLALOM, SLA-READY, SPECS, STRATEGIC, SUNFISH, SWITCH, TREDISEC, TRESCCA, WITDOM.

The Free Flow of Data initiative within the Digital Single Market poses new challenges with regards to data ownership, data location, data access and privacy, to name a few. The cluster members are currently discussing the importance of advanced security and data protection mechanisms to make the initiative a reality. The identification of challenges towards the next H2020 WP 2018-2019 made by the Cluster include a classification of the challenges according to the main working areas of the Free Flow of Data: Free movement of data, Location of data, Ownership, Interoperability, Usability, Access to (Public) Data, Certification, Contracts and Switch of CSPs.

In the Action by Cluster, the projects that have identified the challenge or are already working on it have been identified[1] as outlined in the tables below.

---

[1] https://eucloudclusters.files.wordpress.com/2015/05/dpspcluster-whitepaper-v3-1.pdf

Table 1 Overview of current challenges identified by the DPSP cluster so far.

Challenge	Description	Projects addressing issue
Full control of data flow	Control of whole flow including data in transit and data in use, but also data at rest, meaning controlled access and usage of data across country and cloud boundaries. Context based access control policies are part of this challenge.	COCO CLOUD, ESCUDO-CLOUD.
Efficient searchable encryption	For enabling to efficiently search and edit the encrypted data stored and processed in the cloud.	PAASWORD
Privacy preserving cloud-based (identity) services	Improved and novel cryptographic methods to securely protect, store and share (private) data, including encrypted identity data.	CREDENTIAL
Fully secure APIs	In order to enable to securely communicate the identity and user attributes (authentication and authorization) among cloud services.	PAASWORD
Data Protection legal framework transparency.	For both cloud consumers and cloud providers.	CLARUS, CLOUDWATCH2
Definition and enactment of fine-grained security policies.	Integration and composition of security and privacy policies across different cloud services.	STRATEGIC
Security-aware SLA management support for security and privacy terms formalisation, negotiation, composition, monitoring, continuous assurance and automation.	All these applied to multi-cloud or federated cloud-based applications and cloud-services themselves.	MUSA, SPECS, SLA-READY, SWITCH
Risk assessment frameworks for applications at scale	Innovative frameworks to assess risk in multi-technology and distributed applications mixing cloud, IoT, Big Data, or mobile addressing security assurance, automated deployment, monitoring and decision making.,...	MUSA
Secure dynamic composition of cloud services	Including dynamic benchmarking and brokering of Cloud services for multi-cloud scenarios as well as federation of clouds.	PRISMACLOUD
Cloud Security Certification.	Based on cloud security standards and auditing schemes.	CLOUDWATCH2
Security- and privacy-by-design in cloud services.	Advanced mechanisms and tools to support the security and privacy intelligence from the early stages of the design of the services.	PRISMACLOUD, CLARUS
Continuous control of security, privacy conditions and obligations, and adherence to them	Including continuous monitoring, assurance, enforcement, and automated reaction in inter-clouds, multi-cloud, federated clouds.	COCO CLOUD, SUNFISH , MUSA, ESCUDO-CLOUD.
Efficient secure and privacy-preserving multi-tenancy in Infrastructure, Platform and Software as a service models.	Including deduplication on encrypted multi-tenant data, or mechanism for checking integrity and availability of multi-tenant data.	TREDISEC
Improve market readiness of security and privacy solutions from projects.	Providing an online marketplace that enables the digital single market to access innovative open source applications with guidance on sustainability and future project exploitation.	APPHUB, CLOUDWATCH2

Table 2 Identified topics & recommendations

Topic	Description	Recommendation and benefit to future cloud market
There is a need of fully understanding the technical implications of the Free Flow of Data initiative with respect to cloud security, privacy and protection of data.	The European Commission is currently working on a Legislative Proposal on Free Flow of Data (due in Nov 2016) which would mean a change in cloud context towards the realisation of the Digital Single Market vision.	Elaboration of a Whitepaper to discuss in deep the technical problems and possible solutions towards the completion of the Free Flow of Data Initiative, which will serve to clarify which are the current results in the projects that are already (partially) supporting some of the solutions.
There is a need for specialised discussions to provide value added innovation on cloud security and privacy.	As cloud security, data protection and privacy are very much related to each other, the cluster grouped the challenges identified in order to organise the discussions with the aim to better understand the implications and propose solutions.	Creation of working groups within the cluster for allowing specialised discussions on the technical issues: Security and privacy-by-design, Trust & Interoperability (Chaired by CloudWATCH2), and Advanced data protection mechanisms.
There is a need for improving market readiness and usability of security and privacy solutions from projects.	The European Cloud Economy needs the cloud R&I space include standards, transparent pricing and better uptake of new services. The clustered projects need to think strategically, looking at technology and business model as part of the same equation. While challenging, interoperable cloud services play a very important role in extending the market and in bringing business benefits to both the supply and demand sides.	Strongly collaborate with DG-CNECT Cloud CSAs like APPHUB and CLOUDWATCH2 to support the Cluster achieving in its mission of increasing the market impact of the projects' technological results.
There is a need to improve accessibility and communication with the wider market.	The deliverables and outcomes of projects across clusters must be communicated effectively in order to engage with industry stakeholders and identify areas of future collaboration.	An online directory of projects that uses simpler language to describe what a project does, which stakeholder it is relevant for and the correct process for engaging with a project on the projects' terms.

Conclusion and actions for the DPSP Cluster

In 2015 the Cluster set the basis for a fruitful collaboration among the clustered projects towards increasing their impact. Following this, in 2016 the Cluster started the work for joint results and dissemination activities.

Among other results, two major deliverables have been produced so far: a) the Map of synergies between the clustered projects, which identifies the commonalities and gaps in research topics and approaches of the projects[2] and b) the Whitepaper on data protection, security and privacy challenges of multi-cloud applications in the Digital Single Market[3]. In this Whitepaper the need of further research on cloud technologies' security was identified, particularly towards the full completion of the DSM Initiative #14: Free flow of data. For example, the need of extending the research on: security- and privacy-by-design in cloud, full control of data flow, efficient searchable encryption, fully secure APIs, Security-aware SLA management support, Definition and enactment of fine-grained security policies, Continuous control of security and privacy conditions and obligations and adherence to them, Efficient secure and privacy-preserving multi-tenancy in Infrastructure, Platform and Software as a Service models and Cloud Security Certification.

The evolution of the collaborative actions in the near future will lead to the elaboration of a second Whitepaper, this time focused on the future technological solutions needed for the Free Flow of Data initiative, and identification of the pieces of work already available in the projects that have initiated the path towards such solutions.

Other joint dissemination actions are also taking place. For example, the Cluster is working on its active participation in Cloud Forward 2016 where the member projects intend to take profit of not only the research work presentation tracks but also of the SME event where the projects would make direct contact with potential stakeholders of their solutions.

All the information about the Cluster results and planned activities can be found at the cluster webpages[4].

---

[2] https://eucloudclusters.files.wordpress.com/2015/05/dpsp_cluster_map-of-synergies_v2-0.pdf
[3] https://eucloudclusters.files.wordpress.com/2015/05/dpspcluster-whitepaper-v3-1.pdf
[44] https://euclouddusters.wordpress.com/data-protection-security-and-privacy-in-the-cloud/