Challenges for trustworthy (multi-)Cloud-based services in the Digital Single Market

Version: 28 January 2016

Authors:
Aljosa Pasic, ATOS, COCO CLOUD project.
Beatriz Gallego, ATOS, TREDISEC project.
Bernd Zwattendorfer, Graz University of Technology, CREDENTIAL project.
Bojan Suzic, TU Graz, SUNFISH project.
Elsa Prieto, ATOS, WITDOM project.
Erkuden Rios, Fundación Tecnalia Research & Innovation, MUSA project and DPSP Cluster coordinator.
Julia Vuong, CAS Software AG, PaaSword project.
Massimiliano Rak, Second University of Naples/CeRICT, SPECS project.
Nicholas Ferguson, TRUST-IT SERVICES LTD, CLOUDWATCH2 project.
Nuria Rodríguez, ATOS, STRATEGIC project.
Peter H. Deussen, Fraunhofer Institute for Open Communication Systems, AppHub project.
Pierangela Samarati, Università degli Studi di Milano, ESCUDO-CLOUD project.
Roberto Cascella, Trust-IT Services, CLARUS and SLA-Ready projects.
Sabrina de Capitani, Universitá delgi Studi di Milano, ESCUDO-CLOUD project.
Simone Braun, CAS Software AG, PaaSword project.
Stephan Krenn, AIT Austrian Institute of Technology GmbH, CREDENTIAL project.
Stephanie Parker, Trust-IT Services, SLA-Ready project.
Thomas Länger, Université Lausanne, PRISMACLOUD project.
Thomas Lorünser, AIT Austrian Institute of Technology, PRISMACLOUD project.
Zhiming Zhao, University of Amsterdam, SWITCH project.

Abstract: The future Digital Single Market (DSM) poses a number of research challenges for future years. Particularly, the DSM Initiative #14 on "Free flow of data" directly impacts on a number of security and privacy issues on (multi-)cloud-based services and cloud services. The objective of this White paper is to develop an initial map of challenges identified by the DPSP Cluster projects related to the DSM Initiative #14 topics at the right level of abstraction that could be reused by the EC and policy makers. The map includes collection of the challenges more relevant for the next Horizon 2020 Work Programme 2018-2020.

Keywords: Cloud computing, data protection, security, privacy, Digital Single Market, DSM.

1. Introduction

This White paper collects the future research challenges identified by the Cluster of EU-funded research projects working on the areas of data protection, security and privacy in the Cloud (DPSP Cluster) launched in April 2015 by DG-CNECT of European Commission.

The cluster and the projects within are described in the cluster's website[1].
The research challenges were identified as research gaps towards the full completion of the Initiative #14: *Initiatives on data ownership, free flow of data (e.g. between cloud providers) and on a European Cloud* of the Digital Single Market[2] initiative by the European Commission.
Particularly, the work focuses on the challenges related to those areas of research addressed by the clustered projects, namely security, privacy and data protection in (multi-)cloud-based applications and services or cloud services themselves.
The timeframe of the challenges identified spans short term (2016-2017), mid term (2018-2020) and long term (beyond 2020). The mid term and beyond challenges are those more relevant for the future Horizon 2020 (H2020) Work Programme 2018-2020 that the European Commission is starting.

In the following, we first provide in Section 2 a short description of the objectives of the Digital Single Market Initiative #14, in order to better understand the context of the challenge identification work. In Section 3 we describe the methodology followed for identifying the challenges and in Section 4 we contextualise the challenges that are collected in Section 5.
In Section 6 we map the identified challenges with main topics addressed by the DSM Initiative #14. And in Section 7 we summarize those challenges identified for the mid term (2018-2020) which are of most importance at the time of writing as they should be the ones addressed by the next H2020 Work Programme. Finally, the Section 8 concludes the whitepaper.

2. The Digital Single Market Initiative #14

The Digital Single Market (DSM)[3] is the Pilar I of the Europe 2020 Strategy[4]. The DSM strategy *aims to open up digital opportunities for people and business and enhance Europe's position as a world leader in the digital economy*[5].
The Initiative #14 addresses the following actions by the Commission, as it is summarized in the DSM document:
The Commission will propose in 2016 a European 'Free flow of data' initiative that tackles restrictions on the free movement of data for reasons other than the protection of personal data within the EU and unjustified restrictions on the location of data for storage or processing purposes. It will address the emerging issues of ownership, interoperability, usability and access to data in situations such as business-to-business, business to consumer, machine generated and machine-to-machine data. It will encourage access to public data to help drive innovation. The Commission will launch a European Cloud initiative including cloud services certification, contracts, switching of cloud services providers and a research open science cloud.

Note that we have underlined the main topics addressed by the Initiative #14 to which the challenges identified in this document will be related when describing them in Section 5. And these topics will be used in Section 6 to group the challenges identified.

[1] https://eucloudclusters.wordpress.com/data-protection-security-and-privacy-in-the-cloud/
[22] http://ec.europa.eu/priorities/digital-single-market/docs/dsm-communication_en.pdf, Section 4.1
[3] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN
[4] http://ec.europa.eu/priorities/digital-single-market_en
[5] https://ec.europa.eu/digital-agenda/en/digital-single-market

Note also that the DSM is going under a public consultation process aimed *at gathering views and opinions on the restrictions faced by users, consumers and businesses when they access or provide information, shop or sell across borders in the European Union*[6], and it is expected that the results of the consultation are soon made publicly available. The results of this consultation may complement the challenges identified in the present white paper as they collect the points of view from consumers, businesses, national authorities at all levels and interested organisations about major restrictions and issues for cross-EU services and data.

3. Methodology

The methodology applied in this White paper is a bottom-up analysis of technological achievements and conclusions from the DPSP Cluster projects trying to identify possible technology enablers of Digital Single Market (DSM) Initiative #14. In other words we tried to map research issues and gaps coming from research projects on what is feasible or will be feasible in the near future, with policy analysis that focuses on what is desirable or what is expected in the near future.

The analysis of DSM Initiative #14 policy started at the highest level of abstraction, namely identifying the main DSM Initiative #14 topics where the potential of technological breakthroughs from EU research projects could have impact e.g. as "policy enablers" or "policy support". Then these topics were discussed among the authors that tried to identify main issues and challenges related to security, privacy and data protection for (multi-)cloud-based and cloud computing services. It is important to notice that public consultation is still ongoing[7] , but some issues (e.g. privacy, certification, etc.) can already be pinpoint as the key issues.

For this bottom-up approach, the 23 projects in the DPSP Cluster were asked to present the technical issues and challenges they identified linked to their research work and possibly linked to the DSM Initiative #14. A total of 16 projects provided their input and overall 47 challenges were identified.

These technical issues are sometimes not expressed in the "market" language, but topics such as "homomorphic encryption", "machine readable policy" or "automated enforcement", need to be expressed and linked, at some point, to DSM Initiative #14 topics of interest. The central contribution of this joint white paper, therefore, is to map clustered projects' contributions and challenges to the DSM Initiative #14 topics at the right level of abstraction that could be reused by the EC and policy makers. The final map is shown in Section 6.

[6] https://ec.europa.eu/digital-agenda/en/news/public-consultation-geo-blocking-and-other-geographically-based-restrictions-when-shopping-and

[7] http://ec.europa.eu/digital-agenda/en/news/public-consultation-regulatory-environment-platforms-online-intermediaries-data-and-cloud

4. Context of the challenges

As explained before, the research challenges were first identified by individual projects and afterwards an analysis was done in order to consolidate and classify them into comprehensive categories according to the topics of DSM Initiative #14.

For the purpose of this White paper, clustered projects were asked to individually express the challenges identified in the context and scope of the project work and results. The projects were inspired on the DSM Initiative #14 while they were asked to be open minded to propose new ideas, even if they did not fit exactly with Initiative #14 topics.
The challenges should be on the areas of work of the clustered projects and they may be technical, business, policy related, etc.

The cluster of EU-funded research projects is named DPSP, data protection, security and privacy in the Cloud which are the focus working areas. Therefore, before going into the description of the challenges, we will briefly explain the terms “security”, “privacy” and “data protection”, as seen from different perspectives.
At the highest level of abstraction **security** challenges are decomposed into confidentiality, integrity, availability and access control challenges.
The term **data protection** is used to describe many things. The recent cloud computing based market segment called “DPaaS” (Data Protection as a Service), for example, is mainly grouping cloud-based operational backup of data and disaster recovery/business continuity (BC/DR) type of solutions. Another problem is that terms *data protection* and *information protection* (or even *information security*) are sometimes used interchangeably.
Similar confusion occurs with **privacy**, which only applies to a specific type of data, namely “personal data”, which is defined in EU Directive 95/46/EC[8]. In this directive, however, data is linked to information[9]. In the proposed EU General Data Protection Regulation, this link goes even further by referring to any information that can be used, directly or indirectly, “by means reasonably likely to be used by the controller or by any other natural or legal person". It is also worth to mention the term *personal identifiable information* (PII), which is sometimes used in Europe, although it actually comes from US legislation.
Data encryption, for example, could be used to protect data at rest or data in transit (data in motion), although some argue (e.g. Bruce Schneier) that using encryption for data at rest is like using it for “communication with future itself”. With the emerging importance of real time communication (e.g. in Internet of Things connected to cloud and Big Data stream processing capabilities), it also becomes obvious that **storage encryption keys** and **real time communication keys** pose two totally different types of challenges.
Data federation or data replication, is another technique to protect data at rest that can be directly linked to DSM challenges and issues such as retaining personal citizen information, location of cloud storage, etc.

[8] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

[9] Article 2a: *'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.*

Data in use is another part of lifecycle protection management and **full memory encryption** is one of the areas to be addressed. It links directly to both confidentiality and integrity challenges, not only for data, but also for software. More recent approaches from "**trusted computing**" research area include use of sandboxes or enclaves, as well as several cryptographic tools, including secure multi-party computation and homomorphic encryption.

In the following Section 5 we describe the challenges collected from the clustered projects. The descriptions follow this format:

- Short name: Short name that summarises the challenge description
- Description: Short description of the challenge.
- Timeframe: Proposed timeframe when the challenge should be tackled by the EU policy makers. There are three possibilities: 2016-2017/2018-2020/beyond
- Project works on it: Whether the project that identified the challenge has already initiated the research on it, or aspects related to it. Yes/No
- Topics of the DSM Initiative #14: Topics of work addressed by the Initiative #14 to which the challenge is related.
- Importance to DSM Initiative #14: Level of importance of the challenge with respect to DSM Initiative #14 objectives. There are three possibilities: high/medium/low importance.
- Risk of not filling the gap: Short description of major risk(s) faced if the challenge is not addressed in the future.

5. Challenges identified by projects

a. AppHub

Challenge 1:

- Short name: **Improve market readiness of security and privacy solutions**
- Description: The majority of EC funded collaborative projects acting in the IT domain produce software under an open source license. For security and privacy solutions, transparency of algorithms and code is a key factor for the validation by a broad community of researchers and users. However, in many cases software developed by those projects fail to deliver sufficient quality and majority to be applicable in a market environment; hence, advantages of open source based software development cannot manifest themselves due to the lack of a community of contributors, evaluators, and users.
- Timeframe: 2018-2020
- Project works on it: Yes
- Topics of the DSM Initiative #14: Usability (usability of security), Access to public data, Research open science cloud (first step to this).
- Importance to DSM Initiative #14: high
- Risk of not filling the gap: Solutions developed in collaborative projects will fail to impact the European market.

b. CLARUS

Challenge 1:

- Short name: **Making the cloud ecosystem secure for outsourced data**
- Description: Current security mechanisms are commonly located within the cloud platform, hence compelling customers trust cloud providers for the way they manage their data. This leaves the cloud as an impractical solution for those customers that value the sensitivity of their data as critical or should comply with specific regulations that force them to treat data with special precautions, reaching higher importance when dealing with business and user sensitive data. Thus, to reach its full potential, cloud computing needs solid security mechanisms that enhance trust in cloud computing by allowing cloud customers greater control on the security and privacy of their data.

  When it comes to outsourcing sensitive data, security and privacy challenges are intertwined around data protection. Regarding security, users want to be assured that no intruder can hack the cloud and/or impersonate them, and that no denial of service will occur.

  To enhance security, CLARUS will also develop an attack-tolerant framework, so that potential security breaches within the cloud can be dynamically detected and appropriate mitigation measures can be activated on-line.
- Timeframe: 2018-2020.
- Project works on it: Yes
- Topics of the DSM Initiative #14: Free movement of data, Access to data.
- Importance to DSM Initiative #14: high
- Risk of not filling the gap: If the challenge is not addressed, cloud potentials could be hindered because of the lack of trust in outsourcing data to third parties. Cloud infrastructures will remain unsecure, with limited or no control of the customers over their data and exposure to practical attacks and malicious users.

Challenge 2:

- Short name: **Privacy-enabling mechanisms to protect sensitive data**
- Description: Regarding privacy, the user wants the guarantee that no one other than herself will be able to see or infer her sensitive data. Notice that privacy is even more challenging than security, because it must hold also with respect to the CSP. If the user wants to use not only the cloud storage but also the cloud computational power, then the challenge is even harder.

  To enhance privacy, CLARUS will implement a set of privacy-enabling mechanisms to ensure that the user's sensitive data are properly protected before they are outsourced to the cloud. Protection will be provided in a way that cloud service functionalities are still preserved, even those that require performing operations (e.g., queries, transformations, calculations) on the protected data. To achieve that, CLARUS draws on and innovates over the current state of the art on functionality-preserving cryptographic (e.g., (partially) homomorphic encryption, searchable encryption, etc.) and non-cryptographic data protection techniques (e.g., data anonymization, document redaction, data splitting and merging, private information retrieval, etc.), with a special focus on preserving the benefits associated with cloud services (functionality, cost-effectiveness, efficiency, etc.).
- Timeframe: 2018-2020 and beyond.
- Project works on it: Yes
- Topics of the DSM Initiative #14: Free movement of data, Ownership, Location of data.
- Importance to DSM Initiative #14: high

- Risk of not filling the gap: If privacy mechanisms are not provided and properly implemented, customers cannot entrust the data to CSPs. Thus, the cloud will not be considered a viable solution for businesses and public organizations that either value high their data or need to abide to specific legislations, such as the health care sector.

Challenge 3:

- Short name: **Data protection and legal jurisdiction**
- Description: One might argue that sensitive data handling in the cloud would be much simpler if the CSP could be assumed to be trusted. However, there are several legal issues here. On the one hand, in many scenarios the data subjects entrust the data controller with their personal data (e.g. healthcare data), but this does not mean they allow the controller to further transfer their data to whoever the controller chooses to trust. On the other hand, the CSP may be under a jurisdiction different from the controller's one. If, say, the CSP is under U.S. law whereas controller and subjects are under E.U. law, the latter law may be violated (for example, in case the personal data of European citizens ends up in the hands of U.S. government agencies).
  To enhance trust, CLARUS will also implement a set of auditing services, so that users can directly supervise how data are being protected and outsourced to the cloud.
- Timeframe: 2018-2020 and beyond.
- Project works on it: Yes
- Topics of the DSM Initiative #14: Free movement of data, Location of data, Ownership, Contracts.
- Importance to DSM Initiative #14: high
- Risk of not filling the gap: CSPs and organisations using cloud services need to comply with the legislation and case law for the protection of data. If the impact of certain legislations is not properly understood by stakeholders, trust, safety, privacy and confidence in cloud computing services cannot be achieved.

Challenge 4:

- Short name: **Interoperability-by-design to overcome mistrust in cloud computing by implementing standardized cloud services**
- Description: Vendor lock-in is a challenge when customers need to exploit the capabilities of different CSPs at the same time or do not want to bind their business to a single CSP for resiliency. For instance, they can rely their data on multiple providers at the same time with potentially different level of confidence, e.g. storing encrypted sensitive data or splitting anonymised data across providers in such a way that the privacy of the user is still preserved. Hence, interoperability for data formats and interfaces of cloud services is the key to ensure compatibility between independent systems.
  Interoperability demands common technical APIs, protocols and data/message format, which can be achieved by following best practices and common guidelines or in its more general form, i.e., by design, adopting open or de-facto standards.
  CLARUS follows an interoperability by design approach by investigating the use of open standards in the architecture design and in the implementation of the CLARUS components. The objective is to implement standards supported by a wide range of Cloud Service Providers (CSPs) and end users, thereby ensuring interoperability in collaborative, standardised and transparent cloud environments. By means of standardisation, the function calls implemented in the interfaces can be made homogeneous for cloud providers that provide similar services (e.g. data storage), so that data interoperability can be achieved among otherwise heterogeneous cloud providers. On the other hand, standards will allow the support of data splitting (for security enhancement, like to meet privacy constraints), merging and replication (for

improved data integrity in front of potential CSPs' failures), thus facilitating the adoption of already available distributed backup solutions as such the integration of the CLARUS solution into the existing cloud infrastructure. Interoperability brings several benefits to CLARUS such as the possibility of implementing more robust security mechanisms and improving reliability and dependability, while increasing transparency and trust in cloud services.

- Timeframe: 2018-2020.
- Project works on it: Yes
- Topics of the DSM Initiative #14: Switch of CSPs, Free movement of data, Interoperability (security interoperability).
- Importance to DSM Initiative #14: high
- Risk of not filling the gap: Vendor lock-in and impossibility to exploit the services of multiple providers.

Challenge 5:

- Short name: **Data anonymisation and access to data**
- Description: Privacy of the data can be achieved with anonymisation by splitting data across cloud providers, thus not requiring encryption. CLARUS will research and adapt non-cryptographic data anonymisation methods for the cloud, turning them into efficient, feasible and utility/functionality preserving alternatives to full data encryption. Anomysation can be achieved by automatic identification of potentially sensitive parts of input documents or data (as done in document sanitisation research) and identification of parts of data that jointly may disclose sensitive data. The appropriate transformation of sensitive data (e.g. generalisation) can ensure the confidentiality while maintaining utility up to a certain level.
  The challenge here will be to develop mechanisms to automatically detect sensitive information and to define rules to obfuscate and automatically reconstruct sensitive data according to their type, structure and involved functionality.
- Timeframe: 2018-2020 and beyond.
- Project works on it: Yes
- Topics of the DSM Initiative #14: Access to data.
- Importance to DSM Initiative #14: high
- Risk of not filling the gap: Without data anonymisation is a valid alternative to data encryption when businesses deal with large quantity of data and require data privacy. This solution will enable a more efficient use of the processing resources.

c. CLOUDWATCH2

Challenge 1:

- Short name: **Improve market understanding and market readiness of services from EC funded projects**
- Description: For European industry and citizens to make the most of the digital economy we need to tackle the most challenging issues. In the cloud R&I space, these challenges include issues such as standards, transparent pricing and better uptake of new services. European Research and Innovation (R&I) projects need to think strategically, looking at technology and pricing 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. Results from projects need to have an impact on the market if they are to become truly sustainable.
  CloudWATCH2 will provide:

- A roadmap to transparent cloud pricing in Europe: The roadmap paints a clear picture of the current cloud landscape and considers the risk if providers do not prepare for potential regulation. This includes a set of calls for action for stakeholders including policy makers, cloud providers, etc.
- Mapping the EU cloud ecosystem of products, services and solutions emerging from EU R&I projects. This involves assessing market readiness of project outputs and providing best practices in mitigating risks associated with open source projects which can ultimately enable faster time-to-value and commercialisation.

- Timeframe: 2016-2017
- Project works on it: Yes
- Topics of the DSM Initiative #14: Research open science cloud.
- Importance to DSM Initiative #14: high
- Risk of not filling the gap: For European industry and citizens to make the most of the digital economy we need to tackle the most challenging issues. In the cloud R&I space, these challenges include issues such as standards, transparent pricing and better uptake of new services. European Research and Innovation (R&I) projects need to think strategically, looking at technology and pricing as part of the same equation. Without this outputs of EC-funded initiatives may not have the desired impact on the DSM. Results from projects need to have an impact on the market if they are to become truly sustainable.

Challenge 2:

- Short name: **Cloud Security Certification & Definition of Risk profiles**
- Description: CloudWATCH2 is currently working on providing a set of risk profiles specifically targeting the public sector. This will include collecting requirements from public sector organisations and identifying association of risks/threats with counter measures. Results will contribute to CloudforEurope work in this area. A set of risk profiles will also be defined specifically for small businesses. The profiles will suggest appropriate security measures associated with different levels of risk. In addition, the advanced security cloud standard profile formulated in CloudWATCH1 will be further refined. A Cloud Adoption Deep Dive workshop at Cloudscape 2016 will focus on cloud security and will examine in particular how projects are addressing security concerns with market requirements in mind.
- Timeframe: 2016-2017 and 2018-2020.
- Project works on it: Yes
- Topics of the DSM Initiative #14: Certification.
- Importance to DSM Initiative #14: high
- Risk of not filling the gap: Trust and security concerns around cloud computing will continue and adoption may not increase as rapidly as possible in these two sectors. Rational risk management practices are key to ensuring specific cases can be correctly understood and addressed. This is important for the public sector, which has needs related to their public interest function, and for European businesses, which need to become cloud leaders in the global market.

Challenge 3:

- Short name: **Data Protection legal framework transparency**
- Description: Legal jurisdiction is another area in which transparency is required and greater trust is demanded by end users. It is becoming increasingly important for CSPs to become more aware of consumer concerns and demonstrate their contractual and technical robustness in order to become more competitive in the global marketplace with its large-scale, multi-national players. CloudWATCH2 is delivering a set of user-

focussed legal recommendations and checklists in order to help companies and public authorities to better understand contractual and EU data protection legal framework. Recommendations should also be useful for cloud service providers in helping them understand user concerns.

- Timeframe: 2016-2017 and 2018-2020.
- Project works on it: Yes
- Topics of the DSM Initiative #14: Usability (usability of security), Contracts.
- Importance to DSM Initiative #14: high
- Risk of not filling the gap: This activity will contribute to making the cloud more transparent to potential adopters by addressing legal aspects, and providing a set of recommendations and checklists. These legal recommendations are also highly relevant for those Cloud Service Providers (CSPs) committed to improving their service offer in view of legal and compliance concerns.
    - Further development of cloud standard profiles for interoperability and security that can facilitate the realisation of an ecosystem of interoperable services for Europe.
    - Cloud interoperability testing in an international developer-oriented and hands-on environment. Findings will be transferred into guidance documents and standards.
    - Production of cloud risk profiles and legal guides to the cloud for private and public organisations to lower barriers and ensure a trusted European cloud market.

d. COCO CLOUD

Challenge 1:

- Short name: **Data flow control**
- Description: Before cloud the common data security approach was preventing data from escaping. With the advent of cloud, disclosure of data, including personal data, is inevitable so the focus should not be on flow prevention, but rather on flow control. Data flow is obviously including data in transit (or data in move) and data in use, but also data at rest (data storage can be understood as flow from “present owner” to “future owner”). In Coco Cloud, protection of data in transit through encryption is combined with protection of data at rest, through the embedding of data into “data object containers (DOC)”. These objects contain data usage policies and data object policies that jointly define data access authorizations and usage conditions and obligations. The main challenge, therefore, for free flow of data is actually to control access and usage of data across country and cloud boundaries. Coco Cloud enforcement engine is able to monitor, collect and assess events that indicate possible violation of data access and usage policies.
- Timeframe: 2018-2020 and beyond.
- Project works on it: Yes
- Topics of the DSM Initiative #14: Free movement of data.
- Importance to DSM Initiative #14: high
- Risk of not filling the gap: Uncontrolled disclosure of personal data in cloud-based services.

Challenge 2:

- Short name: **Control of privacy conditions and obligations and adherence to them**
- Description: In regard to privacy, there is a perception that personal data protection facilitates the free flow of personal information, by regulating the conditions and

obligations under which that information might be used and disclosed. But the challenge here is to monitor not only authorization, but also these conditions and obligations, as well as adherence to the agreed policy that captures these authorizations, obligations and conditions (e.g. data sharing agreement in Coco Cloud).
- Timeframe: 2018-2020 and beyond.
- Project works on it: Yes
- Topics of the DSM Initiative #14: Free movement of data.
- Importance to DSM Initiative #14: high
- Risk of not filling the gap: Lack of trust in cloud-based services and lack of liability evidences.

e. CREDENTIAL

Challenge 1:

- Short name: **Design novel privacy preserving cloud-based (identity) services**
- Description: While the cloud offers several benefits, a couple of issues and challenges particularly with respect to security, privacy, or trust can be found. While there is a need for making cloud storage services or cloud services in general more secure and privacy-friendly, there is also a need for tackling security and privacy challenges in cloud identity management systems. In current state-of-the-art cloud identity management solutions the cloud-based identity provider needs to be fully trusted, as control over plaintext identity data is fully delegated. By now, none of the solutions protect confidentiality and integrity of identity data from provider internal threats. CREDENTIAL tries to tackle this challenge by designing novel secure and privacy-preserving cloud-based identity services. CREDENTIAL will improve the state-of-the-art by storing and processing identity data in the cloud in encrypted format only. Using advanced novel cryptographic technologies, cloud providers are prevented from getting access to plain identity data.
- Timeframe: 2016-2017 and early 2018-2020.
- Project works on it: Yes
- Topics of the DSM Initiative #14: Access to data.
- Importance to DSM Initiative #14: high
- Risk of not filling the gap: Cloud providers hosting identity management systems will still be able to inspect and disclose personal identity information as these data will still be processed in plaintext.

Challenge 2:

- Short name: **Adapt and improve cryptographic methods to securely store and share identity data**
- Description: Current state-of-the-art, identity management systems deployed in cloud environments have in common that the cloud identity services need to be fully trusted, as the cloud service provider has total control over the identity data. In all these approaches, unencrypted identity data is stored at the identity provider in the cloud. Usually, identity data needs particular protection from unauthorized access because of data protection laws and regulations. While state of the art mechanisms to fulfil such requirements already exist (e.g., encrypt data on client-side before transfer and storage in the cloud), such solutions are less flexible because any data processing requires the data to be channelled through the client for decryption, thus abandoning potential benefits of a cloud solution.
  Therefore, CREDENTIAL will focus on developing novel and enhanced existing cryptographic technologies, which allow more than simple storage of encrypted data,

but rather the advanced sharing of encrypted data from within the cloud. CREDENTIAL will improve and develop cryptographic mechanisms, enabling cloud providers to process identity data – without being able to inspect or access the processed identity data in plain text. CREDENTIAL aims to integrate the concept of proxy cryptography and especially proxy re-encryption into cloud-based identity management systems.

- Timeframe: 2018-2020.
- Project works on it: Yes
- Topics of the DSM Initiative #14: Access to data, Interoperability (security interoperability).
- Importance to DSM Initiative #14: high
- Risk of not filling the gap: Cloud solutions using simple data encryption will stay inflexible requiring for any data processing the data to be channelled through the client for decryption

Challenge 3:

- Short name: **Protect access to identity data with strong authentication mechanisms**
- Description: Authentication is an important topic within the cloud computing domain, because many Software as a Service (SaaS) or any other as a Service solutions require identification and authentication mechanisms paired with adequate authorization policies for regulating access control to protected services. Currently – although the weakness is well known – username/password authentication schemes still constitute the dominant approach for protecting cloud applications. To bypass these issues of passwords, CREDENTIAL will develop and provide possibilities to use stronger authentication mechanisms than username/password schemes for authentication at cloud services. CREDENTIAL particularly will focus on the inclusion of strong hardware-based approaches (e.g. TPM, TEE, SE) incorporated in client devices. CREDENTIAL will foster the use of enhanced HW-assisted 2FA mechanisms and will improve existing authentication mechanisms by additional authentication factors.
- Timeframe: 2016-2017 and early 2018-2020.
- Project works on it: Yes
- Topics of the DSM Initiative #14: Access to data, Interoperability (security interoperability).
- Importance to DSM Initiative #14: high
- Risk of not filling the gap: Cloud service applications will still rely on insecure username/password authentication mechanisms and identity data is still on risk to a large range of possible attacks on this weak mechanisms

f. ESCUDO-CLOUD

Challenge 1:

- Short name: **Self-protection of data for users' empowerment**
- Description: Today, users placing data in the cloud need to put complete trust that the Cloud Service Providers (CSPs) will correctly manage the outsourced information. As a matter of fact, although cloud providers can be assumed to employ basic security mechanisms for protecting data in storage, such measures leave data exposed to the cloud providers themselves. If stronger protection under the control of the data owner is to be applied, service functionality is considerably affected. ESCUDO-CLOUD will provide protection guarantees giving the data owners both full control and cloud functionality for their data in the cloud. This goal will be achieved by providing enforceable security, that is, techniques wrapping the data to provide a layer of protection to the eyes of the storing/processing CSP itself, setting the trust boundary

at the client side, which means assuming correct and trusted behaviour only by the client.
- Timeframe: 2016-2017
- Project works on it: Yes
- Topics of the DSM Initiative #14: Ownership.
- Importance to DSM Initiative #14: high
- Risk of not filling the gap: Data protection techniques will not provide effective realization of data ownership in the cloud.

Challenge 2:
- Short name**: Secure and private information sharing in the cloud**
- Description: The consideration of different users who should be granted access to the data stored and processed in the cloud raises several issues, including: the need of providing techniques that data owners can use to regulate the access to their data by other users in a selective way; the need of ensuring integrity of the data to protect them against possible malicious or lazy behaviour of the cloud providers; the need of collaboratively executing queries over data, possibly under the control of different authorities, to ensure both confidentiality and integrity; and the need of defining application-level verification techniques to assess whether the designed techniques provide the expected security guarantees.

  ESCUDO-CLOUD will investigate novel solutions guaranteeing that even without the owner in the loop, access to data will be possible only to authorized users. The project will also investigate solutions for providing secure and selective sharing when queries and services require access to data from multiple providers. It will also provide solutions allowing users of data to verify correctness and integrity of the data returned by the cloud.
- Timeframe: 2016-2017 and 2018-2020.
- Project works on it: Yes
- Topics of the DSM Initiative #14: Access to data.
- Importance to DSM Initiative #14: high
- Risk of not filling the gap: Information sharing techniques will not scale with respect to real data sets.

Challenge 3:
- Short name: **Multi-cloud and federated cloud environments**
- Description: The availability of many different providers in the cloud market permits users to benefit from a varied and rich market offer, with advantages in terms of data availability and performance possibly even at a reduced (economic) costs. The presence of multiple providers can be beneficial for better functionality and security, but at the same time can also introduce new security concerns.

  ESCUDO-CLOUD will design solutions in multi-cloud and federated-cloud scenarios. It will enable users to leverage the availability of multiple providers, to enhance security and reduce costs. In this context it will develop techniques to: define trust metrics allowing data owners to properly select the provider that best meets their needs; define techniques for leveraging multiple providers for security and efficiency; and define a federated secure cloud storage service supporting proper data protection. ESCUDO-CLOUD will also investigate the security problems arising in context where multiple providers need to cooperate for providing services, involving selective sharing of data, which might be even under control of different data authorities. In this context, the project will provide solutions allowing data authorities to regulate data sharing and flow of information.

- Timeframe: 2016-2017
- Project works on it: Yes
- Topics of the DSM Initiative #14: Interoperability (security interoperability), Access to data.
- Importance to DSM Initiative #14: high
- Risk of not filling the gap: Difficulty in designing solutions that require the interaction among different cloud providers.

g. MUSA

Challenge 1:

- Short name: **Risk assessment frameworks for applications at scale**
- Description: With the spreading of cloud, IoT, Big data, etc. software architectures are becoming more and more complex every day. Multi-technology applications that aim to take most out of the at scale combination of such technologies need to face a number of security issues of the technologies both in isolation and in combination, e.g. data location, access control, etc. There is a need for holistic risk assessment frameworks that enable the identification and management of security risks in all the layers in a way that risk information and risk minimization measures are seamlessly interoperable between the layers. Such risk assessment frameworks will need to take into account the "at scale" nature of multi-technology applications where the volume of devices, clouds, connection protocols, providers, etc. can be enormous, and therefore risks depend on the interconnections between the parts.
- Timeframe: 2018-2020
- Project works on it: No
- Topics of the DSM Initiative #14: Interoperability (security interoperability), Free movement of data.
- Importance to DSM Initiative #14: high
- Risk of not filling the gap: Failure in protecting future multi-technology applications.

Challenge 2:

- Short name: **Continuous Assurance of CSP performance**
- Description: As the variety and deployments of cloud services increase and the combination (composition) of cloud offerings became the usual choice of the cloud consumers, the assert "You never use the same cloud twice" is becoming more real than ever with dynamic data flows between interleaved services of different providers. Static self-assessments or third party audits of CSP capabilities and performance are not a solution for such changing environments where the pay-per-use models ask for rapid adaptation of deployments and controls over them. Mechanisms and tools for continuous assurance of both functional behaviour and security behaviour of CSPs are needed. These should be based on Trust models between consumer and CSPs, where evidence collection is combined with trusted protocols for exchange of evidence information. First, a standard taxonomy of controls and evidences is needed for enabling the consumer switching the CSP without modifying the assurance mechanism.
- Timeframe: 2018-2020 and beyond.
- Project works on it: Yes
- Topics of the DSM Initiative #14: Certification, Switch of CSPs.
- Importance to DSM Initiative #14: high
- Risk of not filling the gap: Having means for evidence based control of CSP performance will not only make the trust in clouds a reality, but will allow faster replacement of CSPs.

Challenge 3:

- Short name: **Standard certificates of CSP, including security features**
- Description: The ever changing cloud offerings and the future multi-cloud environments with dynamic changes in cloud combinations in use will ask for machine-readable standardised CSP certifications that allow the automatic comparison and selection of offerings while enable transparency. Such certifications would need to be based on standard taxonomies for cloud models, cloud capabilities, performance and security evidences, security controls in use, etc. The certificates would need to support modular certification (for updates in cloud services), combined certification (for combinations of cloud services) and dynamicity of evidences (not static audits). Novel certification models and mechanisms around such standard certificates are also needed, with trusted exchange of certificates between the parties (CSP to consumer, CSP to CSP, etc.).
- Timeframe: 2018-2020
- Project works on it: Yes
- Topics of the DSM Initiative #14: Certification, Switch of CSPs.
- Importance to DSM Initiative #14: high
- Risk of not filling the gap: Impossibility of automatic comparison of CSP offerings, impossibility of automatic switching of CSPs, not exploiting the full potential of cloud, vendor lock-in.

Challenge 4:

- Short name: **Dynamic benchmarking and brokering of Cloud offers**
- Description: The proliferation of Cloud service offers and models will ask for intelligent brokering systems aimed at easing the discovery, comparison, selection, integration and protection of cloud services. They will be of most importance for cloud-based applications that need to access multiple service providers at a time. The poor description of Cloud offers and lack of control that cloud consumers suffer today should be replaced by systems and mechanisms that allow legally benchmarking cloud features offered by CSPs of different nature so as rapid decisions on which cloud services to use can be made. The service marketplace approach will no longer be feasible when the scale, nature and evolutions of cloud offers increases in the future, unless we have tools that are able to search for and compare offers, according to both functional and non-functional features (security and privacy included). Other novel ad-hoc discovery and integration approaches may also be possible provided the legal constraints of the first step, benchmarking of CSPs' offers, are solved.
- Timeframe: 2018-2020
- Project works on it: Yes
- Topics of the DSM Initiative #14: Switch of CSPs, Interoperability (security interoperability), Free movement of data.
- Importance to DSM Initiative #14: high
- Risk of not filling the gap: Vendor lock-in and impossible or inefficient movement of data among cloud providers.

Challenge 5:

- Short name: **Composition of evolving security-aware SLAs**
- Description: In future applications that will dynamically replace, swap and combine different cloud services, there is a clear need for the applications of being able to negotiate and combine the contracts or Service Level Agreements (SLA) of the services in use. The challenge is to make it possible the composition of third party offerings into a single application that is able to guarantee a combined SLA to its customers. Such

combined SLA should take into account the likely continuous evolutions and updates of the SLAs of the cloud services in use. The challenge resides on stating in the offered SLA controls and metrics for the overall application based on controls on the services in use. This is of utmost importance for cross-border services where the controls may need to provide different evidences to fulfil the countries' regulations.
- Timeframe: 2018-2020
- Project works on it: Yes
- Topics of the DSM Initiative #14: Contracts, Switch of CSPs, Interoperability (security interoperability), Free movement of data.
- Importance to DSM Initiative #14: high
- Risk of not filling the gap: Vendor lock-in and impossible or inefficient movement of data among cloud providers.

h. PAASWORD

Challenge 1:

- Short name: **Fully secure APIs**
- Description: APIs - like security frameworks like PaaSword will provide - are carrying potential sensitive information within channels and opening a potential attack point. The solution can be to secure the channels by using SSL/TLS. But then we have to deal among others with how to generate/manage valid certificates from internal/external certificate authorities as well as configuration issues with platform services and software integration. Moreover, supporting external APIs needs to be handled carefully by deciding if to test every API passing JSON/XML messages or if it is possible to accept input from users/applications for standard injection flaws and cross-site request forgery attacks. And additionally, as a third open question transferability of authentication and authorization mechanisms to APIs has to be considered. This includes for example questions like: Can encryption of user names and passwords be managed by APIs? Can we guarantee continuity between internal identity management systems and attributes and those extended by APIs from cloud providers?
- Timeframe: 2018-2020
- Project works on it: Yes
- Topics of the DSM Initiative #14: Free Movement of Data, Interoperability (security interoperability).
- Importance to DSM Initiative #14: high
- Risk of not filling the gap: Increased number of cyberattacks that exploit vulnerabilities in APIs.

Challenge 2:

- Short name: **Access Control Policies based on context attributes**
- Description: Authorization and Authentication mechanisms based only on usernames and passwords are not sufficient for securing highly sensitive information which needs to be available everywhere and at any time. Combining a standard authorization and authentication mechanism by username and password with user-context information, i.e. geolocation, device, browser, etc., can increase the security level drastically. Dealing with different data types opens another issue that is that each data type has its own context attributes which need to be taken into account.
- Timeframe: 2016-2017 and 2018-2020.
- Project works on it: Yes
- Topics of the DSM Initiative #14: Access to data.
- Importance to DSM Initiative #14: high

- Risk of not filling the gap: Insufficient security level for highly sensitive information that has high availability requirements.

Challenge 3:

- Short name: **Searchable Encryption**
- Description: Encrypted data in cloud-based solutions needs to be searchable and editable. In order to ensure that cloud service provider cannot learn anything about the stored data by analysing the search keywords and/or the response also the search keywords need to be protected. The native approach consisting of downloading the whole dataset, decrypting it, working on it and re-encrypting the data before uploading it again is very ineffective and inefficient. A possible approach to address may be by defining a searchable encryption scheme which also includes search keywords and which is efficient on different types of devices with different resources.
- Timeframe: 2018-2020 and beyond
- Project works on it: Yes
- Topics of the DSM Initiative #14: Free movement of data, Ownership, Location of data.
- Importance to DSM Initiative #14: high
- Risk of not filling the gap: Impossibility of identifying, selecting and searching on encrypted data in the cloud.

i. PRISMACLOUD

Challenge 1:

- Short name: **Security and privacy by design in cloud services**
- Description: Users of cloud services and applications need to a great extent rely on contractual security guarantees regarding vital security requirements, as e.g. confidentiality or integrity of their data. An alternative for end-users is to implement complex cryptographic wrappers (including cryptographic key management) themselves, thus neutralising part of the convenience advantages of cloud computing. Cloud providers often only add security to cloud applications and services retroactively and without transparency. The challenge is provide enabling tools and methodologies which help to build services with security as a dedicated function and built it into the systems from the start “by design” and ideally protect data from end-to-end.
- Timeframe: 2016-2017, 2018-2020 and beyond.
- Project works on it: Yes
- Topics of the DSM Initiative #14: Usability (usability of security).
- Importance to DSM Initiative #14: high
- Risk of not filling the gap: Communities requiring a high security level may be barred from moving to the cloud for compliance reasons as well as because they value their data too much to expose them to prevailing risks in the cloud. New business ideas cannot be realised, because users do not entrust the proposed services without additional security and privacy guarantees.

Challenge 2:

- Short name: **Authenticity and verifiability of data and infrastructure use**
- Description: Besides the evident privacy and confidentiality issues associated with cloud usage, this new IT delivery model also introduces additional problems related to authenticity, verifiability and accountability. Basically, the question is how we can ensure that the cloud works as it is intended or claimed to do and how can the cloud be held accountable if deviations occur. Thereby, one may not only be concerned with the data itself, but also with processes (tasks/workflows) executing in the cloud and processing the data. Moreover, such concerns may also be related to the used

infrastructure itself. The challenge is to preserve the authenticity of data throughout cloud based work flows and have means to verify the processing steps undertaken in to cloud environment.
- Timeframe: 2016-2017 and 2018-2020.
- Project works on it: Yes
- Topics of the DSM Initiative #14: Free movement of data, Access to data.
- Importance to DSM Initiative #14: high
- Risk of not filling the gap: Applications from the high-assurance domains or business relevant data processing cannot be outsourced, hence, this industry cannot benefit from the economic and technical advantages of the cloud computing trend.

Challenge 3:
- Short name: **Confidentiality, integrity and availability for data at rest**
- Description: Protecting all three main security properties (confidentiality, integrity and availability) while at the same time enabling collaboration among dynamic groups of users for data stored in an external cloud infrastructure is a challenging task. Currently, most cloud storage offerings store the data either unencrypted or apply encryption which remains under complete control of the cloud service provider; only a marginal minority of cloud storage providers let the user exert full control and do not claim access to cryptographic keys. The typical cloud storage provider has to be fully trusted to provide effective protection of the data as regards confidentiality and integrity, including all copies and replications created for availability purposes in all layers of the storage architecture.
- Timeframe:2016-2017
- Project works on it: Yes
- Topics of the DSM Initiative #14: Access to data, Interoperability (security interoperability).
- Importance to DSM Initiative #14: high
- Risk of not filling the gap: Cloud based data sharing can be an enabler for many businesses to share information with different stakeholders in a very efficient way. Without secure cloud based services, self-hosted versions would have to be deployed, which is less convenient for smaller companies, hence, they would not adopt this way of collaboration with, e.g. suppliers or customers.

Challenge 4:
- Short name: **Development of a methodology for secure service composition**
- Description: In the last years, researchers suggested a large number of cryptographic protocols preserving and enhancing users' privacy in the cloud. Furthermore, following the provable security paradigm, many of those services have been formally proved secure. However, many of those proofs consider the protocol to be executed as a stand-alone application, not interacting with any other protocols, which is often not the case in the real world. Unfortunately, academic and real-world examples have shown that the security of "provably secure" protocols can be broken outside this idealised single-protocol world. This problem of composability has been addressed by multiple frameworks (UC, GNUC, etc.), but solutions there are often computationally expensive. It is therefore necessary to enable the provable secure composition of primitives with only minimum computational overhead.
- Timeframe: 2018-2020
- Project works on it: Yes
- Topics of the DSM Initiative #14: Interoperability (security interoperability).
- Importance to DSM Initiative #14: medium

- Risk of not filling the gap: Practical attacks on presumably secure privacy-enhancing protocols.

Challenge 5:

- Short name: **Cloud Standardisation gap**
- Description: Currently, there are more than 20 organisations active in standardisation, and virtually hundreds of standards published governing all kinds of aspects relevant for cloud computing. It seems that the current unclear situation is voluntarily induced by major market players to foster incompatibilities and customer lock-in. Although "Cutting through the Jungle of Standards" is defined "Key Action 1" of the European cloud computing strategy, and specific actions for the resolution of the situation were implemented (and are on-going), there is no remedy for the situation expected in the nearer future.
- Timeframe: 2016-2017
- Project works on it: Yes
- Topics of the DSM Initiative #14: Interoperability (security interoperability) and Certification (Standards).
- Importance to DSM Initiative #14: medium
- Risk of not filling the gap: User lock-in with a single cloud provider, lack of trust in the security of cloud applications and services due to lack of proper certification.

j. SLA-Ready

Challenge 1:

- Short name: **Simpler contractual terminology and commonly used taxonomy**
- Description: Eurostat, and many European business and trade associations highlight the lack of knowledge about cloud computing as a major barrier to adoption, particularly complex contractual terminology and the lack of a commonly used taxonomy. A common vocabulary is a crucial aspect to understand and communicate the concepts that underpin cloud computing and to make comparisons between SLAs. SLA-Ready will propose a SLA Common Reference Model to address these challenges. SLA-Ready lowers the barrier by guiding prospective cloud customers through each crucial step of the SLA lifecycle, showing them what to do, what to expect and what to trust, also in terms of compliance. Such an approach is also important to help customers gain a better understanding of the security levels and data protection offered by the CSP, as well as monitor performance and security when using a cloud service. SLA-Ready builds on expert work on SLAs with several partners contributing to the EC Guidelines on SLAs as a best-practice guide for the industry, with the aim of improving the uptake of cloud services by the European private sector.
- Timeframe: 2018-2020.
- Project works on it: Yes
- Topics of the DSM Initiative #14: Free movement of data, Usability (security usability), Contracts.
- Importance to DSM Initiative #14: high
- Risk of not filling the gap: If the challenge is not addressed, companies, and in particular SMEs, cannot make an informed decision on what services to use, what to expect and what to trust.

Challenge 2:

- Short name: **Standardisation and transparency in SLAs**
- Description: Top barriers to adoption of cloud services by small businesses are lack of clearly defined terms and conditions in contracts, lack of pricing transparency, and the

lack of balance between the risks and responsibilities of the customer and the CSP. Many prospective clients find cloud services too complicated, too risky and too untrustworthy and prefer not to use cloud services. SMEs need specialised legal terminology and clauses, and checklists to evaluate the risks/responsibilities that prospective cloud customers have to undertake.

The SLA-Ready Common Reference Model (CRM) will benefit the industry by integrating a set of SLA components, e.g. terminology, SLA attributes, Service Level Objectives (SLO), guidelines, as well as best practices and relevant standards to fill identified gaps in the current SLA landscape. Standardisation is the critical to build consensus on best/good practices through an-depth analysis of the current standards landscape and industry-led initiatives. The use of standardised Cloud SLAs is a critical step towards better understanding the terms and conditions of the services contracted and easier comparison of the CSPs' cloud offer.

- Timeframe: 2016-2017.
- Project works on it: Yes
- Topics of the DSM Initiative #14: Free movement of data, Ownership, Location of data.
- Importance to DSM Initiative #14: high
- Risk of not filling the gap: Limited trust in cloud computing services.

k. SPECS

Challenge 1:

- Short name: **User-centric Security SLA Negotiation**
- Description: The typical Cloud user is typically not a security expert, nevertheless will have some security requirements to fulfil (e.g., due to regulatory compliance) usually expressed in an informal manner. Due to this cultural gap in Cloud security, it is a common practice for users to "blindly trust" their CSP and only to react (e.g., change their provider) after a security incident has occurred. This problem worsens if we take into account the ever increasing number of CSPs available in the Cloud ecosystem. A number of natural concerns arise. Despite the assumption that a given CSP "seems" secure, is it actually "secure enough" for my applications? How do I compare different CSPs with regards to security? The Cloud security community represented by workgroups at the European Network and Information Security Agency (ENISA) and the Cloud Security Alliance (CSA), has identified that specifying security parameters in Service Level Agreements (Security SLAs) is useful to establish a common semantic in order to manage Cloud security from two perspectives, namely (i) the security level being offered by a CSP and, (ii) the security level requested by a Cloud user.

  Despite the state of the art efforts aiming to build and represent security parameters in Cloud SLAs, there are no available user-centric solutions (i.e., empowering Cloud customers) to offer the systematic mechanisms to manage their whole life-cycle. As state of art, CSP's currently do not offer any rigorous specification SLAs, formally describing their security features.
- Timeframe: 2016-2017.
- Project works on it: Yes
- Topics of the DSM Initiative #14: Free movement of data, Contracts, Respect of customer rights.
- Importance to DSM Initiative #14: high
- Risk of not filling the gap: Limited trust in CSPs, Cloud not adopted in critical sectors, increase of security incidents.

Challenge 2:

- Short name: **Security SLA Automatic Implementation**
- Description: The Cloud security community represented by workgroups at the European Network and Information Security Agency (ENISA) and the Cloud Security Alliance (CSA), has identified that specifying security parameters in Service Level Agreements (Security SLAs) is useful to establish a common semantic in order to manage Cloud security from two perspectives, namely (i) the security level being offered by a CSP and, (ii) the security level requested by a Cloud user.

  Security SLA implementation is the phase during which the actions needed to respect the SLA (i.e., keep a sustained QoSec2) are effectively taken. This may imply activation of software modules, acquisition of resources (in the correct amount), but even dynamic reconfiguration of resources after an alert is generated. From user's view, Enforcement is simply the application of the service requirements explicitly requested into the SLA. From the Service provider's view, Enforcement is the phase where SLA requirements are effectively applied on the acquired resources else economic or legal penalties apply.

  At state of art Security SLA are usually not automatic implemented, but only preconfigured services are offered to customers, so security cannot be offered "as-a-service" according to user requirements.
- Timeframe: 2016-2017 and 2018-2020.
- Project works on it: Yes
- Topics of the DSM Initiative #14: Free movement of data, Contracts.
- Importance to DSM Initiative #14: high
- Risk of not filling the gap: Offerings to cloud customers are limited, limited adoption of Cloud solution for customers that have specific and not common security requirements.

Challenge 3:

- Short name: **Security SLA Monitoring**
- Description: The typical Cloud user is typically not a security expert, nevertheless will have some security requirements to fulfil (e.g., due to regulatory compliance) usually expressed in an informal manner. The Cloud security community represented by workgroups at the European Network and Information Security Agency (ENISA) and the Cloud Security Alliance (CSA), has identified that specifying security parameters in Service Level Agreements (Security SLAs) is useful to establish a common semantic in order to manage Cloud security from two perspectives, namely (i) the security level being offered by a CSP and, (ii) the security level requested by a Cloud user.
  Despite the state of the art efforts aiming to build and represent security parameters in Cloud SLAs, there are no available solutions able to support customers to monitor its own Security SLAs and verify that they are being concretely respected.
- Timeframe: 2016-2017 and 2018-2020.
- Project works on it: Yes
- Topics of the DSM Initiative #14: Free movement of data, Contracts, Respect of customer rights.
- Risk of not filling the gap: Limited trust in cloud computing; conflicts among cloud customers and cloud service providers among the respect of SLAs.

l. STRATEGIC

Challenge 1:

- Short name: **Secure interoperable authentication in cross-border scenarios**
- Description: Despite the benefits of the cloud in the public administrations, security and privacy management mechanisms (along with related policies) are not yet fully integrated into public cloud services.
  STRATEGIC integrates mechanisms for secure access to information for the purpose of authenticated and authorized access to information, but also for the purpose of data protection. Special emphasis is paid in secure interoperable authentication in cross-border scenarios, where end-users should provide authentication information (attributes, properties) enabling authentication against their home provider and/or facilitating the cloud provider to perform the authentication on their behalf.
- Timeframe: 2016-2017 and 2018-2020.
- Project works on it: Yes
- Topics of the DSM Initiative #14: Free movement of data, Access to data (data federation), Access to public data, Interoperability (security interoperability).
- Importance to DSM Initiative #14: high
- Risk of not filling the gap: Cybersecurity attacks in cross-border public services that use cloud computing by unauthorised access to data.

Challenge 2:

- Short name: **Definition and enactment of fine-grained security policies**
- Description: STRATEGIC also implements security policy management mechanisms based on the integration of policies across different nodes of its cloud infrastructures in order enable the definition and enactment of fine-grained policy mechanisms. Secure access and data protection mechanisms will be horizontally provided for the services of the STRATEGIC framework that require them. The latter will be designed on the basis of security-by-design principles that blend security aspects into core elements of the STRATEGIC framework.
- Timeframe: 2016-2017 and 2018-2020.
- Project works on it: Yes
- Topics of the DSM Initiative #14: Free movement of data, Access to data (data federation), Access to public data, Interoperability (security interoperability).
- Importance to DSM Initiative #14: high
- Risk of not filling the gap: Failure to comply with security and privacy policies across services and increased number of cybersecurity issues in cloud services.

m. SUNFISH

Challenge 1:

- Short name: **Protected data sharing for federated clouds**
- Description: As the presence of sensitive information in data sets impacts the security classification levels of whole sets, the data sharing processes with other entities or subsystems might be considered as unacceptable from the systems' security viewpoint. There are, however, use cases that do not require the access to complete data sets to accomplish their tasks successfully. Instead, their process flows might rely on restricted and lower-sensitivity parts of the data, or their security-conforming and context-based representations. There is, therefore, a need to enable cross-entity collaborative data sharing and processing framework that dynamically establishes data sharing across domains and jurisdictions, considering both security policies, legal requirements, as well as context and process satisfiability criteria. By applying

techniques such as data masking, format preserving encryption, anonymization and context-based access control, the currently restricted resources could be reused for data processing across the members of cloud federations.
- Timeframe: 2016-2017.
- Project works on it: Yes
- Topics of the DSM Initiative #14: Free movement of data, Access to data, Access to public data.
- Importance to DSM Initiative #14: high
- Risk of not filling the gap: Lack of security in data sharing across entities and domains in cloud federations.

Challenge 2:
- Short name: **Security policy management and enforcement in heterogeneous cloud federations**
- Description: Federation of private clouds of public administrations allows the usage optimization of their infrastructures, as well as data and resource sharing between entities that rely on different infrastructures and processes. Additionally, these entities may host the data with different sensitivity levels, being subjected to various legal and privacy requirements. The integration of such environments requires transparent policy management and administration, allowing the definition of common federation policies, policies on the level of each member entity and their alignment between heterogeneous and cross-domain environments. The enforcement of these policies needs to consider various aspects of data security and context-dependent requirements, allowing on-the-fly execution of operations that would protect sensitive data or its parts by applying the techniques such as data masking, tokenization, format-preserving encryption or anonymization. The policy enforcement furthermore needs to consider the applicable legal requirements for each federation member, performing the enforcement of legal requirements in a transparent manner.
- Timeframe: 2016-2017 and 2018-2017.
- Project works on it: Yes
- Topics of the DSM Initiative #14: Access to data, Interoperability (security interoperability), Location of data.
- Importance to DSM Initiative #14: high
- Risk of not filling the gap: Insecure and untrustworthy heterogeneous cloud federations that are not compliant with all regulations over federation members or have members' security policies misaligned.

Challenge 3:
- Short name: **Continuous monitoring and security assurance of inter-cloud communication**
- Description: In a standard approach, the enforcement of security policies in inter-cloud federations can be performed along lines of communication and components present in the federated environment. However, taking into account various levels of data sensitivity, data- and user-specific security requirements, as well as requirements arising from different jurisdictions and existence of various data sharing and processing layers, additional means to monitor the security conformance of inter-cloud processes need to be provided. Performed as an independent and non-blocking process, these means have to consider the complexity of cloud integrations and availability of multiple layers and data sharing paths. They additionally need to allow automated reactions to security breaches and violations of security contracts.
- Timeframe: 2016-2017 and 2018-2020.
- Project works on it: Yes

- Topics of the DSM Initiative #14: Access to data, Contracts, Ownership, Location of data.
- Importance to DSM Initiative #14: high
- Risk of not filling the gap: Security breaches in data access and sharing among clouds and violations of data- and user-specific security requirements.

n. SWITCH

Challenge 1:

- Short name: **Security and privacy terms in SLA Negotiation**
- Description: The customer needs to put his data on the cloud, so it is essential that the customer can ensure that his data is safe, and that it is neither revealed by the cloud provider nor stolen by a malicious agent. Therefore it is useful to be able to define a controlled vocabulary for describing security requirements. This vocabulary should provide terms by which to evaluate and measure security during negotiations. Between the customer and provider, there should be a mechanism by which to monitor compliance with these security terms.
- Timeframe: 2018-2020
- Project works on it: No
- Topics of the DSM Initiative #14: Free movement of data, Switch of CSPs, Contracts.
- Importance to DSM Initiative #14: high
- Risk of not filling the gap: Security remains hard to measure and any security or privacy leakage remains difficult to detect.

Challenge 2:

- Short name: **SLA transmission security**
- Description: Currently, SLAs are transmitted between customers and providers in plain text. This will not be secure in cases where SLAs include information about the negotiation process between the customer and provider. It might reveal certain private data of either customers or providers—for example, a malicious agent may be able to discover the price floor of a cloud provider from studying the SLA negotiation process. The private personal information of the customer may also leak.
- Timeframe: 2018-2020
- Project works on it: No
- Topics of the DSM Initiative #14: Free movement of data, Switch of CSPs, Contracts.
- Importance to DSM Initiative #14: high
- Risk of not filling the gap: Traditional encryption methods have a high overhead and so are not good for quick negotiation; without provable transmission security however, information may be leaked.

o. TREDISEC

Challenge 1:

- Short name: **Deduplication on encrypted multi-tenant data**
- Description: Tenants do not trust each other, and might not share secret material. When we require cloud storage systems to handle data in encrypted form from multiple, mistrusting tenants, there are no known ways in which deduplication can be carried out. Moreover, deduplication of data breaks the paradigm over which cryptographic secure deletion hinges, namely, that secure deletion can be obtained by breaking one of the links of the cryptographic chain of keys that decrypts the required datum; indeed, in presence of deduplication, multiple such chains exist from each of the individual, mistrusting uploaders. The challenge is to leverage existing or novel

cryptographic protocols and system security mechanisms which offer strong data confidentiality guarantees while permitting data deduplication across multiple tenants.
- Timeframe: 2018-2020
- Project works on it: Yes
- Topics of the DSM Initiative #14: N/A.
- Importance to DSM Initiative #14: high
- Risk of not filling the gap: Cloud infrastructures and services would remain insecure when prioritizing efficiency-related requirements (multi-tenancy, deduplication) over security aspects (confidentiality).

Challenge 2:
- Short name: **Mechanisms to check the integrity and availability of multi-tenant data in presence of storage efficiency**
- Description: current PoR/PDP solutions have not been analysed in conjunction with data deduplication and require specific pre-processing of data by its legitimate owner prior to outsourcing. These techniques fail if data is shared in the cloud by multiple-tenants because either (i) the key material used cannot be shared amongst mistrusting entities or (ii) the pre-processing causes the data to be unsuitable for deduplication.
- Timeframe: 2018-2020
- Project works on it: Yes
- Topics of the DSM Initiative #14: Access to data.
- Importance to DSM Initiative #14: high
- Risk of not filling the gap: Cloud infrastructures, and the services built on top of them, would remain insecure when prioritizing efficiency-related requirements (multi-tenancy, deduplication) over security aspects (integrity, availability).

Challenge 3:
- Short name: **Privacy-preserving analytics/processing over confidential and efficient outsourced databases.**
- Description: Although classical encryption algorithms ensure data confidentiality, they unfortunately prevent the cloud from operating over encrypted data. This requires the data to be downloaded and decrypted on the client to execute any query on it, making any serious Database as a Service offering questionable and is the way many traditional DBMS like Sybase, Oracle, DB2 or solutions like Dropbox appear to work when they claim to encrypt data and provide cloud storage. Moreover, the queries issued by the user and the result of the queries should remain confidential to the cloud. The challenge is on new techniques that enable the processing of encrypted data in an efficient and privacy-preserving manner (e.g. searchable encryption or private information retrieval), guaranteeing efficient data processing that scales with large amounts of outsourced data.
- Timeframe: 2018-2020
- Project works on it: Yes
- Topics of the DSM Initiative #14: Free movement of data, Access to data.
- Importance to DSM Initiative #14: high
- Risk of not filling the gap: Cloud infrastructures and services would remain insecure when prioritizing efficiency-related requirements (scalability, efficient data processing) over security aspects (confidentiality).

p. WITDOM

Challenge 1:

- Short name: **Effective protection of personal and critical data**
- Description: In untrusted environments like the cloud, new security challenges arise from the very moment that data is being processed by external third parties. The data must be protected not only from access by unauthorized agents, but also from the parties that perform processing and storage, which are not necessarily trusted. This cannot be achieved only with traditional cryptosystems and current security frameworks. Advanced privacy enhancing technologies and encryption techniques are needed for performing verifiable operations over the encrypted or obfuscated data without the need of decryption (including techniques like efficient homomorphic encryption, perturbation techniques, secure multiparty computation and others), and thus without having access to their clear-text linkable version.
- Timeframe: 2016-2017
- Project works on it: Yes
- Topics of the DSM Initiative #14: Interoperability (security-interoperability), Access to data, Switch of CSPs.
- Importance to DSM Initiative #14: high
- Risk of not filling the gap: Free flow of data should guarantee the compliance with EU data protection regulation and preserve users' data efficiently. Uncertainty about rights to use data hinders the development of many data-based solutions (developments, technologies, services).

Challenge 2:

- Short name: **User control of his personal data**
- Description: Currently the data owner needs to rely on an "access controller" to enforce its policies. Since the access controller may be in an un-trusted environment (i.e. the Cloud), current access control systems cannot provide an efficient and flexible service with assured security guarantee. Risks relate mainly to the un-trusted environment "Cloud" in which the outsourced data need end-to-end protection measures at all times.

  By increasing the control of the users over their own private data, instead of relying on a fully-trusted third party to enforce her or his access control policies (by means of advanced privacy enhancing techniques, and cryptographic process integrity verification primitives) users are empowered to specify their privacy and security preferences over their personal data and their outsourced processes and guarantee their enforcement, achieving a more assured control over their data.
- Timeframe: 2016-2017
- Project works on it: Yes
- Topics of the DSM Initiative #14: Ownership.
- Importance to DSM Initiative #14: high
- Risk of not filling the gap: Lack of users trust can prevent a successful implementation of the initiative.

6. Mapping of challenges to DSM Initiative #14

In this section we show the map of the challenges identified by the projects and the areas addressed by the DSM Initiative #14. Note that *ChNo* refers to the order number of challenge in subsections of Section 5, i.e. *Challenge No* identified by each project.

DSM Initiative #14 topics	Challenges (as in Section 5)
Free movement of data	CLARUS Ch1, CLARUS Ch2, CLARUS Ch3, CLARUS Ch4, COCO CLOUD Ch1, COCO CLOUD Ch2, MUSA Ch1, MUSA Ch4, MUSA Ch5, PAASWORD Ch1, PAASWORD Ch3, PRISMACLOUD Ch2, SLA-READY Ch1, SLA-READY Ch2, SPECS Ch1, SPECS Ch2, SPECS Ch3, STRATEGIC Ch1, STRATEGIC Ch2, SUNFISH Ch1, SWITCH Ch1, SWITCH Ch2, TREDISEC Ch3.
Location of data	CLARUS Ch2, CLARUS Ch3, PAASWORD Ch3, SLA-READY Ch2, SUNFISH Ch2, SUNFISH Ch3.
Ownership	CLARUS Ch2, CLARUS Ch3, ESCUDO-CLOUD Ch1, PAASWORD Ch3, SLA-READY Ch2, SUNFISH Ch3, WITDOM Ch2.
Interoperability (security interoperability)	CLARUS Ch4, CREDENTIAL Ch2, CREDENTIAL Ch3, ESCUDO-CLOUD Ch3, MUSA Ch1, MUSA Ch4, MUSA Ch5, PAASWORD Ch1, PRISMACLOUD Ch3, PRISMACLOUD Ch4, PRISMACLOUD Ch5, STRATEGIC Ch1, STRATEGIC Ch2, SUNFISH Ch2, WITDOM Ch1.
Usability (usability of security)	AppHub Ch1, CLOUDWATCH2 Ch3, PRISMACLOUD Ch1, SLA-READY Ch1.
Access to data	CLARUS Ch1, CLARUS Ch6, CREDENTIAL Ch1, CREDENTIAL Ch2, CREDENTIAL Ch3, ESCUDO-CLOUD Ch3, PAASWORD Ch2, PRISMACLOUD Ch2, PRISMACLOUD Ch3, STRATEGIC Ch1, STRATEGIC Ch2, SUNFISH Ch1, SUNFISH Ch2, SUNFISH Ch3, TREDISEC Ch2, TREDISEC Ch3, WITDOM Ch1.
Access to public data	AppHub Ch1, STRATEGIC Ch1, STRATEGIC Ch2 SUNFISH Ch1.
Certification	CLOUDWATCH2 Ch2, MUSA Ch2, MUSA Ch3, PRISMACLOUD Ch5 (Standards).
Contracts	CLARUS Ch3, CLOUDWATCH2 Ch3, MUSA Ch5, SLA-READY Ch1, SPECS Ch1, SPECS Ch2, SPECS Ch3, SUNFISH Ch3, SWITCH Ch1, SWITCH Ch2.
Switch of CSPs	CLARUS Ch4, MUSA Ch2, MUSA Ch3, MUSA Ch4, MUSA Ch5, SWITCH Ch1, SWITCH Ch2, WITDOM Ch1.
Research open science cloud[10]	AppHub Ch1, CLOUDWATCH2 Ch1.

[10] http://horizon-magazine.eu/article/european-science-cloud-horizon_en.html

Other topics	Challenges (as in Section 5)
Improve market readiness of EU projects' results	CloudWatch2 Ch1.
Respect of customer rights	SPECS Ch1, SPECS Ch3.
Leverage of efficiency vs. security	TREDISEC Ch1

7. Summary of the challenges in the context of the next H2020 Work Programme

According to the timeframe specified for the challenges identified (in Section 5), there are a set of challenges for mid term, i.e. for the years 2018 to 2020. These challenges are recommended to be addressed by the next H2020 Work Programme 2018-2020.

In total there are 35 challenges for mid term that cover the following areas:

Project	Challenge	DSM Initiative #14
APPHUB	Improve market readiness of security and privacy solutions	Usability (usability of security), Access to public data, Research open science cloud (first step to this).
CLARUS	Making the cloud ecosystem secure for outsourced data	Free movement of data, Access to data.
	Privacy-enabling mechanisms to protect sensitive data	Free movement of data, Ownership, Location of data.
	Data protection and legal jurisdiction	Free movement of data, Location of data, Ownership, Contracts.
	Interoperability-by-design to overcome mistrust in cloud computing by implementing standardized cloud services	Switch of CSPs, Free movement of data, Interoperability (security interoperability).
	Data anonymisation and access to data	Access to data.
CLOUDWATCH2	Cloud Security Certification & Definition of Risk profiles	Certification.
	Data Protection legal framework transparency	Usability (usability of security), Contracts.
COCO CLOUD	Data flow control	Free movement of data.
	Control of privacy conditions and obligations and adherence to them	Free movement of data.
CREDENTIAL	Design novel privacy preserving cloud-based (identity) services	Access to data.
	Adapt and improve cryptographic	Access to data, Interoperability (security

Project	Challenge	DSM Initiative #14
	methods to securely store and share identity data	interoperability).
	Protect access to identity data with strong authentication mechanisms	Access to data, Interoperability (security interoperability).
ESCUDO-CLOUD	Secure and private information sharing in the cloud	Access to data.
MUSA	Risk assessment frameworks for applications at scale	Interoperability (security interoperability), Free movement of data.
	Continuous Assurance of CSP performance	Certification, Switch of CSPs.
	Standard certificates of CSP, including security features	Certification, Switch of CSPs.
	Dynamic benchmarking and brokering of Cloud offers	Switch of CSPs, Interoperability (security interoperability), Free movement of data.
	Composition of evolving security-aware SLAs	Contracts, Switch of CSPs, Interoperability (security interoperability), Free movement of data.
PAASWORD	Fully secure APIs	Free Movement of Data, Interoperability (security interoperability).
	Access Control Policies based on context attributes	Access to data.
	Searchable Encryption	Free movement of data, Ownership, Location of data.
PRISMACLOUD	Security and privacy by design in cloud services	Usability (usability of security).
	Authenticity and verifiability of data and infrastructure use	Free movement of data, Access to data.
	Development of a methodology for secure service composition	Interoperability (security interoperability).
SLA-READY	Simpler contractual terminology and commonly used taxonomy	Free movement of data, Usability (security usability), Contracts.
SPECS	Security SLA Automatic Implementation	Free movement of data, Contracts.
	Security SLA Monitoring	Free movement of data, Contracts, Respect of customer rights.
STRATEGIC	Secure interoperable authentication in cross-border scenarios	Free movement of data, Access to data (data federation), Access to public data, Interoperability (security interoperability).
	Definition and enactment of fine-grained security policies	Free movement of data, Access to data (data federation), Access to public data,

Project	Challenge	DSM Initiative #14
		Interoperability (security interoperability).
SUNFISH	Security policy management and enforcement in heterogeneous cloud federations	Access to data, Interoperability (security interoperability), Location of data.
	Continuous monitoring and security assurance of inter-cloud communication	Access to data, Contracts, Ownership, Location of data.
SWITCH	Security and privacy terms in SLA Negotiation	Free movement of data, Switch of CSPs, Contracts.
	SLA transmission security	Free movement of data, Switch of CSPs, Contracts.
TREDISEC	Deduplication on encrypted multi-tenant data	N/A.
	Mechanisms to check the integrity and availability of multi-tenant data in presence of storage efficiency	Access to data.
	Privacy-preserving analytics/processing over confidential and efficient outsourced databases.	Free movement of data, Access to data.

Note that in all of them the level of importance related to DSM Initiative #14, as defined by clustered projects, was high. The only exception is the challenge on *Development of a methodology for secure service composition* which importance was considered medium.

In summary, we can group the challenges above in the following challenge categories:

- **Full control of data 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.
- **Fully secure APIs** that securely enable the interoperability of identity, authentication and authorization between cloud stakeholders.
- **Continuous control of security and privacy conditions and obligations and adherence to them**, including continuous monitoring, assurance, enforcement, and automated reaction in inter-clouds, multi-cloud, federated clouds.
- **Definition and enactment of fine-grained security policies.**
- **Security and privacy by design in cloud services.**
- **Privacy preserving cloud-based (identity) services:** Improved and novel cryptographic methods to securely protect, store and share (private) data, including encrypted identity data.
- **Efficient searchable encryption** for enabling to efficiently search and edit the encrypted data stored and processed in the cloud.
- **Security-aware SLA management support** for security and privacy terms formalisation, negotiation, transmission, composition, monitoring, continuous

assurance and automation. All these applied to multi-cloud or federated cloud-based applications and cloud-services themselves.

- **Risk assessment frameworks for applications at scale.**
- **Secure dynamic composition of cloud services, including dynamic benchmarking and brokering** of Cloud services for multi-cloud scenarios as well as federation of clouds.
- **Efficient secure and privacy-preserving multi-tenant data storage and processing.**
- **Cloud Security Certification.**
- **Data Protection legal framework transparency.**
- **Improve market readiness of security and privacy solutions from projects.**

8. Conclusions

This white paper is the result of an exercise of collaboration among the projects participating in the DPSP Cluster initiated by DG-CNECT. Even if not all the clustered projects have provided inputs, we consider that the challenges herein are a valuable input to EU policy makers as they represent the ideas and points of view of a significant number of projects leading the Commission supported research on security, data protection and privacy in the cloud at the EU level.

The work collects a total of 47 challenges mapped to the 7 work topics of the DSM Initiative #14, in order they can be easily discussed in the context of particular topics addressed by the initiative.

The DPSP Cluster members and authors of this work would like to show their availability and interest in helping to understand the readers, particularly EU policy makers, the research challenges herein as well as their technical implications. For any doubts on the challenges or any other aspect related to the cluster, the reader can contact the cluster coordinator[11].

[11] erkuden.rios@tecnalia.com