Research and Innovation Challenges in Data Protection, Security and Privacy in the Cloud:

Map of synergies of the clustered projects – Version 2.0

Authors:

Beatriz Gallego-Nicasio Crespo, ATOS Spain S.A., Spain, TREDISEC project,
Elsa Prieto, ATOS Spain S.A., Spain, WITDOM project
Erkuden Rios, Tecnalia, Spain, MUSA project,
Massimiliano Rak, CeR ICT, Italy, SPECS project,
Peter Deussen, Fraunhofer Institute for Open Communication Systems, Germany, APPHUB project.
Pierangela Samarati, Universita Degli Studi di Milano, Italy, ESCUDO-CLOUD project,
Roberto Cascella, Trust-IT Services Ltd, Italy, CLARUS and SLA-READY projects,
Simone Braun, CAS Software AG, Germany, PAASWORD project
Stephan Krenn, AUSTRIAN INSTITUTE OF TECHNOLOGY GmbH, CREDENTIAL project
Thomas Lörunser, AIT Austrian Institute of Technology GmbH, Austria, PRISMACLOUD project,

January 15, 2016

Content

Document changes history

Version	Publication date	Publication media	Changes
1.0	12.12.2015	E-mail to all DPSP project members	First version
2.0	15.01.2016	DPSP cluster intranet	• New inputs from SLA-Ready and CREDENTIAL projects • Updates from PaaSword project • Document changes history information

1. Introduction

1.1. Aim

The present open access document aims to depict the map of research topics and innovations of the projects in the Data Protection Security and Privacy in the Cloud cluster (from now on DPSP cluster for short). The DPSP cluster includes projects and actions on Cloud partially funded by the European Commission through the H2020-LEIT-ICT, FP7-Collaboration-ICT, and CIP-ICT-PSP programmes. The document summarizes the objectives and research topics of the projects in the cluster and identifies the common topics of interest, the common used technologies and tools, the common development directions, and the commonly used standards. This information serves to identify the synergies between the projects in the form of key topics for collaborations and take-up's between the projects and actions. Therefore, the document is called the Map of synergies of the clustered projects.

1.2. Scope

The document collects the contributions of the representatives of the following projects involved in the DPSP cluster:

- CLARUS
- CREDENTIAL
- ESCUDO-CLOUD
- MUSA
- PAASWORD
- PRISMACLOUD
- SLA-READY
- SPECS
- TREDISEC
- WITDOM

and the Collaboration and Support Action:

- APPHUB.

The Cluster official website is available at: https://eucloudclusters.wordpress.com/data-protection-security-and-privacy-in-the-cloud/

The website provides information on the cluster objectives and activities and refers to the websites of the integrating projects and actions.

1.3. Organisation

The document is organized as follows. The next Section 2 reminds the open research topics on security, data protection and privacy as defined by the Horizon 2020 Work Programme for the years 2016 and 2017. The section also describes the classification of the research topics developed by the DPSP Cluster. Section 3 shortly describes the research and innovation challenges and approach of the cluster actions and projects. Section 4 is showing the synergies among the cluster actions and projects in the form of maps from the point of view of research, innovation, technologies and standards. The Section 5 concludes the document with the explanation of future work of the Cluster.

2. Following the R&I challenges defined by H2020 WP 2016-2017

The cluster gathers representatives of projects and actions funded by the European Commission under the H2020-LEIT-ICT, FP7-Collaboration-ICT, and CIP-ICT-PSP programmes. These projects and actions are addressing diverse research and innovation (R&I) challenges as described in the project proposal calls, respectively ICT-07-2014 - Advanced Cloud Infrastructures and Services[1], ICT-09-2014 - Tools and Methods for Software Development[2], ICT-32-2014 - Cybersecurity, Trustworthy ICT[3], ICT-2013.1.5 - Trustworthy ICT[4], ICT-2013.1.2 - Software Engineering, Services and Cloud Computing[5], ICT-2011.1.4 - Trustworthy ICT[6] and CIP-ICT-PSP.2013.1.1- Cloud of public services[7]. For details on the addressed challenges see the project and action descriptions from the next section.

The clustered projects are covering a multitude of topics around security, data protection and privacy of both Cloud services and applications and services based on Cloud services. The new H2020 Work Programme (WP) for 2016-2017 identifies a number of hot topics around security, privacy and data protection that future projects will need to address. Even if these aspects are horizontal to all topics in the WP, not only to those related to Cloud computing, the Cluster has identified the following main topics from the WP in which R&I on Data Protection, Security and Privacy in the Cloud may have room:

Table 1. H2020 Work Programme 2016-2017 topics where R&I on Data Protection, Security and Privacy in the Cloud may have room.

H2020 Work Programme 2016-2017 topic
ICT-06-2016: Cloud Computing • Trust, security and privacy in decentralised cloud infrastructures and across multiple cloud providers, including aspects of data integrity, data localisation and data confidentiality.
DS-01-2016: Assurance and Certification for Trustworthy and Secure ICT systems, services and components Assurance: • Reliability and safety assurance at individual phases of the SDLC • Reliability and quality development and validation of highly dynamic systems Security Certification:

[1] https://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/290-ict-07-2014.html
[2] https://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/285-ict-09-2014.html
[3] https://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/273-ict-32-2014.html
[4] http://cordis.europa.eu/programme/rcn/18677_en.html
[5] http://cordis.europa.eu/programme/rcn/18712_es.html
[6] http://cordis.europa.eu/programme/rcn/16700_en.html
[7] http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/fp7/calls/cip-ict-psp-2013-7.html

- Emerging threats, compositional certification and reuse of components in the context of certified systems and certification throughout the operational deployment of a product or a service.
- Reduce the cost and duration of the certification process.

DS-02-2016: Cyber Security for SMEs, local public administration and Individuals

DS-03-2016: Increasing digital security of health related data on a systemic level

- Secure storage of information including personal data, safe exchange of data over a number of architectures of differing security levels preventing unauthorised access, loss of data and cyber-attacks.

DS-04-2016: Economics of Cybersecurity

- Cybersecurity cost-benefit framework
- Incentives and business models:

DS-05-2016: EU Cooperation and International Dialogues in Cybersecurity and Privacy Research and Innovation

DS-06-2017: Cryptography

- Flexible encryption beyond partial homomorphic encryption
- Anonymization, obfuscation, etc.
- Ultra-lightweight cryptology & anonymity in communications
- Authenticated encrypted token research for mobile payment solutions and related applications.
- Innovative cryptographic primitives and complementary non-cryptographic privacy-preserving mechanisms to enforce privacy at various levels (e.g. pairing based cryptography).
- New techniques, e.g. quantum safe cryptography
- Quantum key distribution
- Automated proof techniques for cryptographic protocols.

DS-07-2017: Addressing Advanced Cyber Security Threats and Threat Actors

- Detection and response against sophisticated, target, multi-faceted attacks over (critical) cyber infrastructures.
- Anomaly detection, visualisation tools, big data analysis, threat analysis, deep-packet inspection, protocol analysis, forensics, etc. + interdisciplinary research.

DS-08-2017: Privacy, Data Protection, Digital Identities

Privacy-enhancing Technologies (PET) :

- Privacy Risks Management Framework

General Data Protection Regulation in practice:

- Assist organisations to implement the GDPR

Secure digital identities:

- Evidence based Ids (correlation of soft proofs of Id)
- Pseudonyms
- Verification of mobile Id docs
- Leverage existing European electronic identification and authentication platforms

With the aim to jointly work towards the identification of future research challenges and trends, the clustered projects have identified a number of key areas of research and innovation around security, data protection and privacy. These key areas will be considered in the following of the document to classify the projects' contributions and generate the map of synergies. The key areas are:

- **Methodologies:** Security and privacy methodologies and tools for security and privacy-aware engineering of cloud services and cloud-based services and applications. These include security-by-design and privacy-by-design techniques as well as security and privacy requirements engineering, modelling and policy management.

- **Encryption:** Encryption mechanisms and all other cryptographic techniques that help in ensuring integrity, confidentiality, and other data protection objectives.

- **Data Security**: Models, methods and tools for defining, implementing or ensuring data security as general concept, including data integrity, confidentiality, protection, privacy, ownership, location, retention, processing.

- **Federated systems:** Models, methods and tools to enable security and privacy-aware federated systems.

- **Security technologies**: Technologies, systems and tools that support security and privacy in services and systems.

- **System compliance:** Models, methods and tools for specifying and ensuring or enforcing system compliance, including accountability, certification and standardisation.

- **Risk management:** Models, methods and tools for managing cyber risks.

- **Legal and social security:** Models, methods and tools for supporting legal and social aspects of cyber security, including raising awareness, education, building trust, economics of cyber security, etc.

The key areas above help in classifying the different topics of interest for starting the collaboration between the cluster members for identification of common research interests and potential gaps. This will allow the establishment of new initiatives between the specialists involved in the cluster. A secondary goal is to help the initiatives which will respond to the H2020 Work Programme 2016-2017 call to easily identify the actions and projects that are currently working on the topics of interest and to build on top of their results if possible.

3. R&I challenges as defined by the cluster actions

3.1 APPHUB

General information:
Project name: APPHUB - The European Open Source Marketplace.
Call: H2020-ICT-2014-1, Topic: ICT-07-2014 - Advanced Cloud Infrastructures and Services, Type: Coordination and Support Action (CSA), Duration: 2 years (started on 1st Jan, 2015), Web site: http://www.apphub.eu.com

AbbHub consortium comprises the Fraunhofer Institute for Open Communication Systems (coordinator, software design and development), OW2 (open source community (community building and dissemination), and UShareSoft (technology provider, software design and development, platform operator). Web site:

Aim:

Open source software is the generic name for both a legal construct to share intellectual property and an approach to cooperative software development. While this approach has demonstrated its ability to produce world-class software, the potential benefits and efficiencies of open source are not, however, always achieved, indeed, far from it. In particular, many collaborative research projects that put their results under an open source license fail to deliver software that is useful for the European economy (a) due to quality issues resulting from the lack of proper open source project governance, and (b) due to the lack of a sustainable community that develops this software further after the end of the project. The CSA AppHub has been created to help open source projects implement more efficient community and market outreach strategies, and to provide guidelines and best practices to improve software production processes and to produce high quality software.

Approach:

The aim of the AppHub project is to support the market outreach strategies of EU-supported open source by launching AppHub, the European open source market place. AppHub is a service platform that will help the market to seamlessly identify, position and implement the software outcomes of these projects. The partners that will develop, run and promote AppHub over this two-year project and beyond combine unparalleled expertise in open source community management, EU research projects and a breakthrough technology in software asset management.

AppHub will be based on three interrelated services:

- The AppHub Directory allows placing software assets as part of a reference architecture and thus identifying rapidly ways to compose various open source assets into a service architecture.
- The AppHub Factory lets users build and maintain full software stacks as templates using a visual "point and click" interface or APIs.
- The AppHub Marketplace provides users with self-service access to pre-packaged business and IT applications via a customizable, white-labelled app store, and to deploy them in various cloud infrastructures.

Expected impact:

- Better connect EU-supported open source projects with users. The AppHub marketplace will reduce barriers to open source adoption and will make it easy for potential users and integrators to deploy and run the software produced by EU-supported open source projects on many different cloud service providers' platforms.
- Improved market readiness and reputation of EU-supported open source projects. AppHub will provide EU-supported projects with a full service support that will make them better prepared for market acceptance.
- Stronger EU community to support the growth of EU-supported open source project. AppHub will improve community support for EU-supported open source projects and for EU-generated open source software in general.
- Build global visibility and build market position of EU-supported open source projects. AppHub will help enhancing the global recognition of EU open source projects through improved community support, better open source management of open source projects, and greater ease of access to the software. EU-generated open source software in general promoted through AppHub will gain greater visibility and a better market position.

3.2 CLARUS

General information:
Project name: CLARUS - A framework for user centred privacy and security in the cloud.
Call: H2020-ICT-2014-1, Topic: ICT-07-2014 - Advanced Cloud Infrastructures and Services, Type: RIA, Duration: 3 years (started on 1st Jan, 2015), Web site: http://clarussecure.eu

Aim:
Although cloud computing offers many benefits to its users, security issues such as confidentiality and privacy are still major concerns to those intending to migrate to the cloud. Current security mechanisms are commonly located within the cloud platform, hence compelling customers to trust cloud providers. However, customers might be reluctant to outsource sensitive data due to lack of control over its storage and management. 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.

The main objective of the CLARUS project is to build trust in cloud computing services by developing a secure and privacy-preserving framework for outsourcing sensitive data to honest-but-curious clouds and processing these data in the cloud using the cloud's computational resources. CLARUS will allow end users to monitor, audit and control the stored data without impairing the functionality and cost-saving benefits of cloud services. Enhancing privacy, security and trust of end users with respect to the cloud providers is the main focus of the CLARUS project.

Approach:
CLARUS will take a holistic security-by-design approach that views security as a system property that must be continuously managed during the whole lifetime cycle of a system. Moreover, in order to achieve transparency in the way data are processed by all involved parties, the developed protocols will be the object of standardisation efforts. In addition, the CLARUS solution must be compliant with and support current and future European data protection legislation.

The CLARUS solution is envisioned as a proxy located in a domain trusted by the end user (e.g., a server in her company's intranet, a plug-in in the user's device) that implements security and privacy-enabling features towards the cloud service provider.

- 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.
- CLARUS will rely on and innovate 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 anonymisation, 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.).
- 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.

- 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.

In this way, the user's privacy, security and trust can be significantly enhanced with respect to current cloud security solutions both regarding honest-but-curious cloud providers and potential attackers (insiders as well as outsiders), while still preserving cloud functionalities, and within the Platform-as-a-Service (PaaS), Infrastructure-as-a-Service (IaaS) and Software-as-a-Service (SaaS) models.

Expected impact:
The beneficiaries of the CLARUS solution will be potential cloud customers like companies, public organisations and e-government administrations, which could thereby be motivated to embrace the benefits of trusted cloud services while retaining full control over any potentially sensitive data they outsource to the cloud. Cloud providers will also benefit from an agnostic trust-enabling solution like CLARUS that will open new market opportunities with a broader range of users.

A customer category comes from the healthcare sector, which will gain from more transparent standardised auditable and controllable cloud services. CLARUS will offer security and privacy-enabling mechanisms to ensure that the patient records are properly protected before outsourcing to the cloud service provider. This means they can now leverage the full capabilities of cloud computing for processing and storing medical records while preserving the privacy of the patients' data.

In the long term, initiatives like CLARUS can pave the way to developing more transparent, standardised, auditable and controllable cloud services, which will be beneficial for all stakeholders.

3.3 CREDENTIAL

General information:
Project name: CREDENTIAL – Secure Cloud Identity Wallet

Call: H2020-DS-2014-1, Topic: DS-02-2014 Access Control, Type: IA, Duration: 3 years (started on 1st Oct, 2015), Web site: https://credential.eu

Aim:
CREDENTIAL aims on developing, testing, and showcasing innovative cloud-based services for storing, managing, and sharing digital identity information and other highly critical personal data with a demonstrably higher level of security and privacy than other current solutions. This is achieved by advancing novel cryptographic technologies and improving strong authentication mechanisms.

Digital identity management (IdM) is an essential tool for managing access to information technology (IT) resources and is an enabler for seamless interaction between systems, organizations, and end users. In order to be fully and broadly accepted, IdM must involve secure identification and authentication processes and protect users' privacy. This is especially true for high-assurance application domains such as e-Business, e-Government, or e-Health.

Identity management is currently experiencing a paradigm shift towards cloud computing that has shaped the ICT world during recent years. By now, numerous IdM systems and solutions are available as cloud services, providing identity services to applications operated both in closed domains and in the public cloud. This service model is often referred to as Identity (and Access) Management as a Service (IDMaaS). However, no satisfactory approaches currently exist which allow the storage and sharing of identity data by service providers in a privacy preserving manner – meaning without the identity provider learning the credentials and associated data.

The vision of CREDENTIAL is to fill this gap and develop a more trustworthy solution by combining secure and efficient identity management technologies with cryptography for cloud computing. Users will be able to store identity data in a cloud-based IDMaaS system of an identity provider such that the confidentiality and authenticity of the data is upheld even from the provider.

Approach:
CREDENTIAL intends to combine novel cryptography for data sharing, the cryptography being already mature from a research perspective but not yet commercially available, with strong multi-factor authentication into a novel class of privacy preserving cloud based identity management systems and bring them to market-readiness. The overall development effort is embedded in accompanying tasks for holistic security treatment and user-friendliness, as well as for business and exploitation planning. The developed tools will be intensely tested and evaluated in different relevant application do-mains to guarantee maximal impact and commercial grade tools as CREDENTIAL outcome.

The approach of CREDENTIAL is subsequently illustrated based on the following goals, which are all equally important to bring the vision of CREDENTIAL to reality:

Adapt and improve cryptographic methods to securely store and share identity data in the cloud:

Identity providers, secure storage vaults etc. that are sharing personalized data currently have unlimited access to the raw data. The idea of CREDENTIAL of being able to securely store and process identity data in the cloud in terms of advanced sharing with relying parties in the contest of identity management is to make use of proxy cryptography and in particular proxy re-encryption. Proxy re-encryption is an encryption

scheme, which allows third parties to transform ciphertexts, which are encrypted for a certain user, so that they can be decrypted by another user. This means that cloud identity providers can store and re-encrypt data, which was encrypted by a user, for a certain relying party without getting access to the data itself. With this approach, the benefits of cloud computing can be exploited for identity management in a privacy-preserving way.

Protect access to identity data with strong authentication mechanisms:

The release of (identity) data by cloud providers to relying parties must be protected by user authentication. Due to usability reasons, state-of-the-art mechanisms are based on simple password schemes. The main focus of CREDENTIAL is on strong authentication mechanism employing multiple factors suitable for 'authentication to the cloud'. A strong focus will be on hardware-based approaches, be it hardware located on the server (HSM) or built-in hardware security modules in local or mobile devices.

Development of a user-friendly and portable system for identity data access and management:

CREDENTIAL will follow a security by design concept and develop a secure architecture in a comprehensive and holistic approach. Usability and user requirements are elicited and considered right from the start and included into the whole design and development cycle. Security complexities will be hidden at most as possible from the user and users should be able to access and manage their cloud identity wallet from everywhere with the possibility to use different strong authentication mechanisms.

Creation of enabling technologies for cloud service providers and identity data consumers:

The main work of CREDENTIAL consists of advancing novel technology and its integration into holistic security models and making it usable for cloud identity management. On the application layer, where entities (identity provider, relying party, etc.) communicate with each other, the exchange of encrypted identity data must be supported. Here existing protocols, standards and solutions will be analysed and assessed if and to which extend the existing protocols can be enhanced or can be used out-of-the-box for the exchange of encrypted identity data.

Transfer of project results into market-ready identity management technologies and standards:

To evaluate and validate the capabilities of CREDENTIAL tools and bring developed components to market-readiness, CREDENTIAL will setup piloting scenes for e-Government solutions, e-Health services and e-Business applications. All these domains handle very sensitive data. They are collecting, storing and manipulating personalised identity data of third parties – often citizens – to provide better and more efficient services for them. CREDENTIAL will showcase in its pilots how added value to these services ca be generated by protecting personalized data accordingly.

Expected impact:
According to the great importance and current relevance of the project goals, CREDENTIAL expects significant impact in many areas. CREDENTIAL will enable a new class of security and privacy preserving identity services in the cloud with a demonstrably higher level of security, compared to current identity services.

CREDENTIAL is expected to produce impact through the development of next generation identity management services:

- to achieve beneficial impact in society, industry, and research in Europe,
- in accordance with the European Cloud Computing Strategy and the European strategy on identity management;

- to remove a major inhibitor against cloud adoption in security relevant domains (in almost all domains, but especially to citizens' private data)
- by developing cloud based identity services which preserve more privacy for citizens,
- for delivering input and strengthening the position of European industries in the tough competition with non-European market leaders,
- to strengthen European innovation capabilities in a highly competitive field.

3.4 ESCUDO-CLOUD

General information:
Project name: ESCUDO-CLOUD - Enforceable Security in the Cloud to Uphold Data Ownership.
Call: H2020-ICT-2014-1, Topic: ICT-07-2014 - Advanced Cloud Infrastructures and Services, Type: RIA, Duration: 3 years (started on 1st Jan, 2015), Web site: http://www.escudocloud.eu

Aim:
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, all CSPs apply security measures in the services they offer, but these measures either assume full trust in the CSP and allow it to have full access to the data, or greatly limit the functionality that the CSP is able to offer in accessing the outsourced data.

ESCUDO-CLOUD will provide protection guarantees giving the data owners both full control and cloud functionality for their data in the cloud.

Approach:
ESCUDO-CLOUD develops modular solutions and tackles the security problems from different angles and perspectives. In particular, it considers four dimensions that help in defining the challenges to be tackled: security properties (confidentiality, integrity, availability); sharing requirements (access by data owners, selective sharing with other users/owners); access requirements (upload/ download, fine-grained retrieval, write operations); cloud architectures (single cloud provider, multi cloud and federated cloud).

These dimensions, with their different configurations, correspond to different scenarios and challenges to be addressed. ESCUDO-CLOUD will tackle these issues and challenges with a gradual approach and will provide modular techniques and tools that can be applied as needed in different environments. In particular, ESCUDO-CLOUD will guide the structure of the work based on sharing requirements and cloud architectural assumptions (which define the three main scenarios of reference, addressed in the technical work packages of the project) and, within them, it will investigate how to guarantee security properties and satisfy access requirements.

Expected impact:
ESCUDO-CLOUD will be beneficial to both data owners and CSPs. Data owners will be enabled to outsource their data while maintaining control over them, with the ability to regulate access to them and share them with other users in a selective way and with assurance that their data will remain protected from the CSPs. Data owners will then be able to rely on CSPs and use their services for a wider range of applications. This will benefit both companies as well as individual users.

CSPs will significantly benefit, in addition to the increased market penetration that robust data ownership would provide, from reduced regulatory risks, audit costs, and general security threats that they would have to face in the absence of such protection. Freeing providers from the worries of protecting data, ESCUDO-CLOUD will allow them to even handle the data outside their own control. For instance, it will enable a provider itself to rely on other services for outsourcing storage and computation, behaving as a broker providing a virtualised cloud service, without worrying about the possible improper exposure of user information, which is guaranteed to be self-protected. This will benefit both larger as well as smaller players in the market.

3.5 MUSA

General information:
Project name: MUSA - MUlti-cloud Secure Applications.
Call: H2020-ICT-2014-1, Topic: ICT-07-2014 - Advanced Cloud Infrastructures and Services, Type: RIA, Duration: 3 years (started on 1st Jan, 2015), Web site: www.musa-project.eu, Reference publication: [1].

Aim:
The most challenging applications in heterogeneous cloud ecosystems are those that are able to maximise the benefits of the combination of the cloud resources in use: multi-cloud applications. They have to deal with the security of the individual components as well as with the overall application security including the communications and the data flow between the components.

The main objective of MUSA is to support the security-intelligent lifecycle management of distributed applications over heterogeneous cloud resources, through a security framework that includes: security-by-design mechanisms to allow application self-protection at runtime, and methods and tools for the integrated security assurance in both the engineering and operation of multi-cloud applications.

Approach:
The MUSA framework leverages security-by-design, agile and DevOps approaches in multi-cloud applications, and enables the security-aware development and operation of multi-cloud applications.

MUSA approach combines i) a preventive security approach, promoting Security by Design practices in the development and embedding security mechanisms in the application, and ii) a reactive security approach, monitoring application runtime to mitigate security incidents, so multi-cloud application providers can be informed and react to them without losing end-user trust in the multi-cloud application.

The MUSA framework will be composed of:

1. MUSA IDE: an IDE for creating the multi-cloud application taking into account its security requirements together with functional and business requirements,

2. MUSA security libraries: a set of security mechanisms embedded in the multi-cloud application components for self-protection at runtime,

3. MUSA Decision Support Tool + deployer: an automated deployment environment that, based on an intelligent decision support system, will allow for the dynamic distribution of the components according to security needs, and

4. MUSA Security Assurance Platform: a software platform in form of a SaaS that will support multi-cloud application runtime security control and transparency to increase user trust.

Expected impact:
The main impacts of MUSA can be summarize as:

- Improve the competitive innovation capacities of European cloud sector by providing multi-cloud application developers and operators (particularly SMEs) with the MUSA security framework which includes open source tools to enable the security-intelligent and integrated lifecycle management of multi-cloud applications.

- Reduce the data security incidents in multi-cloud applications through the assurance of a secure behaviour of individual cloud-based components and the overall application, even if the data are processed and/or stored by untrustworthy or opaque cloud providers.
- Enhance cloud consumers' trust on clouds by providing them with tools for expressing their security needs and keeping them informed on the security and performance faults of the multiple cloud services in use.
- Boost the adoption of clouds even in advanced applications that use sensitive data, through the demonstration that cloud security risks can be minimized by using MUSA tools.

The project will demonstrate and evaluate the economic viability and practical usability of the MUSA framework in highly relevant industrial applications representative of multi-cloud application development potential in Europe.

3.6 PAASWORD

General information:
Project name: PAASWORD - A Holistic Data Privacy and Security by Design Platform-as-a-Service Framework Introducing Distributed Encrypted Persistence in Cloud-based Applications.
Call: H2020-ICT-2014-1, Topic: ICT-07-2014 - Advanced Cloud Infrastructures and Services, Type: RIA, Duration: 3 years (started on 1st Jan, 2015), Web site: http://paasword.eu

Aim:
Although enterprises recognize the compelling economic and operational benefits of running applications and services in the Cloud, security and data privacy concerns are the main barriers in Cloud adoption. PaaSword aims at fortifying the trust of individuals and corporate customers in cloud services and increasing the adoption rate of cloud-based solutions. The focus is on safeguarding both corporate and personal data for cloud infrastructures and storage services.

Approach:
As the most critical target for attacks is the data persistency layer and the database itself. PaaSword introduces a holistic data privacy and security by design framework with main aim to protect users' sensitive data stored in the cloud. The framework is based on a searchable encryption scheme enhanced with sophisticated context-aware access control mechanisms. An innovative approach for key management maximizes customers' control over their data. PaaSword extends the Cloud Security Alliance's cloud security principles by capitalizing on recent innovations on (a) distributed encryption and virtual database middleware technologies that introduce a scalable secure Cloud database abstraction layer combined with sophisticated distribution and encryption methods into the processing and querying of data stored in the Cloud; (b) context-aware access control that incorporate the dynamically changing contextual information into novel group policies implementing configurable context-based access control policies and context-dependent access rights to the stored data at various different levels; and (c) policy governance, modelling and annotation techniques that allows application developers to specify an appropriate level of protection for the application's data, while the evaluation of whether an incoming request should be granted access to the target data takes dynamically place during application runtime.

The implementation of enterprise security governance in cloud environments is supported by a novel approach towards context-aware access control mechanisms that incorporate dynamically changing contextual information into access control policies and context-dependent access rights to data stored in the cloud. Finally, PaaSword supports developers of cloud applications through code annotation techniques that allow specifying an appropriate level of protection for the application's data.

Expected impact:
PaaSword directly addresses one of the most critical issues with security of cloud technologies. The main results of PaaSword will be:

- PaaSword holistic framework
- Reference architecture
- Searchable encryption scheme for secure queries
- Policy access & context-aware security models
- Policy enforcement middleware
- Dedicated IDE plug-in
- PaaSword demonstrators

Thus, PaaSword maximizes the trust of individuals and corporate customers in cloud applications and services, as well as enhances the ability of the European software and Cloud Computing industry to deliver

them. It enables European enterprises to unlock valuable business, economic and operational benefits of migrating to the cloud. PaaSword will accelerate the adoption of Cloud Computing and further improve the competitive position of cloud providers. Five demonstrators will prove PaaSword's potential through their integration in industrial, real-life services and applications in the context of PaaS, Public sector, Logistics chain, CRM and ERP related use cases.

3.7 PRISMACLOUD

General information:
Project name: PRISMACLOUD - PRIvacy and Security MAintaining services in the CLOUD
Call: H2020-ICT-2014-1, Topic: ICT-32-2014 - 2014 - Cybersecurity, Trustworthy ICT, Type: RIA, Duration: 3,5 years (started on 1st Feb, 2015), Web site: https://prismacloud.eu/

Aim:
Building security and privacy into cloud services "by design" and as core functionalities rather than as a wrapper or add-on. Through the integrated use of cryptography it shall enable customers from domains with high security requirements to profit from a movement of their applications and data to the cloud.

The PRISMALCOUD project is dedicated to the development of methods and tools to increase the security of cloud based services as well as technologies to increase the privacy of users interacting with the cloud.

The PRISMACLOUD team identified several challenges in current cloud systems and service offerings, which effectively stand against the deployment of sensitive data and applications to the cloud. These challenges include information security concerns, like (1) the still not sufficiently solved problem of protecting the confidentiality of data at rest over its life-cycle in the cloud, (2) the problem of verifiability of operations and calculations delegated to the cloud, and (3) the threat of users losing their privacy if moving to cloud based services. To address these challenges, a set of suitable cryptographic primitives was chosen or proposed by the applicants of the project, and three applications in real-world use cases selected for demonstrating the feasibility of the approach.

Approach:
We want to provide a synthesis of existing work, of the results of related (European) research projects, and of original research results provided by the PRISMACLOUD consortium, yielding software and service platforms for the implementation of a wide range of security enabled cloud applications and services. We will evaluate the applicability with the implementation of three demonstrators in the fields of smart city, eHealth, and eGovernment. The project specifically addresses the European Cloud Computing Strategy and complements its research and development program with activities for the dissemination of results into standardisation. The approach in PRISMACLOUD is user centered in all its aspects and tries to protect user data from end-to-end.

The project will provide reference implementations, plus accompanying research results in the fields of cryptographic research in cloud crypto primitives, human computer interaction, certification, and cybercrime analysis of opportunities in connection with secure cloud systems which could be adopted by a broad user basis after the project.

Expected impact:
The PRISMACLOUD consortium includes cloud and infrastructure providers which are interested to deploy applications and services based upon PRISMACLOUD technology.

The main idea and ambition of PRISMACLOUD is to enable end-to-end security for cloud users and provide tools to protect their privacy with the best technical means possible - by cryptography.

To make this idea come true PRISMACLOUD comprises following fields of core innovations:

- Verifiability of data and infrastructure use
- User privacy and anonymisation
- Securing data at rest

- Secure and efficient implementations
- Methodology, tools and guidelines for fast adoption

3.8 SLA-READY

General information:
Call: H2020-ICT-2014-1, Topic: ICT-07-2014, Type: CSA, Duration: 2 years (started on 1st Jan, 2015), Web site: http://sla-ready.eu

Aim:
Today, whilst many organisations are reliant on cloud resources, contracts for cloud services often contain Service Level Agreements (SLAs) with technical & legal provisions that are inappropriate, difficult to understand &/or illegal. Similarly, the application of established data protection concepts can be problematic, with uncertainties as to what is regulated, who is responsible & which laws apply. Building on the work conducted by Standard Developing Organisation (SDOs), SLA-Ready is a new European initiative that aims to deliver a reference model for Cloud SLAs & a set of best-practices & services to support cloud customers in the use of cloud SLAs through their life cycle. SLA-Ready implements a service-driven approach specifically designed for SMEs. The SLA-Ready service approach will support SMEs with practical guides, and a social marketplace, which encourages them to carefully plan their journey and make it strategic through an informed, stepping-stone approach, so the cloud and applications grow with their business.

Approach:
The project will create the two distinct and concrete outcomes: the reference model for SLAs and a set of digital services to support cloud customers in the use and reasoning of SLAs.

The SLA-Ready reference model will be developed by: (i) identifying common sector-specific requirements (functional, non-functional, security, data protection, legal, and business), (ii) analysing the cloud SLA landscape (research and industrial initiatives at both EU and international levels), and, (iii) integrating the feedback obtained through the SLA-Ready Advisory Board and early adopters. Furthermore, SLA-Ready will engage and ensure coordinated, global collaborations with relevant SDOs to guarantee that both the contributed reference model is well-aligned with (upcoming) best practices and, its international approach is endorsed and accepted.

A set of services (created through synergies with other EU projects and instantiated through the SLA-Ready Social Marketplace) will be provided by SLA-Ready to support cloud customers in assessing, selecting, negotiating and monitoring cloud services based on their business requirements, risk profile and budget. Reference model and services will be offered through the sla-ready.eu portal and will be complemented with a series of tutorials targeting cloud customers (including SMEs) to stimulate the wider uptake and awareness of SLA-Ready's common reference model.

Expected impact:
The project will improve the uptake of cloud by the European private sector, especially SMEs. Firms will benefit from a social market place, tutorials-as-a-service, decision-making services and practical guides supporting the entire SLA life cycle. The SLA-Ready Common Reference Model will benefit the industry by integrating a set of SLA components, e.g. common vocabularies, SLO service metrics and measurements, as well as best practices and relevant standards to fill identified gaps in the current SLA landscape.

3.9 SPECS

General information:
Project name: SPECS - Secure Provisioning of Cloud Services based on SLA management.
Call: FP7-ICT-2013-1, Topic: Trustworthy ICT, Type: STREP, Duration: 2,5 years (started on 1st Nov, 2013), Web site: www.specs-project.eu, Reference publication: [2]

Aim:
The Cloud offers attractive options to migrate corporate applications without the corporate security manager needing to manage or secure any physical resources. While this "ease" is appealing, several security issues arise, typical examples are: (i) access of unauthorized CSP personnel to data residing remotely with the Cloud Service Provider (CSP), (ii) assessment of a CSP's ability to meet the corporate security requirements, (II) comparison of security trades-offs offered by different CSPs or the capability for a customer to monitor and enforce the agreed Cloud security levels with the CSP. SPECS aims at offering a solution for such problems, offering mechanisms to specify Cloud security requirements and assess the standalone and comparative security features offered by CSPs and offering the ability to integrate desired corporate security services into Cloud services. SPECS offers systematic approaches to negotiate monitor and enforce the security parameters specified in Service Level Agreements (SLA) and to develop and deploy security services that are "Cloud SLA-aware", implemented as an open-source Platform-as-a-Service (PaaS).

Approach:
SPECS offers an open source framework to offer Security-as-a-Service, by relying on the notion of security parameters specified in Service Level Agreements (SLA) and providing the techniques to systematically manage their life-cycle. The SPECS framework addresses both CSP's and users to provide techniques and tools for:

- Enabling user-centric negotiation of security parameters in Cloud SLA, along with a trade-off evaluation process among users and CSPs, in order to compose Cloud services fulfilling a minimum required security level.
- Monitoring in real-time the fulfillment of SLAs agreed with CSPs, notifying both users and CSPs, when a SLAs are not being fulfilled.
- Enforcing agreed SLA in order to keep a sustained Quality of Security (QoSec) that fulfills the specified security parameters. SPECS' enforcement framework will also "react and adapt" in real-time to fluctuations in the QoSec by advising/applying the requisite countermeasures.

The proposed framework has an open-source core, and offer simple interfaces to motivate its adoption. It will offer a set of reusable PaaS components for service developers to enable them to integrate SPECS' SLA-oriented security mechanisms into existing Cloud services. Using real case studies SPECS demonstrates that the SPECS framework and architecture can be integrated "as-a-Service" into real life Cloud environments, with a particular emphasis on small/medium CSPs and end users.

Expected impact:
SPECS Security SLA Model relies on the actual Cloud and SLA standards and the SPECS Consortium actively engages with the standardization bodies and participates in the process of building the SLA standards. SPECS framework can help a larger adoption and diffusion of standardized security SLAs and to the definition of standard security metrics. SPECS approach enable End-users to compare CSPs in terms of security properties, in such a way it helps End-users to be aware of the choice done and helps in increasing the trust in the adoption of the cloud paradigm. SPECS framework was adopted to produce a Security Metric Catalogue, which aims at collecting existing and novel security metrics, representing them in a standard format.

3.10 TREDISEC

General information:
Project name: TREDISEC - Trust-aware, REliable and Distributed Information SEcurity in the Cloud.
Call: H2020-ICT-2014-1, Topic: ICT-32-2014 - Cybersecurity, Trustworthy ICT, Type: RIA, Duration: 3 years (started on 1st Apr, 2015), Web site: www.tredisec.eu

TREDISEC is a European collaborative Research and Innovation Action funded by the H2020-ICT-2014-1, ICT-32-2014 programme of the European Commission under grant agreement no. 644412. In this project, started on April 1st 2015, nine renowned research institutions and industrial players with balanced expertise in all technical aspects of both security and cloud are working together for fulfilling the challenges of the project: Atos Spain (project coordinator), NEC Europe, IBM Research, ETH Zurich, Eurecom, Arsys Internet, Greek Research and Technology Network, SAP SE and Morpho (SAFRAN group).

Aim:
From a practical standpoint, the ambition of this project is to develop systems and techniques that make the cloud a secure and efficient place to store data. We plan to step away from a myriad of disconnected security protocols or cryptographic algorithms, and to converge instead on a (possibly standardized) unified framework where resulting primitives are integrated, while following the end-to-end security principle as closely as allowed by functional and non-functional requirements.

Approach:
The advent of cloud storage and computation services however comes at the expense of data security and user privacy. To remedy this, customers nowadays call for end-to-end security whereby only end-users and authorized parties have access to their data and no-one else. In the TREDISEC project, we address this problem and we develop systems and techniques which make the cloud a secure and efficient heaven to store data.

More specifically, TREDISEC addresses the confidentiality and integrity of outsourced data in the presence of a powerful attacker who controls the entire network. In addition, our proposed security primitives support data compression and data deduplication, while providing the necessary means for cloud providers to efficiently search and process encrypted data.

TREDISEC leverages existing or novel cryptographic protocols and system security mechanisms, which offer strong data confidentiality, integrity and availability guarantees while permitting efficient storage and data processing across multiple tenants.

Expected impact:
TREDISEC aims at creating technology that will impact existing businesses and will generate new profitable business opportunities long after the project is concluded.

Requirements for the technical work build upon two premises, contributing to providing a higher level of security and/or privacy, at marginal additional cost compared to traditional ICT technology. First, the security primitives adopted should require no changes in the user applications and minimum changes in the component encrypting client data, making it easier to integrate into current systems. Second, the adopted solutions should enable the cloud to process data efficiently enough to maintain its client-base, and to scale well for large amounts of data and users.

We argue that the results of TREDISEC will have a big impact in business (both large companies and SMEs), allowing them to achieve greater business throughput and lowering the barriers to enter new markets. Notice that we are fully aware of the problem of adoption of new technologies by companies and

believe that TREDISEC will cover at least three of the top five barriers: security, data protection, trust, data access, and portability

3.11 WITDOM

General information:
Project name: WITDOM - empoWering prIvacy and securiTy in non-trusteD envirOnMents.
Call: H2020-ICT-2014-1, Topic: ICT-32-2014 - 2014 - Cybersecurity, Trustworthy ICT, Type: RIA, Duration: 3 years (started on 1st Jan, 2015), Web site: http://witdom.eu/

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

WITDOM puts particular focus in data-outsourcing scenarios, where new threats, vulnerabilities and risks due to new uses require end-to-end security solutions that will withstand progress for the lifetime of applications they support.

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

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

Approach:
WITDOM will deliver the following products:

- The WITDOM framework, aligned with concurrent projects and advancing the SoTA. The WITDOM E2E framework acknowledges the following aspects:
    - Driven by Privacy by Design (PbD) principles, holistic, E2E privacy/ security time-resistant, efficient solutions & guarantees.
    - Methods to quantify information leaked in traces left by crypto primitives to achieve sufficient & adequate privacy levels
    - New trustworthiness-enhanced business models for exploitation, supporting Data Protection (DP) law, leading to reduce the need for trust in third parties.
- The WITDOM platform, based on a global privacy-and-security-by-design architecture for secure outsourced processing of sensitive data, adapted to different Cloud platforms.
- An integral toolkit featuring:
    - Privacy enhancing techniques, perturbation mechanisms and privacy metrics
    - Cryptographic privacy techniques supporting encrypted processing
    - Cryptographic techniques for integrity and verifiability of outsourced processes
- Two prototypes in the project scenarios: eHealth and Financial Services
- A methodology and metrics to quantifiably evaluate the end-to-end privacy levels achieved

Expected impact:
The project will demonstrate and validate the WITDOM framework and overall approach in in two practical and privacy-sensitive scenarios

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

Besides these domain-specific demonstrators, WITDOM's platform and protection components can be leveraged in many other privacy-sensitive domains (e.g. smart cities), scaled to address big data scenarios enabling novel privacy-enhanced business models.

4. Maps

4.1 Research point of view

The following table identifies in which key research areas the projects have worked or are currently working on. These key areas are those identified by the Cluster members around security, data protection and privacy, as explained in the introductory section.

	MUSA	CLARUS	ESCUDO-CLOUD	SPECS	PRISMACLOUD	WITDOM	TREDISEC	PaaSword	AppHub	SLA-READY	CREDENTIAL
Methodologies											
Security-by-design methods	X	X			X		X	X			X
Privacy-by-design methods/tools and PET	X	X			X	X	X	X			X
Security models and policies	X	X	X	X	X		X	X		X	X
Privacy models and policies	X		X	X	X		X	X		X	X
Security requirements specification	X		X	X				X		X	X
Privacy requirements specification	X	X	X	X		X		X		X	X
Encryption											
Homomorphic encryption		X			X	X	X				
End-to-End Encryption		X	X	X	X	X	X				X
Cryptography		X			X	X	X	X			X
Lightweight Encryption							X				
Proxy Re-Encryption											X
Quantum cryptography											
Anonymization		X			X	X					
Data security											
Data integrity	X	X	X		X	X	X			X	X
Data confidentiality	X	X	X		X		X	X		X	X
Data protection	X	X	X	X	X		X	X		X	X
Data privacy	X	X	X		X	X	X	X		X	X
Data ownership		X	X		X		X	X		X	X
Data location	X			X				X		X	
Data retention	X									X	
Data processing						X				X	
Data authenticity											X

	MUSA	CLARUS	ESCUDO-CLOUD	SPECS	PRISMACLOUD	WITDOM	TREDISEC	PaaSword	AppHub	SLA-READY	CREDENTIAL
Federated systems											
Security interoperability		X					X	X			X
Privacy interoperability		X						X			X
Federated access control		X		X			X				X
Public private partnership											
Security technologies											
Security negotiation				X			X				
Software vulnerability detection				X			X				X
Web Security				X				X			
(secure) Digital identities				X			X				X
Security-by-design tools	X	X			X		X	X			X
Privacy-by-design tools	X	X			X			X			X
Forensics tools											
Security monitoring tools	X	X		X							
Intrusion detection systems		X		X							
Intrusion prevention systems				X							
Automated security management	X	X		X							
SIEM (Security Information and Event Management)				X							
Machine readable security SLAs	X			X							
System compliance											
Compliance	X			X						X	X
Accountability					X		X			X	
Trustworthiness of CSP	X		X	X	X					X	X
Security certification					X					X	X
Privacy certification					X					X	
Security standardisation		X		X	X					X	X
Privacy standardisation		X		X	X					X	X
Informed consent											X
Security SLA	X			X						X	
Security assurance	X			X	X						
Security metrics	X	X	X	X						X	

	MUSA	CLARUS	ESCUDO-CLOUD	SPECS	PRISMACLOUD	WITDOM	TREDISEC	PaaSword	AppHub	SLA-READY	CREDENTIAL
Risk management											
Information sharing				X							X
Risk management	X										
Threat analysis	X						X				X
Incident reporting	X										
Cyber attacks				X			X				
Cyber-incidents simulation											
Privacy disclosure											
Privacy metrics						X					
Legal and social security											
Raising awareness	X	X		X	X		X			X	X
Confidence building (Trust)	X	X		X	X		X			X	
Legal framework		X				X				X	
NIS education and training											
Forensic methodologies											
Secure internet for children											
Cyberdefense					X						
Transparency about security	X	X		X	X		X			X	X
Preventing mass-surveillance/censorship							X				
Security economics	X			X							
International cooperation									X		

4.2 Examples of contributions

The following table identifies concrete examples of which are the projects' contributions in the key areas identified around security, data protection and privacy.

CLUSTERED PROJECTS' CONTRIBUTIONS	
Methodologies	
Security-by-design methods	• MUSA offers a MUSA IDE that allows specifying the security properties of multi-cloud applications in both the application model and the Service Level Agreement (SLA) model. The specification language is a CloudML extension. • PRISMACLOUD will investigate how the developed cryptographic tools could be integrated into design methodologies and propose security patterns for secure cloud services. • CLARUS views security as a system property that must be continuously managed during the whole lifetime cycle of a system. • PaaSword: Privacy & Security-by-design framework for Platform-as-a-Service: code annotation techniques, searchable encryption schemes, context-aware authorization and access control, XACML extensions, novel key management mechanism, IDE-plugin. • CREDENTIAL: A security by design concept will be reached through the translation of privacy principles into privacy targets, which are part of the security risks assessment that will also be conducted as part of the privacy and security design.
Privacy-by-design methods/tools and PET	• MUSA offers a MUSA IDE that allows specifying the security properties of multi-cloud applications in both the application model and the Service Level Agreement (SLA) model. The specification language is a CloudML extension. The specification can include privacy properties. • PRISMACLOUD: Provides and advances tools like malleable and functional signatures which can be used as PET to provide similar features like anonymous credentials. • CLARUS implements a set of privacy tools relate to mechanisms that preserve the confidentiality of transmitted or stored data. • PaaSword: Privacy & Security-by-design framework for Platform-as-a-Service: code annotation techniques, searchable encryption schemes, context-aware authorization and access control, XACML extensions, novel key management mechanism, IDE-plugin. • CREDENTIAL develops advanced solutions to data minimization following the privacy by design paradigm and the use of privacy enhancing technologies (PETS)
Security models and policies	• MUSA offers a Security SLA generator tool for multi-cloud applications that enables the creation of SLAs that include security and data protection controls in the SLA related to the controls required over the Cloud Service Providers in use. • MUSA offers a CloudML based modelling tool that enables the creation of multi-cloud application specifications that include security and data protection requirements. • SPECS offers a Security SLA Model in order to represent and quantitatively evaluate the Level of security of a

	service and/or of a Cloud Service Provider. • ESCUDO-CLOUD provides models and policies for enabling secure and private information sharing in the cloud. • PRISMACLOUD will further develop existing holistic security models and make them applicable for secure service composition in the cloud. • CLARUS defines and use a set of Security Policies to determine the type of operations and computation on the data, thus allowing defining how to protect the outsourced datasets. • PaaSword: ontological context-aware security models and access policies • SLA-Ready accounts for security policies from Standardised aspects of cloud Service Level Agreements for the definition of requirements meant to serve the SLA Common Reference Model. • CREDENTIAL: Holistic security models are developed aiding the composition of cryptographically secure building blocks into cloud identity and Access management services that fully use the potential of the underlying cryptoraphic primitives.
Privacy models and policies	• MUSA offers a Security SLA model based on SPECS model that also includes privacy terms (see below). • SPECS offers a Security SLA Model in order to represent and quantitatively evaluate the Level of security of a service and/or of a Cloud Service Provider. It includes privacy terms. • ESCUDO-CLOUD provides models and policies for enabling secure and private information sharing in the cloud. • As far as anonymisation is concerned, CLARUS relies on vertical splitting to enable computations in the cloud. It will also use other models (k-anonymity, etc.) when compatible with the operations to be performed on the cloud. • PaaSword: ontological context-aware security models and access policies. • SLA-Ready accounts for privacy policies from Standardised aspects of cloud Service Level Agreements for the definition of requirements meant to serve the SLA Common Reference Model. • CREDENTIAL will innovate by applying privacy features such as data minimization to identity management solutions by the help of cryptographic technologies to enable application also in the cloud domain.
Security requirements specification	• MUSA offers an extended CloudML language that enables the specification of security and data protection requirements of (multi-)cloud based applications. • SPECS Offers a Security SLA negotiation methodology that helps to specify security requirements. • ESCUDO-CLOUD supports a rich set of security and privacy requirements from large storage and service providers as well as from small companies and data owners, producing comprehensive solutions with actual deployment in real operational environments. • PRISMACLOUD uses the French EBIOS tool for the threat and risk assessment; PRISMACLOUD writes a Security Target according to Common Criteria ISO/EN 15408 for a selected technology. • PaaSword: Risk modelling process based on OWASP and STRIDE threat classification. • SLA-Ready: Security requirements are considered for the definition of SLA terms and SLOs in the SLA Common Reference Model. • CREDENTIAL: Specific CREDENTIAL tasks will focus on non-functional security requirements for the CREDENTIAL core components and subsequent security analysis from the perspective of the different stakeholders involved in the reference use-cases
Privacy requirements specification	• MUSA offers an extended CloudML language that enables the specification of security and data protection requirements of (multi-)cloud based applications. It includes some privacy requirements. • SPECS Offers a Security SLA negotiation methodology (which includes privacy terms) that helps to specify privacy requirements. • ESCUDO-CLOUD supports a rich set of security and privacy requirements from large storage and service providers as well as from small companies and data owners, producing comprehensive solutions with actual

	deployment in real operational environments. • WITDOM: Definition of the SPACE methodology for requirements elicitation, combining the PRIPARE project's with the co-creation methodology. • CLARUS works in different scenarios when a data owner organisation owning data can specify the privacy requirements, in which way outsourced data should be stored and processed, and who has the right to access and operate on the data. • PaaSword: Risk modelling process based on OWASP and STRIDE threat classification. • SLA-Ready: Privacy requirements are considered for the definition of SLA terms and SLOs in the SLA Common Reference Model. • CREDENTIAL will elicit legal, socio-economic and technical privacy requirements for cloud identity management technologies.
Encryption	
Homomorphic encryption	• WITDOM: o Use of BGV/YASHE (RLWE) for typical polynomial ops o Use of other encryption schemes and problems (LTV, NTRU-based) for efficiency o SHE and/or Hardware assisted FHE o Homomorphic encryption/decryption engine (ring LWE) • CLARUS implements a Homomorphic Encryption (HE) module. Provided with the description of the operation, the module picks the most suitable encryption scheme and stores the metadata needed to carry out the encryption and decryption correctly in a dedicated database.
End-to-end encryption	• SPECS Offers End-to-end Encryption security mechanisms. • PRISMACLOUD wants to introduce several crypto primitives which provide full end-to-end security and do not have to rely on trust assumptions regarding intermediary cloud providers. • CLARUS implements a Storage with encryption module that takes as input the data to be encrypted and uploaded and the access policy that specifies which party can retrieve it from the CSP. The Module runs in the end-user trusted domain. • CREDENTIAL aims on end-to-end encrypted and secured federated identity management solutions in heterogeneous distributed environments with advanced sharing capabilities
Cryptography	• MUSA offers cryptographic libraries that can be embed in the multi-cloud applications to enforce data encryption when needed. These libraries are based on existing open source solutions. • WITDOM: Cryptographic dynamic data masking. • PRISMACLOUD: The project proposes about ten cryptographic primitives to address (1) the still not sufficiently solved confidentiality of data at rest over its life-cycle in the cloud, (2) the problem of verifiability of operations and calculations delegated to the cloud, and (3) the threat of the predominant user privacy disaster in many commercially available cloud services. • CLARUS relies on cryptographic techniques to preserve and operate on the data. • PaaSword: Searchable encryption schemes. • CREDENTIAL will improve appropriate cryptographic mechanisms to resolve privacy concerns and put the user in control of her identity data – instead of the cloud service provider.
Lightweight encryption	-
Proxy Re-Encryption	• CREDENTIAL will improve proxy cryptograpyh and especially proxy re-encryption mechanisms, enabling cloud providers to process identity data – without being able to inspect or access the processed identity data in plain

	text.
Quantum cryptography	-
Anonymization	• WITDOM: o Generalization: k-anonymity, l-diversity, t-closeness. o Data Obfuscation o Randomization: noise addition, permutation. o Differential privacy mechanisms o Non cryptographic data Masking • PRISMACLOUD will provide advanced (efficient) algorithms for the k-anonymization of large sets of data (100M records) • CLARUS implements dedicated modules to store, search and compute over anonymised data.
Data security	
Data integrity	• MUSA provides techniques and tools for ensuring the data integrity requirements are fulfilled in multi-cloud applications. • ESCUDO-CLOUD provides techniques ensuring the integrity of data and computations. • WITDOM: Protocol for verifying the integrity and consistency for untrusted cloud differential privacy. • PRISMACLOUD proposes a cryptographic primitive for the use of malleable signatures which allow controlled modification (or redaction) of certain parts of cryptographically signed data without the signature losing its validity. • CLARUS ensures data integrity • SLA-Ready considers use cases requiring data integrity property for capturing the Service Level Objective (SLO) requirements of the Common Reference Model • CREDENTIAL will develop and improve efficient cryptographic techniques and methods to protect integrity of identity data in the cloud.
Data confidentiality	• MUSA provides techniques and tools for ensuring the data confidentiality requirements are fulfilled in multi-cloud applications. • ESCUDO-CLOUD provides techniques for ensuring the protection of data confidentiality. • PRISMACLOUD relies on information theoretically secure algorithms for secure storage in a partially trusted multi cloud environment (Secret Sharing) which support passive and active adversaries. • CLARUS ensures data confidentiality. • PaaSword: Mechanisms against data theft: data only processed based on user approval and key provision. • SLA-Ready considers use cases requiring data confidentiality property for capturing the Service Level Objective (SLO) requirements of the Common Reference Model • CREDENTIAL: CREDENTIAL will develop and improve efficient cryptographic techniques and methods to protect confidentiality identity data in the cloud.
Data protection	• MUSA provides techniques and tools for ensuring the protection of data in multi-cloud applications. • SPECS Offers Security mechanisms that supports data-protection SPECS Applications devoted to Storage Services has security mechanisms devoted to Data protection. • ESCUDO-CLOUD provides techniques ensuring self-protection of data at a reduced cost in terms of computational resources, auxiliary storage and latency when accessing data. • PRISMACLOUD implements several crypto primitives to protect confidentiality, integrity, and availability of data in multi cloud environments.

	• CLARUS ensures data protection. • PaaSword: Distributed and encrypted data storage (SQL & NoSQL). • SLA-Ready considers use cases requiring data protection property for capturing the Service Level Objective (SLO) requirements of the Common Reference Model related to processing sensitive data • CREDENTIAL will develop and improve efficient cryptographic techniques to securely protect data especially with respect to confidentiality, integrity, and authenticity.
Data privacy	• MUSA provides techniques and tools for ensuring the data privacy requirements are fulfilled in multi-cloud applications. • ESCUDO-CLOUD provides usable techniques enabling data owners to use services of CSPs for storing, managing or processing data in the cloud while enjoying data security and privacy. • PRISMACLOUD uses anonymous credentials do minimise data exposure during transactions. • CLARUS ensures data privacy • SLA-Ready considers use cases requiring data privacy property and legal aspects for capturing the Service Level Objective (SLO) requirements of the Common Reference Model related to processing sensitive data • CREDENTIAL follows well-established data privacy principles such as data minimization based on selective or minimum disclosure.
Data ownership	• ESCUDO-CLOUD provides effective and deployable solutions allowing data owners to maintain control over their data when relying on CSPs for data storage, processing, and management. • CLARUS ensures data ownership of the outsourced dataset(s) a user has created. The user is allowed to modify permissions of the other users on his/her outsourced dataset(s). • PaaSword: Data only processed based on user approval and key provision. • SLA-Ready considers use cases requiring data ownership property and derived legal aspects for capturing the Service Level Objective (SLO) requirements of the Common Reference Model related to processing sensitive data • CREDENTIAL aims on putting the user under maximum control of her identity data and access to non-encrypted data is only possible by respective authorization.
Data location	• MUSA provides techniques and tools for ensuring the data location requirements are fulfilled in multi-cloud applications. • SPECS supports a geoLocation security metric. SPECS Application devoted to Next generation data Center has mechanisms devoted to manage Data location related issues. • PRISMACLOUD will provide tools for strong and dependable encryption of end-user data in multi cloud environments, rendering the selection of data location irrelevant. • PaaSword: Placement and geolocation-aware access policies. • SLA-Ready introduces a data location Service Level Objective (SLO) as important requirement of the Common Reference Model related to processing sensitive data related to processing sensitive data
Data retention	• MUSA provides techniques and tools for ensuring the data retention requirements are fulfilled in multi-cloud applications. • SLA-Ready considers a data retention period for the data in the definition of the SLO requirements of the Common Reference Model to guarantee law enforcement access.
Data authenticity	• CREDENTIAL will develop and improve efficient cryptographic techniques and methods to protect the authenticity of identity data in the cloud.
Federated systems	

Security interoperability	• CLARUS enables the coordination of multiple CLARUS proxies to provide collaborative services. APIs based on standards can be made available to programmers for a seamless development of end-user cloud-based applications. • PaaSword: Compliance with our generic ontological context-aware security and access control models. • CREDENTIAL will consider different levels of assurance for exchanging identity in a secure and interoperable manner.
Privacy interoperability	• CLARUS enables the coordination of multiple CLARUS proxies to provide collaborative services. APIs based on standards can be made available to programmers for a seamless development of end-user cloud-based applications. • PaaSword: Compliance with our generic ontological context-aware security and access control models. • CREDENTIAL will consider different levels of assurance for exchanging identity in a privacy-preserving and interoperable manner.
Federated access control	• SPECS AAAaaS application supports solution for federated access control. • PRISMACLOU provides a robust access controls system tailored for secret sharing based storage in a cloud-of-cloud setting. • CLARUS might support interoperable authentication mechanisms such as a Federated ID framework • CREDENTIAL will provide the technical foundations to enable end-to-end encrypted and secured federated identity management solutions in heterogeneous distributed environments with advanced sharing capabilities not available today.
Public private partnership	-
Security technologies	
Security negotiation	• SPECS offers an independent module (SPECSMOnitoring Core) devoted to Security SLA Negotiation.
Software vulnerability detection	• SPECS offers a SVA (Software Vulnerability Assessment) security mechanism and proposes a set of security metrics associated to it. • CREDENTIAL will report on the assessment of vulnerabilities present in federated IAM systems in general and the CREDENTIAL system in particular.
Web security	• SPECS offers a Secure Web Container application which supports development of Secure Web applications.
(secure) Digital identities	• SPECS AAAaaS application enables and supports OAUTH. • PRISMACLOUD provideS cloud crypto primitives for strong anonymity and pseudonymity. • The vision of the CREDENTIAL consortium is to develop, test, and showcase innovative cloud-based services for storing, managing, and sharing digital identity information and other highly critical personal data with a demonstrably higher level of security than other current solutions.
Security-by-design tools	• MUSA provides an IDE for specifying in the multi-cloud application design the security aspects and for allowing embedding in the application security mechanisms that will be activated at runtime when needed. • CLARUS implements a set of security-by-design tools that preserve integrity and confidentiality of the transmitted data. Security is viewed as a system property that must be continuously managed during the whole lifetime cycle of a system. • CREDENTIAL aims to improve security and privacy technologies, i.e. cryptographic primitives, protocols and authentication mechanisms, to be used as a toolbox for the building blocks of next-generation cloud identity data encryption services designed within CREDENTIAL.

Privacy-by-design tools	• MUSA provides an IDE for specifying in the multi-cloud application design the privacy aspects and for allowing embedding in the application privacy mechanisms that will be activated at runtime when needed. • CLARUS implements a set of privacy tools relate to mechanisms that preserve the confidentiality of transmitted or stored data. • CREDENTIAL aims to improve security and privacy technologies, i.e. cryptographic primitives, protocols and authentication mechanisms, to be used as a toolbox for the building blocks of next-generation cloud identity data encryption services designed within CREDENTIAL.
Forensic tools	• PRISMACLOUD: several tools by PRISMACLOUD have a secondary use in cloud forensics (e.g. graph signatures for virtual infrastructures). A publication on this is pending.
Security monitoring tools	• MUSA offers a multi-cloud application monitoring service within the MUSA Security Assurance Platform (SaaS). • SPECS offers an independent module (SPECS Monitoring Core) devoted to monitor the security levels granted to customers. • PRISMACLOUD: see forensics tools • CLARUS implements a Monitoring module to ensure that the framework is attack-tolerant
Intrusion detection systems	• SPECS offers a security mechanisms devoted to Intrusion detection and protection • CLARUS uses a set of intrusion detection techniques to detect potential attacks.
Intrusion prevention systems	• SPECS offers a security mechanisms devoted to Intrusion detection and protection
Automated security management	• MUSA Security Assurance Platform is able to continuously monitor the behaviour of the multi-cloud applications and automatically activate security and privacy enabling mechanisms in the multi-cloud applications when needed. • SPECS SLA Platform and Core Services offers a fully automated solution to secure a cloud service according to a Security SLA. • CLARUS implements automated management of Security Policies via the Security Policy Management module that defines different protection rules based on the data type and the underlying data/communication protocols for each dataspace.
SIEM (Security Information and Event Management)	• SPECS offers an independent module (SPECS Monitoring Core) which acts as collector of information for a SIEM.
Machine readable security SLAs	• MUSA offers a Security SLA model that enables the composition of Security SLAs. This Security SLA is based on SPECS Security SLA. • SPECS offers a machine readable format, according to WS-Agreement, for representing and automate the management of Security SLAs.
System compliance	
Compliance	• MUSA Security Assurance Platform enables the verification of Security SLA fulfilment at runtime for multi-cloud applications. • SPECS Security SLAs are based on standard Security controls and help to verify the compliance of a Service/CSP to standard security baselines. • SLA-Ready considers the definition of privacy compliance metrics in the definition of the requirements of the SLA Common Reference Model • During the last project phase CREDENTIAL considers to push project results in standardization and compliance frameworks.
Accountability	• SLA-Ready considers the CSP accountability term for the definition of the requirements of the SLA Common Reference Model

Trustworthiness of CSP	• MUSA Decision Support Tool allows the selection of CSPs for multi-cloud applications. The selection is based on security requirements stated in the Security SLA and a match-making process of those requirements with the CSP's self-assessment information and other sources of information of CSP offerings. MUSA Security Assurance Platform will allow at operation the verification of the fulfilment Security SLA. • SPECS Offers tools to compare and evaluate CSPs according to their self-assessment security information. SPECS Platform, integrated into a CSP helps in offering services protected by Security SLAs, improving the trustworthiness among CSC and CSP. • ESCUDO-CLOUD provides solutions for measuring and comparing the security guarantees offered by different providers in terms of confidentiality, integrity, and compliance with SLAs. • SLA-Ready offers tools via the CSA STAR Registry to compare the capabilities of the CSPs • CREDENTIAL aims to develop and improve cryptographic technologies to be used even if the CSP cannot be considered fully trustworthy (honest but curious). •
Security certification	• PRISMACLOUD fosters the integration of results of the project to be integrated into the EuroCloud Star Audit methodology and maybe others. • SLA-Ready identifies the importance of having security certification. • CREDENTIAL considers the integration of project results into appropriate cloud security methodologies or standards.
Privacy certification	• SLA-Ready identifies the importance of having privacy certification.
Security standardisation	• SPECS actively contributes to standardization bodies and Security SLA models and terms are built according to the state-of-art standards. • PRISMACLOUD has a dedicated work item to disseminate project results into cloud security standards. A standards action plan will be elaborated. • CLARUS leverages the state-of-the-art security standards to implement an interoperable framework. • SLA-Ready contributes to standardisation bodies with Security SLA terms and models. • CREDENTIAL considers disseminating appropriate project results to relevant security standard activities.
Privacy standardisation	• SPECS actively contributes to standardization bodies and Security SLA models and terms are built according to the state-of-art standards. • CLARUS considers the state-of-the-art privacy standards to implement an interoperable framework. • SLA-Ready contributes to standardisation bodies with Privacy SLA terms and models. • CREDENTIAL considers disseminating appropriate project results to relevant privacy standard activities.
Informed consent	• CREDENTIAL will pilot its results in e-Health scenarios, thus informed consent will performed whenever necessary.
Security SLA	• MUSA extends the Security SLA of SPECS with compositional features. The MUSA Security Assurance Platform is able to detect violations of such composite Security SLA. • SPECS offers a Security SLA Life Cycle and Model, a PaaS devoted to offer services according to the Security SLA life cycle and modules to automate negotiation, monitoring and enforcement of Security SLAs. • SLA-Ready introduces the use of terms to specify security and privacy policies.
Security assurance	• MUSA offers an integrated tool, the MUSA Security Assurance Platform (SaaS) that is able to monitor and enforce (at least partially) the secure behaviour stated in the Security SLA of the multi-cloud application. The Platform is also able to notify on imminent and detected violations of the Security SLA.

	• SPECS offers tools to help CSC and CSP to verify the security assurance through Security SLAs.
Security metrics	• MUSA extends the SPECS format of security metrics (see below) to include multi-cloud metrics. • SPECS offers a machine readable format, built according to existing standards, to represent security metrics. SPECS offers a Security Metrics catalogue API to manage collection of metrics and a Metric Catalogue Web Application to manage and store security metrics. • ESCUDO-CLOUD provides techniques and algorithms to perform security assessment based on the quantitative and qualitative analysis of security information. ESCUDO-CLOUD provides security metrics to allow users to reason about security risks and to assess the protection techniques and the compliance with Security and Privacy Level Agreements. • CLARUS monitoring module is focused on security and privacy preserving and is going to focus on keeping track on a set of defined metrics. • SLA-Ready considers a set of metrics to verify security and privacy compliance of Cloud Service Providers.
Risk management	
Information sharing	• Within CREDENTIAL personal and identity data is shared across different stakeholders in encrypted and privacy-preserving format only.
Risk management	• MUSA provides a Decision Support Tool (DST) that allows the selection of CSPs to deploy the multi-cloud application components. This DST first allows the definition of the risk profile of the multi-cloud application that will drive the CSP selection.
Threat analysis	• MUSA risk profile definition process in the Decision Support Tool (DST) is based on a threat analysis over the intangible and tangible assets that the multi-cloud application provider wants to protect. • PRISMACLOUD: A threat and risk analysis is carried out for a defined target of evaluation. • CREDENTIAL will perform appropriate threat analyses on CREDENTIAL cloud identity wallet technologies.
Incident reporting	• MUSA provides a Security Assurance Platform (SaaS) that enables the continuous monitoring of the security behaviour of multi-cloud applications and provides notifications of imminent and detected Security SLA violations.
Cyber attacks	• SPECS studies and lists cyberattack for the services covered by the Security SLA in SPECS Application, with special care to cyberattacks to web applications. • PRISMACLOUD will specifically assess the impact of potential illicit use or misuse of secure cloud infrastructures to foster, enhance, and promote cybercrime.
Cyber-incidents simulation	-
Privacy disclosure	-
Privacy metrics	• WITDOM: Entropy, Mean Square Error (MSE), k-anonymity, l-diversity
Legal and social security	
Raising awareness	• MUSA will provide a Guide on Security-intelligent lifecycle management of multi-cloud applications. • Adoption of Security SLAs, as proposed by SPECS and MUSA, raises the awareness of security risks and threat and of needs for security countermeasures. • PRISMACLOUD will analyse the potential impact of the proposed new secure cloud systems for end users. PRISMACLOUD will provide a hand-book on secure cloud usage for end users to enable sound decisions when entrusting most sensitive data in secure cloud services. • CLARUS promotes awareness creation of privacy risks, limitation of technological solutions and of the legal

	framework, and importance of standards in cloud computing via a dedicated set of actions. • SLA-Ready aims at raising awareness of the lack of a clear SLA framework for SMEs, in particular targeting privacy and security aspects in SLAs. The SLA-Ready service approach will support SMEs with practical guides, and a social marketplace, which encourages them to carefully plan their journey and make it strategic through an informed, stepping-stone approach, so the cloud and applications grow with their business. • CREDENTIAL will provide HowTo's and best-practice guidelines for IdM software producers and standard organizations facilitating the easy take-up of proxy cryptography.
Confidence building (Trust)	• MUSA Decision Support Tool allows the selection of CSPs for multi-cloud applications. The selection is based on security requirements stated in the Security SLA and a match-making process of those requirements with the CSP's self-assessment information and other sources of information of CSP offerings. MUSA Security Assurance Platform will allow at operation the verification of the fulfilment of the Security SLA. • SPECS Offers tools to compare and evaluate CSPs according to their self-assessment security information. SPECS Platform, integrated into a CSP helps in offering services protected by Security SLAs, improving the trustworthiness among CSC and CSP. • CLARUS is all about improving trust in cloud computing and securely unlocking sensitive data to enable new and better cloud services. • SLA-Ready will provide a set of services (created through synergies with other EU projects and instantiated through the SLA-Ready Social Marketplace) to support cloud customers in assessing, selecting, negotiating and monitoring cloud services based on their business requirements, risk profile and Budget, thus building confidence in cloud services.
Legal framework	• WITDOM: o Data Protection Directive and forthcoming Regulation o European Cyber Security Strategy and forthcoming Network Information Security Directive o OECD privacy principles o Convention 108 and forthcoming modernization o Specific regulation of scenarios o Article 29 Data Protection Working Party Opinions (i.e. Opinion 05/2014 on Anonymisation Techniques) • CLARUS analyses the current legal framework for data protection. • SLA-Ready analyses legal and sociological dimensions impacting the usage of cloud services. Moreover, it proposes a set of requirements in the definition of SLA terms to address the legal framework.
NIS education and training	-
Forensic methodologies	-
Secure internet for children	-
Cyberdefense	• PRISMACLOUD will specifically assess the impact of potential illicit use or misuse of secure cloud infrastructures to foster, enhance, and promote cybercrime.
Transparency about security	• MUSA provides a Security Assurance Platform (SaaS) that enables the continuous monitoring of the security behaviour of multi-cloud applications and provides notifications of imminent and detected Security SLA violations. MUSA also extends SPECS Security SLAs. • SPECS Security SLAs offers a clear and transparent way to represent security granted by CSPs to CSCs. • CLARUS sets out to change the mistrust in cloud computing by implementing standardised cloud services, and

	therefore, be transparent with regard to data management, privacy and security. In particular, via the CLARUS proxy, the user has full control of where her data are stored in the cloud, how they are protected and how computations are made on them. • SLA-Ready aims at providing a set of guidelines to SMEs and citizens to improve transparency about the provision of services with transparent security and privacy terms associated. • CREDENTIAL will provide appropriate mechanisms to ensure transparency on processed identity data to the user.
Preventing mass-surveillance/censorship	-
Security economics	• MUSA supports the selection of the combination of cloud services that best matches the multi-cloud application security, functional and business requirements, according to the priorities set by the multi-cloud application DevOps team and business managers. • SPECS Security SLAs enable multiple business models, based on the offerings of Security SLAs to Customers.
International cooperation	-

4.3 Innovation map

The following table identifies the innovative tools and technologies that are developed by the different clustered projects.

NOTE: The table does not provide the innovations from MUSA and CLARUS projects as these two projects have not started their results implementation yet.

TOOL/SERVICE NAME	BRIEF INFO	OPEN SOURCE (Y/N)	SUPPPORTED LICENSES (if open source)	COMMUNITY	PATENT	INTENDED MARKET	DATE OF RELEASE	LINK (URL)
PROJECT: SPECS								
SPECS SLA Platform	The SPECS SLA Platform is composed of a set of web applications that, run on top of an existing Platform-as-a-Service, enable the management of cloud services according to Security SLA life cycle	Y	Apache			Cloud Service Providers, Cloud Service brokers	Available	bitbucket.org/specs-team
SPECS SLA Negotiation	The SPECS SLA negotiation module is composed of a set of web applications that, run on top of SPECS SLA Platform, enable the negotiation of Security SLA	Y	Apache			Cloud Service Providers, Cloud Service brokers	Available	bitbucket.org/specs-team
SPECS SLA Enforcement	The SPECS SLA enforcement module is composed of a set of web applications that, run on top of SPECS SLA Platform, enable the implementation and remediation of Security SLA	Y	Apache			Cloud Service Providers, Cloud Service brokers	Available	bitbucket.org/specs-team
SPECS SLA Monitoring	The SPECS SLA monitoring module is composed of a set of applications that, run on top of SPECS SLA Platform and enable continuous monitoring of Security SLA	Y	Apache			Cloud Service Providers, Cloud Service brokers	Available	bitbucket.org/specs-team
SPECS Secure Web Container	This SPECS Application offers web continers over multiple CSPs secured through the SPECS Platform	Y	Apache			Cloud Service Providers, Cloud Service brokers	Available	bitbucket.org/specs-team

TOOL/SERVICE NAME	BRIEF INFO	OPEN SOURCE (Y/N)	SUPPPORTED LICENSES (if open source)	COMMUNITY	PATENT	INTENDED MARKET	DATE OF RELEASE	LINK (URL)
SPECS Secure Storage	This SPECS Application offers DBaaS over multiple CSPs secured through the SPECS Platform	Y	Apache, GPL			Cloud Service Providers, Cloud Service brokers	Available	bitbucket.org/specs-team
SPECS Security Metric Catalogue	This Application offers a REST API ad a Web Interface to manage a catalogue of standard security metrics	Y	Apache			Cloud Service Providers, Cloud Service brokers	April 2016	bitbucket.org/specs-team
SPECS Security Reasoner	This SPECS Application offers a solution to evaluate and compare CSPs according to their declarations in the CSA STAR repository	Y	Apache			Cloud Service Providers, Cloud Service brokers	Available	bitbucket.org/specs-team
SPECS and ViPER	This solutions integrates the SPECS Framework into the ViPER Storage controller and enable to manage next data center storage solutions acoording to Security SLAs					Cloud Service Providers, Cloud Service brokers	April 2016	
PROJECT: AppHub								
AppHub Open Souce Marketplace	The marketplace provides three interrelated services: The AppHub Directory allows placing software assets as part of a reference architecture and thus identifying rapidly ways to compose various open source assets into a service architecture. The AppHub Factory lets users build and maintain full software stacks as templates using a visual "point and click" interface or APIs. The AppHub Marketplace provides users with self-service access to pre-packaged business and IT applications via a customizable, white-labelled app store, and to deploy them in various cloud infrastructures.	N		EC funded projects, OW2 community, European industry engages in open source	N	European SMEs and public sector as main open source users	01/10/2016	https://directory.apphub.eu.com/

TOOL/SERVICE NAME	BRIEF INFO	OPEN SOURCE (Y/N)	SUPPPORTED LICENSES (if open source)	COMMUNITY	PATENT	INTENDED MARKET	DATE OF RELEASE	LINK (URL)
PROJECT: WITDOM								
Anonymization component	this component will introduce hide, perturb, generalize data, as well as possibly add new data in order to prevent identification of individuals based on attributes, and/or inference of real value of attributes.					Cloud-based services developers	2016	
Secure Signal Processing (SSP) component	Realizes signal processing operations of signals in an encrypted or obfuscated form in order to prevent disclosure or sensitive information while being processed					Cloud-based services developers	2016	
Cloud brokerage component	distributes data among private/public Clouds depending on the trust level of the user on these entities (from a privacy point of view). to prevent sensitive information from leaving a trusted domain					Cloud-based services developers	2016	
Recrypt box	HW-based Homomorphic encryption/decryption engine					Cloud-based services developers	2016	
SHE library	C++ Implementation of SHE					Cloud-based services developers	2016	
ConSec	Federated cloud security framework					Cloud-based services developers	2015	
CloudProof	cloud store consistency and end-to-end security framework					Cloud-based services developers	2015	
VICOS	Verification of integrity and consistency					Cloud-based services developers	2015	
Data masking and de-sensitisation component	Data masking and de-sensitisation					Cloud-based services developers	2016	
Protection Orchestrator	Responsible of orchestrating available protection mechanisms to protect data before leaving the					Secured Services Developers		

TOOL/SERVICE NAME	BRIEF INFO	OPEN SOURCE (Y/N)	SUPPPORTED LICENSES (if open source)	COMMUNITY	PATENT	INTENDED MARKET	DATE OF RELEASE	LINK (URL)
	trusted domain							
PROJECT: PRISMACLOUD								
Archistar (Secure Storage Network)	Software framework to build secure distributed cloud-of-clouds storage systems for archiving and file sharing.	Y	Not decided yet for final release.	NA	NA	Storage solution and infrastructure as a service providers.	Final: 2018	http://Archistar.at
FPE/OPE Library	Library for Format and Order Preserving encryption	N	NA	NA	Complex format-preserving encryption Scheme. US Patent Application Number: 14/296484, filed 6/5/14	Data security & privacy in various fields such as finance, healthier, etc.	February 2018	TBD
Anonymization Service	Service for anonymization of data	N	NA	NA	NA	Anonymization solution for eHealth and other Data providers.	Final: February 2018	TBD
P-IAM	Authentication, Authorization and Auditing OASIS SAML-based components based on open source (OpenAM) implementation which belongs to Federation Identity Managers technologies and which can be combined with PI Hub asset (i.e. use system specific user identifiers) to provide a privacy-protecting implementation of IAM for systems dealing with personal and/or sensitive information.	Y	CDDL 1.0	NA	NA	Identity Access Manager	NA	NA

TOOL/SERVICE NAME	BRIEF INFO	OPEN SOURCE (Y/N)	SUPPPORTED LICENSES (if open source)	COMMUNITY	PATENT	INTENDED MARKET	DATE OF RELEASE	LINK (URL)
	Single sign-on and federated authentication across multiple IT domains / organizations is supported. Different multi-factor authentication mechanisms are supported (strong authentication) both for mobile and web-based clients.							
ETRA Alert Monitoring	Tool developed in FP7 SECCRIT project able to correlate log and event information coming from ETRA Applications, Virtual Machines and other software systems	N		N/A	N/A	ETRA Alert Monitoring		NO
OSSEC	Host-based Intrusion Detection System. It has a correlation and analysis engine, integrating log analysis, file integrity checking, Windows registry monitoring, centralized policy enforcement, rootkit detection, real-time alerting and active response	Y	GNU General Public License (version 2)	OSSEC Github: https://github.com/ossec/ossec-hids	OSSEC			OSSEC Github: https://github.com/ossec/ossec-hids
PROJECT: PaaSword								
PaaSword Reference Architecture	PaaSword Reference Architecture, describing the main middleware components, mechanism and their interactions	Y				Cloud Carriers Cloud Service Developers Cloud Security Providers Other Cloud Stakeholders EU-funded research and innovation projects on Cloud	10/2015	
PaaSword Context-Aware Security Model	PaaSword Context-Aware Security Model, associating types of access to specific data objects and circumstances under which this should be allowed	Y				Cloud Service Providers Cloud Service Consumers Cloud Brokers Cloud Security	12/2015	

TOOL/SERVICE NAME	BRIEF INFO	OPEN SOURCE (Y/N)	SUPPPORTED LICENSES (if open source)	COMMUNITY	PATENT	INTENDED MARKET	DATE OF RELEASE	LINK (URL)
						Providers Other Cloud Stakeholders		
PaaSword Access Policies Model	PaaSword Access Policies Model, allowing the ontology-based description of both static and dynamically-generated context-based access control policies	Y				Cloud Service Developers Cloud Service Providers Cloud Service Consumers Cloud Brokers Cloud Carriers Public Administrations	12/2015	
Access Policies Management System	Access Policies Management System, allowing the PaaSword rule enforcement mechanism to use available access policies					Cloud Providers Public Administrations Cloud Security Providers	09/2016	
XACML-based Context-aware Policy Access Model	XACML-based Context-aware Policy Access Model, the PaaSword access model encompassing the Context-Aware Security and the Access Policies Model.	Y				Cloud Service Providers Cloud Service Consumers Cloud Brokers Cloud Carriers Public Administrations EU-funded research and innovations projects on Cloud Cloud Standardisation bodies	03/2016	
Key Management Mechanism	Key Management Mechanism, transparent key-usage mechanisms					Cloud Service Providers Cloud Service Consumers Cloud Brokers Cloud Security Providers	09/2016	

TOOL/SERVICE NAME	BRIEF INFO	OPEN SOURCE (Y/N)	SUPPPORTED LICENSES (if open source)	COMMUNITY	PATENT	INTENDED MARKET	DATE OF RELEASE	LINK (URL)
						Public Administrations		
Data Access Object Annotation Mechanisms and IDE plugin	Data Access Object Annotation Mechanisms and IDE plugin allowing the creation of object annotations according to the XACML-based model.					Cloud Service Developers	12/2016	
Data Access Object Annotation Interpreter						Cloud Service Developers	12/2016	
Data Access Object Annotation Governance and Validity Control mechanism						Cloud Service Developers Cloud Service Providers	12/2016	
PaaSword Policy Enforcement Business Logic						Cloud Service Developers	12/2016	
Searchable Encryption Scheme	Searchable Encryption Scheme, extending existing data store encryption schemes to support range queries					Cloud Service Developers Cloud Security Service Providers Public Administrations EU-funded research and innovation projects on Cloud Academic Audience	12/2015	
Distribution Algorithms and Encryption Schemes and Query Synthesis Mechanisms	Distribution Algorithms and Encryption Schemes and Query Synthesis Mechanisms, used for the implementation of a Virtual Database, suitable for both SQL and no-SQL databases and the execution of complex queries					Cloud Service Developers Cloud Service Providers Public Administrations EU-funded research and innovation projects on Cloud Academic Audience	12/2016	
Physical	Physical Distribution and					Cloud Service	12/2016	

TOOL/SERVICE NAME	BRIEF INFO	OPEN SOURCE (Y/N)	SUPPPORTED LICENSES (if open source)	COMMUNITY	PATENT	INTENDED MARKET	DATE OF RELEASE	LINK (URL)
Distribution and Encryption Mechanism	Encryption Mechanism, a complex encryption scheme using various, suitable encryption mechanisms for different columns, supporting the required queries					Developers Cloud Service Providers Public Administrations EU-funded research and innovation projects on Cloud		
PaaSword Data Privacy and Security by Design Framework		Y				Cloud Service Developers Cloud Security Providers Cloud Service Consumers Public Administrations Other Cloud Stakeholders EU-funded research and innovation projects on Cloud	09/2017	
Five PaaSword Demonstrators		N				Cloud Service Developers Cloud Security Providers Cloud Service Consumers Public Administrations Other Cloud Stakeholders End users of cloud based services/applications EU-funded research and innovation projects on Cloud	12/2017	
PaaSword		Y				Cloud Service	12/2017	

TOOL/SERVICE NAME	BRIEF INFO	OPEN SOURCE (Y/N)	SUPPPORTED LICENSES (if open source)	COMMUNITY	PATENT	INTENDED MARKET	DATE OF RELEASE	LINK (URL)
Methodology incl. adoption guidelines for practitioners						Developers Cloud Service Providers Cloud Security Providers Other Cloud Stakeholders EU-funded research and innovation projects on Cloud		

4.4 Technologies used within the projects

The following table identifies, for each project, which are the technologies used. [8]

	MUSA	CLARUS	ESCUDO-CLOUD	SPECS	PRISMACLOUD	WITDOM	TREDISEC	PaaSword	AppHub	SLA-Ready	CREDENTIAL
Cloud technologies											
CloudML											
Cloud Foundry											
VMWare				X					X		
XEN									X		
KVM				X					X		
OpenStack				X		X		X	X		
OpenNebula									X		
CloudStack									X		
Eucalyptus				X					X		
Chef				X		X					
Puppet						X					
Jclouds				X							
Libcloud											
DeltaCloud											
OSv											
RabbitMQ											
Intel SGX											
Vert.x (or ZMQ),											
Zookeeper											
Security technologies											
OpenVAS				X							
Nikto				X							
OpenSCAP				X							
CVE (Common Vulnerabilities and Exposure)				X							

- [8] MUSA and CLARUS projects have not started their results implementation yet.
- CREDENTIAL is currently evaluating the technologies to be used.

	MUSA	CLARUS	ESCUDO-CLOUD	SPECS	PRISMACLOUD	WITDOM	TREDISEC	PaaSword	AppHub	SLA-Ready	CREDENTIAL
OWASP ZAP				X							
OSSEC				X							
Alien Vault OSSIM											
SNORT				X							
BroIDS											
TOR											

4.5 Standards used and contributed to

The following table identifies the standards used by the different clustered projects and the ones contributed to. [9]The table follows the notation:

U = standard used in the project.

C = project results have contributed to the standard.

	MUSA		CLARUS		ESCUDO-CLOUD		SPECS		PRISMACLOUD		WITDOM		TREDISEC		PaaSword		AppHub		SLA-Ready		CREDENTIAL	
OGF																						
	U	C	U	C	U	C	U	C	U	C	U	C	U	C	U	C	U	C	U	C	U	C
OGF GFD.192 Web Services Agreement (WS-Agreement)							X															
OGF GFD.193 WS-Agreement Negotiation							X															
OGF OCCI																						
CSA																						
	U	C	U	C	U	C	U	C	U	C	U	C	U	C	U	C	U	C	U	C	U	C
CSA Cloud Control Matrix	X						X	X											X	X		
CSA Cloud Trust Protocol								X											X	X		
CSA Cloud Audit							X												X	X		
CSA Consensus Assessments Initiative Questionnaire							X	X											X	X		
CSA Privacy Level Agreement							X	X											X			
CSCC																						
	U	C	U	C	U	C	U	C	U	C	U	C	U	C	U	C	U	C	U	C	U	C
CSCC Practical Guide to Cloud Computing							X												X			
CSCC Public Cloud Service Agreements: What to Expect and What to Negotiate							X												X			
CSCC Security for Cloud Computing: 10 Steps to Ensure Success							X												X			
CSCC Practical Guide to Cloud Service Level Agreements							X												X			
CSCC Cloud Security Standards: What to Expect & What to Negotiate							X												X			

[9] No information on standards used and contributed to is given for:

- PRISMACLOUD project since this project has already identified several relevant standards from the given list for a potential use in the project—but owed to the fact that the project has only started in February 2015, it is not yet decided, which standards will effectively be regarded and referenced. As regards the dissemination of results into standards, a standards action plan is currently being developed but there were no decisions taken yet on the exact strategy for the dissemination. The PRISMACLOUD project has a dedicated work item to this goal.
- CLARUS project since this project has not yet started the implementation.
- CREDENTIAL is currently evaluating the standards to be used and where its results will be contributed to

	MUSA		CLARUS		ESCUDO-CLOUD		SPECS		PRISMACLOUD		WITDOM		TREDISEC		PaaSword		AppHub		SLA-Ready		CREDENTIAL	
IETF																						
	U	C	U	C	U	C	U	C	U	C	U	C	U	C	U	C	U	C	U	C	U	C
IETF(OAUTH Working Group) Web Authorization Protocol (OAuth).							X															
NIST																						
	U	C	U	C	U	C	U	C	U	C	U	C	U	C	U	C	U	C	U	C	U	C
NIST 800-53 Rev. 4: Security Controls	X						X															
NIST SP 80-145: The NIST Definition of Cloud Computing	X						X															
NIST SP 500-292: NIST Cloud Computing reference Architecture	X						X															
NIST RATAX	X						X	X											X			
ISO/IEC																						
	U	C	U	C	U	C	U	C	U	C	U	C	U	C	U	C	U	C	U	C	U	C
ISO/IEC 17788	X						X	X											X			
ISO/IEC 17789	X						X	X														
ISO/IEC 19086 (Part1,2,3,4)							X	X											X			
ISO/IEC 27004							X												X			
ISO/IEC 27017							X	X														
ISO/IEC 17826: Cloud Data Management Interface (same as SNIA CDMI)																						
ISO/IEC 17203: Open Virtualization Format (OVF) specification																						
DMTF																						
	U	C	U	C	U	C	U	C	U	C	U	C	U	C	U	C	U	C	U	C	U	U	U	U
DMTF DSP0263: Cloud Infrastructure Management Interface (CIMI) Model and REST Interface over HTTP Specification																						
DMTF DSP0264: Cloud Infrastructure Management Interface - Common Information Model (CIMI-CIM)																						
OASIS																						
	U	C	U	C	U	C	U	C	U	C	U	C	U	C	U	C	U	C	U	C	U	C	U	C
OASIS: Topology and Orchestration Specification for Cloud Applications (TOSCA)											X											
OASIS: Open Data Protocol																						
OASIS: Common Alerting Protocol (CAP) v1.2																						
OASIS: Identity Metasystem Interoperability (IMI) v1.0																						

	MUSA		CLARUS		ESCUDO-CLOUD		SPECS		PRISMACLOUD		WITDOM		TREDISEC		PaaSword		AppHub		SLA-Ready		CREDENTIAL	
OASIS: Key Management Interoperability Protocol Specification v1.2																						
OASIS: Security Assertion Markup Language (SAML) v2.0							X															
OASIS: Web Services Security v1.1.1							X															
OASIS: WS-Security Policy v1.3							X															
OASIS: WS-Trust v1.4																						
OASIS: WS-Reliability (WS-R) v1.1																						
OASIS: WS-Secure Conversation v1.4																						
ETSI																						
	U	C	U	C	U	C	U	C	U	C	U	C	U	C	U	C	U	C	U	C	U	C
ETSI CSC	X			X			X	X								X			X	X		

5. Conclusions and future work

This document describes the initial map of synergies among the projects participating in the Data Protection, Security and Privacy in the Cloud Cluster. The map is the first document born from the collaboration of the clustered projects. Although this initial version collects the contributions from only part of the projects in the cluster, it is expected that future versions will complete the map.

The clustered projects are pursuing collaboration towards getting greater impact of the projects. In this path, the first step is the identification of commonalities and gaps in the research carried out by the projects.

The document thus serves to set a common view of the on-going research aspects already covered by current initiatives. It is also expected that the document helps also outsiders of the Cluster to get the overall picture of the EU-funded research on cyber security, privacy and data protection aspects related to Cloud computing, both for Cloud technologies themselves and for services and systems that exploit them.

The map of synergies will constitute the basis for the identification of research gaps in the projects with respect to fully addressing the challenges set in current H2020 Work Programme 2016-2017 and beyond. In this line, the Cluster is also working in the elaboration of a Whitepaper on Future challenges of security and privacy research towards making the Digital Single Market a reality.

6. References

[1] Erkuden Rios, Eider Iturbe, Leire Orue-Echevarria, Massimiliano Rak, Valentina Casola: Towards Self-Protective Multi-Cloud Applications - MUSA - a Holistic Framework to Support the Security-Intelligent Lifecycle Management of Multi-Cloud Applications. CLOSER 2015 - Proceedings of the 5th International Conference on Cloud Computing and Services Science, Lisbon, Portugal, 20-22 May, 2015.SciTePress 2015, ISBN 978-989-758-104-5, pp 551-558

[2] M. Rak, N. Suri, J. Luna, D. Petcu, V. Casola, U. Villano, Umberto, Security as a Service Using an SLA-Based Approach via SPECS, Procs. 2013 IEEE 5th International Conference on Cloud Computing Technology and Science (CloudCom), vol.2, no., 1-6, 2-5 Dec. 2013