Service Level Agreement-based GDPR Compliance and Security assurance in (multi)Cloud-based systems

E. Rios[1], E. Iturbe[1], X. Larrucea[1], M. Rak[2], W. Mallouli[3], J. Dominiak[4], V. Muntés[5], P. Matthews[6], L. Gonzalez[7]

[1] Fundación Tecnalia Research & Innovation, Derio, Spain
[2] University of Campania Studies Luigi Vanvitelli, Naples, Italy
[3] Montimage Research & Development, Paris, France
[4] CA Technologies, Warszaw, Poland
[5] CA Technologies, Barcelona, Spain
[6] CA Technologies, Berkshire, UK
[7] FAST Lab., Tampere University of Technology, Tampere, Finland

* E-mail: erkuden.rios@tecnalia.com

Abstract: Compliance with the new European General Data Protection Regulation (Regulation (EU) 2016/679) and security assurance are currently two major challenges of Cloud-based systems. GDPR compliance implies both privacy and security mechanisms definition, enforcement and control, including evidence collection. This paper presents a novel DevOps framework aimed at supporting Cloud consumers in designing, deploying and operating (multi)Cloud systems that include the necessary privacy and security controls for ensuring transparency to end-users, third parties in service provision (if any) and law enforcement authorities. The framework relies on the risk-driven specification at design time of privacy and security level objectives in the system Service Level Agreement (SLA) and in their continuous monitoring and enforcement at runtime.

1. Introduction

The entry into force of the European General Data Protection Regulation (Regulation (EU) 2016/679, from now on GDPR) in May 2018 has definitively increased the concerns on better assuring privacy measures adopted by software systems. Privacy capabilities are intrinsically related to security capabilities in personal data processing information systems. Even the GDPR itself requires that personal identifiable information (PII) shall be *processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').* (Article 5.1(f)).

Therefore, there is a need to follow a holistic approach to risk assessment that addresses both privacy and security threats. This is even more challenging in (multi)Cloud-based systems because of the need of controlling not only system components' own risks but also those of the Cloud providers. Security, privacy and data protection continue to be major barriers to Cloud adoption [1]. The users' concerns on security and privacy of Cloud systems strive from the lack of trust, visibility and auditability of the privacy and security controls the Cloud providers offer in their services.

Since the arrival of GDPR, solving these issues is an urgent necessity for cloud consumers and providers acting as data processors or controllers, because the personal data processing principles in Article 5.1(a) 'lawfulness, fairness and transparency' and Article 5.2 'accountability' require systematic privacy assessment and evidence collection for assurance and transparency towards data subjects, collaborators in processing and supervisory authorities.

In this paper we propose a novel approach to ease assurance and transparency of Cloud-based systems by means of the use of Cloud Service Level Agreements (SLAs), which are defined as a *contract framework that defines the terms and conditions necessary to fulfil the obligations of a Cloud Service Provider (CSP) for the service(s) offered to a Cloud Service Consumer (CSC)* [2].

The paper presents our solution to SLA-based privacy and security assurance for (multi)Cloud applications, i.e. applications or services that use or have their components deployed in distributed Cloud services. The solution relies on the MUSA DevOps approach to enable the complete risk-driven life-cycle management of (multi)Cloud applications using SLAs. The advances brought include methods for the risk-driven selection of Cloud services to use, the automatic creation of the SLA offered by the application, and the continuous assurance at runtime of the security and privacy service level objectives specified in the SLA.

The solution presented is supported by the *MUSA framework* which is an open source integrated tool suit developed as the core result of the European Union's H2020 project MUSA [3] and is being extended with IoT privacy features in the European Union's H2020 project ENACT [4]. The work herein extends previous works [5] [6] by adding privacy SLA analysis and the full description of the risk assessment process and selection of cloud services in MUSA based on both security and privacy controls. The MUSA SecAP assurance tool [5] has also been extended with behaviour analysis and the solution validation included privacy controls.

The paper is structured as follows. Section 2 provides a review of the state of the art on Cloud SLAs usage for security and privacy assurance in Cloud systems. Section 3 introduces the complete MUSA methodology and framework for Security and Privacy SLA Assurance in (multi)Cloud-based systems. Section 4 presents the proposed risk-driven selection of Cloud services. Section 5 introduces the process to obtain the Composed SLA of (multi)Cloud-based applications. Section 6 presents the operational assurance methods proposed in the solution. Section 7 introduces the experimental results obtained in the validation of the methodology. Finally, Section 8 ends the paper with concluding remarks on the work and future lines of research.

2. Security and Privacy SLAs in Cloud

The standard ISO/IEC 20000-1 defines a Service Level Agreement (SLA) as a *documented agreement between the service provider and customer that identifies services and service level objectives* (SLOs). With the terms *Security SLA* and *Privacy SLA* or *Privacy Level Agreement* (PLA) we therefore respectively refer to the agreements that specify *security level objectives* and *privacy level objectives* offered by a service, which can be considered as part of an overall SLA or as complementary to agreements on other service level objectives, such as quality or performance SLOs.

In the Cloud Computing context, a Cloud SLA is a *contractual agreement between the Cloud Service Provider (CSP) and the Cloud Service Customer (CSC) specifying the security grants offered by the consumed Cloud service* [7]. The Cloud Security SLA and Cloud PLA would express respectively the *security policy* and *privacy policy* of Cloud services offered to CSCs. And a (multi)Cloud-based system would therefore offer a Security SLA and PLA that depend on the Cloud Security SLA and Cloud PLA of the Cloud services it uses.

2.1. Security Level Agreements in Cloud

The use of Cloud SLAs has been significantly explored in the last years with the aim of increasing trust in Cloud systems and facilitating their adoption. Recent projects such as SPECS [8], SLA-READY [9] and SLALOM [10] and guidelines such as CSCC's [11] have significantly advanced in Cloud SLA reference models and Cloud SLA life-cycle management systems.

Still the generation of (multi)Cloud-based system SLAs and their use for GDPR compliance and security assurance that we propose in our work remained as unresolved challenges so far. With our methodology we aim at starting the path towards full automation of security and privacy assurance in Cloud-based composite services.

An extract of the reference model of Cloud SLA we use in our approach is shown in Fig 1. The model is a derivation of the SPECS Security SLA model [12] where we have consolidated the concepts to embrace the privacy perspective, thus integrating Security SLA with PLA.

As shown in the model, an *SLA* defines the *Service Level Objectives (SLOs)* and associated *controls*. *Controls* ensure that the Cloud service's and/or the organisational CSP's *capabilities* satisfy the necessary *requirements* derived from the *policies*, which can range from regulations (like GDPR) to organisational policies or orders. The *SLOs* are expressed in terms of *metrics* to quantitative and unambiguously specify the capability levels guaranteed in the SLA. Therefore, Security SLAs associate to each service both the *security controls* that are implemented on top of it and the *Service Level Objectives (SLOs)* of the *security capabilities* of the service and its provider.

In our approach we adopt the NIST Security and Privacy Control Framework revision 5 Draft [13] to define the controls, which extends the previous version of the framework and defines, besides *security controls*, *privacy controls* that are specifically devoted to meet privacy requirements and to manage the privacy risks in an organisation, and *joint controls* that can meet privacy and security requirements at a time. Security controls are defined by NIST as *the safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information*, while privacy controls are *the administrative, technical, and physical safeguards employed within an agency to ensure compliance with applicable privacy requirements and manage privacy risks*.

NIST organises the controls in families, such as Access Control (AC), Identification and Authentication (IA), Risk Assessment (RA), System and Communications Protection (SC), System and Information Integrity (SI), etc. And a new Privacy Authorization (PA) family has been added.

The advantages of NIST over other security control frameworks for Cloud such as Cloud Security Alliance's

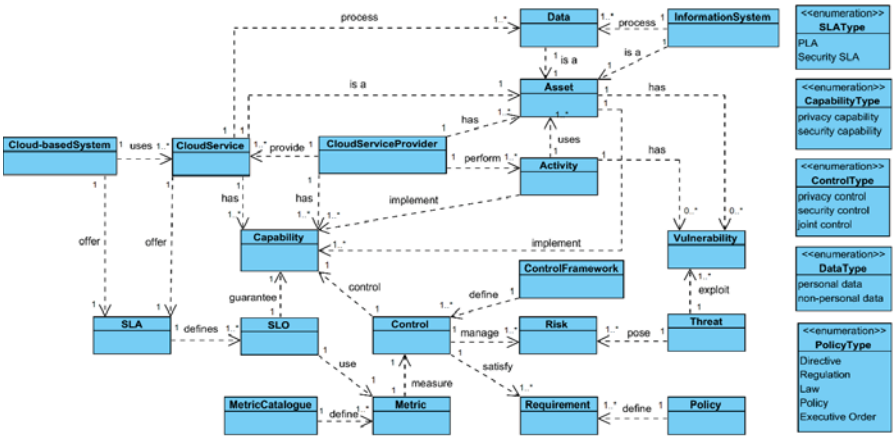

Fig. 1. *SLA model integrating PLA and Security SLA.*

Cloud Control Matrix (CCM) [14], ISO/IEC 27017 are its greater maturity, granularity of the controls and the integration of privacy and security controls.

The MUSA implementation of the SLA is based on the well-known WS-Agreement standard. The metrics to set the security SLOs are selected from the MUSA Security Metric Catalogue presented in [15] which maps security threats to security controls and corresponding metrics. The catalogue is freely available in the community [3], proposed and enriched with results from different research projects (e.g. SLALOM [10], SLA-READY [9], SPECS [8] and MUSA [3]), standardization bodies (e.g. NIST SLA [16] and ISO) and consortia like The Centre for Internet Security (CIS). The collection of metrics therein is currently being extended to include a comprehensive catalogue of privacy threats, controls and metrics as well.

It is worth outlining that this paper explicitly addresses the problem of proposing a methodology to support security and privacy issues in a technical way, clearly identifying privacy and security requirements and to suggest related countermeasures. For what regards the compliance to actual regulation, like GDPR, especially in terms of legal aspects compliance, few concrete experiences are available (as an example [17]), and we hold over the topic for a future work.

2.2. Privacy Level Agreements in Cloud

PLAs are intended to describe a service *privacy policy* in form of *privacy controls*. GDPR oriented PLA metamodels can be found in the literature [18], [19]. For Cloud services, standard privacy control definitions are offered by privacy control frameworks such as ISO/IEC 27018 for public Cloud PII processors and the PLA for Cloud services by the Cloud Security Alliance (CSA), named the *Privacy Level Agreement Code of Practise* (PLA CoP) [20]. The CSA's PLA CoP is published as part of their *Code of Conduct (CoC) for GDPR Compliance* and it includes a PLA Template intended to facilitate the declaration of the level of personal data protection a Cloud provider offers to its customers. Following the template, the PLA collects the privacy and security provisions implemented by the CSP acting as data controller or data processor (depending on the case) in a structured way in form of privacy control list.

The CSA's PLA defines a total of 94 privacy controls that CSPs acting as data controllers and/or data processors would specify in their privacy policy. In Table 1 of Appendices section we propose the main relationship between the CSA's PLA controls, the provisions of the GDPR and the Security SLA controls. As seen in the table, we could say that the PLA contains or can refer to the Security SLA of the personal data, as security mechanisms applied by the processor on the PII are required to be expressed as part of the PLA. As explained in previous section, the SLA controls could be expressed by using those of the CSA's CCM [19] or any other security control framework.

2.3. SLAs for multiCloud

In general, multiCloud-based applications have their components deployed in or their components use a priori independent Cloud services. Following this definition, federated Cloud-based and hybrid Cloud-based applications fall in the category of multiCloud applications too.

Therefore, the application is a CSC that can be considered as the composition of individual components that exploit Cloud resources in diverse models (IaaS, PaaS, SaaS). The challenge is therefore the computation of the SLA offered by the application to its customers as a function of how the components are deployed, the type and number of Cloud services they use, the relationships among the Cloud services and among the components themselves and the SLAs offered by each party, i.e. components and Cloud services.

State of the art techniques of SLA composition are limited and mainly focused on reliability and performance controls using different techniques that range from ontology based [21] to WS-Agreement based [22].

Our approach to Security SLA composition is fully detailed in [23] and summarised in Section 5. We are currently extending this solution for PLA composition in multiCloud environments which lacks references in the literature yet.

3. The MUSA DevOps approach to multiCloud Security assurance

The MUSA solution to holistic security assurance in multiCloud applications involves the integration of preventive measures and reactive measures. While MUSA preventive activities aim at preparing the application and defining its SLA including the offered security and privacy controls, the purpose of the reactive activities is to control the actual fulfilment of the defined SLA.

MUSA proposes a DevOps oriented approach to support all the phases of the security- and privacy-aware life-cycle of multiCloud applications, from application privacy-by-design and security-by-design (including the SLA creation) to deployment on Cloud services selected, and finally continuous assurance of SLA fulfillment at operation. MUSA enables multi-disciplinary DevOps teams, which gather together application architects, developers, security architects, business managers, service operators and system administrators, to manage security and privacy risks in all the phases of the multiCloud application life-cycle.

The complete workflow proposed by MUSA thus involves development activities and operation activities of the multiCloud application as shown in Fig 2. While the last three activities are operation activities, the first three activities are development activities that can be considered security- and privacy-by-design practices which prepare the application to be compliant with security and privacy requirements and regulations.

The MUSA approach is supported by the MUSA framework (available in [3]) that seamlessly integrates different tools to support each of the workflow steps. The framework is an open source tool suit offering an integrated Kanban style dashboard to manage the status and progress of all the application components along the application engineering process.

The whole MUSA workflow is made of six main steps (briefly described in the following). Next sections will detail the SLA related activities.

Step1 Modelling: The start of the engineering process is the creation of the application model which specifies both the component level architecture of the application and its Cloud deployment requirements. The model is created in MUSA extended CAMEL language as explained in [24]. The model is a Cloud Provider Independent Model (CPIM) where Cloud requirements of the components are defined without

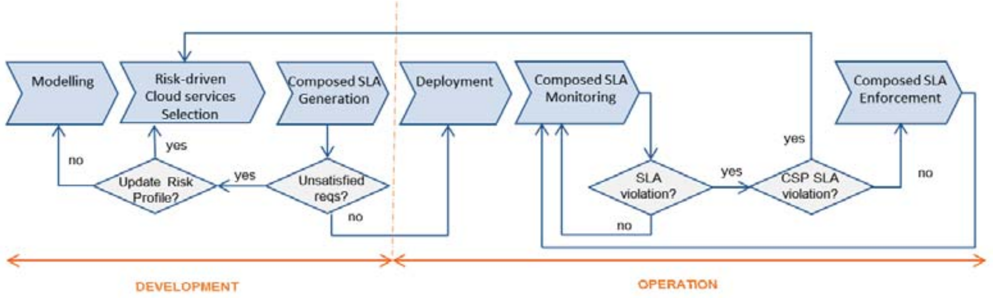

Fig. 2. *MUSA DevOps workflow for SLA-based security assurance in multiCloud*

references to the actual Cloud services that will be selected for the deployment in the next step. The purpose of the model is therefore to define which are the application components, which are their communication relationships, which type and location of Cloud services they need, which are their Cloud resources needs (e.g. size of VM memory, CPU, etc.) and which are the enforcement agents that will optionally operate with them to implement a required security or privacy control (see Section 6).

Step 2 Risk-driven Cloud Services selection*:* In this step the actual Cloud services to use by the application components will be selected so as they match both the requirements stated in the application model expressed as required Cloud resources and the application risk profile. The risk profile is the result of the risk assessment process carried out by analysing the threats against the application components and selecting the desired treatments or controls. This process is supported in MUSA framework by the MUSA Decision Support Tool (DST) and detailed in Section 4 below.

Step 3 Creation of Composed SLA*:* This step consists in the generation of the (multi)Cloud application SLA that can be offered to its clients. The tool in the MUSA framework which supports this functionality is the SLA Generator. The SLA granted will be computed as the composition of the SLAs of the application components and the SLAs of the Cloud services used after an SLA validation process to learn the actual controls that can be effectively supported. The composition methodology is summarised in Section 5.

Step 4 Deployment*:* Once the Cloud services to use are selected and the Composed SLA is obtained, the components of the application will be automatically deployed and the Cloud resources initialised and configured as needed. The monitoring and enforcement agents to be used together with the components are also deployed and configured in this step. They will be the responsible for controlling at operation that the application behaves as promised in the SLA. This step is supported in MUSA framework by the MUSA Deployer, an open source multiCloud broker and deployer that supports OpenStack, Eucalyptus and Amazon AWS.

Step 5 Monitoring of Composed SLA**:** The main objective of compliance and security assurance is to make sure that the Composed SLA holds during application provisioning. This is ensured in MUSA by continuously monitoring the security and privacy levels through metrics defined in the Composed SLA. The monitoring functionality in the MUSA framework is supported by the MUSA Security Assurance Platform that will be described in Section 6.

Step 6 Enforcement of Composed SLA*:* In case actual or potential violations of the promised SLOs are detected, it is necessary to try to enforce the SLOs and take prompt remediation actions to avoid the violation or to recover the security and privacy behaviour as soon as possible. The cause of the violation of the Composed SLA may reside in a failing application component (including enforcement agents used) or a failing Cloud service (i.e. the CSP is not fulfilling its Cloud SLA). Depending on the failing SLO, reaction actions may be procedural activities carried out by the DevOps team (e.g. the redesign of the application to update the architecture and include enforcement agents like the MUSA access control agent) or automatic enforcement mechanisms supported by the multiCloud application itself (e.g. the activation of a data encrypting component) a or by external systems (e.g. the activation of a vulnerability scanner). The enforcement agent management in MUSA framework is part of the MUSA Security Assurance Platform too, as explained in Section 6.

The agile and DevOps paradigms are achieved by two main iteration loops in the workflow. First, at design time the initial CPIM model of the application (in Modelling) and/or its risk profile (in Risk-driven Cloud Services selection) are revisited by the DevOps team until the Composed SLA satisfies all the requirements expressed in both, i.e. until the application architecture and Cloud deployment plan enable to grant a feasible Composed SLA that includes only those controls and levels that can be effectively granted after the selection of the Cloud services to use. Second, at operation time, in case a CSP is identified as the cause of the Composed SLA violation, in order to solve the situation and replace the Cloud service, a redeployment action is tried which would include a new risk assessment iteration.

Following we detail the SLA-related MUSA activities in order to show the crucial role of SLAs for compliance and security assurance in multiCloud-based systems.

4. Risk-driven Selection of Cloud services for multiCloud

In the context of (multi)Cloud applications the challenges associated to privacy-by-design and security-by-design principles increase, due to the possible lack of control over the involved assets in those cases where assets are under the control of external CSP or when assets are elastic, for example, a cluster composed of a varying number of virtual machines. Both scenarios make it difficult to evaluate the level of risks associated and they illustrate the main difference existing between Cloud Security and Security in System Engineering. Security in system engineering assumes that the system under design is completely under control of the designer and it is possible to identify assets and configure them according to the privacy and security requirements at every level of the system architecture. In Cloud-based applications, the assets are frequently under CSPs' control, continuously vary in time and it is less possible for Cloud application designers to impose constraints over their implementation, the attack surface is blurred and new techniques are needed to satisfy privacy and security requirements [25].

With the aim to address (multi)Cloud risk challenges we adopt the SLA-based approach where we rely on the existence of a Security SLA (and PLA) associated to each application component that is not under control of the designer and is offered as a service (i.e. is a Cloud service consumed by the application). Such Security SLA would express the security levels granted by the Cloud service expressed as SLOs measurable by security metrics. Similarly, Cloud PLA would reflect its privacy SLOs and metrics.

In the following we detail how the selection of the Cloud services is made based on the analysis of the threats associated to application components and how the Cloud services' SLAs may tackle them.

4.1. Continuous risk assessment

The risk assessment process in MUSA is considered the key driver to Cloud services selection decision support. Depending on whether the multiCloud application processes PII, risks may involve not only security concerns but also risks to data privacy. MUSA promotes that risk evaluation is a continuous task where multiple perspectives of organisation roles should take part. Whenever the application architecture changes or whenever the security and/or privacy status at runtime is in alert the DevOps team should perform a new risk assessment iteration, which involves the following sub-steps:

4.1.1. Identification of Threats against components: In order to assess the risks in the different components of the application, in MUSA we use a risk model based on the OWASP threat risk modelling [26]. The DevOps team chooses the threats that the component under consideration is susceptible to. These threats may be chosen from a threat catalogue such as that included in the MUSA Security Metrics Catalogue [15], which describes potential threats to different service types taken from expert sources such as the OWASP TOP 10 threats catalogue.

The security threats selected are classified in the STRIDE [27] categories (Spoofing identity, Tampering, Repudiation, Information disclosure, Denial of service and Elevation of privilege). The DevOps team is required to provide the likelihood and impact of each threat and the Composite Risk Index (CRI) of each threat is evaluated as in (1):

$$CRI = Likelihood * Impact \ (1)$$

Both Likelihood and Impact are computed on a scale of 1 to 9 whilst the product is quantized on a scale of 1 to 5. This implies that the CRI ranges from 1 to 25. In our Decision Support Tool (DST) prototype, the likelihood and consequence scales chosen are inspired from [28] and for simplification of the process, the DevOps team is provided with default values of the threat factors with the flexibility to change them at every stage of the risk assessment.

In MUSA risk assessment, the Likelihood and Impact values are further computed from a set of categorisations-based influencers taken from OWASP approach to the CRI [26], where Likelihood factors include *Threat agent factors* and *Vulnerability factors*, while Impact factors can be either *Technical factors* or *Business factors*. The sub-values influencing CRI are grouped by the type of factor and represented by the likelihood of the factor to occur in a scale of 0 to 9, ranging from very unlikely (0) to very likely (9) scenarios. A detailed description of all the concerning factors is available in [26], while a more extensive description of the process can be found in [28].

In order to ease the risk definition, it is advisable that the Technical Impact factors are pre-set with values based on the type of component and nature of the threat. This is how it is done in the threat catalogue within MUSA Security Metrics Catalogue. Business Impact factors on the contrary are not set to default values due to their dependency to the assessed business in question. Therefore, it is necessary that the user always sets the values of the Business Impact factors.

4.1.2. Security controls definition: In this step the DevOps team indicates the security controls that may mitigate the identified threats. After evaluating the threat scores, threats are identified as those requiring treatment (high and medium risk level) and those that may not require treatment (low risk level). This classification is made depending on the threat CRI level.

NIST [13] provides the security and privacy controls for the threats and the threat levels that require treatments. Based on this mapping, the DST prototype obtains the required controls for the threats selected by the DevOps team. These controls are then presented to the DevOps team as suggestions but they are free to extend the choice to all the available security controls if desired. Selected controls are further mapped to the CSA's CCM controls [14]. These controls are later used for the Cloud service selection.

4.1.3. Risk mitigation status definition: The last step required from the DevOps team is the acceptance of the level of the risk mitigation status. In our approach we have leveraged the ROAM model risk mitigation classification [28]. ROAM is a common agile management risk mitigation classification that, according to the countermeasures applied, classifies each threat as: (i) **Resolved**, in case the risk has been answered, avoided or eliminated; (ii) **Owned**, for risks that have been allocated to someone who has responsibility for addressing them; (iii) **Accepted**, if the risk has been accepted and no further actions are required to address it; (iv) **Mitigated**, if an action has been taken (i.e. controls are set) to mitigate the risk, either reducing its likelihood or reducing its impact.

It is pertinent to remark that only threats with status *Accepted* and *Mitigated* can be considered as fully addressed. Threats with status *Owned* are treated as a 'pending' while *Resolved* threats are considered no longer relevant. All these status need to be considered in the subsequent iterations of the continuous threat assessment.

The final output of the risk analysis process is the risk profile of the application in form of the list of security controls required from the Cloud providers, specified per threat and per component so as to mitigate the identified risks.

4.2. Cloud Service Selection on the basis of offered controls

Once the risk profile is finished, a Cloud service match-making process starts to select the services that best match the controls and the requirements in the CPIM model.

4.2.1. Identification of the appropriate CSPs: In order to provide the DevOps team with the set of Cloud services that meet the requirements, the DST prototype is able to look up into multiple datasets. One of the most important data sources for the discovery of the appropriate CSPs is an online version of CSA STAR database in CAIQ format [30] where CSPs have made available the results of their security self-assessment, indicating the CCM security controls they offer. The DST tool is able to consume the source dynamically and process it. Through the responses of the CSPs in the CAIQ and through the reference mapping provided by CSA in [14], the DST retrieves the security controls that are provided by the different CSPs. Another method to make this identification is by using the CCM matrix mapping for security controls to the certification clauses. The DST identifies the public declaration of the certificates hold by the CSPs (available through CAIQ) and identifies in the matrix the security controls provided by those certifications.

As the Risk Assessment phase output is provided in the DST prototype in NIST [13] format, the tool is then using the repository of security control families and cross-certificate mapping proposed by CSA STAR, in order to discover the relationships between the NIST and CCM security controls. It is almost entirely mapped in a many-to-many relation fashion. This way the MUSA DST identifies the CSPs that meet the security controls provisioning that guarantees the threat treatment for each component selected by the user.

4.2.2. Ranking the services based on the risk profile: In order to evaluate and rank the Cloud services on the basis of their capability to address the security requirements of the multiCloud application, we use the risk response evaluation method proposed by Dorfman [31]. This evaluation mechanism is used to identify the extent of threat mitigation provided by the different controls and consequently, what is the overall extent of risk mitigation capability that is provided by the CSP. Using this evaluation it is possible to rank the providers according to the percentage of user requirements fulfillment. It also provides an insight to the user as to which threats are mitigated by a provider and the scope of the mitigation.

The resulting score is an average value of fulfilment of aggregated security controls from all the controls hosted in the same Cloud service. The fulfilment value of a security control in NIST is an average of all the influencing CCM controls and their level of fulfilment by the provider in question. The connection between the Cloud service (e.g. hosting virtual machine) and the component is described in the CPIM of the multiCloud application.

4.2.3. Final decision: Once the alternative Cloud service combinations are ranked by multiCloud application requirements fulfilment percentage, the DevOps team will need to make the final choice of which combination to use. This is a human decision-making process aided by the ranking information presented. The decision should be taken from a multi-disciplinary viewpoint, preferably involving several actors in the DevOps team in order to enrich the decision. Other business factors and performance factors may affect the decision and should be considered.

In those cases where the percentage of security requirements fulfilment is not satisfactory for the DevOps team, a new iteration process may be started by updating the security controls required in the Risk Assessment phase, i.e. by updating the risk profile.

The final selected combination of services is passed to the Composed SLA Generation step described below.

5. Creation of Security SLA for multiCloud

The SLA composition methodology we propose is fully explained in [23]. Herein we provide a brief description for the sake of understandability of the overall MUSA methodology and workflow.

The methodology aims at creating a machine-readable Security SLA of the overall multiCloud application by considering the dependencies of the components among them and with the Cloud services they use.

The ultimate goal is to obtain an SLA that includes the security controls that can be granted by the multiCloud application to its consumers to be later monitored at runtime. This is what we call the *Composed SLA*, which is in fact the set of controls that can be effectively promised for each application component. The controls would be security and/or privacy mechanisms implemented by the component (or by the MUSA enforcement agents that work with the component, if any) or required on the Cloud service it uses.

The methodology consists in the following sub-steps:

- ***Per-component SLAT creation***: From the per-component threat identification and risk assessment step described in Section 4.1.1, the goal is to obtain the SLA Template (SLAT) that describes the desired SLOs for each component. Therefore, the DevOps team associates the SLOs (metrics and metrics values) to each of the desired security controls. These controls are desired in the sense that they do not take into account yet the final deployment context.
- ***Per-component SLA assessment***: The process translates the SLAT of each of the component into the SLA that it can grant. The DevOps team will need to perform a detailed security review of the component by answering a questionnaire we developed to this aim, which is the result of the combination of security assessment methodologies and best practices such as OWASP ASVS 2.0 questions, Berkley DB Best Practices, security controls definition from NIST and CSA CAIQ[30].
- ***Per-application SLA assessment***: The starting point is the Multi-Cloud Application Model (MACM) derived from the application CPIM model created in the initial Modelling step. The MACM captures the deployment architecture as well as the relationships among the services composing the application (e.g. uses,

provides, hosts, etc.). The application level assessment consists in reasoning over such relationships by applying the composition rules on a per security control basis. The composition assumes the controls can be independently evaluated and different composition rules are defined depending on the type of control.

Remarkably, in this technique it is necessary to include the selected MUSA enforcement agents, if any, which would implement security and privacy mechanisms and thus would have to be part of the MACM and follow the assessment process to learn the SLA they can grant so as it can be taken into account in the composition.

The outcome is the *Composed SLA* of the multiCloud application that will be deployed, which contains only those controls that can be granted by the components. The current SLA Generator prototype is capable to inform on the composition results explaining the detail traces and causes of the non-inclusion (if any) of particular security controls in the Composed SLA.

6. SLA-based Security Assurance in multiCloud

Just after successful deployment of both application components and their corresponding agents, the operation and monitoring of the running (multi)Cloud application start. MUSA solution proposes the Composed SLA-based operational assurance and the automation as much as possible of the security and privacy level control and enforcement. In this section we describe the MUSA Security Assurance at operation supported by MUSA Security Assurance Platform (MUSA SecAP). The complete description of the methodology and the platform is provided in **Error! Reference source not found.**.

The methodology involves the Monitoring and Enforcement activities of the MUSA workflow depicted in Fig 2, as follows.

6.1. Continuous Monitoring of Composed SLA fulfilment

The security and privacy levels promised to multiCloud application customers are continuously under scrutiny by DevOps team who keep tracking whether the metrics defined for the controls are reaching the target levels (SLOs). Currently the metrics available in MUSA SecAP are a set of security metrics and privacy metrics from MUSA Security Metrics Catalogue. See more info in MUSA deliverable D4.4 in [3].

Security SLA violations occur when it is detected that a security SLO in the SLA is not reached. Similarly, a PLA violation happens when a privacy SLO is not reached.

In case any SLO is at risk (the threshold level is about not to be reached) an alert is triggered and a notification raised to the DevOps team and other stakeholders subscribed to the alerting system for them to be able to rapidly react and solve the issue.

The main modules in MUSA SecAP that support the Composed SLA monitoring are the Monitoring and Notification services, supported by the Monitoring agents.

The ***Monitoring service*** is in charge of supporting metrics measurement, persistence, root cause analysis and alert triggering. The service extracts from the Composed SLA the required security and privacy metrics and metric objectives and it configures the monitoring agents (see below) accordingly.

The ***Notification service*** is the main service for ensuring transparency. It is responsible for providing visual information on situational awareness, notifying the DevOps team on security and privacy incidents detected, and generating evidence reports from the measurements. The service relies on user subscription to alerts and events they would like to be informed on.

Four ***Monitoring agents*** are offered in MUSA which are automatically deployed and work together with the multiCloud application components as follows:

- The ***Network monitoring agent*** analyses the network traffic from different network interfaces of the virtual machines or containers where the components are deployed. The agent uses an advanced rules engine able to correlate network events to detect performance, operational and security incidents.
- The ***System monitoring agent*** detects server performance degradation and bottlenecks by monitoring operating system resources. The agent relies on Linux *top* command to monitor performance (e.g. running processes, CPU usage, Memory usage, Cache Size, etc.).
- The ***Application monitoring agent*** monitors execution details and other internal conditions of the multiCloud application component in which it is deployed.
- The ***Behaviour monitoring agent*** learns the behaviour of users/systems using the component and creates activity profiles for each object/user on the basis of volume of data for the specific category of application component.

6.2. Reaction to violations of Composed SLA

Whenever an SLO violation or alert event occurs, the Monitoring service in the MUSA SecAP would detect it and the DevOps team would be informed on time by the Notification service. The incident information would include all the necessary information about the failing measurement together with the identified cause and the recommended reaction action. Depending on the cause, the DevOps team reacts applying one of the following processes.

Activation of a MUSA security enforcement agent: MUSA security enforcement agents are preventive security mechanisms or controls that are managed through a message broker by the MUSA Enforcement service in MUSA SecAP. As long as the application CPIM required the use of the enforcement agent to protect a component, it is possible to manage the agent at runtime. Thus, in case the failing SLO can be solved by the activation or re-configuration of the agent, the MUSA SecAP would recommend it to the DevOps team. The three basic enforcement agents offered by the MUSA framework are the following:

- *The* ***high availability (HA) framework*** which is based on the Corosync/Pacemaker stack and provides high availability clustering mechanisms such as scalability, load balancing, automatic failover and routing between services, and secure communications.
- *The* ***identity management (IdM) agent*** that guarantees that only authorised end-users can access application

component services. It supports OpenID Connect and OAuth 2.0.

- *The **access control (AC) agent***: An XACML policy-based ABAC component that ensures that only authorised requesters with authorised attributes can consume services in application component. It relies on component local Policy Enforcement Point (PEP) and Policy Decision Point (PDP) to increase the performance.

***Activation of a MUSA privacy enforcement agent*:** The privacy enforcement agents are similar to security enforcement agents and their duty is to implement privacy specific controls whenever needed at operation. Note that these agents would be required only in those cases where PII is processed by the multiCloud application. For example, the privacy agents could be responsible for automatically implementing data subject's changing processing options according to collected consent, data retention periods or purpose limitations. We are currently developing privacy agents that can be managed as external agents to the application through the MUSA SecAP enforcement dashboard. The key challenge is to make the agent reside external to the components while still avoiding security issues such as data leaks between the component and the agent.

Re-deployment of multiCloud application: When the cause of the detected violation is a failing Cloud service used by one or more components, it would be necessary to replace it with some other Cloud service offering the same functionality and security controls. The MUSA DST will support the DevOps team in searching for the replacement and the MUSA Deployer in deploying again the components that were using the defective service. It is recommended to launch a new iteration from risk assessment step to ensure that the new Cloud service combination with the new Cloud Service still holds the risk profile and requirements.

Re-design of multiCloud application: In case the cause of the violation is a failing component and not a defective CSP, the DevOps team would need to study the cause and correct the failing component code if that is the case, or start the MUSA workflow by Modelling phase where they would update the CPIM model to refine the architecture requirements, include protection components or specify the use of MUSA security or privacy enforcement agents that offer such missing controls (if available).

7. Validation

Our MUSA SLA-based security assurance approach and the supporting tools in MUSA framework have been evaluated in the creation and operation of two real-world multiCloud-based systems:

- Flight scheduling application prototype by Lufthansa Systems, Germany. The analysis of this case study was focused on data integrity, confidentiality, data location and access control.
- Tampere Smart Mobility (TSM) application by Tampere University of Technology, Finland. In this case study we mainly analysed the potential of MUSA DevOps SLA-based approach to ensure high availability, data integrity, confidentiality and privacy of users' personal data such as their mobility footprint.

The validation in both use cases followed the same methodology. A MUSA-independent DevOps team was created gathering experts from development, security, service administration, business areas, etc. of the organisation. After dedicated training sessions on the MUSA framework concept and tool usage, they were required to go hands on with MUSA tools to engineer and operate the multiCloud application. The process followed corresponds to the workflow of Fig 2.

While the benefits of using MUSA for Flight scheduling prototype are described in [32], in this paper we will summarise the results for TSM multi-modal and energy efficient mobility application shown in Fig 3. As it can be seen, this application includes some internal components (in blue): a Journey Planner that calculates the optimum route, an energy Consumption Calculator, a Database that stores users' journey profiles and the Identity Management Module (IdM) for the authentication of the users, and finally the TSM Engine which is a Web service in charge of orchestrating the other components. Note that the IdM component can also be replaced by an external IdM. The application uses also SaaS services (in green) like weather forecasts (FMI), (Google directions) and other open data and services from the Intelligent Transport Systems and Services (ITS) Factory of Tampere City.

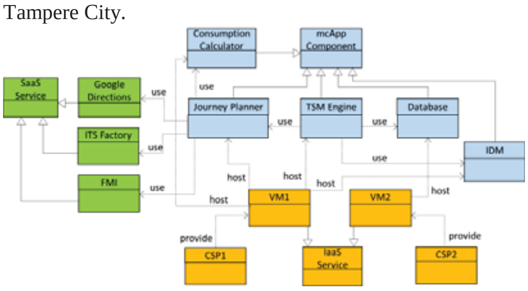

Fig. 3. TSM multiCloud application deployment

Fig 3 also shows (in orange) a possible simple deployment using two IaaS services for the internal components. By following the MUSA workflow, this is the type of information that the DevOps team expressed in the CPIM of the application in the initial Modelling step (see Section 4) together with the selected enforcement agents for the components (see section 6.2). Initially no MUSA agent was selected for TSM application. Then, the DevOps team followed a per-component risk assessment (see Section 5) and the security and privacy controls were selected for all the internal components' SLAs. With this risk profile an initial selection of the Cloud services to use was made.

As part of the SLA Composition step, from the CPIM model an extended version of the MACM model shown in Fig 4 was created as the basis for the composition reasoning.

The desired controls in the risk profile were assessed and validated in the computation of the Composed SLA.

As part of the SLA composition process, some of the initially selected controls were drop off from the final application SLA, e.g. high availability, due to the MUSA HA agent was not selected in this application version and the availability of the selected Cloud services would not enough to meet the desired target (SLO >= 99.98\%). Nevertheless, the selection of Cloud services was decided not to be changed.

An excerpt of the identified threats for TSM Engine (TSM) and Database (DB) components and a partial list of the corresponding controls in NIST [13] and metrics is provided in Table 2 of Appendices section. See MUSA deliverable D4.4 in [3] for the complete list.

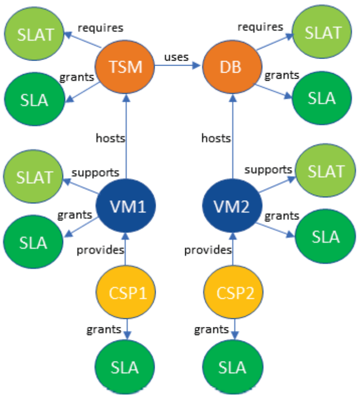

Fig. 4. *MCAM of TSM application for TSM and DB components*

In the deployment phase, the components were successfully deployed using the MUSA Deployer which automatically deployed the MUSA monitoring agents too (see Section 6.1) to be able to measure the specified metrics.

At operation phase, the monitoring of the security metrics in the Composed SLA allowed the application of a set of detection rules which raised diverse alarms in application components. For example, to evaluate the efficiency in access control protection, we launched an access attempt from an unauthorised source and the Notification service immediately raised a violation alarm to the DevOps team together with the recommendation to Use the AC agent with the TSM engine component. The DevOps team re-designed the application including the MUSA AC agent to be deployed with TSM engine. This way the AC agent was activated and helped to recover from the incident. In a further development iteration, the DevOps team decided to replace the AC agent by the HA agent which provides both the required availability and AC protection in a single agent. The same mechanism could be used for protecting access to personal data in DB.

Additional security monitoring and reaction strategies supported by MUSA SecAP for DoS, identity thefts, use of vulnerable components, etc. were evaluated successfully.

Other examples include DB component privacy protection like the activation of a personal data eraser when the MUSA SecAP detected that the disposal date specified in the SLA was passed.

8. Conclusions and future work

Compliance with GDPR and security assurance in multiCloud-based systems are two major challenges obstructing trust and Cloud adoption.

In this paper we have proposed a novel methodology for SLA-based security and privacy assurance in Cloud and multiCloud-based systems that seamlessly integrates security-by-design, privacy-by-design and quantitative assurance at operation. It relies on the use of the Security SLAs and PLAs as the instruments to gain transparency and systematization of the assurance of security and privacy measures offered by the Cloud-based systems and their providers. Security SLAs and PLAs formalise the definition of both information protection functionality and assurance level, for security and privacy capabilities respectively.

The MUSA approach and its supporting open source tool suit, the MUSA framework, have been proved to enable the security-aware design as well as continuous security assurance and evidence collection based on metrics specified for application SLOs defined in the Composed SLA. Assurance in multiCloud applications requires the holistic control of multiple security and privacy capabilities at different components and layers of Cloud. To this aim we propose to adopt joint security- and privacy-by-design strategies as part of a complete DevOps approach for the prompt reaction to incidents at runtime.

The contributions brought by our approach include: (i) the integration of privacy and security assurance in a single DevOps workflow that supports agile and multi-disciplinary holistic and continuous risk assessment, (ii) novel SLA Composition mechanisms that to obtain multiCloud SLAs that are machine-readable and based on security and privacy standards (NIST, CSA) and (iii) operation assurance mechanisms for ensuring Composed SLA fulfilment and early detection of security and privacy flaws in the application components and used Cloud services.

The framework is currently being improved by optimising the SLA composition techniques and the root cause analysis. We are also working in extending the solution for supporting a complete set of privacy controls and metrics.

9. Acknowledgments

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 644429 and No 780351, MUSA project and ENACT project, respectively. We would also like to acknowledge all the members of the MUSA Consortium and ENACT Consortium for their valuable help.

10. References

[1] Deloitte: 'Measuring the economic impact of cloud computing in europe,smart number: 2014/0031', April 2016, http://ec.europa.eu/newsroom/document.cfm?doc_id=41184, accessed 17 December 2018.

[2] ETSI: Interoperability and security in cloud computing, ETSI SR 003 391 v2.0.0 (2015), http://csc.etsi.org/resources/WP3-Report/STF 486 WP3 Report-v2.0.0.pdf, accessed 17 December 2018.

[3] MUSA project: Multi-cloud Secure Applications (2015-2017), https://www.musa-project.eu, accessed 17 December 2018.

[4] ENACT project: Development, Operation, and Quality Assurance of Trustworthy Smart IoT Systems (2018-2020), http://www.enact-project.eu, accessed 17 December 2018.

[5] Rios, E., Iturbe, E., Mallouli, W. and Rak, M., 2017, October. 'Dynamic security assurance in multi-cloud DevOps'. In Communications and Network Security (CNS), 2017 IEEE Conference on. pp. 467-475.

[6] Rios, E., Rak, M., Iturbe, E., & Mallouli, W. (2017). ‘SLA-Based Continuous Security Assurance in Multi-Cloud DevOps‘. CEUR Workshop Proceedings, http://ceur-ws.org/Vol-1977/, accessed 17 December 2018.

[7] Casola, V., De Benedictis, A., Modic, J., Rak, M., Villano, U.: ‘Per-service security sla: a new model for security management in clouds’. Proc. IEEE 25th Int. Conf. on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), 2016, pp. 83-88.

[8] SPECS project: Secure Provisioning of Cloud Services based on SLA management (2013-2016), http://www.specs-project.eu, accessed 17 December 2018.

[9] SLA-READY project: Making Cloud SLAs readily usable in the EU private sector (2015-2016), http://www.sla-ready.eu, accessed 17 December 2018.

[10] SLALOM project: Service Level Agreement - Legal and Open Model (2015-2016), http://www.slalom-project.eu/, accessed 17 December 2018.

[11] Cloud Standards Customer Council, OMG: ‘Practical Guide to Cloud Service Agreements V2.0’, https://www.omg.org/cloud/deliverables/practical-guide-to-cloud-service-agreements.htm, accessed 17 December 2018.

[12] Casola, V., De Benedictis, A., Rak, M., Modic, J., Erascu, M.: ‘Automatically enforcing security slas in the cloud‘. IEEE Transactions on Services Computing (2016)

[13] National Institute of Standards and Technology (NIST), ‘Security and Privacy Controls for Information Systems and Organizations’. NIST SP-800-53, revison 5 Draft.

[14] Cloud Control Matrix (CCM) Alliance, C.S.: Cloud security alliance, cloud controls matrix v3.0.1 (9-1-17 Update), https://cloudsecurityalliance.org/group/cloud-controls-matrix/, accessed 17 December 2018.

[15] Casola, V., Benedictis, A.D., Rak, M., Villano, U.: ‘A security metric catalogue for cloud applications’. Proc. Int. Conf. on Complex, Intelligent, and Software Intensive Systems (CISIS), July 2017, pp. 854-863.

[16] NIST Cloud Computing Program Information Technology Laboratory (2015), ‘Cloud Computing Service Metrics Description NIST SP-500-307’.

[17] Conley, E., Pocs, M. ‘GDPR compliance challenges for interoperable health information exchanges (HIEs) and trustworthy research environments (TREs)’, European Journal for Biomedical Informatics, vol. 14, no. 3, 2018, pp. 48-61.

[18] Ahmadian, A.S., and Jürjens J.. ‘Supporting model-based privacy analysis by exploiting privacy level agreements’ Proc. Int Conf. Cloud Computing Technology and Science (CloudCom), 2016 IEEE , pp. 360-365.

[19] Diamantopoulou, V., Pavlidis, M., & Mouratidis, H. (2017). 'Privacy level agreements for public administration information systems', http://eprints.brighton.ac.uk/17145/, accessed 17 December 2018.

[20] Cloud Security Alliance (CSA), Code of Conduct for GDPR Compliance, https://gdpr.cloudsecurityalliance.org/wp-content/uploads/sites/2/2018/06/CSA-Code-of-Conduct-for-GDPR-Compliance.pdf, accessed 17 December 2018.

[21] Liu, H., Bu, F., Cai, H.: ‘Sla-based service composition model with semantic support’. Proc. Services Computing Conference (APSCC), 2012 IEEE Asia-Pacific, IEEE (2012) 374-37920.

[22] Zappatore, M., Longo, A., Bochicchio, M.A.: 'SLA composition in service networks'. Proc. of the 30th Annual ACM Symposium on Applied Computing - SAC '15, ACM Press (2015) pp. 1219-1224.

[23] Rak, M.: ‘Security assurance of (multi-) cloud application with security sla composition’. Proc. Int. Conf. on Green, Pervasive, and Cloud Computing, Springer (2017) pp. 786-799.

[24] Rios, E., Iturbe, E., & Palacios, M. C. ‘Self-healing Multi-Cloud Application Modelling’. Proc. Int. Conf. on Availability, Reliability and Security, ACM (2017) (No. 93).

[25] ‘How Visibility of the Attack Surface Minimizes Risk’, https://www.sans.org/reading-room/whitepapers/cloud/visibility-attack-surface-minimizes-risk-38540, accessed 17 December 2018.

[26] ‘OWASP Risk Rating Methodology’, https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology, accessed 17 December 2018.

[27] ‘The STRIDE Threat Model’, https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx, accessed 17 Dec 2018.

[28] Ripolles, Oscar; Muntes, Victor; Matthews, Peter; Gupta, Smrati; Dominiak, Jacek; Willeke, Erik; Somoskoi, Balazs: ‘Agile Risk Management for Multi-Cloud Software Development’, IET Software, December 2018, DOI: 10.1049/iet-sen.2018.5295.

[29] Baah, A.: ‘Agile Quality Assurance: Deliver Quality Software-Providing Great Business Value.’ BookBaby, 2017.

[30] Cloud Security Alliance: ‘Consensus Assessments Initiative Questionnaire v3.0.1’, https://cloudsecurityalliance.org/download/consensus-assessments-initiative-questionnaire-v3-0-1/, accessed 17 December 2018.

[31] Dorfmann & Mark S. ‘Introduction to Risk Management and Insurance’ (Prentice Hall, 1997, 6th ed.).

[32] Springer, ‘Digitalization Cases: How Organizations Rethink Their Business for the Digital Age’, https://www.springer.com/us/book/9783319952727, accessed 17 December 2018.

11. Appendices

Table 1 Proposed CSA's PLA relationship with GDPR and security controls in Security SLA

PLA requirement	PLA control	GDPR requirement
1. CSP Declaration of Compliance and Accountability.	DCA-1.1 to DCA-1.4	Art. 24 - Responsibility of the controller, Art. 28 - Processor
2. CSP Relevant Contacts and its Role.	CAR-1.1 to CAR-1.5	Art. 24 - Responsibility of the controller, Art. 26 - Joint controllers, Art. 27 - Representatives of controllers or processors not established in the Union, Art. 28 - Processor, Art. 29 - Processing under the authority of the controller or processor
3. Ways in which the Data will be Processed.	WWP-1.1 to WWP-1.15, WWP-2.1, WWP-3.1 to WWP-3.5, WWP-4.1 to WWP 4.2, WWP-5.1 to WWP-5.9	Art. 25 - Data protection by design and by default
4. Recordkeeping.	REC-1.1 to REC-1.8, REC-2.1 to REC-2.5	Art. 30 - Records of processing activities
5. Data Transfer.	DTR-1.1 to DTR-1.2	Chapter 5 (Art. 44 – 50) - Transfers of personal data to third countries or international organisations
6. Data Security Measures. **(Security Controls -> in Security SLA.)**	SEC-1.1, SEC-1.2, SEC-1.2i - availability, SEC-1.2ii - integrity, SEC-1.2.iii - confidentiality, SEC-1.2.iv - transparency, SEC-1.2.v - isolation (purpose limitation), SEC-1.2.vi - intervenability, SEC-1.2.vii - portability, SEC-1.2.viii - accountability.	Art. 32 - Security of processing, Art. 5 - Principles relating to processing of personal data 1(f) – integrity and confidentiality.
7. Monitoring.	MON-1.1	Art. 4 (1). The information provided to the public and to data subjects, Art. 5 - Principles relating to processing of personal data 1(a) -transparency
8. Personal Data Breach.	PDB-1.1 to PDB-1.7	Art. 33 -Notification of a personal data breach to the supervisory authority, Art. 34 -Communication of a personal data breach to the data subject, Art. 5 - Principles relating to processing of personal data 1(a) - transparency
9. Data Portability, Migration and Transfer Back.	PMT-1.1 to PMT-1.2	Art. 20 - Right to data portability
10. Restriction of Processing.	ROP-1.1	Art. 18 - Right to restriction of processing, Art. 5 - Principles relating to processing of personal data 1(b) - purpose limitation and 1(c) - data minimisation
11. Data Retention, Restitution and Deletion.	RRD-1.1 to RRD-1.2, RRD-2.1, RRD-3.1, RRD-4.1 to RRD-4.5	Art. 16 - Right to rectification, Art. 17 - Right to erasure ('right to be forgotten'), Art. 5 - Principles relating to processing of personal data 1(d) - accuracy and 1(e) - storage limitation.
12. Cooperation with The Cloud Customers.	CPC-1.1 to CPC-1.2	Cooperation with data subject to fulfil Chapter 3 (Art. 12 – 23) -Rights of the data subject
13. Legally Required Disclosure.	LRD-1.1	Art. 31 - Cooperation with the supervisory authority
14. Remedies for Cloud Customers.	RMD-1.1	Art. 77 - Right to lodge a complaint with a supervisory authority, Art. 79 - Right to an effective judicial remedy against a controller or processor.
15. CSP Insurance Policy	INS-1.1	Art. 82 - Right to compensation and liability

Table 2 TSM application controls and metrics (partial lists for TSM Engine and DB components)

(Type* key: S-X: security control, where X can be S/T/R/I/D/E as in STRIDE model; P: privacy control, J: joint control)

Threat in MUSA Metric Catalogue	Type*	Control ID NIST	Metric in MUSA Metric Catalogue	Reaction in MUSASecAP	Comp
Denial of service	S-D	SC-5	Level of redundancy	Deploy additional containers.	TSM, DB
			Service availability	Depends on the root cause: redeploy the VM, restart the application	
Account Hijacking	S-E	IA-5	User account measure, Identity assurance	Use stronger authentication mechanism (e.g. 2 factor authentication), Use MUSA AC agent	TSM, DB
		AC-2	User account measure, Identity assurance, Personnel security screening measure	Deploy MUSA monitoring agent	
Over-privileged applications and accounts	S-E	AC-6	User account measure, Identity assurance	Use 2 factor authentication mechanism, Use MUSA AC agent	TSM
Access token leak in Transport /Endpoints	S-I	SC-8	HTTP to HTTPS redirects	Use HTTP/HTTPS proxy	TSM, DB
CSRF Attack against redirect-uri	S-I	IA-5	User account measure, Identity assurance	Use 2 factor authentication mechanism, Use MUSA AC agent	TSM, DB
		AT-2	HTTP to HTTPS redirects	Use HTTP/HTTPS proxy	
Using components with known vuln.	S-I	RA-5	Vuln. scanning frequency in hours	Update scanning frequency	TSM, DB
Sensitive data disclosure	S-S	IA-5	User account measure, Identity assurance	Use 2 factor authentication mechanism, Use MUSA AC agent	TSM, DB
		SC-23	Identifiers quality, data encryption	Use randomizer for identifiers	DB
Injection flaws	S-T	SI-10	Injection flaw type	Deploy a new version of software with input validation or discard malformed inputs	TSM, DB
Unauthorised access to personal data	P	SI-4(25)	User account measure, Identity assurance	Use 2 factor authentication mechanism, Use MUSA AC agent	DB
	J	SI-6	Availability of Priv. verification service	Deploy privacy verifier	DB
Personal data disclosure	P	SI-20(1)	Level of anonymisation	Use strong anonymisation mechanisms	DB
Personal data retention date passed	P	SI-18	Information disposal due date and time	Activate eraser on time	DB