SLA Model Terms and Specifications:
SLALOM Project Overview and Request for Feedback

SLALOM is an initiative aligned with the European Cloud Strategy [1]. The first phase of the initiative is an 18-month, EC-funded project[1] whose objective is to create a Service Level Agreement (SLA) reference model consisting of model contractual terms and model technical specifications.[2] It seeks to provide clarity and reassurance to the market through establishing a baseline of fair and balanced provisions for cloud SLAs. They can be adopted by most cloud service providers and consumers without great expense yet providing a high level of trustworthiness. The benefits to industry include greater uptake of cloud computing by reducing the recognized [2] barrier to adoption of lack of trust and consequent risk.

The purpose of this document is to give an overview and provide examples of the proposed model terms and specifications, and to ask for market feedback in order to confirm or modify the proposed work. The on-line questionnaire accompanying this document will be available at bit.ly/SLALOMWantsToKnow until 20 March 2015.

Some of the key issues about which market feedback is requested are:

- Structure and format of models: How can the project deliverables be presented so that they are as practical and easy to use as possible? Can improvements be made on the structure and format of the examples presented?
- Core coverage: How broad should core coverage be? What is considered core? How can it be prioritized? To what extent might "core" depend on the market sector and type of cloud used?
- Coverage of scenarios emerging from research: There are a number of topics arising from research which could be addressed including in hybrid, federated and 'fog' clouds, as well as

[1] SLALOM ("Service Level Agreement - Legal and Open Model") is a support action project funded by the European Commission through the Horizon 2020 research programme, with Grant agreement no: 644270. Its consortium comprises: ATOS SPAIN (project lead), Bird & Bird (responsible for the legal track), the National Technical University of Athens (responsible for the technical track), the Cloud Industry Forum (responsible for liaison with the Cloud Service Provider community), and the University of Piraeus (responsible for liaison with the Cloud Adopter community). The project runs for 18 months from 01/01/2015.

[2] The brief of SLALOM is provide two SLA reference models for cloud computing. The first is a set of common legal clauses to cover cloud SLAs and contracts. The second is a standard technical SLA specification. The models cover both current market practice and scenarios emerging from research. The project will find consensus between stakeholders and determinedly promote the models' adoption. The project will use its position to proactively support all community projects researching either cloud computing or cloud-related SLAs.

automated SLA management frameworks. What are the market views about these topics and the amount of coverage they should be given?

Contents

- Scope
- Model terms
- Model specifications
- Alignment to ISO
- Coverage of scenarios emerging from research
- Annex A: About SLALOM
- Annex B: Reference materials and further reading

Scope

SLALOM is a long-term initiative to develop model contractual terms and technical specifications for all cloud computing areas, including emerging and future developments.

The current (and initial) phase of SLALOM is an EC-financed project with the following scope:

- Model contractual terms for cloud computing contracts at the Master Service Agreement (MSA) level, i.e., a legal scope for cloud computing contracts in general.
- Model contractual terms and technical specifications for Service Level Agreements (referred to by the MSA), i.e., a more extensive remit but just for Service Level Agreements.

It should be noted that SLALOM is much more than just SLAs, both in this current project and long-term. Consequently, its scope exceeds that of the proposed ISO/IEC 19086 family of standards for Cloud SLAs. However, for the purpose of SLAs, its scope is closely aligned to these standards. See the section on 'Alignment to ISO' for further details.

Model terms

Model terms are planned at least for the following areas at the Master Service Agreement level (the list is not exhaustive):

- Obligation to Provide Services
- Quality of Service (Reference to SLA Attachment)
- Obligation of The User
- Consideration
- Intellectual Property
- Liability 0f The Parties
- Term and Termination
- Confidentiality Obligations
- Warranties
- Indemnification

- Data Protection
- Law of the Contract
- Jurisdiction

The intention is to draft a template for each section. This will provide the necessary clauses which will be drafted in accordance with legal practice and balancing the rights of each party, taking into consideration the work of expert groups that have debated the issues, such as the group managed by the Justice Directorate of the European Commission. [3]

The following examples show how SLALOM will approach each of the model contractual terms, identifying deficiencies in current practice and establishing a new, fair and unambiguous definition. All examples are from the Master Service Agreement level.

Example 1: Provision of Services

Many cloud computing Master Service Agreements include a clause along the following lines:

> "***Provision of Services"***
>
> *The client may access and use the Service in accordance with this Master Service Agreement*

It could appear there is not an obligation in charge of the provider to supply the services.

A SLALOM-type of clause would be as follows:

> *"**Provision of Services"***
>
> 1. *The Provider shall provide the Services to the User for the Term in accordance with the SLA under Attachment [●] and the terms and conditions of this Master Service Agreement.*
> 2. *The User shall access and use the Services in compliance with all applicable laws and regulations, the Acceptable Use Policy and according to the terms and conditions of the present Master Service Agreement".*

Example 2: Liability including for non-performance against SLA requirements

Several Master Service Agreements provide a wording similar to the following concerning liability issue:

> *"The Provider will not be liable to the User for any direct, indirect, incidental, special, consequential or exemplary damages (including damages for loss of profits, goodwill, use, or data), even if the Provider has been advised of the possibility of such damages. The Provider will not be responsible for any compensation, reimbursement, or damages arising in connection with: (a) User's inability to use the Services, including as a result of any (i) termination or suspension of this Master Service Agreement or User's use of or access to the Service offerings, (ii) Provider's discontinuation of any or all of the Service offerings, or, (iii) without limiting any obligations under the SLA, any unanticipated or unscheduled downtime of all or a portion of the Services for any*

reason. In any case, the Provider's aggregate liability under this Master Service Agreement will be limited to the amount the User actually pays to the Provider under this Master Service Agreement for the Service that gave rise to the claim during the 12 months preceding the claim".

SLALOM can provide different liability clause options:

1) 1° Class Liability: full liability of the provider. Sample clause:

"*The Provider will be liable to the User for the claim, damages and consequences deriving from the breach by the Provider of its material obligations under this Master Service Agreement*".

2) 2° Class Liability: medium liability of the provider (areas of exclusion/limitation to the amount of damages):

"*The Provider will be liable to the User for any direct damages deriving from the material breach by the Provider of the following obligations under this Master Service Agreement: section [●]. The Provider shall be liable to the User for any direct damages deriving from the material breach of its obligations under Section [●], it being understood that the Provider's aggregate liability deriving from the breach of aforesaid obligations will be limited to the amount the User actually pays us under this Master Service Agreement during the 3 months preceding the claim. In any case the total aggregate liability of the Provider under the present Master Service Agreement shall not exceed the amount the User actually pays to the Provider under this Master Service Agreement during the 12 months preceding the claim".*

3) 3° Class Liability: total exclusion of liability of the provider except payment of provided penalties.

"*To the extent permitted by the law, the Provider, save for the payment of the penalties deriving from the failure in fulfilling the SLA, shall not liable to the User for any consequences, claim, damages suffered by the User deriving from the breach by the Provider of its obligations and warranties under this Master Service Agreement*".

The Provider and the User will be able to clearly know the "Class of Liability" they are selling/buying

Example 3: Intellectual property rights

SLALOM MSAs will establish a clear set of rules for distinguishing between:

1) IP of the Provider (OS of the platform; SaaS);

Sample clause:

"The Provider and its licensors shall remain the exclusive owners of any and all Intellectual Property Rights ("IPR") connected, deriving or relating to the Services,

including without limitations, the Software and the Operating System and all relevant improvements or changes related thereto developed or produced during the execution of this Master Service Agreement"

2) IP of the Users (uploaded data and new works created on the cloud);

Sample clause:

"The User shall remain the exclusive owner of any and all IPR connected, deriving or relating to the Content uploaded by the User on the Provider's server through the use of the Services, as changed, implemented and developed by the User during the Term of the Master Service Agreement. The User authorises the Provider, its officers and employees, to store, copy, transmit and use such Content with the exclusive purpose to provide the Services. The Provider, its officers and employees, shall not be entitled to use above Content for any other scope or purpose"

3) IP of Third-Party (contents, software installed on PaaS or IaaS)

Sample clause:

"The User guarantees that the Provider shall have title to use, copy and transmit the User Software or the Third-Parties Software installed on the Provider's servers upon request of the User to provide the Services in accordance with the terms and conditions of the Master Service Agreement. Any other use of the User Software or Third-Parties Software shall be prohibited."

…providing punctual notification of transfer of IPR from one to the others.

Sample of notification:

"This Content/Software is exclusive property of [●]. You will have title to use it for [●] days for the following purpose [●], according to the following modalities [●]".

Example 4: Protection of personally identifiable information component

SLALOM can provide model rules to cover most of the many multi-jurisdiction privacy and data protection compliance needs, also offering multiple-choices to cover:

1) Sector specific requirements

2) Potential secondary purposes

3) Security related requirements

One of the major issues with privacy and data protection compliance for cloud service customers - especially if based in highly privacy and data protection regulated countries (like the European Countries or some APAC Countries) - arises from cross-border transfers that are a typical way to operate in distributed computing models. Indeed, cloud service customer may be subject to restrictions about the physical location of the cloud service customer data, especially if the location of the personal identifiable information is in third countries that do not offer adequate protection.

It is still quite common to read Master Service Agreements that do not cover explicitly the place where the data centers are or that offer options similar to the following:

"Location of Personal Identifiable Information"

> *"The Provider informs the User about the place(s) of the Provider's data center(s) [and the User can select from which data center the Services will be provided]. The User acknowledges and agrees that the Provider can offer the Services with global resources resident in any of its premises in the world. The User declares and warrants that the Personal Identifiable Information accessible to the Provider in connection with the execution of the Services does not require any export license or that there are no restrictions to the transfer of the Personal Identifiable Information to the Provider's global resources."*

Or

> *"… The User agrees that the Provider may transfer the Personal Identifiable Information outside the country, both inside and outside the [European Union], to the entities and countries listed in Annex [x] if the Provider so deems it appropriate or useful to provide the Services…"*

The cloud service customer should be offered being informed in advance in case of possible transfer of the Personal Identifiable Information and be materially offered the possibility to keep control over the data and taking the necessary steps preventing breaches of its privacy and data protection obligations:

> ***"Location of Data Centers" (sample)***
>
> *"For the purposes of the provision of the Services, the Provider shall store the User's data in the countries and on the infrastructures identified in the Annex [x], unless the User requests in writing that the data center(s) delivering the services are based in [y].*
>
> *If the Provider initiates a change to the then-current storage location(s) resulting in a new or additional country of storage of User's data, the Provider will inform the User by advance notice of [x] days, unless the location change has been requested, authorized, or elected by the User, and provided that the User is in the position to obtain the prior authorizations/license from the competent authorities, if so required by the applicable law, or to terminate the Agreement.*
>
> *The transfer of the User's data out of the European Union/APAC shall be governed by the Standard Contractual Clauses or any equivalent legal basis (BCRs/CBPR/EU-US Safe Harbor or EU-Swiss Safe Harbor)."*

Example 5: Expiration and Termination – Exit Process

Sample clause:

> "*The Master Service Agreement commences on the Effective Date and will remain in force for [●] years unless terminated in accordance with this clause.*

Each Party shall have the right to terminate the Master Service Agreement or some specified Service, at any time for convenience upon 15 days written notice to the other Party.

A Party may terminate this Master Service Agreement for cause: (i) upon 20 days written notice to the other Party of a material breach if such breach remains uncured at the expiration of such period, or (ii) if the Provider fails to respect the SLA under Point [●] of Attachment [●] more than twice in a month; (iii) if the other Party ceases or threatens to cease its business activity.

At the termination or expiration of the Agreement, the Provider shall continue to store and make available to the User the Content for 60 days after the expiration or termination date, allowing the User to download or retrieve them.

Upon request of the User, the Provider shall assist the User in the migration of the Content or Third-Party Software in order to enable the User to have the Services provided by a third party provider or to manage/use them autonomously. As consideration for such assistance, the User shall pay the Provider the due amount in accordance with the hourly rate under Attachment [●] to the Master Service Agreement".

Model specifications

Technical specifications related to SLAs will typically be defined in a separate document from the Master Service Agreement (MSA). Nonetheless, they will usually be included in the agreement by reference, and therefore have equivalent force (unless overridden by clauses in the main agreement).

Because of the highly technical nature of such specifications, how they are defined in terms of content can be challenging. Significant reliance must be placed on clear definitions of terms. Because SLALOM intends to align its work with ISO, it is intended to use ISO definitions wherever they exist or are being developed.

Because of the early stage of SLALOM's work, we do not yet have worked examples of technical specifications (i.e. of metric definitions) to show. The most likely approach we will adopt is that defined in the working draft of ISO/IEC 19086-2 (metrics) [4]. We are asking for feedback (via the questionnaire) about the usefulness of this proposed approach.

Note that if a well-structured approach is followed rigorously, then it should be possible to implement metric specifications in a way which supports automation, such as using XML.

The working draft of ISO/IEC 19086-2 defines the following templates for cloud service level metrics[3]:

[3] Text from the working draft of ISO/IEC 19086-2 is © 2015 ISO/IEC

Abstract Metric Definition Template

Abstract Metric (required)
name (required)
referenceId (required)
unit (required)
scale (required)
expression (required when underlying AbstractMetrics are used)
definition (required)
note (optional)

Abstract Metric Rule Definitions (optional)
name (required)
referenceId (required)
definition (required)
note (optional)

Abstract Metric Parameter Definitions (optional)
name (required)
referenceId (required)
parameterType (required)
definition (required)
note (optional)

underlyingAbstractMetrics (required when AbstractMetric is composed)
name (required)
referenceId (required)

Concrete Metric Definition Template

Metric (required)
name (required)
referenceId (required)
note (optional)

Primary Abstract Metric (required)
name (required)
referenceId (required)

Metric Rules (required if primaryAbstractMetric is associated with RuleDefinitions)
value (required)
ruleDefinition - referenceId (required)
note (optional)

Metric Parameters (required if primaryAbstractMetric is associated with RuleDefinitions)
value (may be set during use of the Metric)

parameterDefinition - referenceId (required)
note (optional)

Alignment to ISO

General

SLALOM will align its work to the extent practical to the ISO standards currently under development for Cloud Service Level Agreements. This section of the questionnaire asks for feedback about the overall structure and content of ISO's work as proposed. It is not necessary to know anything about ISO to give meaningful feedback. Indeed, it is particularly valuable to have feedback from people who are not knowledgeable about ISO work to validate that the proposed structure and content make sense from an ordinary commercial perspective.

ISO has created a working group specifically for Cloud Service Level Agreements, which is currently working on three Cloud SLA standards.[4] It is the intention of SLALOM to make its SLA work consistent with this ISO work, and SLALOM has applied for a liaison relationship with that working group to facilitate this alignment.

SLALOM proposes to use the structure of the proposed ISO/IEC 19086-1 as the basis for its SLA work. While the draft standard makes it clear that this structure is not required for SLAs or contracts, nonetheless it provides a reasonable basis for SLALOM's SLA reference models, one which will be internationally recognized.

SLALOM will diverge from the ISO/IEC 19086 family of standards as regards the full scope of model terms at the Master Service Agreement level, notwithstanding that many of these terms do apply to SLAs. Some of this MSA-level SLA coverage furthermore goes beyond what is proposed in ISO/IEC 19086, e.g. in the following areas:

- Cloud SLA management, including the consequences of violation of SLA provisions (payment of penalties, termination of the MSA, etc)
- Liability (with respect to service level issues)

Additional such issues may be identified during the course of SLALOM's work.

SLALOM also proposes to use relevant ISO definitions where they exist, with particular emphasis placed on ISO/IEC 17788:2014 Cloud computing — Overview and vocabulary; and on parts 1, 2, and 3 of ISO/IEC 19086: SLA framework and terminology. We will propose additional definitions where needed, but with the expectation that ISO definitions will eventually take their place.

[4] ISO/IEC JTC1 Subcommittee 38 Working Group 3 (SC38 WG3) Cloud SLAs. The three standards currently being worked on are:

- ISO/IEC 19086: SLA framework and terminology – Part 1: Overview and concepts, at the Committee Draft stage
- ISO/IEC 19086: SLA framework and terminology – Part 2: Metrics, at the Working Draft stage
- ISO/IEC 19086: SLA framework and terminology – Part 3: Core requirements, at the Working Draft stage

Market feedback on this structure will be given to ISO and well as being used by the SLALOM project.

Structure

The ISO SLA structure is given in the drafts of the ISO/IEC 19086 family of standards.[5] The structure given in Committee Draft 1 of ISO/IEC 19086-1 is shown below in **bold**. Those additional components or details which are identified as 'core' in the draft ISO/IEC 19086-3 are shown in *italics*. Note that 19086-3 is at an earlier draft stage, and more likely to evolve, but 19086-1 is also expected to evolve further, in particular to take account of issues recognized during the development of 19086-3.

The questionnaire accompanying this document asks for feedback on which components are 'core', which are the most important, and which are possibly excessive.

- **Covered services component**
- **SLA definitions component**
- **Service monitoring component**
    - *Monitoring parameters*
    - *Monitoring logs*
- **Roles and responsibilities component**
    - *Responsibility list*
- **Accessibility component**
    - *Accessibility standards*
    - *Accessibility policies*
- **Availability component**
    - *Total downtime*
    - *Availability*
    - *Availability percentage*
    - *Uptime*
    - *Uptime percentage*
    - *Allowable downtime*
    - *Downtime*
- **Cloud service performance component**
    - *Cloud service response time component*
        - *Cloud service response time observation*
        - *Cloud service response time mean*
        - *Cloud service response time variance*
        - *Nth percentile of response time*
        - *Cloud service response time over threshold*
        - *Delay duration time*
    - *Cloud service capacity component*
        - *Number of simultaneous cloud service connections*
        - *Limitation of available cloud service resources*
        - *Cloud service throughput*
        - *Cloud service bandwidth*
    - *Elasticity component*
        - *Elasticity*
        - *Speed*
        - *Precision*

[5] The text shown from the drafts of ISO/IEC 19086-1 and ISO/IEC 19086-3 is © 2015 ISO/IEC.

- **Protection of personally identifiable information component**
- **Information security component** *[o/s to be defined]*
- **Termination of service component**
    - *Notification of service termination*
    - *Return of assets*
- **Cloud service support component**
    - *Support plans*
    - *Support costs*
    - *Support methods*
    - *Support contacts*
    - *Support hours*
    - *Service outage support hours*
    - *Service incident notification*
    - *Service incident reporting*
    - *Service incident notification time*
    - *Maximum incident resolution time*
- **Governance component**
    - *Regulation adherence*
    - *Standard adherence*
    - *Policy adherence*
    - *Audit schedule*
    - *Number of failed SLOs*
- **Service reliability component**
    - *Service resilience/fault tolerance component*
        - *Time to service recovery (TTSR)*
        - *Mean time to service recovery*
        - *Maximum time to service recovery (MTTSR)*
        - *Number of service failures*
        - *Network redundancy*
    - *Customer data backup and restore component*
        - *Backup method*
        - *Backup interval*
        - *Backup verification*
        - *Backup restoration testing*
        - *Backup restoration test reporting*
        - *Retention period for backup data*
        - *Number of backup generations*
        - *Alternative methods for data recovery*
    - *Disaster recovery component*
        - *Cloud service provider disaster recovery plan*
        - *Recovery time objective (TRO)*
        - *Recovery point objective (RPO)*
- **Data management component**
    - *Intellectual property rights component*
    - *Cloud service customer data component*
    - *Cloud service provider data component*
    - *Account data component*
    - *Derived data component*
    - *Data portability component*
    - *Data deletion component*
        - *Data deletion process*

        - *Data deletion notification*
        - *Data deletion time*
    - *Data location component*
        - *Data location*
        - *Data location specification capability*
    - *Data examination component*
    - *Law enforcement access component*
- **Attestations, certifications and audits component**
    - *Cloud service attestations*
    - *Cloud service certifications*
    - *Cloud service audits*

Coverage of scenarios emerging from research

One of the provisions of the original SLALOM proposal was that it would include coverage of scenarios emerging from research. We need feedback to assess the importance the market attaches to different areas of research to determine the relative emphasis we should place on these areas in our final deliverables. Some of the major areas of SLA research which are not (clearly) reflected in the ISO structure above are:

- SLAs at different levels
- Multi-level SLA interaction model
- SLA negotiation across multiple layers
- Automated SLA re-negotiation
- Proactive SLA violation detection

Short descriptions of these research areas / outcomes along with potential uses are summarized in the following paragraphs.

SLAs at different levels

Anastasia - focused on the media domain - would like to obtain a cloud service but as a non-technical user, she can only specify terms at a “high-level” (i.e. not related to resource attributes such as CPU or memory). She wants to specify terms at her own “understandable language” level (e.g. frames per second) so that these terms will be translated to the corresponding technical ones.

The IRMOS EU project has proposed two types of SLAs, namely application and technical along with a mechanism for performing the required translation between these agreements.

Multi-level SLA interaction model

Irene is a data analyst in a financial trading company. She aims at utilizing resources / services offered from two different providers, as her service is both computational- and data-intensive and different providers offer the corresponding “best” services. To this end, a model for cloud federations is required. The model is based on automated SLA offer generation and enables the user to negotiate an SLA with the federation and the federation looks for the best way to satisfy it by negotiating SLAs with one or more providers (on behalf of the user).

The CONTRAIL EU project has proposed an approach for SLAs in multi-provider environments, including a scheme for SLA splitting, which allows for service-, resource-, or performance-based SLA splitting and revenue sharing / compensation provision.

SLA Negotiation across multiple layers

Yannis is a doctor and would like to deploy his eHealth application in a cloud environment. The application requires workflow management that highlights the need for software-layer negotiation on top of the infrastructure-layer negotiation. What is more, the negotiation process across these two layers should be transparent, while domain-specific (i.e. medical) knowledge should also be incorporated in the SLA lifecycle without additional human intervention.

The SLA@SOI EU project implemented a framework that enables different protocols to be injected through an engine, so as to facilitate the interaction between the different layers and entities. Since the protocol will be used for specific interaction, it may include domain specific content.

Automated SLA re-negotiation

Michael is an entrepreneur who has developed a new tourist service that mixes virtual and augmented reality. As an interactive real-time application, there are specific requirements (towards the cloud infrastructure that hosts it) which however change during runtime based on the number of end-users. His goal is to sign a contract with a provider, which will allow automated re-negotiation during runtime without human intervention. The re-negotiation should also address cases where the causes and origin of an agreement violation could be addressed by establishing again a process of negotiation.

The IRMOS EU project has developed an SLA re-negotiation mechanism that can be triggered either by the user (e.g. change in application parameters), by one of the providers (e.g. detection of potential SLA violation) or by the application (e.g. elasticity rules). The mechanism allows for automated re-negotiation during runtime without human intervention.

Proactive SLA violation detection

Gabriel is a computer engineer at the operation center of a publication transportation company. The operation center software has been deployed and is running on a cloud infrastructure. There are specific requirements for downtime (near zero) and availability of these mission critical services. Therefore, he sets explicit values for the aforementioned terms and requires “proactive” mechanisms that will protect his application from any performance degradation or failure.

The VISION Cloud EU project has proposed a proactive SLA violation detection mechanism that bases estimations on the analysis of monitoring data. The analysis enables discovering of repetitive patterns and identification of potential relationships between the different parameters to identify dependencies that may affect the evolution of the parameter values during runtime.

Feedback on these, and on any other unmentioned areas of SLA research, is requested via the questionnaire.

Annex A: About SLALOM

SLALOM: Building a common model for cloud computing SLAs

Slalom is a new European initiative that seeks to remove uncertainty in cloud computing SLAs through standard models. The initiative was launched in January 2015 with the mission to help drive the uptake of cloud services with service level agreement (SLA) model legal clauses and technical specifications.

Industry analysts repeatedly point to uncertainty around legal issues as a major barrier to cloud adoption. Questions such as *who owns my data when I place it in the cloud? What happens if the service provider goes bust? What happens to my applications and data if I miss a payment?* And *which jurisdiction governs my contract*? are common and legitimate questions posed by businesses every day, and these issues are the tip of the iceberg. Furthermore trying to compare providers can become complex when metrics are not uniformly defined. Without like-for-like comparisons, it is difficult to determine the true value proposition, which providers are selling.

A number of groups at European and International scale, such as the European Cloud Partnership and ISO are working towards the standardization of cloud SLAs, debating the distribution of responsibilities between the actors and identifying critical issues that should be addressed. SLALOM is going further, by generating an open and ready-to-use set of model SLA contractual terms and technical specifications for metrics. Adopters will have significant assurance because of using a trustworthy base, which is practical, fair, and understandable, while saving time and resources.

> *"SLALOM will take theory to practice, providing a trusted verifiable starting point for providers and business users to negotiate SLAs for doing business in the Cloud in a simple, fair and transparent way."*
>
> Daniel Field, Project Coordinator, Atos

The initiative is backed by the European Commission and the first stage of the initiative is financed through the H2020 programme, running for 18 months with a budget of 700,000 Euros. The initial members of the SLALOM consortium are global service provider ATOS (project lead), legal firm Bird and Bird (responsible for the legal track), the National Technical University of Athens (responsible for the technical track), the Cloud Industry Forum (responsible for the cloud service provider liaison track) and the University of Piraeus

(responsible for the cloud adopter liaison track). External collaborators and contributors are welcome.

For more information on the initiative contact the coordinator Daniel Field (daniel.field@atos.net), or visit our website slalom-project.eu. SLALOM is funded by the EC under Grant agreement 644270.

Annex B: Reference materials and further reading

A number of (non-exhaustive) further avenues are listed below for readers who wish to better understand the gamut of initiatives taking place in this area within the European Commission. Additionally readers interested in collaborating or becoming involved in this work are invited to contact the SLALOM consortium directly.

The European Strategy on Cloud Computing

In September 2012, the EC published a document entitled "Unleashing the Potential of Cloud Computing in Europe" [1], which identified what the potential impact of cloud on the economies of Europe was, and then identified some steps which should be taken to capture the benefits.

The European Cloud Partnership

One of the actions of this strategy was to establish the European Cloud Partnership [5]. This is a board of executives and representatives from member states.

The ECP produced a report [6], entitled "Establishing a Trusted Cloud Europe", which identified two groups of actions:

- creation of a flexible common framework of best practices, and
- systematic consensus building.

The Cloud Select Industry Groups

The ECP also established a number of Cloud Select Industry Groups (C-SIGs). The C-SIG on SLAs has produced a sequence of 3 reports:

- A short report, produced by Atos, describing 11 key SL indicators;
- A much more comprehensive document from Gartner, including many details derived from their standard texts on cloud service levels;
- A smaller Task force of 5 organisations, each addressing particular aspects of the subject: Performance, Security, Data Management, Personal Data Protection;
- A detailed set of guidelines for SLA standardisation published in June 2014.

A further EC expert group is working on cloud computing contracts, debating the fairness and conflicting perspectives on the clauses regularly found in cloud contracts [3].

ETSI actions on cloud standards

As a further action under the EC cloud Strategy, the European Telecommunications Standards Institute (ETSI) was tasked with "cutting through the jungle of standards", and map existing cloud computing standards in collaboration with all relevant stakeholders. That working group produced a useful analysis [7] of the applicable standards within the arena of cloud.

European Projects

Over recent years a number of European research consortia have investigated and applied SLA lifecycle management frameworks in the context of cloud computing. An expert group was formed

by the European Commission to survey the research outcomes stemming from these projects, and to discuss how these outcomes address the complete SLA lifecycle. Their conclusions were published in June 2013. This report also provided a set of recommendations to support the on-going policy work on SLAs of the Cloud Select Industry Group (SIG), while identifying the research outcomes that can be exploited for the implementation of the recommendations [8].

Additionally, a number of grants have been awarded to research consortia to investigate specific aspects legal, security and data protection in Cloud computing. These include:

The **CIRRUS** project, which delivered recommendations on cloud security standards, certification schemes, as well as international cooperation. In addition a CEN workshop agreement on cloud security assurance has been launched, with an eye on future cloud trends and models. The CIRRUS Green paper is used as the input to several EU trusted cloud initiatives: http://www.cirrus-project.eu/

SLA-READY is a project initiated in January 2015. The consortium aims to make cloud customers, especially small- and medium-sized enterprises (SMEs), SLA-aware, educating and advising them on SLAs. SLA-Ready gives businesses "pain relief" from the SLA challenge, reducing risks and creating certainties. http://www.sla-ready.eu/

The **CUMULUS** Initiative, which collects multiple types of evidence regarding security, including service testing and monitoring data and trusted computing proof. It has models for hybrid, incremental and multilayer security certification with different levels of automation in the certification process steps. http://www.cumulus-project.eu/

The **Coco-Cloud** project, which is delivering machine readable data sharing agreement (DSA) that can define how user data is used, for which purpose and in which context. The main achievement is, however, the automated enforcement of these agreements in the cloud, as well as the contribution to automated evidence-based audits of privacy policies. http://www.coco-cloud.eu/

WITDOM, a group whose research goal is to protect sensitive data in cloud cryptographically, by applying the privacy-by-design paradigm. WITDOM's data protection methods will be tailored to the risks associated with different classes of data. http://www.witdom.eu/

References

[1] Unleashing the potential of Cloud Computing in Europe, COM(2012) 529 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF
[2] IDC, Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely Barriers to Uptake.
http://ec.europa.eu/information_society/activities/cloudcomputing/docs/quantitative_estimates.pdf
[3] http://ec.europa.eu/justice/contract/cloud-computing/expert-group/index_en.htm
[4] ISO/IEC 19086: SLA framework and terminology – Part 2: Metrics, SC38 WG3 N56, version with WG3 comments on CSA expert contribution on 19086-2, uploaded 23 January 2015.
[5] http://ec.europa.eu/digital-agenda/en/european-cloud-partnership
[6] http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=4935
[7] http://www.etsi.org/images/files/Events/2013/2013_CSC_Delivery_WS/CSC-Final_report-013-CSC_Final_report_v1_0_PDF_format-.PDF
[8] http://ec.europa.eu/digital-agenda/en/news/cloud-computing-service-level-agreements-exploitation-research-results