SLA-Ready
Making Cloud SLAs readily usable in the EU private sector

www.sla-ready.eu

Title: Engagement Plan for Standardisation and International Cooperation

Author(s): Jesus Luna, Daniele Catteddu, CSA

Contributor(s): Neeraj Suri, TUD; Silvana Muscella, Nicholas Ferguson, Stephanie Parker, Trust-IT; Thierry Floriani, Guillaume Jahan, Numergy

Date: 27 April , 2015

Coordination and Support Action
Grant Agreement no: 644077
ICT-07-2014: Advanced Cloud Infrastructures and Services

Executive Overview

SLA-Ready is a European initiative driving a common understanding of service level agreements for cloud services (Cloud SLA). With greater standardisation and transparency, organisations can make an informed decision on what services to use, what to expect and what to trust. SLA-Ready services will support SMEs with practical guides, and a social marketplace, encouraging them to carefully plan their journey and make it strategic through an informed, stepping-stone approach, so the cloud and applications grow with their business.

In SLA-Ready, standardisation is a core activity that aims to increase the impact of the common reference model that will be developed within the SLA-Ready project, through alignment with relevant standards and best-practices, and to efficiently orchestrate contributions to a well-defined set of Cloud SLA-related standardisation initiatives (including ISO/IEC 19086). In order to achieve this vision, it is necessary to have clearly defined approach and strategy that allow partners to methodologically focus on selected standardisation activities related to our core Cloud SLA topic.

In SLA-Ready, Work Package 3 (WP3) coordinates activities on International Co-operation, Consensus and Standardisation. This deliverable presents (1) the strategy defined by Work Package 3 to focus on a specific set of related standardisation initiatives, (2) the approach to continuously develop and analyse the standards being considered by SLA-Ready for potential contributions, and (3) the initial feedback from standardisation activities where SLA-Ready has started to collaborate (in particular inputs from the latest ISO/IEC SC38 meeting).

The next version of this deliverable (D3.2)[1] will report the results and contributions from WP3 to selected standardisation bodies, and will provide a refined version of the initial SLA-Ready's standardisation strategy and approach based on achieved outcomes. As part of SLA-Ready's sustainability plan, Deliverable 3.2 will also start drafting the roadmap/strategy for contributing to relevant standardisation activities the timeframe of which is beyond the project's duration (i.e. post December 2017).

1 Deliverable 3.2 "Standardisation and International Cooperation Initial Report", December 2015 (month 12 of the project).

SLA - Ready
Making Cloud SLAs readily usable in the EU private sector

Table of Contents

Table of Tables

Table of Figures

Document information

Deliverable number	D3.1
Deliverable title	Engagement Plan for Standardisation and International Cooperation
Deliverable Nature	Report
Deliverable dissemination level	Public
Contractual delivery	April 2015
Actual delivery date	April 2015
Author(s)	Jesus Luna and Daniele Catteddu (Cloud Security Alliance)
Contributor(s)	Neeraj Suri (TUDA), Silvana Muscella, Nicholas Ferguson, Stephanie Parker (Trust-IT), Thierry Floriani and Guillaume Jahan (Numergy)
Reviewer(s)	Nicholas Ferguson (Trust-IT)
Task(s) contributing to the deliverable	Task 3.1 Standardisation, Best Practices and Recommendations, Task 3.2 International cooperation, consensus building and coordination with the SLA-Ready Advisory Board
Target audience(s)	Cloud Service Providers, Policy Makers, Standardisation Bodies
Total number of pages	44

Disclaimer

SLA-Ready has received funding under Horizon 2020, ICT-07-2014: Advanced Cloud Infrastructures and Services. The information contained in this document is the responsibility of SLA-Ready and does not reflect the views of the European Commission.

1. Introduction

This section introduces the importance of standards/best-practices for SLA-Ready, along with a general overview of this deliverable.

1.1. SLA-Ready and Standards

Co-operation with international organisations, and contributing to relevant standardisation initiatives of the best practices developed by the SLA-Ready consortium, are central tasks in the project. Both tasks are meant to enhance the impact of the project's outcomes. WP3 will be the gateway used to orchestrate the co-operation with international organisations, and to send and receive feedback from standardisation development organisations (SDOs), EU/international working groups, and other forums relevant to the project.

In order to realise the vision of SLA-Ready and produce results with a high impact to the cloud community, there are WP3 deliverables aimed at guaranteeing that:

- The best practices produced in the project timeline target the key components of a cloud SLA, e.g. terminology, metrics and specific security/privacy/performance requirements.
- The work is relevant to the international community, as the cloud is global by nature and seeks solutions that can be applied by organisations regardless of their geographical location.
- The best practices are coherent with the work in progress within the standardisation community.

Moreover, as highlighted by ETSI CSC [1]

> "*there are relatively few existing standards that apply to SLA for cloud services. The main requirement for standardisation in relation to SLA is the creation of an agreed set of terminology and definitions for Service Level Objectives, and an associated set of metrics for each service level objective […] For cloud service providers, such standard definitions would make it easier to create SLAs that describe their services*".

These notions are central to SLA-Ready's WP3.

Moreover, as highlighted by EU funded projects like CIRRUS[2] and CloudWatch[3], (prospective) cloud standards need to be understandable also to non-expert cloud customers willing to uptake this technology. The definition of practices to make standards more user-friendly is another challenge for SLA-Ready's WP3, which will seek to develop customer-centric best practices (please refer to "D3.3 A Business Guide to Service Level Agreements: How to be a well-advised user of cloud services" at month 24).

In order to guarantee that SLA-Ready's outcomes fulfil the objectives presented in the previous paragraphs, it is necessary to create strategic and high-impact synergies with selected of SDOs and standard incubator working groups (WGs). WP3 has designed both (1) a strategy to focus the project's contribution to a selected group of SDOs, and (2) a methodological approach to develop and orchestrate the actual contribution. Both, strategy and approach are presented in this deliverable.

1.2. Positioning D3.1 within SLA-Ready

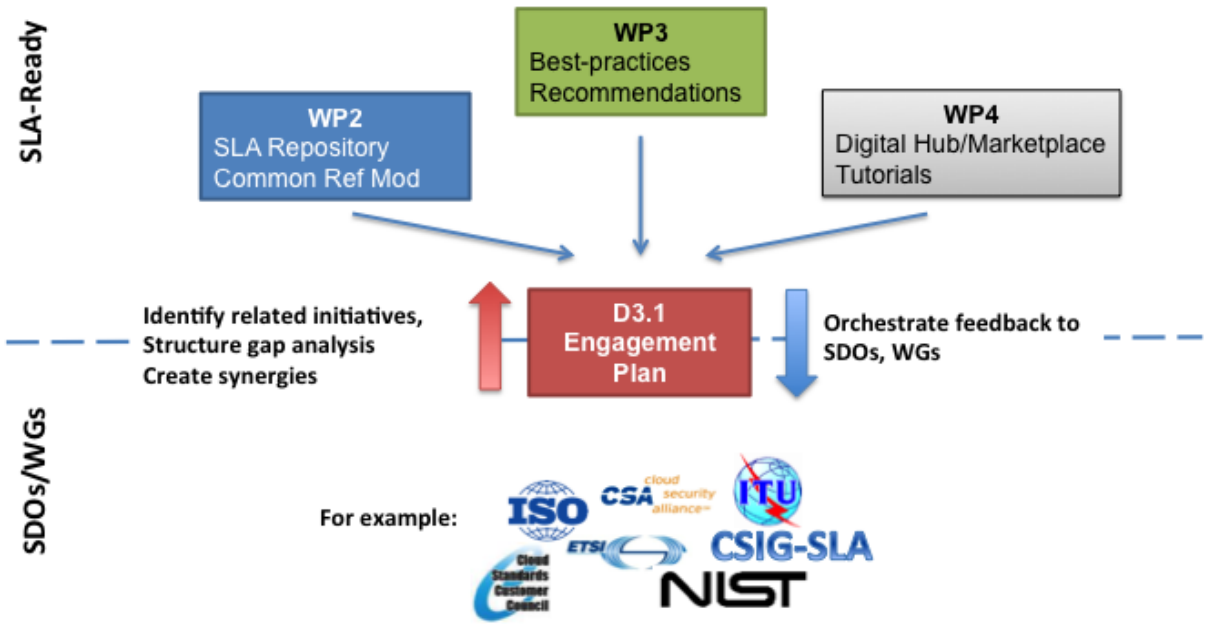
Deliverable 3.1 relates to most of the tasks taking place in SLA-Ready's work packages as highlighted in Figure 1. D3.1 defines a strategy and develops an approach to identify and engage/collaborate with relevant SDOs and standard incubator working groups based on an initial landscape analysis (Sect. 3 and 4). The approach presented in this document also establishes a sub-task to continuously monitor, and engage, wherever relevant, new initiatives. The strategy developed by D3.1 will be used to receive external feedback, and help align SLA-Ready's contributions to real-work requirements (e.g., WP3's best-practices and recommendations). The red arrow in Figure 1 illustrates this process.

The blue arrow in Figure 1 represents the role of D3.1 in the orchestration of contributions coming from SLA-Ready to identify SDOs/WGs. This is the case of WP2's Common Reference model, and WP4's Tutorials-as-a-Service which will be mostly based on developed recommendations. Contributions to standards/best-practices must be carefully planned in order to match the timelines established by the corresponding SDOs/WGs.

2 See, for example, EU FP7 Project CIRRUS "Certification, InteRnationalisation and standaRdisation in cloUd Security". Online: http://www.cirrus-project.eu/.

3 EU FP7 Project CloudWatch, http://www.cloudwatchhub.eu/.

Figure 1. D3.1 within SLA-Ready.



1.3. Structure of this Report

The rest of this report is organised as follows: Section 2 presents WP3's strategy and approach to identify relevant standardisation initiatives and EU/international collaborations of interest. Section 3 performs an initial analysis of the relevant SDOs/WGs landscape, based on the approach introduced in the previous chapter. Finally, Section 4 presents the conclusions of this report.

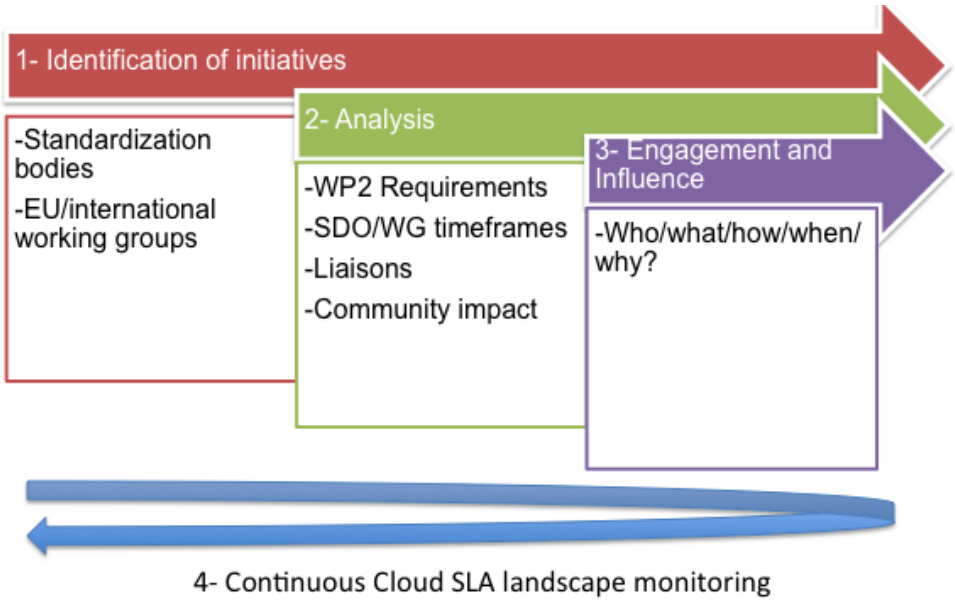
2. Standardisation Strategy and Approach

This section presents the strategy and approach that will be guiding the SLA Ready activities in the area of standardisation and international cooperation. Given the limited resources available for standardisation and international cooperation, the adopted strategy aims to achieve the highest possible impact by focusing on contributions to/receiving feedback from a limited number of highly relevant standards. The approach to implement this strategic vision foresees (1) the identification of the most relevant SDOs and standard incubators WGs initiatives, (2) an analysis of on-going standardisation activities and the input coming from WP2, and (3) the active contribution to the identified standardisation efforts also via the best practices developed by WP2. This section will also elaborate on an activity to (4) continuously monitor the cloud SLA standardisation landscape, e.g. to identify new/incubation standardisation initiatives relevant to WP3.

2.1. WP3 Methodology

Figure 2 highlights the methodological approach that will be put in place to engage with SDOs and standard incubator WGs, and at the same time maximise the community impact of SLA-Ready's outcomes. Our approach comprises three well-identified and incremental stages illustrated by the three arrows in Figure 2. Each approach is built on top of a set of guiding principles, which are illustrated by the text boxes in Figure 2.

Figure 2. Overview of the proposed WP3 approach.



Stage 1 will analyse the relevant SDOs/WGs landscape in order to identify a baseline set of standards/best practices (published or in progress). This will include looking at the activities currently on-going within for instance ISO/IEC, NIST, and CSA.

Stage 2 will feed the baseline into the analysis to be performed by WP3 to further focus on standardisation efforts. The analysis is based on well-defined/realistic criteria, and aligned to WP2's activities.

Stage 3 will see the strategic identification of SDO/WGs initiatives used to establish synergies, and make the actual contributions.

Stage 4 will see the continuous monitoring and analysis of the SLA standardisation/best practices landscape, in order to identify new initiatives that might be of interest for SLA-Ready.

The rest of this section presents in further details the proposed strategy.

2.2. Stage 1 - Identifying relevant initiatives

In order to implement its strategic vision, WP3 will perform a preliminary identification of those standardisation/best-practices initiatives that are relevant to the topic of Cloud SLAs. This activity will take place right at the beginning of the project, and will use as a baseline the following sources of information:

- ETSI Cloud Standards Coordination (CSC) report [1], which includes a list of 147 standards/best-practices (cf., Appendix 2) corresponding to organisations like ISO/IEC, NIST, OGF, and CSA. The ETSI CSC list cover security and privacy, but also aspects like performance.
- Cloud Security Alliance's International Standardisation Council (CSA ISC[4]), which coordinates all standardisation efforts within CSA. As part of its mission, CSA ISC keeps track of (Cloud) standards relevant to security and privacy. At the time of writing this report, the CSA ISC list contained 126 entries (cf., Appendix 3, limited only to standards and not to best-practices).
- Feedback from the Advisory Board (AB): the AB will provide support to this task by leveraging their expertise in the area of SLAs, in particular related to standardisation/best-practices initiatives that have not being considered so far by SLA-Ready.

4 See https://cloudsecurityalliance.org/isc/.

- Inputs from the ISO/IEC SC38 meeting (March-2015) where the following standards were discussed: 19086-Part 1 (vocabulary), 19086-Part 2 (metrics), and 19086-Part 3 (requirements),19086-Part 1 (vocabulary), 19086-Part 2 (metrics), and 19086-Part 3 (requirements). Members of SLA-Ready will participate in the SC38 meeting and their feedback will be part of the present report (cf., Section 3). The next version of this D3.1 will also consider the outcomes from the ISO/IEC SC27 meeting where the fourth part of the ISO/IEC 19086 standard (security and privacy) will be discussed. SLA-Ready has given priority to this standard from the beginning of the project.

This strategic identification will provide an initial baseline for performing the analysis (cf., Section 2.3). WP3 will also update (and re-analyse) this baseline during the duration of the project through its continuous monitoring of the Cloud SLA standardisation landscape (cf., Section 2.5).

2.3. Stage 2 - Driving the analysis

Both of the lists of standards/best-practices (cf., Appendixes 1 - 2) will be analysed, as discussed in the rest of this section, in order to fulfil two main objectives:

1. Focus on a small set of standards/best-practices, taking into consideration the finite resources available to WP3 and their relative importance for SLA-Ready. The actual selection criteria is defined below.
2. Identify opportunities to contribute in the chosen standards/best-practices, taking as input:
    a. The outcomes from WP2 (preliminary reference model for Cloud SLAs),
    b. The results from the upcoming ISO/IEC SC38 meetings (March-2015 and October-2015), and
    c. The selected entries organised according to the SLA life cycle.

The analysis methodology proposed by WP3, acknowledges the strategic vision to focus SLA-Ready's efforts while contributing to standardisation bodies. For this reason, our analysis considers three main criteria:

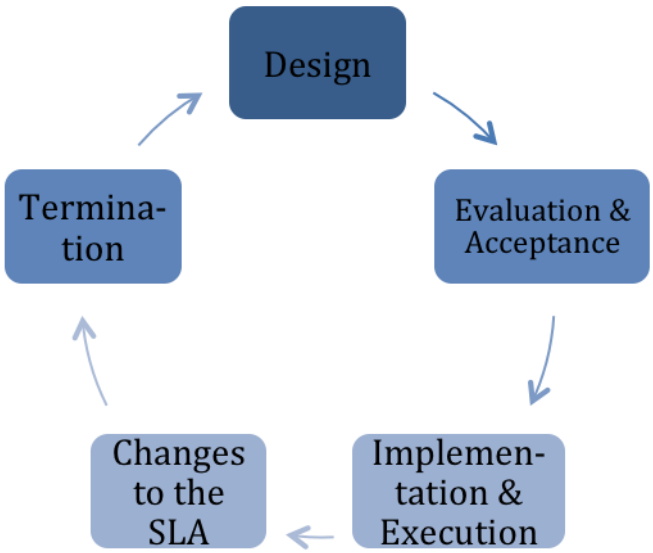
1. **Relevance:** this criterion is useful to identify if a selected standard is directly related to the topic of (Cloud) Service Level Agreements. The relevance of a standard/best-practice should take into account the identified SLA life cycle (as shown in Figure 3, and aligned to WP2).

2. **Opportunity/feasibility:** this second criterion directly relates to the actual opportunity to provide contributions to the respective standardisation body/organisation. The main driver for this criterion is the fact that SLA-Ready's contributions will be feasible only if the following two conditions are fulfilled:
    a. A liaison from any of the SLA-Ready partners exists with the identified standardisation body, in such a way that a formal mechanism exists to communicate and trace the contribution once submitted.
    b. The timeliness of potential contribution is another criterion that directly relates to SLA-Ready's opportunity to provide relevant feedback to identified initiatives (e.g., is the standard on a revision stage? Has a new work item/study period[5] started to be discussed on the standardisation body?). The consortium acknowledges that relevant standards might have a maintenance period falling outside SLA-Ready's duration, therefore avoiding the project to contribute.
3. **Impact:** this final criterion refers to the degree of development associated to a potential contribution from SLA-Ready, and the actual importance (from the standardisation perspective) of such contribution. For example, SLA-Ready's framework could represent a sound/mature contribution to Cloud SLA vocabularies, but not in relationship to the monitoring of SLAs.

The three identified criterion should provide further guidance to WP3 in order to refine the baseline list of identified standards/best-practices (cf., Section 2.2), and therefore aid to focus/prioritise SLA-Ready's contributions. Furthermore, this "refined baseline" will become a concrete starting point for the detailed analysis in relationship to the framework being developed by WP2. The final outcome of this stage will be a reduced number of relevant standards/best-practices, along with a well-identified set of elements where SLA-Ready's contributions can be focused (e.g., vocabularies, metrics, and best-practices).

5 According to the ISO/IEC terminology.

Figure 3 Cloud SLA life-cycle (based on D2.1).



2.4. Stage 3 – Engagement and influence

Once the strategic focus of WP3 has been defined after Stage 2, the main activity to be performed is to orchestrate the contributions from other WPs (in particular WP2) to the identified standard/best-practice. This orchestration should take place in such a way that timeliness and traceability are guaranteed. With respect to the former, it is important for WP3 to establish an individual plan for each one of the identified initiatives to influence. This planning should be fully aligned to the specific timeline established by the governing body (e.g., ISO/IEC, ETSI, IEEE, etc.), and take also into account the potential delays introduced by procedures out of SLA-Ready's control. For example, the CSA ISC working group requires all potential contributions to be agreed by unanimous vote of the members and this might add some unavoidable delays to the overall process. Timeliness is related to the blue arrow in Figure 1.

Traceability is another important aspect to be guaranteed in this stage, and refers to WP3 following-up the progress of the provided contribution after its submission to the governing body of the standard/best-practice. This aspect is useful to provide feedback to the SLA-Ready partners generating the actual contribution, so it can be further refined in case of being necessary. Traceability corresponds to the red arrow in Figure 1.

2.5. Stage 4 - Monitoring the SLA landscape

The final stage in SLA-Ready's strategy to influence relevant standards/best-practices can be seen as a feedback loop in the whole process, where Stages 1 – 3 are periodically repeated in order to adapt WP3 to the (dynamic) Cloud SLA landscape. Even though

renowned standardisation bodies have their strategies defined well in advance (e.g., ISO/IEC and its 19086 family of standards), it is true that the best-practices landscape is much more dynamic and relevant initiatives might appear depending on the identified cloud community needs (as in the case of CSA's working groups).

3. Cloud SLA Standardisation Landscape - preliminary

This section shows the preliminary results of applying WP3's approach (discussed in Section 3), for the purpose of creating a baseline of standards and best practices where to focus SLA-Ready's strategic contributions during the project's duration. In order to provide a comprehensive analysis of the Cloud SLA landscape, the scope[6] of this section considers standardisation bodies, working groups developing related best practices, and research initiatives (e.g., past/on-going EU-funded projects) also working on this particular field (contribution to Cloud SLA standards).

3.1. Standardisation Bodies

The standardisation strategy presented in the previous section was applied to both the list of standards/best practices developed by the ETSI CSC report [1], and also the standards being followed by the CSA ISC working group (partially based on the outputs from the latest ISO/IEC SC38 meeting[7]).

Our preliminary analysis of the ETSI CSC list resulted in the identification of 28 entries (between standards and best practices) that are relevant for the activities in SLA-Ready (please refer to Annex 1). The refined ETSI CSC list identified 15 SDOs/working groups with initiatives related to the topic of Cloud SLAs. The vast majority of the identified related works are from CSA (6), followed by TMF (3), and OGF/CSCC/NIST and GICTF (each one with 2 entries).

While some of these initiatives have a specific focus (e.g., CSA's are security and privacy-related), some others have a broader scope (e.g., CSCC's reports). We must highlight that not all of the identified initiatives fulfil the "opportunity" criteria (cf., Section 4), meaning that either an SLA-Ready liaison with the standards organisation does not exist or that the standard is not being currently revised. In any case, all of the identified entries should be taken into consideration for the development of SLA-Ready's conceptual model in WP2. A more detailed analysis of each individual entry, based on WP3's strategic approach, will be reported in the next version of this deliverable.

Based on the analysis of the CSA ISC list our approach also identified a set of standards of interest for SLA-Ready (cf., Table 1). Some of these are directly related to the topic of Cloud SLAs (e.g., the 19086 family of standards), whereas others relate to SLAs from the life cycle (e.g., ITU-T Y.e2ecslm-Req) or the security-as-a-service (e.g., ITU-T

6 The results presented are relevant at the time of writing this report.

7 March, 2015 in Vienna, Austria.

Y.cloudSECasaservice) perspectives. More generally, all selected entries relate to the SLA life cycle for example:

- ITU-T X.CSCDataSec focuses on the decision making stage, where customers build their criteria for selecting a Cloud service. Similarly, ITU-T Y.cloudtrustmodels considers the CSP perspective by proposing a risk management framework as part of the SLA life cycle.
- Operational aspects of the Cloud SLA, in particular related to (continuous) monitoring, are proposed by ISO/IEC 27004 and 27007.
- Finally, SLA termination is discussed in ISO/IEC 19086-P1.

Table 1 below presents the selected entries from CSA ISC working group, which takes into account not only their relevance to the topic of Cloud SLAs, but also the opportunity that the consortium will have to contribute during the project's life time. This can be observed by the fact that most of the ISO/IEC initiatives are currently in their early stage of development (e.g., study periods, and working drafts). More information about the life cycle of ISO/IEC standards can be found in [2]. Table 1 also considers those standards of relevance to SLA-Ready based on the discussions and outcomes from the latest ISO/IEC SC38 meeting.

Table 1. Preliminary WP3 focus based on the CSA ISC list of standards and the latest ISO/IEC SC38 meeting

SDO	Project #/ Projects Reference #	Title/Topic	Relevance to SLA-Ready (preliminary analysis)
ITU-T SG13	Y.cloudSECasaservice	Framework for security as a cloud service	Relevant to the overall SLA life-cycle.
ITU-T SG13	Y.cloudtrustmodels	Framework for cloud security trust and risk management	Preliminary draft has some links to the importance of SLAs.
ITU-T SG13	Y.e2ecslm-Req	End-to-end cloud service lifecycle management	Potentially can include a discussion on the "holistic" role of SLAs (whole supply chain).
ITU-T SG13	Y.inter-cloud-sec	Security Aspects of Inter-Cloud Computing	Early draft discusses continuous security monitoring based on (SLA) metrics.
ITU-T SG17	X.CSCDataSec	Guidelines for Cloud Service Customer Data Security	May be related to SLA-Ready's best-practices.

SDO	Project #/ Projects Reference #	Title/Topic	Relevance to SLA-Ready (preliminary analysis)
ISO/IEC SC27 WG1	27004	Information security management – Monitoring, measurement, analysis and evaluation	Discusses important aspects associated to the management of Cloud security SLAs.
ISO/IEC SC27 WG1	27007	Guidelines for information security management systems auditing	SLA-Ready might contribute with a discussion on the role of auditors and SLAs.
ISO/IEC SC27 WG3	19791	Information technology – Security techniques -- Security assessment of operational systems	As above, SLA-Ready might contribute with a discussion on the role of security assessment and SLAs.
ISO/IEC SC27 WG3	Study Period	Continuous security monitoring of operational systems	Terms of reference in this study period may fit the SLA topic.
ISO/IEC SC27 WG4	27044	Guidelines for security information and event management (SIEM)	Research community has identified a strong link among SLA management and SIEM.
ISO/IEC SC27 WG4	19086-4	Cloud computing – Service Level Agreement (SLA) Framework – Part 4: Security and privacy	Highly relevant standard for SLA-Ready given its SLA focus.
ISO/IEC SC27 WG4	27036-4	Information security for supplier relationships – Part 4: Guidelines for security of cloud service	Early draft with potential to integrate a discussion on the role of SLAs.
ISO/IEC SC38 WG3	19086-1	Cloud computing – Service Level Agreement (SLA) Framework – Part 1: Overview and concepts	Highly relevant standard for SLA-Ready given its SLA focus.
ISO/IEC SC38 WG3	19086-2	Cloud computing – Service Level Agreement (SLA) Framework – Part 2: Metrics	Highly relevant standard for SLA-Ready given its SLA focus.

SDO	Project #/ Projects Reference #	Title/Topic	Relevance to SLA-Ready (preliminary analysis)
ISO/IEC SC38 WG3	19086-3	Cloud computing – Service Level Agreement (SLA) Framework – Part 3: Core requirements	Highly relevant standard for SLA-Ready given its SLA focus.

As mentioned early in this section, a more comprehensive analysis of the selected SDO initiatives will be the focus of the upcoming Task 3.1 activities in SLA-Ready.

3.2. Advisory Board, Supporters and Working Groups

In order to iteratively validate and enhance SLA-Ready outcomes, the project shall engage an Advisory Board (AB) of external experts. Members are drawn from a variety of countries to reflect the importance of international collaboration in this area and of leveraging best practices from countries with more experience in this field. Each AB member already contributes to a working group that is active in the area of SLAs. They are expected also to assist SLA-Ready in gaining influence over key SDOs and WGs for better alignment and interaction of their initiatives. Indeed, AB members are expected to play a key role in ensuring that SLA-Ready outputs have real impact and benefit the cloud SLA life-cycle. As outlined in Sections 2.3 and 2.4, it is important that SLA-Ready can engage and influence SDOs. AB members can provide key information on SDO mechanisms, requirements and goals so that SLA-Ready input is both timely and appropriate. Members are therefore selected based on their involvement with selected SDOs. The AB contributions to SLA-Ready shall be publicly acknowledged.

AB members will support activities focusing on the following activities associated with different Work Package tasks:

- **WP2**: Contribute to consensus building through the collective elicitation of technical, socio-economic and legal requirements identified in D2.1.
- **WP3**: Facilitate the adoption of a set of expert-validated, standards-aligned outcomes, namely the Reference Model for SLAs, and shall support the best practices/recommendations and new services provided by SLA-Ready. This will include the following:
    - Advice on the progress of SLA-Ready activities and outputs.

- Information on current standards landscape in particular the SDOs/WGs they are involved with and how SLA-Ready outputs can contribute to these activities. This could include gaps in current standards or documents that SLA-Ready can address; re-iterations of current standards or documents to which SLA-Ready can contribute; or new activities or standards being proposed.
- Practical information and links regarding adoption of SLA-Ready outputs in relevant documentation and relevant timelines and guidelines.

- **WP4**: Facilitate the dissemination of a set of expert-validated, standard-aligned outcomes, namely the reference model for SLAs and, best practices/recommendations and services that will ultimately facilitate cloud adoption. WP4 also provides core messaging on the business case for standardisation, especially to promote its importance to SMEs. An added bonus of WP4 messaging comes from knowledge and strong links to the Internet of Things (IoT) community. Capturing insights will therefore be an added value of SLA-Ready as the potential of cloud computing in Europe increasingly shifts towards IoT rather than generic cloud services only. Sharing these insights with the target audiences of SLA-Ready will not only ensure timely communications on trends impacting on the uptake of cloud services but also shed light on key issues like security. From an international perspective, WP4 can also be a channel for disseminating co-operation between Europe and Japan, South Korea and the U.S. on the future internet, further linking it to the AB and supporters of SLA-Ready, as detailed below.

3.3. Potential AB members

Robert Bohn, National Institute of Standards and Technology (NIST), US
Standards initiative: NIST Cloud Computing Reference Architecture and Taxonomy Working Group & ISO/IEC19086
Potential contribution to SLA-Ready: Collaboration related to ISO/IEC 19086 (Parts 1 – 3), NIST WGs, and other US-based initiatives.

Margot Dor, ETSI, FR
Standards initiative: ETSI Cloud Standards Coordination
Potential contribution to SLA-Ready: Feedback on lists of selected standards, and planned ETSI activities.

Peter Deussen, Fraunhofer FOKUS, DE
Standards initiative: ISO country representative, Germany
Potential contribution to SLA-Ready: Feedback on lists of selected standards and Germany-based WGs.

John Kennedy, Intel Labs. UK
Standards initiative: OGF OCCI (Open Cloud Computing Interface)
Potential contribution to SLA-Ready: Feedback on activities related to OCCI in the field of SLAs.

Laura Lindsay, Microsoft, US
Standards initiative: Co-editor, ISO19086
Potential contribution to SLA-Ready: Collaboration related to ISO/IEC 19086 (Parts 1 – 3). Feedback on lists of selected standards.

Seungyun Lee, Electronics and Telecommunications Research Institute, KR
Standards initiative: Convenor, ISO, JTC 1 SC 38
Potential contribution to SLA-Ready: Distributed Application Platforms and Services (DAPS) Korea; Collaboration related to ISO/IEC 19086 (Parts 1 – 3). Feedback on lists of selected standards.
Beniamino Di Martino, Second University of Naples, Italy
Standards initiative: Cloud Standards Customer Council
Potential contribution to SLA-Ready: Feedback on lists of selected CSCC standards, and feedback on research initiatives.

Monique Morrow, Cisco Systems, US
Standards initiative: ITU-T
Potential contribution to SLA-Ready: Feedback on lists of selected standards, and planned ITU-T activities.

Toshihiro Suzuki, Oracle, JP
Standards initiative: Co-editor, ISO19086 Part 1
Potential contribution to SLA-Ready: Collaboration related to ISO/IEC 19086. Feedback on selected standards and WGs

Wolfgang Ziegler, Fraunhofer SCAI, DE
Standards initiative: OGF WS-Agreement representative
Potential contribution to SLA-Ready: Feedback on lists of selected standards, and planned OGF activities.

An AB Terms or Reference (ToR) describes the tasks requested of members. This is shown in Annex 4.

In addition to the AB Members, SLA-Ready shall seek the support of technical and non-technical stakeholders that can aid its strategic goal as flexibly as possible. These stakeholders shall be referred to as "Supporters", operating mainly on a volunteer basis so as to ensure different perspectives are represented and to gain the broadest possible consensus.

The approach shall be international in scope and target representatives whose viewpoints cover SME target groups, privacy and security issues, IT procurement and business aspects. Mutual visibility shall be ensured through logos and/or expert profiles, as appropriate. Such interaction will also cover future Internet experts and stakeholders.

Interaction shall take place during project and external events (e.g. side meetings, panel debates) and/or through interviews (e.g. phone, face-to-face, email) based on clearly defined and commonly agreed criteria for seeking the expertise and stakeholder communities represented. More details on this group are included in D4.1 "Communication and Dissemination Plan".

Besides, SLA-Ready shall liaise with and build upon existing EU/international WGs of interest for the project, in the same manner as for SDOs. Such WGs includes but are not limited to:

Table 2 Selected Working Groups of interest for the project

Working group	Focus	Value for SLA Ready
Cloud Select Industry	European Commission (EC) (DG	This WG can provide

Group – Subgroup on Service Level Agreement (C-SIG-SLA)[8]	CONNECT) set up the C-SIG-SLA. This industry group provides a set of SLA standardisation guidelines for cloud service providers and professional cloud service customers, while ensuring the specific needs of the European cloud market and industry are taken into account. The C-SIG SLA also has a sub-committee in charge of providing feedback to ISO/IEC 19086.	meaningful insight from a larger panel of experts and stakeholders targeting the same transparency and clarification on SLAs. Members of SLA-Ready are part of the referenced C-SIG SLA sub-committee.
Cloud Select Industry Group – Subgroup on Certification (C-SIG-Certification)[9] and ENISA's Cloud Certification page[10]	EC (DG CONNECT) set up the C-SIG-Certification, an industry and certification organisations group to provide a detailed list of cloud relevant security certification schemes and a so-called Meta framework to compare those schemes as regards cloud customers' security requirements.	This WG provides requirements on security that could be reflected in SLAs as it is a customer concern. Certification could be thus viewed as a is recognised level of security to value/express as SLA.
Cloud Select Industry Group – Subgroup on data protection (C-SIG-Code of conduct)	EC (DG CONNECT) set up the C-SIG-Code of conduct, an industry group to provide a set of data protection guidelines for professionals and customers which principles may be voluntarily endorsed.	This Code of conduct could be a basis for SLOs, depending on the level of implication in the data processing.
Expert Group on Cloud Computing Contracts[11]	EC (DG Justice and Consumers) set up this group of data protection experts, industry and customers stakeholders and lawyers or academia, to assist the EC in the identification of safe and fair contract terms and conditions for cloud computing services for consumers and small firms. The group shall take into account existing best market practices in contract terms and conditions in cloud computing contracts, as well as the relevant provisions of Directive 95/46/C	Various working papers on availability, liability, content and transfer of data, to be reinterpreted for SME (as opposed to consumers and small firms that are the focus of this WG).

8 http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?action=display&doc_id=6138.

9 http://bookshop.europa.eu/en/certification-schemes-for-cloud-computing-pbKK0414719/.

10 https://resilience.enisa.europa.eu/cloud-computing-certification.

11 http://ec.europa.eu/justice/contract/cloud-computing/expert-group/index_en.htm.

WG for definition for trusted cloud with the French security agency	Provides a detailed list of cloud relevant security requirements and defines the corresponding certification scheme. This certification will be a pre-requisite to French government data.	More or less all the EU governments have the same security requirements. This could be interesting basis for developing high security level SLAs.

4. Conclusions and Next Steps

This report presents the strategy and methodological approach proposed by WP3 to identify highly significant standards/best-practices, on which SLA-Ready's efforts will focus. This deliverable also includes preliminary results of the initial collection and analysis of the standardisation information gathered during the first 4 months of SLA-Ready.

Together with the an initial list of standards and best-practices identified, SLA-Ready will also focus on relevant efforts developed under the auspices of the CSA (namely Cloud Control Matrix, CloudAudit, Cloud Trust Protocol, Privacy Level Agreement, Open Certification Framework). The standards and best practices currently selected as priorities are in the areas of SLA, metrics for information security, security information and event management, auditing, assessment, supply chain management.

A wish-list of experts that will make up the SLA-Ready Advisory Board has also been established. Representing SDOs and working groups in particular related to Table 1 and Annex 2, the AB members will now be contacted (using the ToR shown in Annex 4) and invited to join the group. Based on positive replies to this invitation, potential collaboration will be further defined including (1) how the individual can contribute to the outputs of SLA-Ready, and (2) how SLA-Ready can contribute to their organisations/WGs that they represent.

It is important to note that priorities identified after the preliminary analysis presented in this report may be reviewed based on the collection of further input during the execution of WP3 activities.

As concluded at the last ISO/IEC SC38 meeting (March 2015), it is likely that priority will be given to the ISO/IEC 19086 standards (Parts 1-2-3-4) both because it is the most relevant in the scope of SLA-Ready activities, and because it is the standard where SLA-Ready is most likely to generate impact (based on the approach presented in this report). In addition, there are opportunities for SLA-Ready to provide support to ISO/IEC 19086-2 in the creation of use cases describing a particular implementation of SLAs (e.g. "Scenarios"), and to ISO/IEC 19086-4 that will specifically cover Security and Privacy related SLAs.

References

[1] European Telecommunications Standards Institute. "Cloud Standards Coordination – Final Report." Technical Report. Online: http://www.etsi.org/images/files/Events/2013/2013_CSC_Delivery_WS/CSC-Final_report-013-CSC_Final_report_v1_0_PDF_format-.PDF 2013.

[2] International Organisation for Standardisation (ISO). "How does ISO develop standards." Online: http://www.iso.org/iso/home/standards_development.htm

Annex 2 – ETSI Cloud Standards Coordination: list of standards and best-practices relevant to SLA-Ready

This annex presents the list of standards/best-practices relevant to the work in SLA-Ready and based on the ETSI CSC report [1] (list partially contributed by partner CSA). The corresponding analysis is summarised in Section 3 of this deliverable.

Organisation/ group	ID	Title	Description
ATIS	ATIS-0200008	Trusted Information Exchange (TIE)	This document describes the Trusted Information Exchange requirements for ATIS CSF (Cloud Services Forum)-defined services.
CSA	CCM \3.0	Cloud Control Matrix	A set of controls for cloud providers which, aligned with CSA guidance, cover risks associated with cloud security and help differentiate the lines between host responsibility and customer responsibility.
CSA	Security Guidance	Security Guidance for Critical Areas of Focus in Cloud Computing	Outlines key issues and provides advice for both Cloud Computing customers and providers within 15 strategic domains.
CSA	CTP	Cloud Trust Protocol	Protocol and API definition for cloud security property monitoring. CTP is the mechanism that provides information about the elements of transparency as applied to cloud service providers.
CSA	A6	Cloud Audit	The goal of CloudAudit is to provide a common interface and namespace that allows enterprises who are interested in streamlining their audit processes (cloud or otherwise) as well as cloud computing providers to automate the Audit, Assertion, Assessment, and Assurance of their infrastructure (IaaS), platform (PaaS), and application (SaaS) environments and allow authorised

Organisation/ group	ID	Title	Description
			consumers of their services to do likewise via an open, extensible and secure interface and methodology.
CSA	CAIQ	Consensus Assessments Initiative Questionnaire	This questionnaire provides a set of questions a cloud consumer and cloud auditor may wish to ask of a cloud provider. It provides a series of "yes or no" control assertion questions which can then be tailored to suit each unique cloud customer's evidentiary requirements.
CSA	PLA	Privacy Level Agreement	Baselines for compliance with data protection legislation and best practices by defining a standard format for Privacy Level Agreements (PLAs) and standards, through which a cloud service provider declares the level of privacy (personal data protection and security) that it sustains for the relevant data processing.
CSCC	n/a	Public Cloud Service Agreements: What to Expect and What to Negotiate	Customer view of cloud service agreements & SLAs
CSCC	n/a	Practical Guide to Cloud Service Level Agreements	Explanation of SLAs for cloud computing
CSMIC	SMI Framework 2	Service Measurement Index - measures for Cloud Services	

Organisation/ group	ID	Title	Description
ENISA	ProcureSecure	Procure Secure - A guide to monitoring of security service levels in cloud contracts	A practical guide aimed at the procurement and governance of cloud services. This guide provides advice on questions to ask about the monitoring of security.
ETSI / TC CLOUD	TR 103 125	SLAs for Cloud services	The document aims to review previous work on SLAs including ETSI guides from TC USER and contributions from EuroCIO, etc, and to derive potential requirements for cloud specific SLA standards.
ETSI / TC USER	EG 202 009-3	Quality of telecom services; Part 3: Template for Service Level Agreements (SLA)	Since the publication of EG 202 009, additional work has been completed among the user organisations while new QoS related standards have been made available by ETSI
FI-WARE	n/a	SLAware: Service Level Agreements Specification	
GICTF	n/a	Use Cases and Functional Requirements for Inter-Cloud Computing	Inter cloud use cases and requirements
GICTF	n/a	Technical requirements for inter cloud networking	Specifications for inter cloud
ITU-T	FG Cloud Part 5	Cloud security	To identify cloud security threats and requirements
NIST	SP 500-292	NIST Cloud Computing reference Architecture	NIST Cloud Computing reference Architecture

Organisation/ group	ID	Title	Description
NIST	800-53 Rev. 4	Security Controls	Security and Privacy Controls for Federal Information systems and organisations.
OCCI	OCCI-SLA	OCCI Service Level Agreements	This document produced by the OCCI provides a high-level definition of a Protocol and API in relation with the SLAs extension of the OCCI Core Model.
OGF	GFD.192	Web Services Agreement (WS-Agreement)	The Web Services Agreement Specification (WS-Agreement), a Web Services protocol for establishing agreement between two parties, such as between a service provider and consumer.
OGF	GFD.193	WS-Agreement Negotiation	The WS-Agreement Negotiation specification, a Web Services protocol for multi-round negotiation of an agreement between two parties, such as between a service provider and consumer.
QuEST Forum	TL9000	TL 9000 Measurements Handbook	The TL9000 Measurements Handbook Release 5.0 is a comprehensive guide to measurements processing, usage, responsibilities and requirements. It identifies performance measurements in the key areas of hardware, software, common, outage and service quality.
SLA@SOI	D.A5a	SLA: An abstract syntax for Service Level Agreements	Machine readable specification for SLAs.
TMF	GB917	SLA Management Handbook	This handbook provides a full set of definitions, rules and methodology for the specification, deployment and management of SLAs, as well as useful tools and best practices, for use by both Customers and Service Providers.

Organisation/ group	ID	Title	Description
TMF	GB963	Cloud SLA Application Note	This application note is intended for Enterprise Cloud Service Providers desiring to offer a commercially credible SLA based on ECLC "Enterprise-Grade External Compute IaaS v1.0", and for an Enterprise Customer seeking enterprise-grade SLAs.
TMF	TR178	Enabling End-to-End Cloud SLA Management	This Technical Report takes an outside-in look by reviewing existing relevant SLA-related industry work (DMTF, OGF, NIST, CSMIC, ITU-T, ISMA, OASIS and other), and then comparing with the best practices from the TM Forum SLA management Handbook (GB917).

Annex 3 – CSA International Standardisation Council – list of observed standards (March-2015)

Next we report the list of standards being monitored by CSA's ISC working group, partially based on the outcomes from the latest ISO/IEC SC38 meeting. As discussed in the present report, SLA-Ready is using this list as part of its baseline set of considered standards (please refer to Section 3 for more information).

SDO	SDO Reference number	Title/Topic
ITU-T SG13	Q18/13 Y.ccic	Framework of inter-cloud for network and infrastructure
ITU-T SG13	Q17/13 Y.BigData-reqts	Requirements and capabilities for cloud computing based big data
ITU-T SG13	Q26/13 Y.cceco	Cloud computing: ecosystem, use cases and general requirements
ITU-T SG13	Q18/13 Y.cciaas	Cloud computing - Functional requirements of Infrastructure as a Service
ITU-T SG13	Q27/13 Y.ccinfra	Cloud computing infrastructure requirements
ITU-T SG13	Q18/13 Y.ccnaas	Cloud computing - Functional requirements of Network as a Service
ITU-T SG13	Q8/13 Y.cloudtrustmodels	Framework for security as a cloud service
ITU-T SG13	Y.Cloud-SIDE-Reqts	High level requirements and capabilities for cloud enabled service environment

ITU-T SG13	Q8/13 Y.cloudSECasaservice	Framework for cloud security trust and risk management
ITU-T SG13	Q8/13 Y.clouduse&req	Cloud security use cases and requirements
ITU-T SG13	Q17/13 Y.daas	Requirement and reference architecture of desktop as a service
ITU-T SG13	Q19/13 Y.e2eccrmr	End-to-end cloud computing resources management requirements
ITU-T SG13	Q19/13 Y.e2ecslm-Req	End-to-end cloud service lifecycle management
ITU-T SG13	Q8/13 Y.inter-cloud-sec	Security Aspects of Inter-Cloud Computing
ITU-T SG13	Q6/13 Y.VNC	Resource control and management for virtual networks for cloud services (VNCs)
ITU-T SG17	Q10/17 X.ccidm	Requirement of IdM in cloud computing
ITU-T SG17	n/a	Guidelines for Cloud Service Customer Data Security
ITU-T SG17	Q8/17 X.goscc	Guidelines of operational security for cloud computing
ITU-T SG17	Q8/17 X.sfcse	Security functional requirements for Software as a Service (SaaS) application environment
SC27 WG1	SC27 N14733	Information security management systems — Overview and vocabulary

SC27 WG1	SC27 N14717	Information Security Management System – Guidance
SC27 WG1	SC27 N14741	Information security management – Monitoring, measurement, analysis and evaluation
SC27 WG1	WG1 N00027	Information security – Risk management
SC27 WG1	SC27 N14704	Requirements for bodies providing audit and certification of information security management systems
SC27 WG1	WG1 N00008	Guidelines for information security management systems auditing
SC27 WG1	WG1 N00012	Guidelines for auditors on information security controls
SC27 WG1	SC27 N14706	Sector-specific application of ISO/IEC 27001 – Requirements
SC27 WG1	SC27 N14732	Information security management for inter--sector and inter--organisational communications
SC27 WG1	SC27 N14712	Guidelines on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
SC27 WG1	WG1 N00023	Review of Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry

SC27 WG1	WG1	Competence requirements for information security management systems professionals
SC27 WG1	SC27 N14704	Mapping the Revised Editions of ISO/IEC 27001 and ISO/IEC 27002
SC27 WG1	SC27 N14710	Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organisations
SC27 WG1	SC27 N14714	Code of practice for information security controls for cloud computing services based on ISO/IEC 27002
SC27 WG1	WG1 N00022	Future Version Development of ISO/IEC 27000
SC27 WG1	WG1 N00024	Cloud Risk Management (CRM)
SC27 WG2	SC27 N14754	Modes of operation for an n-bit block cipher
SC27 WG2	SC27 N14758	Prime number generation
SC27 WG2	WG2 N1005	Hash-functions – Part 3: Dedicated hash-functions
SC27 WG2	SC27 N14762	Key management – Part Part 3: Mechanisms using asymmetric techniques
SC27 WG2	WG2 N1007	Key management – Part 4: Mechanisms based on weak secrets
SC27 WG2	SC27 N14764	Key management – Part 6: Key derivation

SC27 WG2	SC27 N14756	Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms
SC27 WG2	SC27 N14757	Cryptographic techniques based on elliptic curves – Part 1: General
SC27 WG2	WG2 N1003	Encryption algorithms – Part 6: Homomorphic encryption
SC27 WG2	SC27 N14774	Blind digital signatures – Part 1: General
SC27 WG2	SC27 N14776	Blind digital signatures – Part 2: Discrete logarithm based mechanisms
SC27 WG2	WG2 N1013	Secret sharing – Part 1: General
SC27 WG2	WG2 N1015	Secret sharing – Part 2: Fundamental mechanisms
SC27 WG2	WG2 N1010	Anonymous entity authentication — Part 3: Mechanisms based blind signature
SC27 WG2	SC27 N14759	Anonymous entity authentication — Part 4: Mechanisms based on weak secrets
SC27 WG2	SC27 N14772	Lightweight cryptography – Part 5: Hash-functions
SC27 WG2	WG2 N1002	Entity authentication – Part 2: Mechanisms using symmetric encipherment algorithms
SC27 WG2	WG2 N1003	Entity authentication – Part 3: Mechanisms using digital signature techniques
SC27 WG2	WG2 N1030	CfC for Study Period on Required security properties in key management mechanisms

SC27 WG2	WG2 N1044	CfC for Study Period on Random bit generation
SC27 WG2	WG2 N1031	CfC for Study Period on Revision of ISO/IEC 11770-4
SC27 WG2	WG2 N1032	CfC for Study Period on Review of UK proposal for a new mechanism in ISO/IEC 11770-3
SC27 WG2	WG2 N1033	CfC for Study Period on Amendment to ISO/IEC 29192-2
SC27 WG2	WG2 N1034	CfC for Study Period on MACs to include Chaskey
SC27 WG3	SC27 N14891	Testing Methods for the Mitigation of Non-invasive Attack Classes Against Cryptographic Modules
SC27 WG3	SC27 N13713	Cryptographic algorithms and security mechanisms conformance testing
SC27 WG3	WG 3 N1111	Catalogue of Architectural and Design Principles for Secure Products, Systems, and Applications
SC27 WG3	WG 3 N1114	Guidance for developing security and privacy functional requirements based on ISO/IEC 15408 techniques -- Security assessment of operational systems
SC27 WG3	WG 3 N1117	Information technology – Security techniques -- Security assessment of

		operational systems
SC27 WG3	SC 27 N14451	Physical Security Attacks, Mitigation Techniques and Security Requirements
SC27 WG3	WG 3 N1122	Competence requirements for information security testers and evaluators — Part 1 Introduction, concepts and general requirements
SC27 WG3	WG 3 N1135	Competence requirements for information security testers and evaluators — Part 2: Knowledge, skills and effectiveness requirements for ISO/IEC 19790 testers
SC27 WG3	WG 3 N1137	Security evaluation of presentation attack detection for biometrics
SC27 WG3	SC27 N14871	Refining Software Vulnerability Analysis Under ISO/IEC 15408 and ISO/IEC 18045 - Part 1: Using publicly available information security resources **
SC27 WG3	WG 3 N1123	Refining Software Vulnerability Analysis Under ISO/IEC 15408 and ISO/IEC 18045 - Part 2: CWE and CAPEC based software penetration testing**

SC27 WG3	WG 3 N1124	Test tool requirements and test tool calibration methods for use in testing noninvasive attack mitigation techniques in cryptographic modules — Part 1: Test tools and techniques
SC27 WG3	WG 3 N1136	Test tool requirements and test tool calibration methods for use in testing noninvasive attack mitigation techniques in cryptographic modules — Part: 2 Test calibration methods and apparatus
SC27 WG3	SC27	High-assurance evaluation under ISO/IEC 15408/18045
SC27 WG3	SC27 N14867	Physically unclonable functions for non-stored security parameter generation
SC27 WG3	SC27 N14444	Continuous security monitoring of operational systems
SC27 WG3	SC 27 N14425	Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408
SC27 WG3	SC 27 N14853	Guidelines for Testing Cryptographic Modules in their Operational environment
SC27 WG4		Selection, deployment and operation of intrusion detection and prevention systems (IDPS)

SC27 WG4	SC27 N14792	Storage security
SC27 WG4	SC27	Guidance on assuring suitability and adequacy of incident investigation methods
SC27 WG4	SC27	Guidelines for the analysis and interpretation of digital evidence
SC27 WG4	SC27 N14888	Incident investigation principles and processes
SC27 WG4	WG4	Guidelines for security information and event management (SIEM)
SC27 WG4	WG4	Guidelines for the use and management of Trust Service Providers – Part 1: Overview and concepts
SC27 WG4	WG4	Guidelines for the use and management of Trust Service Providers – Part 2: Guidelines on information security of PKI Trust Service Providers
SC27 WG4	WG4	Guidelines for the use and management of Trust Service Providers – Part 3: Guidelines on provision of services by PKI Trust Service Providers
SC27 WG4	SC27 N14806	Cloud computing – Service Level Agreement (SLA) Framework – Part 4: Security and privacy
SC27 WG4	SC27	Network security – Part 1: Overview and concepts

SC27 WG4	SC27	Network security – Part 6: Securing wireless IP network access
SC27 WG4	SC27	Application security – Part 2: Organisation normative framework
SC27 WG4	WG4	Application security – Part 3: Application security management process
SC27 WG4	SC27	Application security – Part 5: Protocols and application security control data structure
SC27 WG4	WG4	Application security – Part 5-1: Protocols and application security controldata structure – XML Schemas
SC27 WG4	SC27	Application security – Part 6: Security guidance for specific applications
SC27 WG4	WG4	Application security – Part 7: Application security control attribute predictability
SC27 WG4	SC27	Information security incident management – Part 1: Principles of incident management
SC27 WG4	SC27	Information security incident management – Part 2: Guidelines to plan and prepare for incident response
SC27 WG4	SC27	Information security incident management – Part 3: Guidelines for incident response operations
SC27 WG4	SC27 N14811	Information security for supplier relationships – Part 4: Guidelines for security of cloud service

SC27 WG4		Electronic discovery – Part 1: Overview and Concepts
SC27 WG4	WG4	Electronic discovery – Part 2: Guidance for governance and management of electronic discovery
SC27 WG4	WG4	Electronic discovery – Part 3: Code of Practice for electronic discovery
SC27 WG4	WG4	Electronic discovery – Part 4: ICT readiness for electronic discovery
SC27 WG4	WG 4 N636	CfC on the Cloud Adapted Risk Management Framework Study Period (Joint study with WG 1)
SC27 WG4	WG 4 N625	CfC on the Cloud Security Assessment and Audit Study Period
SC27 WG4	WG 4 N678	CfC on the Cloud Security Components Study Period
SC27 WG4		CfC for Security Architecture Framework Study Period
SC27 WG5	WG 5 N9	Identity proofing
SC27 WG5	WG 5 N7	Privacy impact assessment – Methodology
SC27 WG5	SC27 N14687	A framework for access management
SC27 WG5		Privacy capability assessment model (Revised)

SC27 WG5	SC27 N14681	Telebiometric authentication framework using biometric hardware security module
SC27 WG5	SC27 N14683	A framework for identity management Part 2: Reference architecture and requirements
SC27 WG5	SC27 N14685	ISO/IEC CD 24760-3 A framework for identity management Part 3: Practice
SC27 WG5	WG 5 N11	Code of practice for the protection of personally identifiable information
SC27 WG5	SC 27 N14179	A privacy-respecting identity management scheme using attribute-based credentials
SC27 WG5	WG 5 N22	Age verification
SC27 WG5	WG 5 N23	Identity management and privacy technologies
SC27 WG5	WG 5 N17	User friendly online privacy notice and consent
SC27 WG5	WG 5 N21	Potential technical issues of ISO/IEC 29115 when applied in national ID infrastructures
SC38 WG3	SC38 N	Cloud computing – Service Level Agreement (SLA) Framework – Part 1: Overview and concepts
SC38 WG3	SC38 N	Cloud computing – Service Level Agreement (SLA) Framework – Part 2: Metrics

SC38 WG3	SC38 N	Cloud computing – Service Level Agreement (SLA) Framework – Part 3: Core requirements
SC38 WG4	SC38 N	Cloud Computing -- Interoperability and Portability
SC38 WG5	SC38 N	Cloud Computing - Data and its Flow

Annex 4 – Terms of Reference for Advisory Board Members

SLA-Ready Advisory Board (AB)

Terms of Reference

Introduction & Context

SLA-Ready is a European initiative driving a common understanding of service level agreements for cloud services with greater standardisation and transparency so firms can make an informed decision on what services to use, what to expect and what to trust. SLA-Ready services will support SMEs with practical guides, and a social marketplace, encouraging them to carefully plan their journey and make it strategic through an informed, stepping-stone approach, so the cloud and applications grow with their business.

Aim, Roles and Outputs of the Advisory Board

A series of worldwide experts chosen for their unique know-how and expertise in relevant areas of cloud computing (e.g., standardisation and technology) have given their commitment to becoming a member of the SLA Ready Advisory Board. The SLA-Ready Advisory Board (AB) is composed of dynamic, high-level leaders and champions from industry and standard development organisations at European and global level. The main responsibility of these international representatives will be to provide stakeholder action plans driving forward the project objectives. The AB will directly interface with the SLA-Ready Project Management Board (PMB) through regular phone calls. **Each member of the AB shall be obliged to sign a non-disclosure agreement no later than 30 calendar days after their nomination or before any confidential information will be exchanged, whichever date is earlier.**

The principal aims and outputs of the AB can be thus summarised as follows:

Consultative: Contributing to the definition of the strategic directions to be followed by the SLA-Ready consortium during a conference call held every two months over the 24-month period. The SLA-Ready Consortium will provide the AB, ten days prior to the scheduled call, a brief Executive Summary of the Actions undertaken by the consortia in advance of the call. This summary will include progress, advances and main findings with a 2-month action plan. The AB will be expected to provide constructive and pragmatic feedback on the document during the call and ways to move forward. Members will also support consensus building through the collective elicitation of technical, socio-economic and legal requirements. The involvement of the Advisory Board will thereby also facilitate

the adoption of a set of expert-validated, standards-aligned outcomes, namely the Reference Model for SLAs, and support the best practices/recommendations and new services provided by SLA-Ready.

Liaising (with other initiatives): Facilitating the project to establish a worldwide network of relationships with relevant communities, funding agencies, European and international organisations and industries for the purpose of exchanging ideas and disseminating the project outputs/findings.

Supporting promotion: Promoting SLA-Ready benefits to relevant end-user communities and beneficiaries and the **participation to at least to one face to face meeting** that the project will organise in conjunction with the project main events over the 24 months.

AB Members will support activities focusing on the following activities associated with different Work Package activities:

WP2 Definition of the Common Reference Model: Facilitate the adoption of a set of expert-validated, standards-aligned outcomes, namely the Reference Model for SLAs, and shall support the best practices/recommendations and new services provided by SLA-Ready. The contributions to SLA-Ready shall be publicly acknowledged. Each member already contributes to a working group that is active in the area of SLAs.

WP3 International Cooperation, Consensus, and Standardisation: Contribute to consensus building through the collective elicitation of technical, socio-economic and legal requirements identified in D2.1.

WP4 Communications, Impact and Exploitation: Facilitate the dissemination of a set of expert-validated, standard-aligned outcomes namely reference model for SLAs and, best practices/recommendations and services that ultimately will facilitate cloud adoption.

Members are drawn from a variety of countries to reflect the importance of international collaboration in this area and of leveraging best practices from countries with more experience in this field. They are expected also to assist SLA-Ready in gaining influence over key SDOs and WGs for better alignment and interaction of their projects with SLA-Ready. Indeed, members are expected to play a key role in ensuring that SLA-Ready outputs have real impact and benefit to the SLA life-cycle.

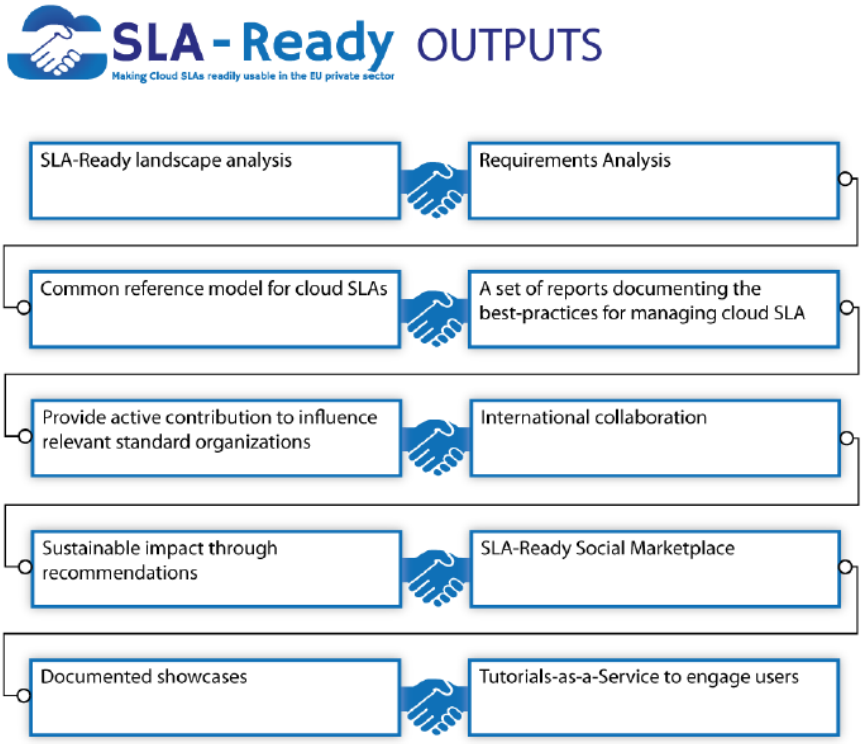
More on SLA-Ready and project outputs

The SLA-Ready project and the resulting reference model, best practices, recommendations and support services will help the European industry and cloud customers to better understand the potential benefits of cloud computing, how to respect the cloud legal framework, and how manage the technical risks (e.g., security and privacy-related) related to cloud computing.

SLA-Ready builds on expert work in Europe on service level agreements (SLAs) with the aim of improving the uptake of cloud by the European private sector, especially SMEs. Firms will benefit from a social market place, tutorials-as-a-service, decision-making services and practical guides supporting the entire SLA life cycle. The SLA-Ready Common Reference Model will benefit the industry by integrating a set of SLA components, e.g. common vocabularies, SLO service metrics and measurements, as well as best practices and relevant standards to fill identified gaps in the current SLA landscape.

SLA-Ready has received funding from the European Commission under Horison 2020 - H2020-ICT-2014-1/644077.

The principle outputs of SLA-Ready are clearly depicted in the table below.



Reimbursement Process

The Advisory Board members will have a lead-time of one month after the meetings to send their reimbursement form.