Secure Provisioning of Cloud Services
based on SLA Management

SPECS Project

SHARED GLOSSARY

Version 2.0
31 October 2014

The activities reported in this deliverable are partially supported
by the European Community's Seventh Framework Programme under grant agreement no. 610795.

Glossary[1]

#ref	*Term*	**Definition**
M6#1	***Activity (cloud computing activity)***	A specified pursuit or set of tasks. (ISO/IEC 17789)
M6#2	***Alert***[2]	An event (*M12#4*) triggered to indicate a warning of failure to meet one or more SLOs (*M6#39*) defined within an SLA (*M6#37*).
M12#1	***Alert threshold***[3]	A measured level related to any part of the SPECS security SLA hierarchy (*M12#11*) at which, if exceeded, an SLA alert (M6#2) occurs.
M6#3	***Application artifact***	A collection of artifacts (*M6#5*), which can be instantiated in an executable environment. Examples: a Java JAR file, a binary executable file, a folder containing the configured installation of software.
M6#4	***Application***	An execution of an application artifact (*M6#5*).
M6#5	***Artifact***	A specification of a physical piece of information that is used or produced by a software development process, or by deployment and operation of a system.
M6#6	***Broker (cloud service broker)***	A cloud service partner (*M6#14*) that negotiates relationships between cloud service customers (*M6#13*) and other cloud service providers (*M6#15*). (ISO/IEC 17788)
M6#7	***Cloud application***	An application (*M6#4*) that offers cloud services (*M6#11*) and consumes cloud resources (*M6#10*).
M6#8	***Cloud capability type***	A classification of the functionality provided by a cloud service (*M6#11*) to the cloud service customer (*M6#13*) based on resources (*M6#35*) used. (ISO/IEC 17788) NOTE: the cloud capability types belong to three sets: application capability type, infrastructure capability type and platform capability type.
M6#9	***Cloud platform***	An application (*M6#4*) that offers cloud services (*M6#11*) of the cloud platform capability type (*M6#8*). NOTE: a cloud platform manages cloud applications through the deployment and management services and owns the artifacts that enable the cloud applications' execution.
M6#10	***Cloud resource***	Any resource (*M6#35*) delivered and controlled by services offered by a cloud service provider (*M6#15*).
M6#11	***Cloud service***	One or more capabilities offered via cloud computing invoked using a defined interface. (ISO/IEC 17788)
M6#12	***Cloud service category***	A group of cloud services (*M6#11*) that possess some common set

[1] The defined terms will be periodically maintained by the SPECS consortium based (among others) on the maturity achieved by the relevant standards.
[2] Updated.
[3] New.

		of qualities. (ISO/IEC 17788) NOTE: a cloud service category can include capabilities from one or more cloud capability types (*M6#8*).
M6#13	***Cloud service customer (CSC)***	A party (*M6#30*) which is in a business relationship for the purpose of using cloud services (*M6#11*). (ISO/IEC 17788) NOTE: a business relationship may not necessarily imply financial agreements.
M6#14	***Cloud service partner (CSN)***	A party (*M6#30*) which is engaged in support of, or auxiliary to, activities of either the cloud service provider (*M6#15*) or the cloud service customer (*M6#13*), or both. (ISO/IEC 17788)
M6#15	***Cloud service provider (CSP)***	A party (*M6#30*) that makes cloud services (*M6#11*) available. (ISO/IEC 17788)
M6#16	***Component***	A functional building block needed to engage in a cloud computing activity (*M6#1*), backed by an implementation. (ISO/IEC 17789)
M12#2	***Control***[4]	Specification of a process or property related to a particular aspect (e.g., security) of an information system.
M12#3	***Control category***[4]	The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, individuals, other organizations, and the Nation. In this project the top-level category of a SPECS security SLA hierarchy (*M12#11*), as it appears on the security control framework being used (e.g., CCM, ISO/IEC 27001, NIST SP 800-53).
M6#17	***End-user***	A party (*M6#30*) that assumes only the role of cloud service customer (*M6#13*) in a target service (*M6#59*) invocation chain (*M6#24*). It signs an SLA (*M6#37*) that covers the target services (*M6#59*).
M6#18	***Enforcement (module)***	A module in SPECS that collects all the components (*M6#16*) involved in the phases of implementation (*M6#22*) and remediation (*M6#32*) of the SLA life cycle phases.
M12#4	***Event***[4]	Any detectable or discernible occurrence that has significance for the management of the IT infrastructure or the delivery of IT service and evaluation of the impact a deviation might cause to the services. Events are typically notifications created by an IT service, configuration item or monitoring tool. (ITIL 2011)
M6#19	***External CSP***	A cloud service provider (*M6#15*) that provides the target service(s) (*M6#59*).
M6#20	***Framework***	A (software) framework is a universal and reusable software solution dedicated to develop components, applications, products, and services. Software frameworks include support programs, compilers, code libraries, tool sets, and application programming interfaces (APIs) that bring together all the different components to

[4] New.

		enable development of a project or solution.
M6#21	***Hosting CSP***	A cloud service provider (*M6#15*) that makes the SPECS framework (*M6#49)* available using its own resources (i.e. SPECS components (*M6#45*) may have access to information and services not available in a public cloud).
M6#22	***Implementation (phase)***	It is the phase of the SLA life cycle during which a cloud service provider (*M6#15*) implements an SLA (*M6#37*).
M6#23	***Interaction Model (IM)***	A description of the roles (*M6#36*) assumed by all the parties (*M6#30*) and all the components (M6#16) in a specific usage scenario.
M6#24	***Invocation chain***	A chain of cloud services (*M6#11*) where the involved parties (*M6#30*) play the roles (*M6#36*) of cloud service providers (*M6#15*) and/or cloud service customers (*M6#13*) with respect to a sequence of cloud services (*M6#11*), whose composition leads to the provisioning of the target service (*M6#59*).
M12#5	***Key concern***[5]	Concern of the SPECS framework (*M6#49*) that is relevant to its validation; the SPECS key concerns are: End-users (*M6#17*), invocation chains (*M6#24*), SPECS services (*M6#56*), target services (*M6#59*), SLA life cycle and kinds of provided SLOs (*M6#39*).
M12#6	***Key concern item***[5]	Each single value that can be assumed by a key concern (*M12#5*) that has to be used/assigned/stressed by a validation scenario (*M12#13*) in order to cover it.
M12#7	***Metric***[5]	A standard of measurement that defines the conditions and the rules for performing the measurement and for understanding the results of a measurement. (NIST "Cloud computing service metrics description" draft)
M6#25	***Module***	A collection of components (*M6#16*).
M12#8	***Monitoring event***[5]	An event (*M12#4*) which can be associated with an SLO metric that the Monitoring module (*M6#27*) considers significant.
M6#26	***Monitoring (phase)***	It is the phase of the SLA life cycle during which the target service (*M6#59*), covered by the SLA (*M6#37*), is monitored.
M6#27	***Monitoring (module)***	A module in SPECS framework (*M6#49*) that collects all the components (*M6#16*) involved in the activities of monitoring SLA life cycle phase (*M6#26*).
M6#28	***Negotiation (phase)***	It is the phase of the SLA life cycle during which a cloud service provider (*M6#15*) and a cloud service customer (*M6#13*) try to find an agreement on an SLA (*M6#37*).
M6#29	***Negotiation (module)***	A module in SPECS framework (*M6#49*) that collects all the components involved in the activities of negotiation SLA life cycle phase (*M6#28*).
M12#9	***Notification***[5]	A message sent using the SPECS SLA Platform (*M6#57*) in order to communicate the occurrence of certain monitoring events (M12#8) that might affect the validity of certain SLOs (*M6#39*).

[5] New.

M6#30	***Party***	A natural person or legal person, whether or not incorporated, or a group of either. (ISO/IEC 17788)
M6#31	***Redress***	An activity (*M6#1*) of the cloud service provider (*M6#15*) which involves the reconfiguration of component implementation and/or the start of new components implementation, in order to enable the cloud service provider (*M6#15*) to respect an agreed SLA (*M6#37*).
M6#32	***Remediation (phase)***	It is the phase of the SLA life cycle during which a cloud service provider (*M6#15*) applies remedies (*M6#33*).
M6#33	***Remedies***	Remedies are provided by the cloud service provider (*M6#15*) to the cloud service customer (*M6#13*) in the event the service fails to meet the service level objectives (*M6#39*) defined in the SLA (*M6#37*). The SLA shall specify remedies for the failure to meet SLOs (*M6#39*). (ISO/IEC CD 17788.2)
M6#34	***Renegotiation (phase)***	It is the phase of the SLA life cycle during which a cloud service provider (*M6#15*) and a cloud service customer (*M6#13*) try to change an already agreed SLA (*M6#37*).
M6#35	***Resource***	Any physical, virtual or software element that has a state.
M6#36	***Role***	A set of activities (*M6#1*) that serves a common purpose. (ISO/IEC 17788)
M12#10	***Security control***[6]	A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements. (NIST 800-53)
M6#37	***Service Level Agreement (SLA)***	Documented agreement between the service provider and customer that identifies services and service targets. (ISO/IEC 20000-1 (2011))
M6#38	***Service Level Agreement (SLA) implementation***	Implementing the cloud SLA (*M6#37*) involves interfacing management systems to the cloud service (*M6#11*) or implementing other systems to monitor cloud service levels, report failures to meet SLOs (*M6#39*) and claim remedies (*M6#33*). In some cases, the cloud service provider (*M6#15*) may need to assist the cloud service customer (*M6#13*) with implementing the cloud SLA (*M6#37*). Cloud service customers (*M6#13*) should also include the cloud SLA (*M6#37*) in their internal audit processes. (ISO/IEC CD 17788.2)
M6#39	***Service Level Objective (SLO)***	Service Level Objective represents the quality of service aspect of the agreement. Syntactically, it is an assertion over the terms of the agreement as well as such qualities as date and time. (WS-Agreement)
M6#40	***Software component***	A software element independent, self-contained and that provides well-defined interfaces in order to be used by third parties (*M6#30*) by composition activities (*M6#1*).
M6#41	***SPECS administrator***	A role (*M6#36*) assumed by the SPECS owner (*M6#53*), which includes all the activities (*M6#1*) devoted to manage and configure SPECS services (*M6#56*), applications and components. The SPECS administrator is also responsible for managing: (i) all

[6] New.

		available repositories (i.e., monitoring and enforcement services, CSP SLA, SPECS SLA), (ii) the signing/termination/changing content of SPECS SLAs, and (iii) the End-users and related access control policies.
M6#42	***SPECS application***	A cloud application (*M6#7*) built as a collection of SPECS components (*M6#40*), managed and deployed over the SPECS Enabling Platform (*M6#47*), which offers the SPECS security services (*M6#55*).
M6#43	***SPECS application developer***	A party (*M6#30*) assuming the sub-role of developer (sub-role of cloud service partner) that uses the SPECS framework (*M6#49*) to develop SPECS applications (*M6#42*).
M6#44	***SPECS cloud service category (SPECS services)***	A collection of all cloud services (*M6#11*) developed, managed and/or offered by the SPECS framework (*M6#49*).
M6#45	***SPECS component***	A cloud application (*M6#7*) managed and deployed over the SPECS Enabling Platform (*M6#47*) that offers SPECS services (*M6#56*).
M6#46	***SPECS Core cloud service category (SPECS Core services)***	A collection of all the SPECS services (*M6#56*) belonging to the SPECS Negotiation (*M6#52*), SPECS Monitoring (*M6#51*) and SPECS Enforcement (*M6#48*) cloud service categories (*M6#12*).
M6#47	***SPECS Enabling Platform cloud service category (SPECS Enabling Platform services)***	A collection of all SPECS services (*M6#56*) belonging to the cloud platform capability type (*M6#8*).
M6#48	***SPECS Enforcement cloud service category (SPECS enforcement services)***	A collection of all the SPECS services (*M6#56*) dedicated to Enforcement (*M6#18*).
M6#49	***SPECS framework (SPECS)***	The framework (*M6#20*) that supports a SPECS owner (*M6#53*) to develop, deploy and manage SPECS services (*M6#56*).
M6#50	***SPECS framework developer***	A party (*M6#30*) assuming the sub-role of developer (sub-role of cloud service partner) that develops and maintains the SPECS framework (*M6#49*).
M6#51	***SPECS Monitoring cloud service category (SPECS monitoring services)***	A collection of all the SPECS services (*M6#56*) dedicated to Monitoring (*M6#26*).
M6#52	***SPECS Negotiation cloud service category (SPECS negotiation services)***	A collection of all the SPECS services (*M6#56*) dedicated to Negotiation (*M6#28*).
M6#53	***SPECS owner***	A party (*M6#30*) that owns the SPECS framework (*M6#49*) and uses it to provide SPECS services (*M6#56*). NOTE: the SPECS owner is a party (*M6#30*) assuming the role of a cloud service provider for SPECS services (*M6#56*). When SPECS security services (*M6#55*) are granted by an SLA (*M6#37*), the SPECS owner is the one signing the SLA (*M6#37*), as the cloud

		service provider (*M6#15*).
M6#54	***SPECS Platform cloud service category (SPECS platform services)***	A collection of all the SPECS services (*M6#56*) of SPECS Enabling Platform (*M6#47*) cloud service category (*M6#12*) and of the SPECS SLA Platform cloud service category (*M6#57*).
M6#55	***SPECS security service***	A SPECS service (*M6#56*) offered to cloud service customers (*M6#13*) by a SPECS application (*M6#42*).
M12#11	***SPECS security SLA hierarchy***[7]	Multi-level and hierarchical structure representing s security SLA (*M6#37*) in SPECS. This hierarchy links together all the elements of the security SLA (*M6#37*) that are relevant to SPECS that is, the control category (*M12#3*), control (*M12#2*), SLO (*M6#39*), and the metric (*M12#7*).
M6#56	***SPECS service***	One of the cloud services (*M6#56*) of the SPECS cloud service category (*M6#44*).
M6#57	***SPECS SLA Platform cloud service category (SPECS SLA Platform services)***	A collection of all the SPECS services (*M6#56*) dedicated to SLA (*M6#37*) management.
M6#58	***SPECS system administrator***	A role (*M6#36*) assumed by the SPECS owner (*M6#53*), which includes all the activities (*M6#1*) devoted to manage all physical and infrastructural resources used to set-up and execute the SPECS Enabling platform (*M6#47*).
M6#59	***Target service(s)***	Cloud service(s) (*M6#11*), whose capability are of interest of the End-user (*M6#17*), covered by an SLA (*M6#37*), and that are at the end of an invocation chain (*M6#24*).
M12#12	***User story***[7]	Definition of the real world context in which a validation scenario (*M12#13*) may take place.
M12#13	***Validation scenario***[7]	Specification of an expected behaviour of the SPECS framework (*M6#49*) within the context of a user story (*M12#12*) and soliciting one or more key concerns (*M12#5*) by covering some of their key concern items (*M12#6*).
M6#60	***Violation***[8]	An event (*M12#4*) triggered to indicate the failure to meet one or more SLOs (*M6#39*) defined within an SLA (*M6#37*).
M12#14	***Violation threshold***[7]	A measured level related to any part of the SPECS security SLA hierarchy (*M12#11*) at which, if exceeded, an SLA violation (*M6#60*) occurs.

[7] New.
[8] Updated.