Requirements Document

Cloud Services

Indicative Requirements for Cloud Service Providers

Issue Date: 17-04-2014
Authors: Branko Radojevic (CARNet), Andres Steijaert (SURFnet)

This document has been produced with the financial assistance of the European Union. The contents of this document are the sole responsibility of DANTE and can under no circumstances be regarded as reflecting the position of the European Union.
MAR/14

Table of Contents

Executive Summary 3

1 Building the GÉANT Cloud Catalogue 4
1.1 Approach 4

2 Requirements for Cloud Service Providers 6
2.1 Intellectual Property Rights and Ownership 6
2.2 Legal Aspects 6
2.3 Security 8
2.4 Continuity 8
2.5 Confidentiality 9
2.6 Communication 10
2.7 Billing 11
2.8 Technical Requirements 11

Glossary 13

Table of Figures

Figure 1.1: Delivery approach for cloud services 5

Executive Summary

The GÉANT3plus Service Activity - Support to Clouds (SA7) is actively helping NRENs (National Research and Education Networks) to deliver cloud services to their communities, with the right conditions of use. It is also engaging with the existing NREN brokerages to promote an efficient and coordinated pan-European approach, where appropriate, by building on existing experience and supplier relationships.

By aggregating demand across the community and negotiating integrated brokerage and service delivery (framework contracts, terms and conditions of use) NRENs and the research and education community will be able to get the best possible value from cloud services.

The goal is to acquire and manage the delivery of services from providers to the pan-European GÉANT community. These parties can be commercial vendors as well as NRENs, and other research and education communities. The goal is to provide an attractive, well-balanced portfolio of cloud services, published online in the GÉANT Cloud Catalogue, an informative list of cloud providers.

This document lists an indicative set of basic requirements (baseline) that cloud providers would be requested to follow in order to be listed in the GÉANT Cloud Catalogue. Non-provision of the listed requirements would not be a reason for exclusion from GÉANT Cloud Catalogue, but instead allows the cloud provider to clearly demonstrate to the GÉANT Customer (NRENs, Users, Institutions) their commitment to listed requirements.

1 Building the GÉANT Cloud Catalogue

1.1 Approach

This requirement list is made available in order to provide all prospective Cloud Service Providers (CSPs) with the set of indicative basic user requirements.

At least once a year DANTE will make public a Prior Information Notice (PIN) that will invite CSPs to list their Cloud Services (CS) in GÉANT Cloud Catalogue. The PIN will forward CSPs to GÉANT's Cloud webpage, where detailed information about inclusion into the catalogue will be made available.

After a CSP has walked through the requirements, it is welcome to approach the GÉANT Cloud team with one or multiple Cloud Services (CSs), the CSP would like to be included in the GÉANT Cloud Catalogue.

The CSP will then fill in a self-assessment form that will be reviewed by the GÉANT Cloud Team (to check if CS meets the user requirements). After successful review, the CS is then listed in the GÉANT Cloud Catalogue. The review is based on a red / amber / green (RAG) scoring system of each of the indicative elements identified in this document, and points are allocated based on compliance / compatibility with these points and allocated a rating according to the following scale.

GREEN	Fully applicable	10 points
AMBER	Partially applicable	5 points
RED	Not applicable	0 points

All CSPs listed in the GÉANT Cloud Catalogue will be presented in order of the score achieved through the self-assessment process.

In addition, the CSPs are welcome to work with GÉANT Cloud Team on any requirements that cannot be met at the time of completing the self-assessment, in order to comply with them and improve their overall score.

Note that the Cloud Catalogue will be provided for information only. Its aim is to help European Research and Education (R&E) Institutions in Europe proceed with CS procurement. Successful listing does not confer any form of accreditation by GÉANT as a cloud provider.

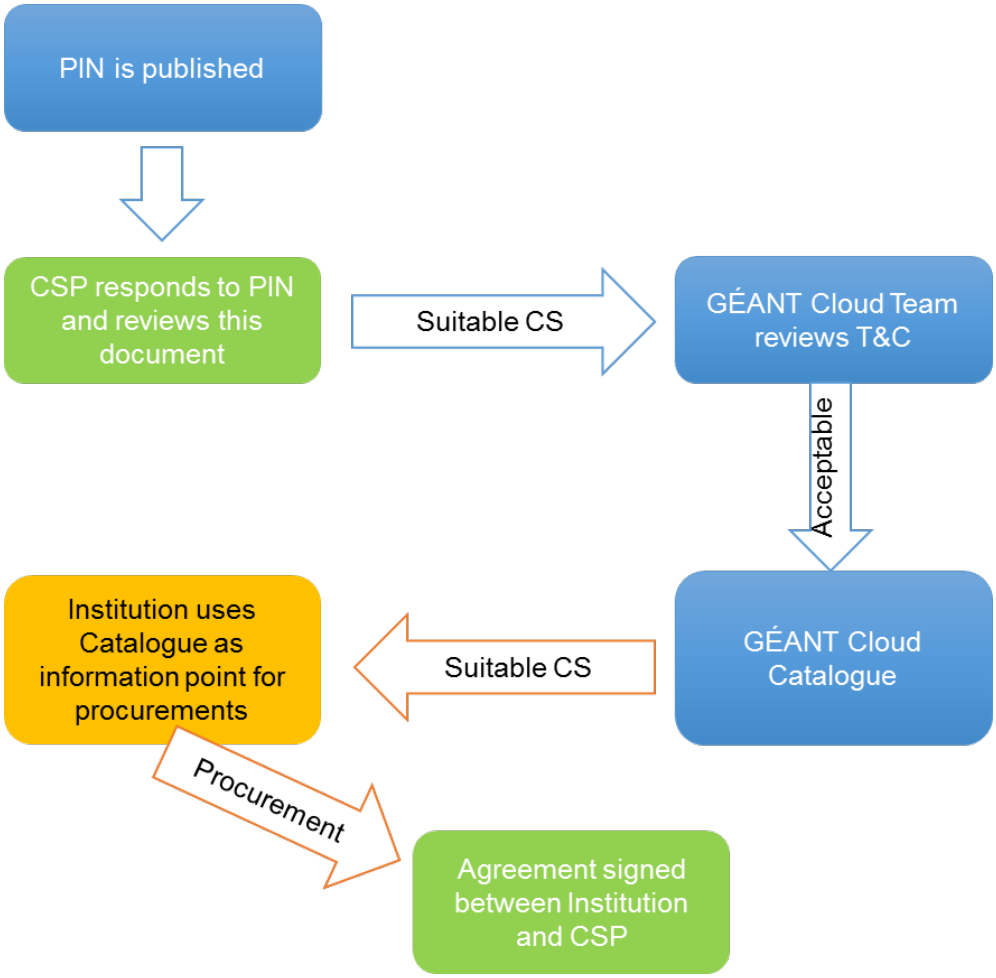

Figure 1.1: Delivery approach for cloud services

2 Requirements for Cloud Service Providers

The following sections outline a number of technical, commercial and contractual objectives of a typical user when sourcing cloud services. It is envisioned that they will form the basis of an SCP's self-assessment.

2.1 Intellectual Property Rights and Ownership

2.1.1 Intellectual Property Rights

All intellectual property rights, including any copyright or database right to the Data (i.e. the file and/or files with the Data) will at all times remain vested in Institution, the User concerned, or their respective licensor(s).

2.1.2 CSP Data Control

The CSP is a data processor, which should be clearly stated in any subsequent Service Agreement. The CSP will process the Data in a proper and careful manner, and in accordance with the applicable regulations. The CSP is responsible for the quality and availability of the CS. Controlling authority over the Data is vested in the Institution and/or the User concerned.

2.1.3 Data Ownership

Data is and remains under ownership of Institution/User producing data, or by the entity that is storing the data if the Data producer has passed its rights to such an entity. At no time will a provider acquire rights to any Data, for any other purpose than providing the CS. This may include troubleshooting aimed at preventing, detecting and repairing problems affecting the operation of the CS and the improvement of features that involve the detection of, and protection against, emerging and evolving threats to the user (such as malware or spam).

2.2 Legal Aspects

2.2.1 Governing Law

If requested by the Institution, the CSP will need to grant the Institution the ability to sign subsequent Service Agreement under its own national law.

2.2.2 Concordance with National Privacy Act(s)

If requested by Institution, the CSP will produce annual verification of private data security compliance in the provided CS, as requested by the Institution's national privacy act.

2.2.3 External Security Audit Certificate

Companies operating in the European Union are not allowed to send personal data to countries outside the European Economic Area unless there is a guarantee that it will receive adequate levels of protection. The Safe Harbour Privacy Principles allows US companies to register their certification if they meet the European Union requirements.

Ahead of any actual committed contract, the GÉANT Customer will require the ability to request certificates of independent security audit to confirm that the CSPs processes are in accordance with the applicable legislation.

For CSPs based in USA, it will be mandatory that they are Safe Harbour certified. Note that for CSPs based in the EU, the USA, the European Economic Area (EEA) or countries which the European Commission considers to have acceptable levels of data protection,[1] it should be assumed that the personal data provisions do apply.

2.2.4 Subcontractors

If the CSP is using subcontractors of any kind in any part of the delivery process, including the support for the CS, then there is a need that subcontractor is also based in the EU, USA, a country on EU list with adequate privacy protection, or that the subcontractor provides an adequate privacy protection safeguarded by other means, such as an auditable User-consent option.

2.2.5 Protection of Minors as Users

The CSPs should safeguard, at least in a written notice, that all actions taken by minors as Users of CS (for example, accepting online Terms and Conditions) will be properly authorised by their parents or legal guardians.

2.2.6 Service Level Agreement

The CSP will ensure that an appropriate SLA with the GÉANT Customer is in place concerning the type of CS offered. In general, this means a User-availability target for the CS of at least 99%, that the Users will be notified in advance of expected downtime if it is impossible to avoid it, and that the CSP will provide a support desk to Users in 24/7 regimes.

[1] http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm

2.2.7 Service Performance Information

GÉANT Customers seek assurances that CSPs will make all agreement and service performance data in their possession available to the GÉANT Customer on first request. The CSP should state their acceptance / rejection of this objective and provide any narrative in respect of their position.

2.3 Security

2.3.1 Cloud Service Security

The CSP will need to put appropriate measures in place to properly ensure the physical and logical security of the CS so as to prevent any loss or damage and any form of unauthorised access, alteration, or provision, or any other wrongful processing of an Institution's Data. The security measures shall become an integral part of the Service Agreement.

2.3.2 Security Incidents Handling

The CSP will have a policy document providing details to an Institution about its process for security incident process handling, and to have easy access to relevant logging and reporting of issues for concerned customers.

2.4 Continuity

2.4.1 Data Backup and Restore

The CSP will ensure sufficient data redundancy and procedures for recovering and restoring data that are designed to reconstruct Data in its original state from before the time it was lost or destroyed. All backups provided by the CSP must be kept up to date.

2.4.2 Compatibility

The CSP shall guarantee the compatibility of the CS with the IT infrastructure and Data of the Institution, for the current version, as well as future versions of the CS under the Agreement's validity period.

2.4.3 Portability

After the contract has been terminated, for whatever reason, all Data and metadata held by the CSP must be easily exported and deleted from all the CSP sites, including backup sites, by the current CSP.

At the request of the Institution, all data will be made available to the subsequent CSP without additional charges. The outgoing CSP will ensure that all Data will be exported in such way that there will be no loss of functionality of the Data or any parts of the Data. In case of the CSPs filling bankruptcy, the Data must be accessible for three months after the day of filling.

2.5 Confidentiality

2.5.1 Data Protection

The CSP should treat all data as though it were confidential, regardless of its classification. The CSP should have no ownership of customer data. Such responsibility should also be cascaded down to relevant third parties

2.5.2 Requests for Data Access from Third Parties

The CSP will conclude a written agreement with any third parties concerned that specifies, in any case, that said third parties also act in accordance with all provisions of the Agreement between the CSP and Institution.

The CSP will make every effort to safeguard data access and the interests of the Institution in case the authorities requested access to Data. The CSP will check if there is a legal obligation to comply with the request and will not cooperate if there is no legal obligation. The CSP will object to the request when appropriate, and will only release a minimum dataset. The CSP is obliged to inform the owner of the Data (Institution) of any such requests as soon as possible.

2.5.3 Personnel

The CSP will ensure that all people it employs sign a confidentiality statement regarding handling and management of confidential data.

2.5.4 Liquidated Damages

For every contravention of its confidentiality obligation by the CSP, the GÉANT Customer will be advised to seek a service credit of no less than one month of service fees. Note that this service should not affect the GÉANT Customer's other remedies within any resultant agreement.

2.6 Communication

2.6.1 Supervision

At the written request of Institution, the CSP will cooperate with the exercise of supervision by or on behalf of Institution of the CS and the CSP's use of confidential Data.

2.6.2 Data Availability

The CSP will make all Data that it has in its possession in the context of performance of the Service Agreement available to Institution at Institution's first request, including any copies that have been made of said Data.

2.6.3 Electronic Data Processing Audit

The CSP is obliged to have an annual review of the CSP's organisation carried out by an independent EDP auditor or expert that it designates in order to determine: that CSP can comply with the provisions of the present Agreement regarding the protection of Data (including Personal Data and privacy aspects); that the CSP is able to comply with the provisions of the present Service Agreement regarding the confidentiality, integrity, continuity, effectiveness, and efficiency of the CS made available by the CSP.

The CSP has the possibility to aggregate summary audit reports for all GÉANT Customers institutions under GÉANT umbrella and deliver it directly to GÉANT Cloud Operations Team, or to offer this report directly to the Institution directly.

2.6.4 Quality Review

If an Institution has a reasonable suspicion that the CSP is non-compliant with provisions of the Service Agreement, are not being complied with, the Institution may request that the CSP carries out a quality review. Prior to the review process, the Institution and CSP will agree on who will perform such a review, and estimate costs of the review process. The costs for such quality review shall be borne by the Institution unless the findings of said review show that the CSP has failed to comply with the provisions of the Agreement. If that is the case, the costs will be borne by the CSP.

The CSP will provide periodical reports to the Institution on data security and any security incidents in the last period.

The CSP will provide adequate and timely information regarding new releases (updates, release calendar) and the roadmap of the CS.

2.6.5 Notification

CSP will immediately notify the Institution if it becomes aware of a suspected or actual breach of confidentiality, loss of confidential Data, breach of the security measures, deterioration of the service, or downtime of the service. The CSP will take all necessary measures, at its own cost, to secure the confidential Data and to rectify the shortcomings in the security measures so as to prevent any further perusal, alteration, or provision, without prejudice to any right of the Institution to damages or other measures. Following the incident, at the Institution's request, the CSP will cooperate with the provision of information about the incident and its resolution to concerned parties.

2.7 Billing

The CSP's billing infrastructure must support cost-effective invoicing/payment processing, and include: hierarchical roles for NRENs (national and regional ones), and institutions that are NRENs institutional users (Universities, Research Institutes, Schools, etc.).

2.8 Technical Requirements

2.8.1 AAI

Where appropriate, and subject to a request by end Users, the CS will support authentication provided by eduGAIN, which is the standard, pan-European, SAML-based authentication and authorisation infrastructure for single-sign on/off.

2.8.2 User Provisioning

If there is need to pre-provision Users, then the CSP will provide practical provisioning methods, e.g. auto-provisioning, batch-provisioning, or similar.

2.8.3 Reporting / Metering / Sales Estimates

The CSP is requested to implement appropriate means of metering current usage of the CSs, appropriate reporting facilities and monthly/annual sales estimates, which are updated dynamically. All reports should be made available online and need to be available on a per-site, Institution, or User-basis.

2.8.4 Network Peering and Associated Networking Costs

GÉANT Customers will wish to access the service via GÉANT (recommended) or specific NREN's infrastructure. This is to overcome issues of latency, bandwidth, data loss, or any other degradation of network connectivity. The CSP should state their acceptance / rejection of this objective and provide any narrative in respect of their position.

Depending on the type of CS in concern (mostly IaaS services, but also applicable to other services, depending on the need of a excellent quality network connection), the CSP should directly connect its network to GÉANT (recommended) or an NREN's network infrastructure, to overcome potential issues with latency, bandwidth, data loss, or any other degradation of network connectivity. Peering will also benefit the CSP with its speedy diagnosis and resolution of service disruptions.

Network peering should be done in accordance with GÉANT Peering Policy in one of the designated GÉANT PoPs. GÉANT considers networking peering to be a win-win solution for both parties. Apart for the connection cost recovery fee, the CSP will not impose any additional fees to the GÉANT network, NREN, Institution or end users. CSPs that charge end users for networking connectivity and/or usage should not impose such charges if the user is coming from the GÉANT network.

Glossary

CS	Any Cloud Service offered by CSP
CSP	Cloud Service Provider
Data	Any data that Institution/User stores in any way at CSP
DANTE	Delivery of Advanced Network Technology to Europe – The coordinator of pan-European research and education (R&E) networking on behalf of Europe's National Research and Education Networks (NRENs)
EDP	Electronic Data Processing
Institution	Any educational/academic/research institution or NREN signing the actual service agreement
NREN	National Research and Education Network
PIN	Prior Information Notice
User	Any person that is considered to be an end user of an Institution