

GN3plus Support to Clouds

Terms & Conditions Requirements for Cloud Service Providers



DRAFT #3.2

GN3plus, SA7, Task 3
Milestone: MS7.3.1

© DANTE on behalf of the GN3plus project.

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7 2007–2013) under Grant Agreement No. 605243 (GN3plus).

Summary

To

This document lists the set of requirements that all cloud providers are requested to meet (baseline).

Table of Contents

| | |
|---|-----------|
| SUMMARY..... | 2 |
| TABLE OF CONTENTS..... | 3 |
| BUILDING GÉANT CLOUD CATALOGUE | 4 |
| 1. DELIVERY APPROACH..... | 4 |
| FIGURE 1 DELIVERY APPROACH FOR CLOUD SERVICES..... | 5 |
| 2. REQUIREMENTS FOR CLOUD SERVICE PROVIDERS..... | 6 |
| <i>i. Intellectual Property Rights and Ownership.....</i> | <i>6</i> |
| <i>ii. Legal Aspects</i> | <i>6</i> |
| <i>iii. Security.....</i> | <i>7</i> |
| <i>iv. Continuity.....</i> | <i>8</i> |
| <i>v. Confidentiality.....</i> | <i>8</i> |
| <i>vi. Communication.....</i> | <i>9</i> |
| <i>vii. Billing</i> | <i>10</i> |
| <i>viii. Technical Requirements.....</i> | <i>10</i> |
| GLOSSARY | 12 |

Building GÉANT Cloud Catalogue

1. Delivery approach

This requirement list is made available in order to provide all prospective Cloud Service Providers (CSPs) with the set of basic requirements; the baseline of requested terms and conditions which should be an essential part of all future Agreements between CSPs and NRENs/Institutions.

At least once a year DANTE will publicly publish a Prior Information Notice (PIN) that will invite CSPs to list their Cloud Services (CS) in the GÉANT Cloud Catalogue. The PIN will point CSPs to the GÉANT Cloud website where detailed information about inclusion into the catalogue is available.

The CSP will do a self-assessment that will be reviewed by the GÉANT Cloud Team. The review is based on a RAG scoring system table, in a way that every requirement (each item) in this document is scored with one of the following colours.

| | | |
|-------|---|-----------|
| GREEN | CSP fully complies with the requirement | 10 points |
| AMBER | CSP meets the requirement partially | 5 points |
| RED | CSP does not meet the requirement | 0 points |

All CSPs will be listed in the GÉANT Cloud Catalogue with their RAG score. This is an indicative position for vendors. They are welcomed to improve on this.

This catalogue is informational only, and helps research and education Institutions in Europe to proceed with the procurement of the CS. NRENs and R&E institutes can use this catalogue for their procurement process: identifying potential suppliers and gaining an understanding what the market can deliver. Successful listing does not confer any form of accreditation by GÉANT for a cloud provider. Only when a procurement is launched by an NREN or institute will the cloud provider commit to their position in contract.

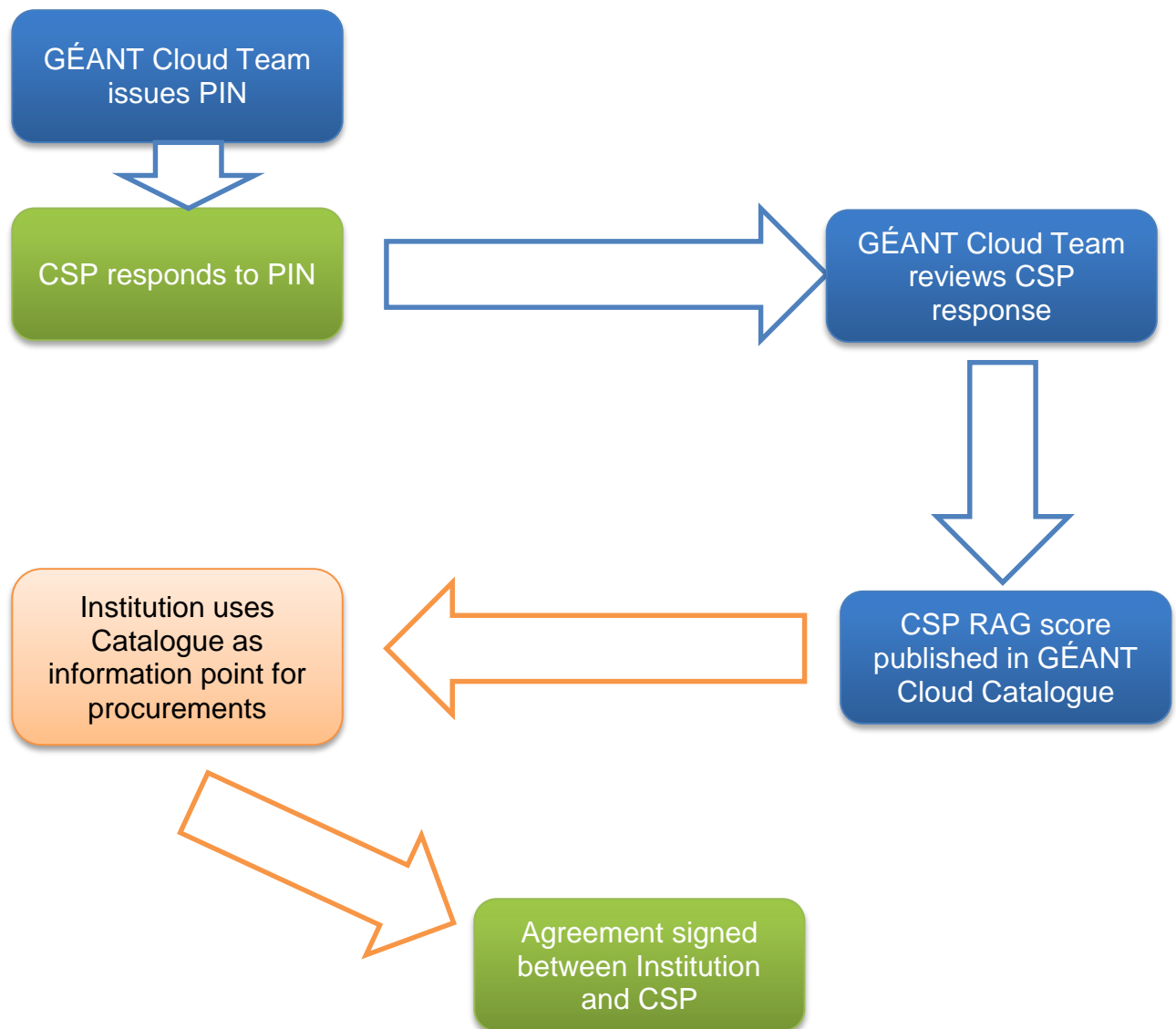


Figure 1 Delivery approach for Cloud Services

2. Requirements for Cloud Service Providers

i. Intellectual Property Rights and Ownership

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).

CSP Controlling over Data

CSP is data processor, and this should be clearly stated in the Agreement. CSP will process the Data in a proper and careful manner and in accordance with the applicable regulations. 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.

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 the second one. Provider at any time will acquire no rights on 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).

ii. Legal Aspects

National Law Governance

If requested by Institution, CSP has to grant Institution ability to sign Agreement under its national law.

Concordance with National Privacy Act(s)

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

External Security Audit Certificate

Before signing the actual Agreement, the Institution has to have ability to request certificate of external security audit that depends on the ownership of the CSP.

For CSPs based in USA, it is mandatory that they are Safe Harbour certified.

For CSPs based in EU, USA, European Economic Area (EEA) or countries which the European Commission considers to have acceptable levels of data protection¹, it is safe to assume that there is always personal data involved (user accounts).

Subcontractors

If provider 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 EU, USA, a country on EU list with adequate privacy protection or that the subcontractor provides an adequate privacy protection safeguarded by other means, like e.g. EU standard contractual clauses.

Protection of Minors as Users

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 authorized by their parents or legal guardians.

Service Level Agreement

CSP will ensure that the appropriate SLA is in place concerning the type of CS offered. In general, this means that the CS will be available to Users for 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 support to Users in 24/7 regimes.

iii. Security

CS Security

CSP will 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 unauthorized access, alteration, or provision, or any other wrongful processing of the Institutions Data. The security measures shall become integral part of the Agreement.

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

Security Incidents Handling

CSP will have a policy document providing details to Institution about their process for security incident handling, and to have easy access to relevant logging for customers concerned.

iv. Continuity

Data Backup and Restore

CSP will ensure sufficient data redundancy and procedures for recovering data that are designed to reconstruct Data in its original state from before the time it was lost or destroyed.

Compatibility

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 period of Agreements validity.

Portability

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

At the request of the Institution, all data will be made available to subsequent CSP without additional charges. Previous 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 CSPs filling the bankruptcy the Data has to be accessible for three months after the day of bankruptcy filling.

v. Confidentiality

Data Protection

CSP will treat confidential Data as confidential. This will concern both data labelled as such by the Institution, or Data for which CSP can assume that confidential Data is concerned.

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

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

Personnel

CSP will be make sure that all people it employs must sign a confidentiality statement regarding confidential data.

Penalty

For every contravention of its confidentiality obligation, CSP will owe an immediately due and payable penalty, no less then one month of service fees, without this affecting Institution's other rights to receive damages.

vi. Communication

Supervision

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

Data Availability

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

EDP Audit

CSP is obliged to have an annual review of CSP's organization 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 CSP is able to comply with the provisions of the present Agreement regarding the confidentiality, integrity, continuity, effectiveness, and efficiency of the CS made available by CSP.

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

Quality Review

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

CSP will report periodically to Institution on data security and any security incidents in the last period.

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

Notification

CSP will notify Institution immediately 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. 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 Institution to damages or other measures. At Institution's request, CSP will cooperate with the provision of information to concerned parties.

vii. Billing

Billing infrastructure must support cost-effective invoicing/payment processing and include hierarchical roles for NRENs (national and regional ones), institutions which are NRENs institutional users (Universities, Research Institutes, Schools, etc.).

viii. Technical Requirements

AAI

If appropriate, and usually requested for the CSs that end-Users use, the CS will support authentication provided by eduGAIN, which is the standardised pan-European SAML-based authentication and authorization infrastructure for single-sign on/off.

User Provisioning

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

Reporting / Metering / Sales Estimates

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

Network Connectivity and Associated Networking Costs

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), CSP should connect its network directly to GÉANT (recommended) or NRENs 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 the speedy diagnosis and resolution of service disruptions.

Network peering should be done in accordance with GÉANT Peering Policy in one of designated GÉANT PoPs. GÉANT considers networking peering to be a win-win solution for both parties. Except for the connection cost recovery fee, CSP will not impose any additional fees to GÉANT, 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 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 agreement |
| NREN | National Academic and Research Network |
| PIN | Prior Information Notice |
| User | Any person that is considered to be an end user of Institution |