

IaaS framework

Results and lessons learned

Andres Steijaert (SURFnet)
GÉANT cloud activity leader

EOSC-hub week

Prague, April 11, 2019

clouds.geant.org

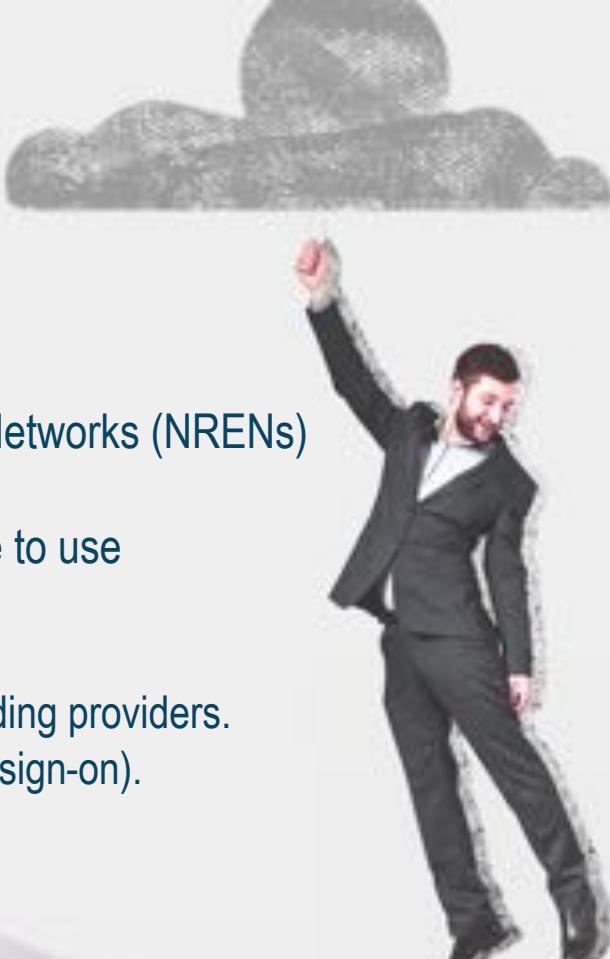


BRINGING THE CLOUD TO THE GROUND

40 European National Research and Education Networks (NRENs) collaborate in their association GÉANT to make cloud services accessible: easy and safe to use for 10,000 institutions and 50 million users.

Unique cloud portfolio:
ready-to-use, legally compliant agreements with leading providers.
Discounts, technical integration (network and single sign-on).

Participate in EOSC-hub WP12



GÉANT, CERN, RHEA & Trust-IT will drive adoption of commercial digital services in the European research community (2019 – 2021)

Stimulate adoption by the research community:
Pan-European Tender
9.5 million euro available for cloud adoption

Part of the European Open Science Cloud

Collective hybrid multi-cloud strategy

Build and buy

INTERNAL: Share sector-specific community clouds

EXTERNAL: Jointly procure public clouds from commercial suppliers

Make services fit the requirements of the R&E community
integrate them with the community's infrastructure
and support NRENs to offer them to their institutions and users

Best value, most favourable conditions of use
Obtained through a collective approach



There is a demand for cloud services

... but it is important to ensure that ...

GET IN

Data is safely handled and meets European and national regulations

Services can be acquired through the institutions' structures:

- Affordable and predictable cost and purchasing models (prevent bill shock)
- Limit network traffic costs and provide network integration
- Log in with institutional account

GET OUT

Data can be moved (to another provider)

Service Delivery Framework

Gather the community's needs and demand

Find and engage with willing service providers

Establish solutions and agreements with capable providers

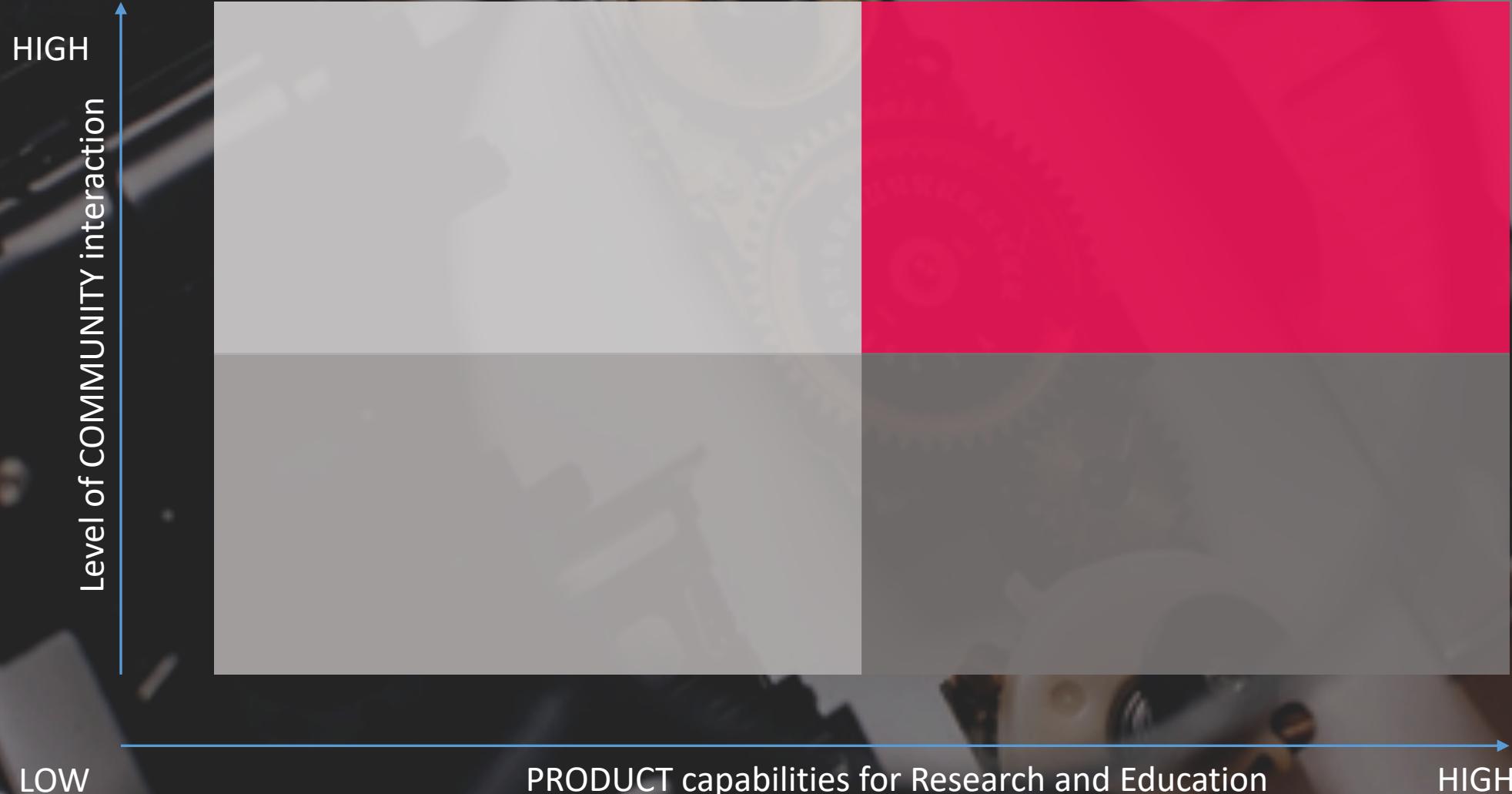
Connect providers to the GÉANT technical infrastructure (network & AAI)

Manage the providers and agreements

Facilitate adoption of the services: help NRENs deliver, for institutions to consume



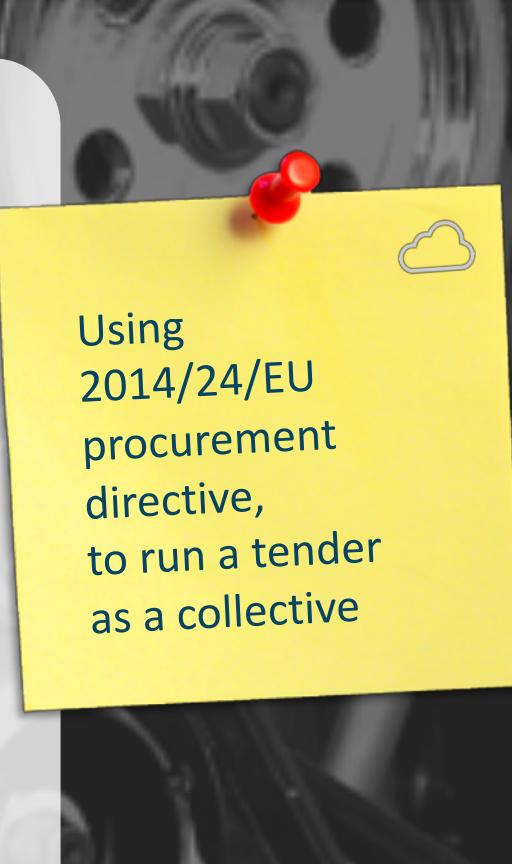
Supplier analysis matrix



Infrastructure as a Service

Pan-European tender and Framework Agreements

- **2016, tender**
Pan-European tender with 36 participating countries for IaaS solutions
Framework agreements with 20 suppliers
- **Since January 2017, agreements available and valid until end of 2020**
procurement-compliant in the EU and EEA,
provide legal compliance,
including EU data protection laws
and allow for institutional-supplier call-off contracts
to take place under local (national) law
- **In 2018**
All agreement were checked for GDPR compliance
and amendments where made where applicable



Using
2014/24/EU
procurement
directive,
to run a tender
as a collective

Infrastructure as a Service

Available offerings, results from a pan-European tender



Amazon Web Services

via resellers



Benefits of the pan-European IaaS framework agreements

Discounted prices
for all institutions,
large and small

Ready-to-use agreements
which comply with EU data
protection law, including GDPR

Invoice billing, no credit card needed, accommodating
capital expenditure through upfront commitments

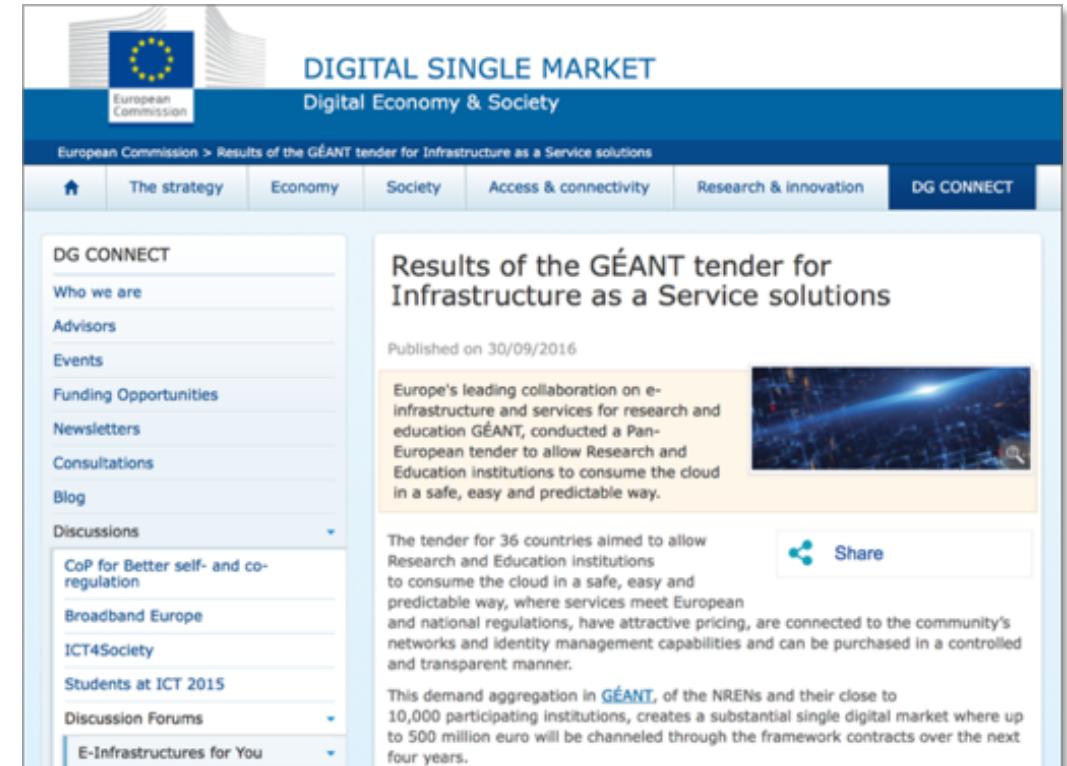
Transfer existing
educational
licenses to the
cloud

Manage
usage and
spending

Sign your
contract under
local law

Reduced traffic costs,
through suppliers' connections
to the GÉANT network

Single sign-on
support (SAML2)



The screenshot shows a webpage from the European Commission's Digital Single Market website. The header includes the European Commission logo and the text "DIGITAL SINGLE MARKET" and "Digital Economy & Society". A navigation bar below the header includes links for "Home", "The strategy", "Economy", "Society", "Access & connectivity", "Research & innovation", and "DG CONNECT". The main content area features a section titled "Results of the GÉANT tender for Infrastructure as a Service solutions", published on 30/09/2016. The text describes Europe's leading collaboration on e-infrastructure and services for research and education. It mentions that GÉANT conducted a Pan-European tender to allow Research and Education institutions to consume the cloud in a safe, easy and predictable way. The tender aimed to allow 36 countries to consume the cloud in a safe, easy and predictable way, where services meet European and national regulations, have attractive pricing, are connected to the community's networks and identity management capabilities and can be purchased in a controlled and transparent manner. The text also notes that this demand aggregation in GÉANT, of the NRENs and their close to 10,000 participating institutions, creates a substantial single digital market where up to 500 million euro will be channeled through the framework contracts over the next four years.

EU institutions can buy the offerings direct
With no need to run their own tender

- The services can be acquired through invoice-based billing (no credit card needed)
- The suppliers offer aggregated user discounts. These same discounts apply to all of the eligible 10,000 institutions, either large or small
- All suppliers support SAML2 to enable single sign-on, some connect to eduGAIN
- Through direct private peerings with the GÉANT network, there is a significant reduction in the data transport charges

IaaS framework uptake

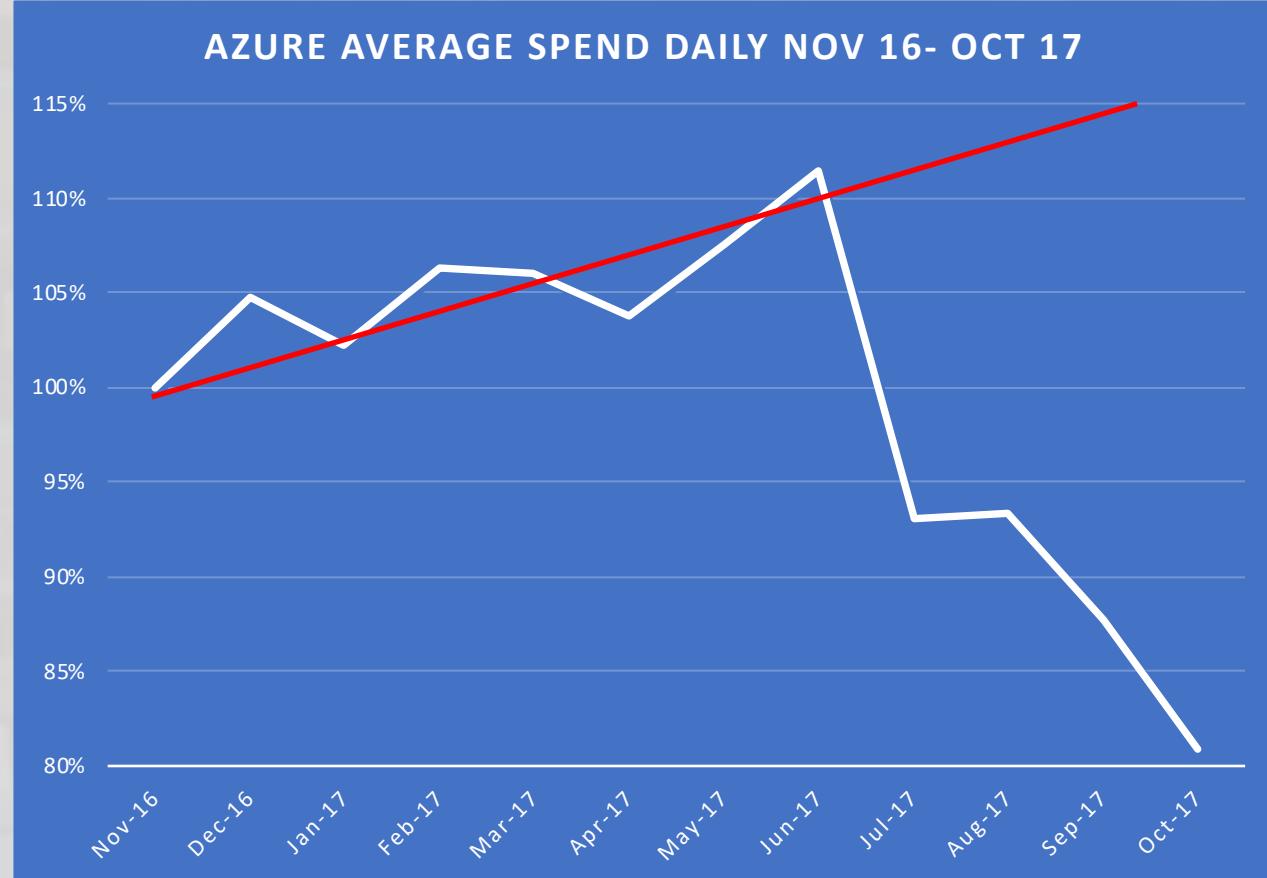
Consumption of the IaaS framework agreements is taking place in 18 countries, by 300+ institutions, who have collectively spent €13 million

Countries with consumption



Cloud catalogue

IaaS cost savings, specific use case



Quality & Qualifications institute (QQI) in Ireland

Achieves substantial savings using the GÉANT IaaS framework agreement

33% cost reduction after QQI worked with the Irish NREN, HEAnet, to transfer their Microsoft Azure workloads to the GÉANT IaaS framework agreement

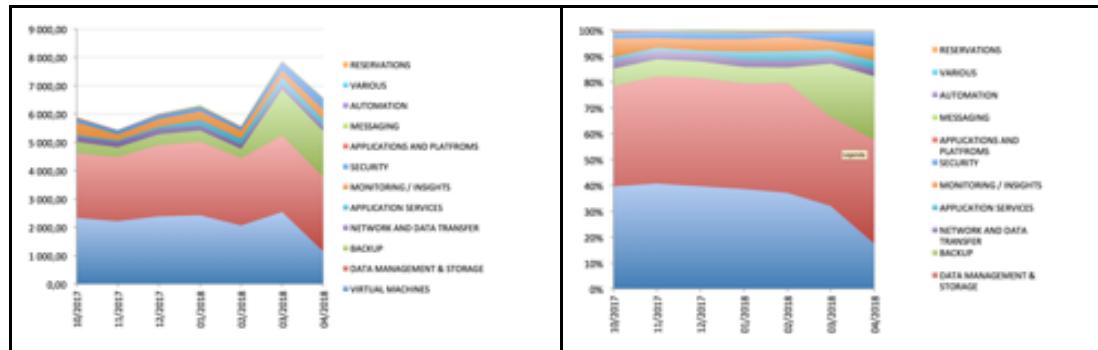
from July 2017 onwards

Cost benchmarking report

Advice on IaaS cost optimisation and cost reductions

Using QQI institutional use case as starting point

“One of the observations made during the analysis, is that the client is still extensively using the pay-as-you-go model. Therefore, implementing more resources in the Reserved Instances approach would be highly beneficial.”



Picture 2. Historical analysis of overall costs and cost structure of the client's cloud services

- ✓ Clean unused storage
- ✓ Look for cheaper regions
- ✓ Be aware that VMs' families frequently change and are upgraded
- ✓ Use the available discounts options available (ask for advice on available options from the supplier, reseller and your NREN)
- ✓ Do not run 24x7 VMs if this is not needed (such as dev instances)
- ✓ Shut down idle or underutilised VMs
- ✓ Use the cloud resources only for the purposes they were procured for

Infrastructure as a Service

Supplier tailor-made offerings (not a public procurement framework agreement)



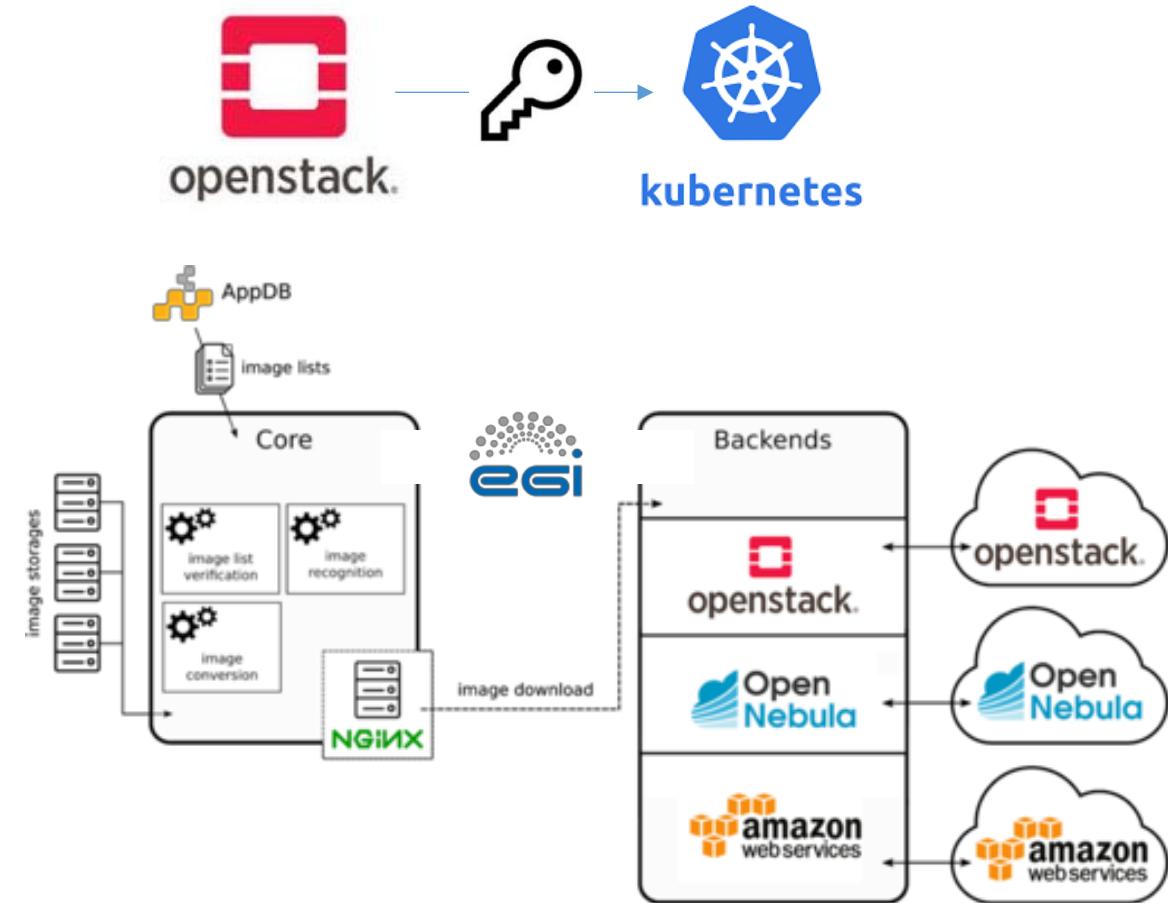
Google
Cloud Platform

Service development

Backend: IaaS cloud connectors

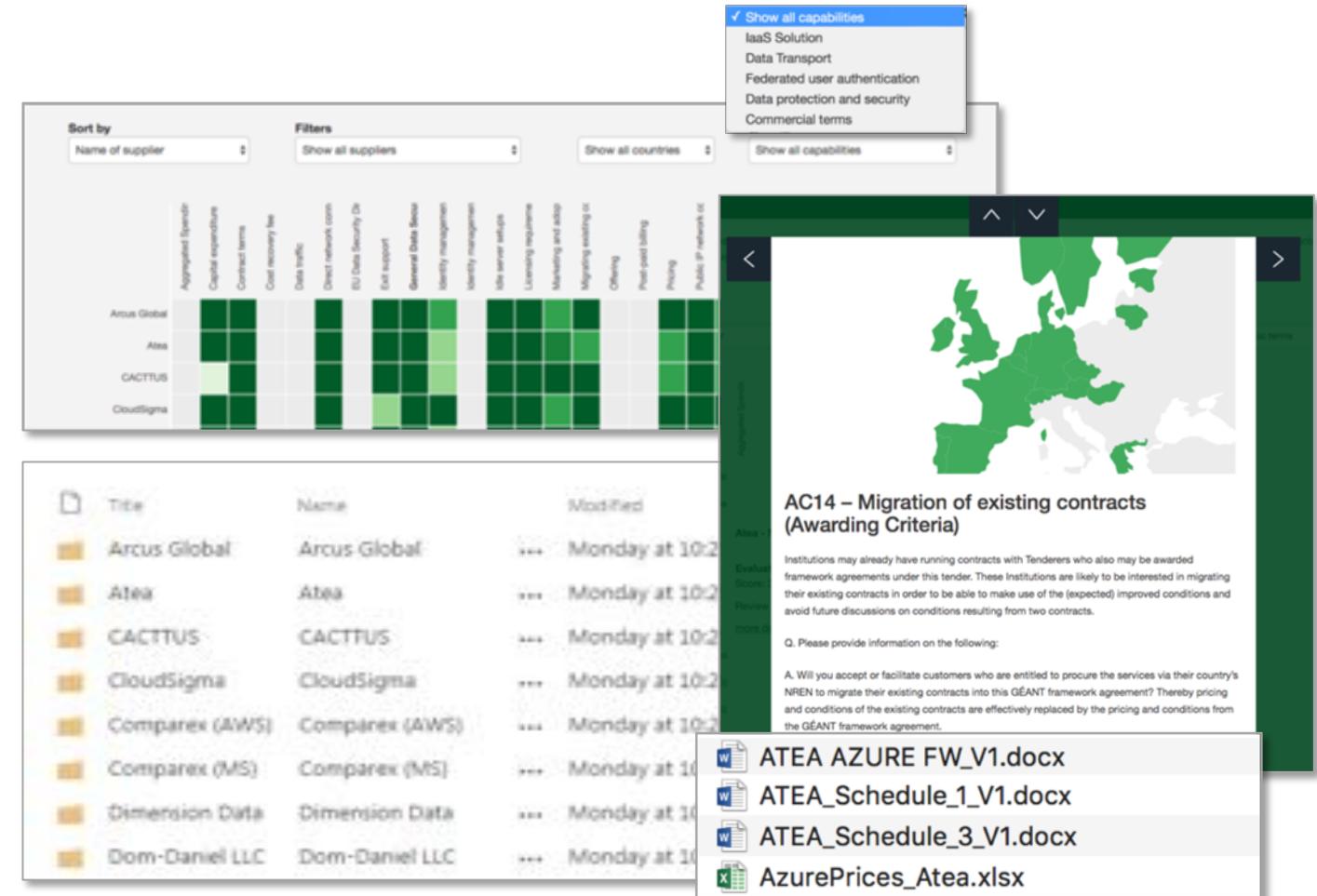
GÉANT developed two underlying IaaS cloud enabling technologies:

1. An **authentication path** between Open Stack and Kubernetes
2. A **cloud data migration tool**:
an extension to the Cloudkeeper tool
 - connecting the EGI federated community cloud (AppDB component)
 - to the AWS public cloud



Service management

1. Community of 140 NREN cloud managers and specialists
2. An intranet workspace for NREN cloud managers
 - Information sharing
 - Manuals and cookbooks on how to deploy the service portfolio
3. Service Catalogue: IaaS Service Matrix
Allows institutions (customers) to compare the available IaaS offerings
4. Contract repository
Allows institutions (customers) to access the agreements
5. Customer helpdesk



The screenshot displays the GÉANT Service Management interface, featuring several key components:

- IaaS Service Matrix:** A grid comparing IaaS capabilities across four suppliers: Arcus Global, Atea, CACTTUS, and CloudSigma. The columns represent various services like Aggregated Spend, Capital expenditure, Contract terms, Cost recovery fee, Data traffic, Direct network conn, EU Data Security Dir, Evt Report, General Data Privacy, Identity management, Identity management, Idle server setups, Licensing mechanism, Marketing and sales, Migrating existing UI, Offering, Pricing, and Public IP network. The matrix uses a color scale from white to dark green.
- Contract Repository:** A list of contracts with details such as Title, Name, and Modified date. Contracts listed include Arcus Global, Atea, CACTTUS, CloudSigma, Companex (AWS), Companex (MS), Dimension Data, and Dom-Daniel LLC.
- Customer Helpdesk:** A panel titled "AC14 – Migration of existing contracts (Awarding Criteria)" containing text about existing contracts and a list of attachments:
 - ATEA AZURE FW_V1.docx
 - ATEA_Schedule_1_V1.docx
 - ATEA_Schedule_3_V1.docx
 - AzurePrices_Atea.xlsx

Data classification tool

For risk management and cloud migration, sourcing decisions

		(y/n)
Confidentiality (1 - Open, 2 - Restricted, 3 - Confidential)		
Can data be accessed publicly without special access rights (user credentials)?		Y
If not, does the data considered contain:		
data related to research projects shared with the project participants		Y
financial data (e.g. budget planning, accounting reports)		Y
personal identifiable data (e.g. customer data, employee data, mail, accounting data, disciplinary matters, qualifications...)		Y

LOW RISK	MEDIUM RISK	HIGH RISK	Data type	On-premise (at the institute)	In country	In EU + EEA	Anywhere, In non-EU non-EEA
Data for public use Loss of confidentiality, integrity, or availability of the data or system has no significant impact	Personally Identifiable data Data is not generally available to the public Loss of the data or system could have a mildly adverse impact	Sensitive (Personally Identifiable) data Loss of the data or system could have a significant adverse impact on our mission, safety, finances or reputation.	public	Y	Y	Y	Y
			unrestricted	Y	Y	Y	Y
			restricted	Y	Y	Y	N
			confidential	Y	Y	Y, but only in community cloud	N
			secret	Y	Y	Y, but only in community cloud	N

Cloud security

Advice, through a number of articles

Cloud Security – Introduction

Welcome to the Cloud Security Resource Area. My name is Eyal Estrin and I am a cloud architect in the

[Read more.](#)

Fundamental Cloud Security Concepts Part 1 – CIA

-by Eyal Estrin, Cloud Architect, Inter-University Computation Center (IUCC) Cloud security is a hot topic worldwide due to both regulation and demand

[Read more.](#)

Fundamental Cloud Security Concepts Part 2 – AAA

-by Eyal Estrin, Cloud Architect, Inter-University Computation Center (IUCC) Our next installment in the alphabet soup of internet security is AAA, or

[Read more.](#)

Fundamental Cloud Security Concepts Part 3 – Encryption and Cryptography

-by Eyal Estrin, Cloud Architect, Inter-University Computation Center (IUCC) One of the important tools at our disposal for ensuring that confidentiality of

[Read more.](#)

Fundamental Cloud Security Concepts Part 4 – Shared Responsibility Model

-by Eyal Estrin, Cloud Architect, Inter-University Computation Center (IUCC) A fundamental security principle in Cloud Computing is the concept of the Shared

[Read more.](#)

Fundamental Cloud Security Concepts Part 5- Compliance

-by Eyal Estrin, Cloud Architect, Inter-University Computation Center (IUCC) Institutions engaging with public cloud service providers need assurance that they can trust

[Read more.](#)

Fundamental Cloud Security Concepts Part 6- Network and Security in Amazon Web Services (AWS)

-by Eyal Estrin, Cloud Architect, Inter-University Computation Center (IUCC) This post addresses another important aspect of cloud security – the

[Read more.](#)

Channel outreach

User stories and use cases on the GÉANT clouds website

Inholland Hogeschool

The Capacity Challenge Inholland is a university of applied sciences with multiple sites offering bachelor and master degrees in a

[Read more.](#)

Lycée des Arts et Métiers-Luxemburg

The Challenge Lycée des Arts et Métiers (LAM) in Luxembourg offers a post-secondary education course on "Installation and Configuration of

[Read more.](#)

ROC Midden Nederland

Strategy: "Cloud Unless" ROC Midden Nederland, a secondary vocational education institution offering adult continuing education, enterprise training and training for

[Read more.](#)

Arcus College (Netherlands)

Why the cloud? Arcus College was no stranger to outsourced ICT services. Through a 2012 joint procurement arrangement for server,

[Read more.](#)

Quality & Qualifications Ireland (QQI)

Why the cloud? QQI needed to improve a vital, mission-critical legacy application that was operating on outdated hardware, inefficient software

[Read more.](#)

App Store for scientists

Together with the University of Bergen and the University of Oslo, UNINETT's HE Cloud Initiative (UH-sky) is working to demonstrate

[Read more.](#)

Educational clouds in Norway – Edulab

The UNINETT HE cloud initiative, UH-sky, together with the Norwegian University of Science and Technology (NTNU), is looking into how

[Read more.](#)

IT-Lab: Is it possible to move the university data centre to the cloud?

Why the cloud? In a collaboration with the University of Agder, UNINETT's HE Cloud Initiative (UH-sky) is exploring the possibility

[Read more.](#)

University Gains Cost-Effective Disaster Recovery Solution

Marquette University didn't have an effective disaster recovery process in place because of the high cost and IT time required

[Read more.](#)

University of Stirling and Microsoft Azure helping to untangle airports

Nobody likes a delay at the airport. Many of us have spent time buckled up, ready for takeoff, wondering why

[Read more.](#)

Coventry University Hits £1 Million Savings Goal with Virtualised Network

When the Coventry University IT team was asked to cut £1 million from its budget, it turned to virtualisation technologies.

[Read more.](#)

Norway: Box for all students

Why the cloud? Students at AHO had access to a personal storage space of 4 Gigabyte on school servers. With

[Read more.](#)

Three steps into the cloud

Level 1: no cloud	Level 2: small clouds	Level 3: big clouds
<ul style="list-style-type: none">• Digital services run locally at the institutions: installed and managed on-premises.• No collaboration between institutes on collective vendor management and procurement.	<ul style="list-style-type: none">• First digital services are moved off campus, to the cloud.• Involves e-mail, lift-and-shift of virtual machines and cloud experimentation.• Single or a few suppliers.• Institutions need support with core components: network, identity management and cloud contracts.• Coordination organisations to establish and make available cloud agreements.• Institutions buy individually.	<ul style="list-style-type: none">• Institutions have a digital transformation strategy, which includes cloud deployments, through structured sourcing decisions.• Services are bought from more suppliers. Services encompass more specialist tools. Serverless, Machine Learning and AI.• Multi cloud usage and management in production environments.• Institutions aggregate volume purchases.• Lead buyer , buys in bulk on behalf of the group



Thank you

Any questions?

www.geant.org



© GÉANT Association
As part of the GÉANT 2020 Framework Partnership Agreement (FPA),
the project receives funding from the European Union's Horizon 2020
research and innovation programme under Grant Agreement No.
856726 (GN4-3).