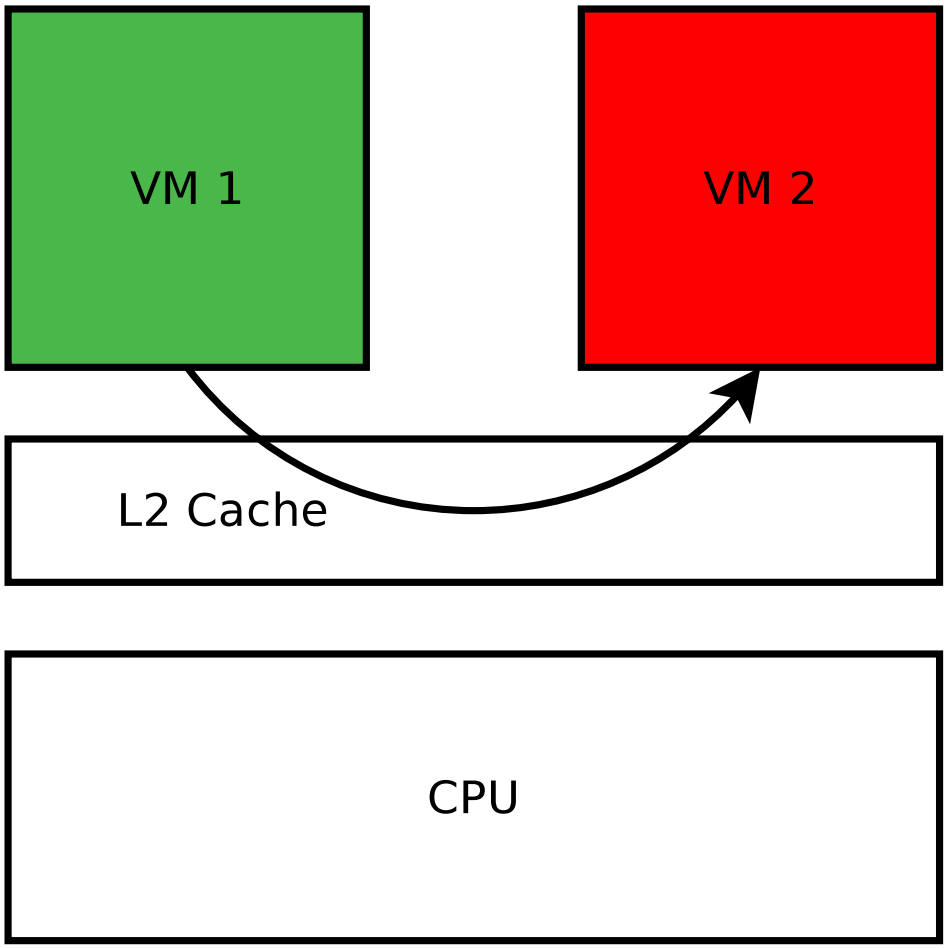
Seed4C: A High-security project for Cloud Infrastructure

J. Rouzaud-Cornabas (LIP/CC-IN2P3 – CNRS) & E. Caron (LIP – ENS-Lyon)

November 30, 2012

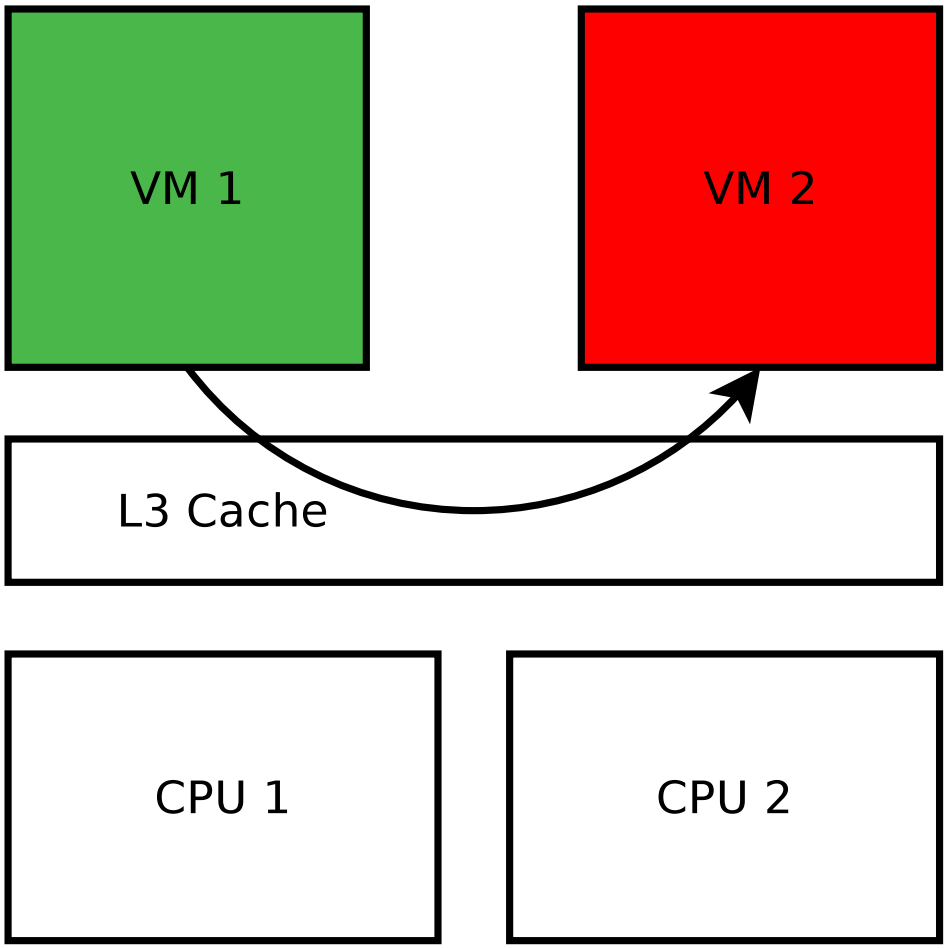
What is missing to bring cloud to better security

- Virtualization is not security



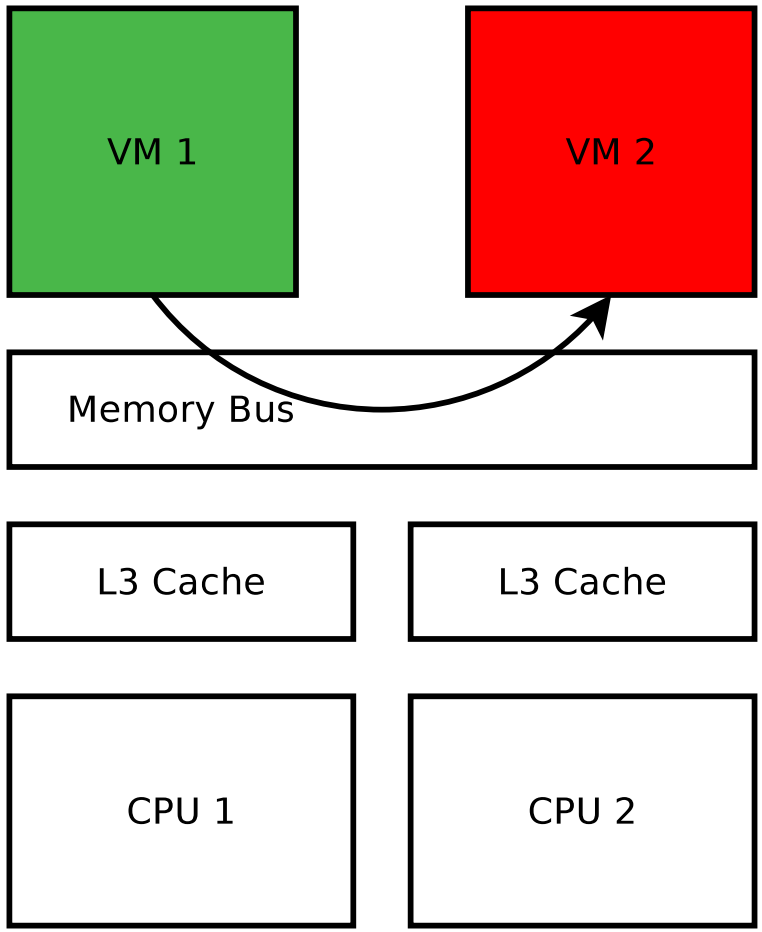
What is missing to bring cloud to better security

- Virtualization is not security



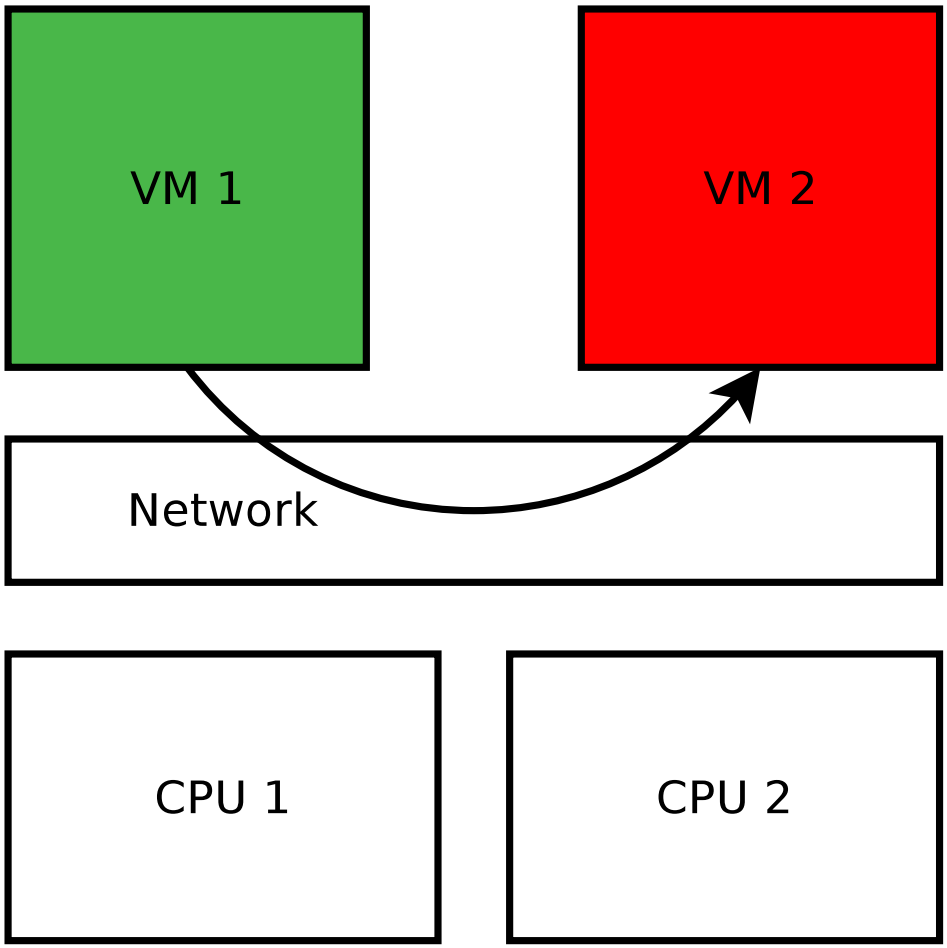
What is missing to bring cloud to better security

- Virtualization is not security



What is missing to bring cloud to better security

- Virtualization is not security

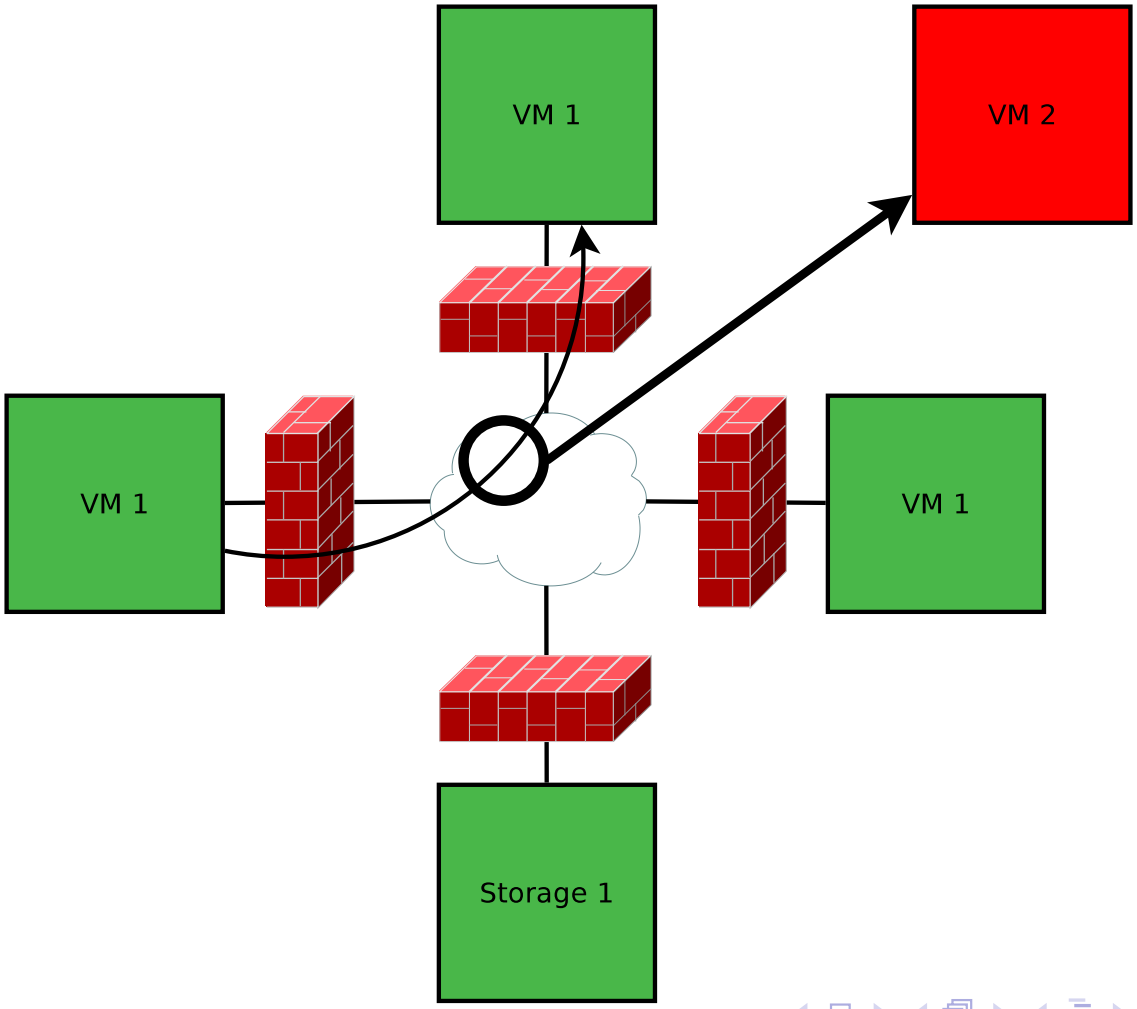


What is missing to bring cloud to better security

- Virtualization is not security $\rightarrow$ **security of Clouds**;
- Not only secure the software running on a single machine

What is missing to bring cloud to better security

- Virtualization is not security → **security of Clouds**;
- Not only secure the software running on a single machine



What is missing to bring cloud to better security

- Virtualization is not security $\rightarrow$ **security of Clouds**;
- Not only secure the software running on a single machine $\rightarrow$ **manage and guarantee the security of a cluster of computers seen as a single entity**;

What is missing to bring cloud to better security

- Virtualization is not security $\rightarrow$ **security of Clouds**;
- Not only secure the software running on a single machine $\rightarrow$ **manage and guarantee the security of a cluster of computers seen as a single entity**;
- Centralized security servers not efficient;

What is missing to bring cloud to better security

- Virtualization is not security $\rightarrow$ **security of Clouds**;
- Not only secure the software running on a single machine $\rightarrow$ **manage and guarantee the security of a cluster of computers seen as a single entity**;
- Centralized security servers not efficient;

A new type of approach is required taking into account the specific cloud architecture

What is missing to bring cloud to better security

- Virtualization is not security $\rightarrow$ **security of Clouds**;
- Not only secure the software running on a single machine $\rightarrow$ **manage and guarantee the security of a cluster of computers seen as a single entity**;
- Centralized security servers not efficient;

The project will deal with the concept of Network of Secure Elements (NoSE)

Use cases

The range of use cases addressed by this concept is broad

- Locking the software execution to a group of specific machines;
- Tying virtual machine execution to specific servers;
- Making sure that only trusted nodes can take part of the computing game;
- Certifying the integrity of results returned by each one of them;
- Collecting evidence and logs securely and irrevocably;
- **Bringing Cloud Security to HPC and Big Data**;
- etc.

Consortium

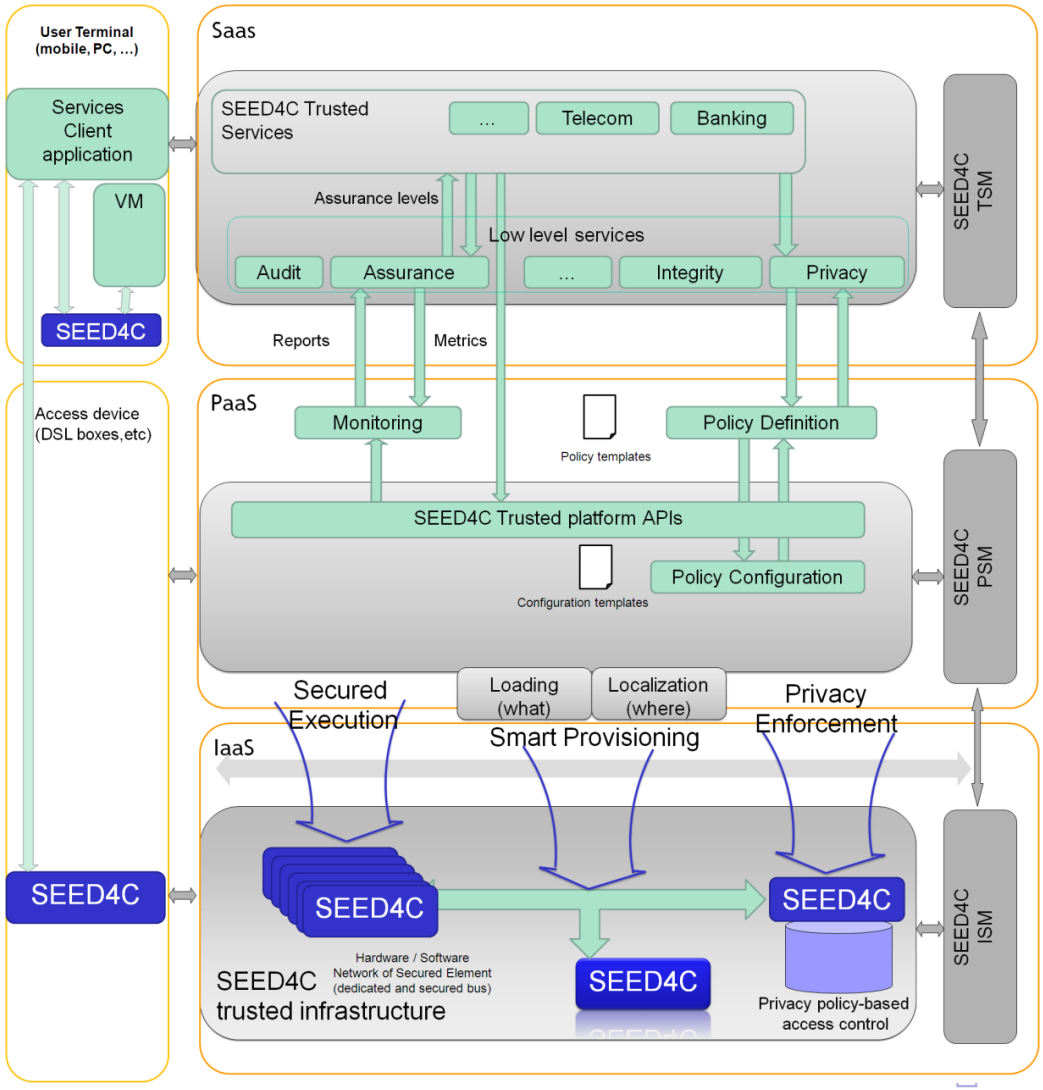
- Finland: VTT, MPY, NSN, Cygate, Novell
- France: Alcatel-Lucent Bell Labs, Gemalto, ENSI Bourges, INRIA, Wallix
- Spain: Innovalia Association, NEXTEL, Software Quality System, 3DIGITS, Vicomtech, IKUSI

- Core skills and experience:
  - Security technologies
  - Infrastructure and Cloud
  - Assurance

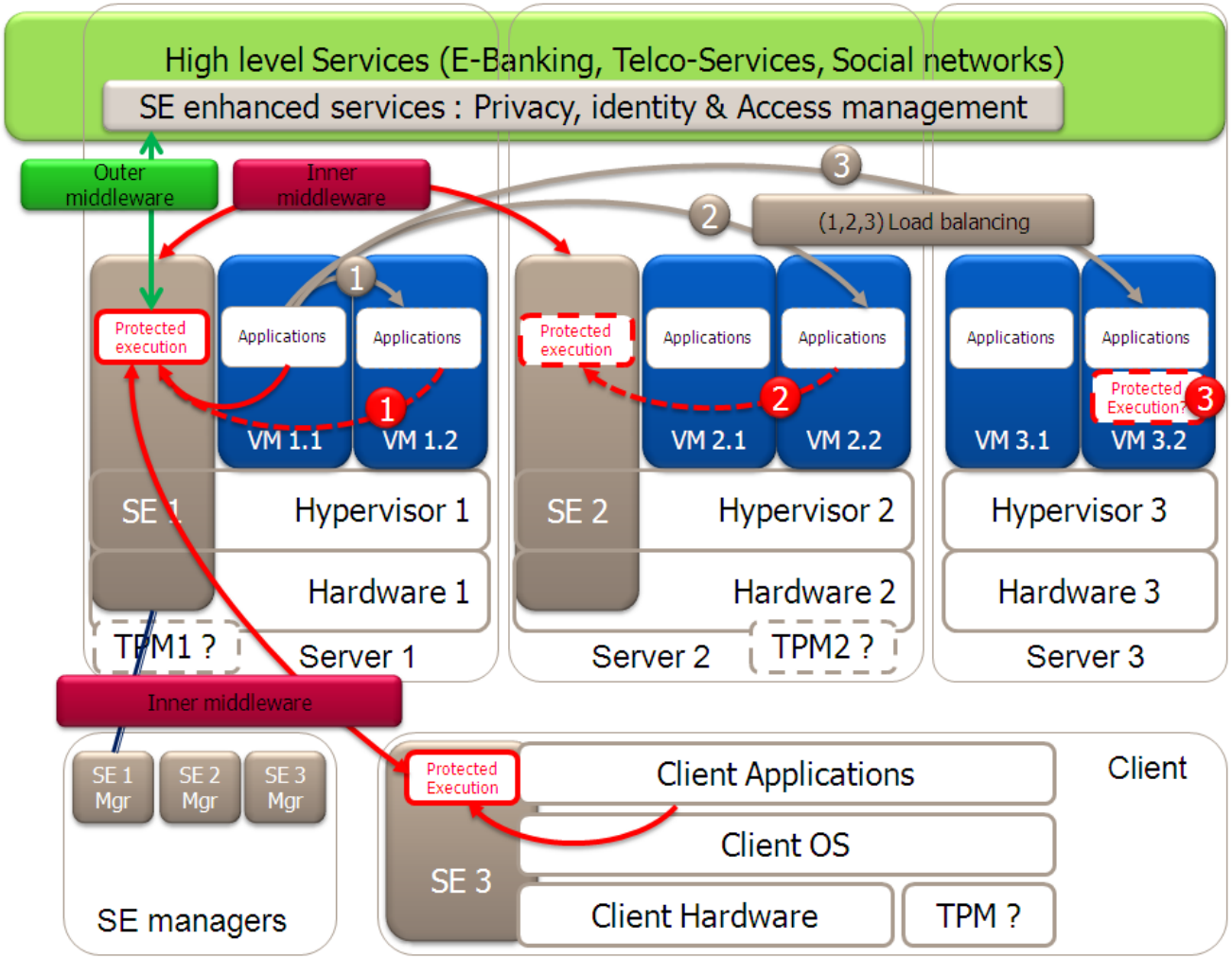
Network of Secure Elements

- Individuals secure elements attached to machines, user or network appliance;
- Establish security association, communicate together to setup a trusted network of machines;
- Propagate security conditions centrally defined to a group of machines;
- Impact of NoSE upon the different layers of the architecture, from hardware to services;

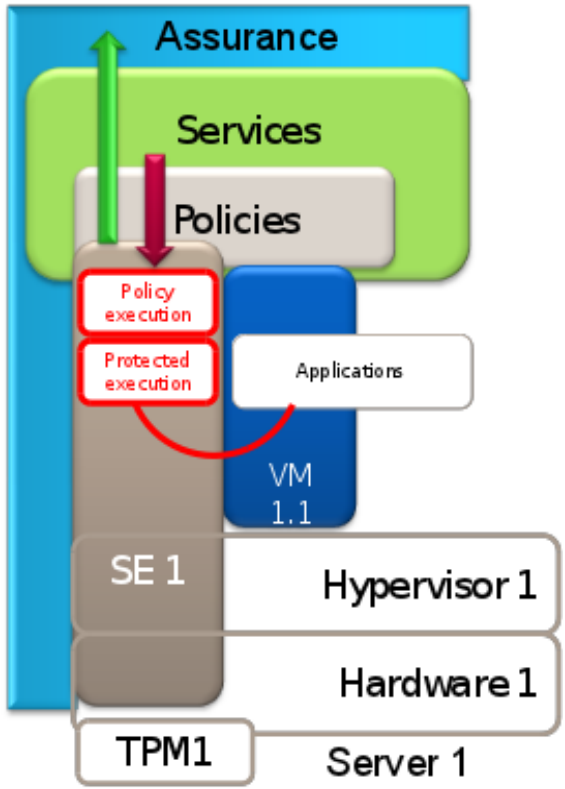
How to distribute Secure elements in IaaS and provide added value to Paas and SaaS



Secure load balancing and middleware



Policies execution and assurance

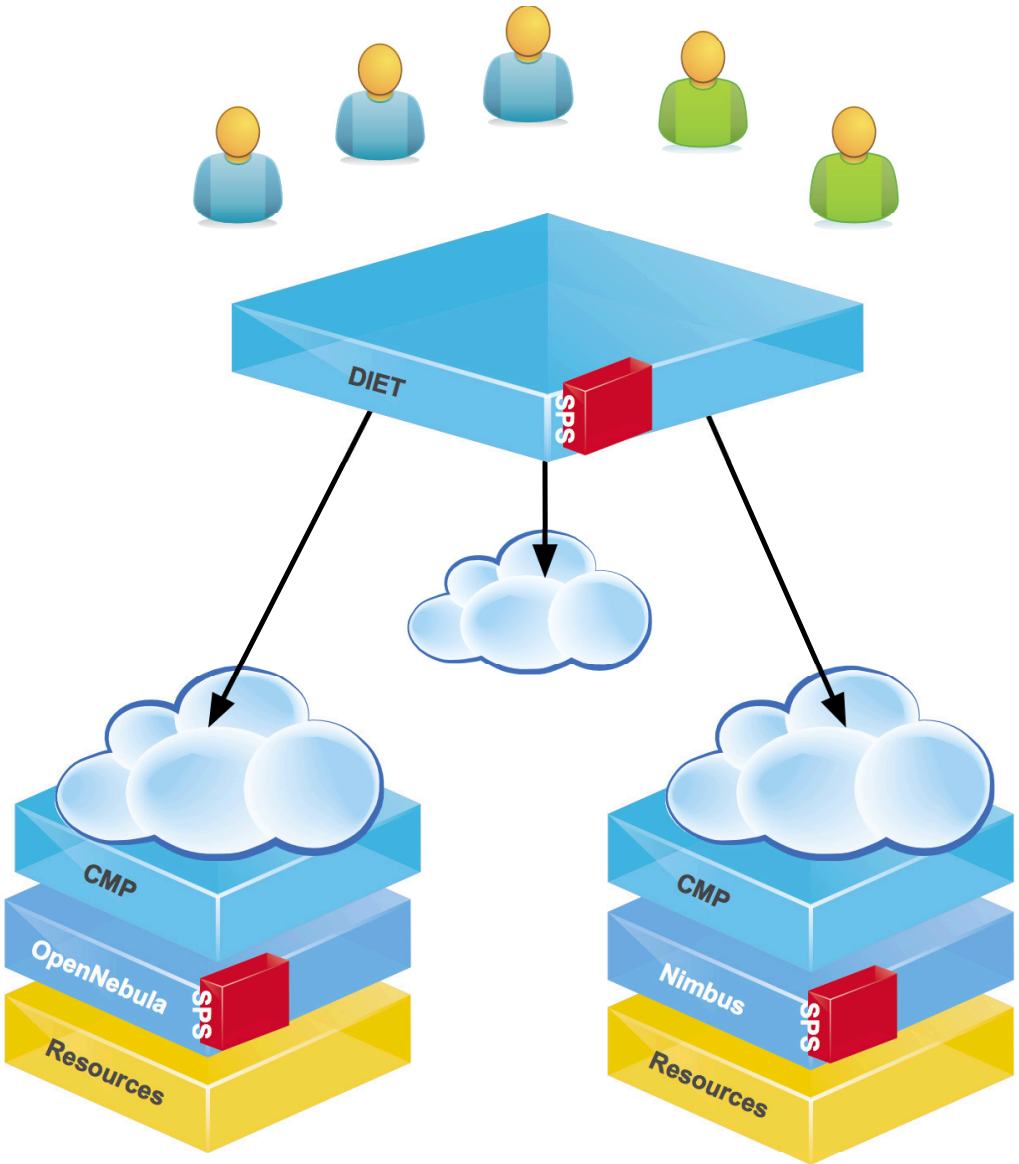


At an upper level, the definition and implementation of security and access control, privacy and identities policies involving secured elements will be specified, as well as the upper middleware.

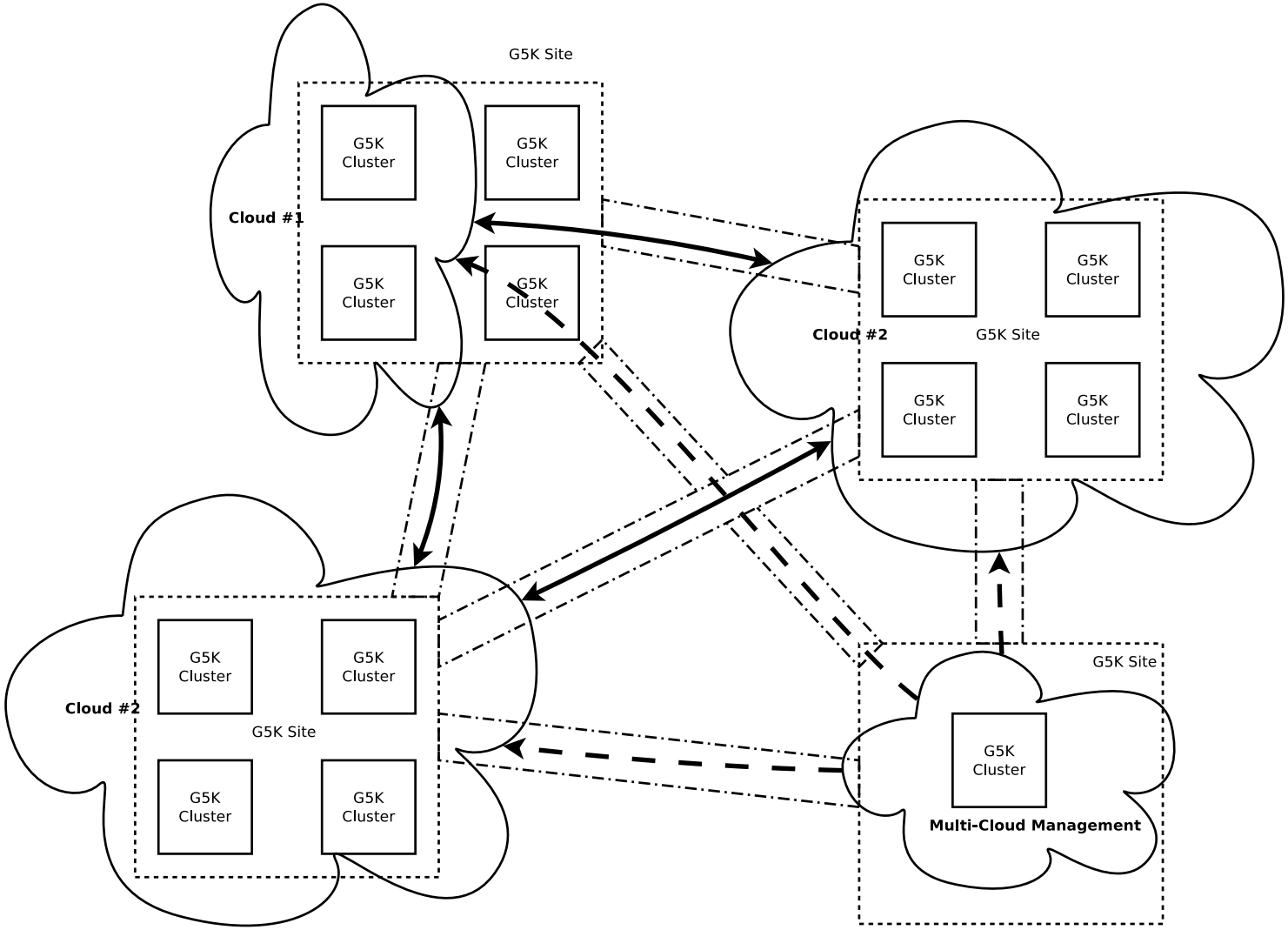
Main output for the project

- New architecture of Cloud Security
- SaaS and PaaS API (Outer Middleware) leading to trusted services and trusted platform
- Protocols for SE exchange and management (Inner Middleware)
- Privacy and identify policies mechanisms
- Data monitoring and traceability mechanisms

Secure Provisioning and Scheduling



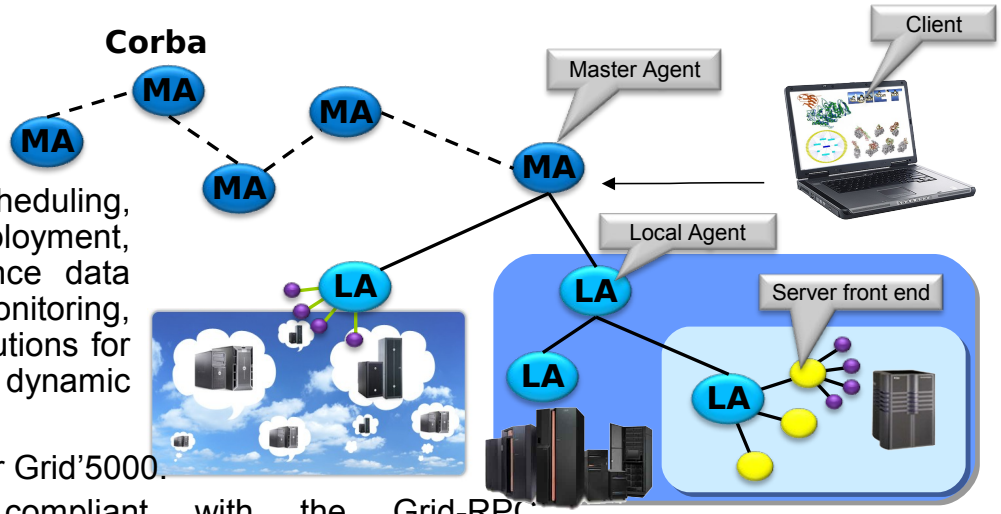
Seed4C on Grid'5000



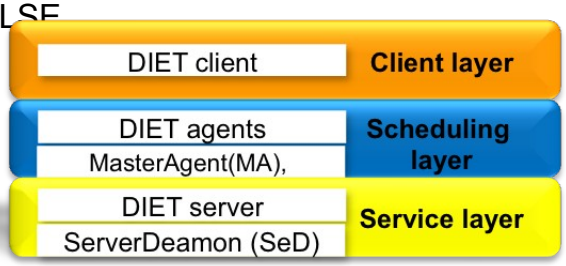
Use case HPC: DIET

DIET Distributed Interactive Engineering Toolbox

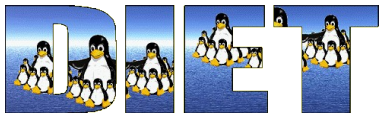
- **Context** : Development of a toolbox for deploying application services providers with a hierarchical architecture for scalability
- **Main research issues:** scheduling, heterogeneity, automatic deployment, interoperability, high performance data transfer and management, monitoring, fault tolerance, genericity of solutions for various applications, static and dynamic analysis of performance, …
- **Validation**: Large validation over Grid'5000.
- **Interoperability**: DIET is compliant with the Grid-RPC standardization for OGF
- **DIET used case**: The Decrypthon project - DIET was selected by IBM -
- **Collaborations**: RNTL GASP, ACI GRID ASP, TLSE, ACI MD GDS, ANR LEGO, ANR GWENDIA, Grid'5000
- **Start'up:** SysFera (created in march 2010).
- **Contact:** F. Desprez, E. Caron, GRAAL Team, LIP ENS (Frederic.Desprez,Eddy.Caron)@ens-lyon.fr
- **Web**: http://graal.ens-lyon.fr/DIET



http://graal.ens-lyon.fr/DIET

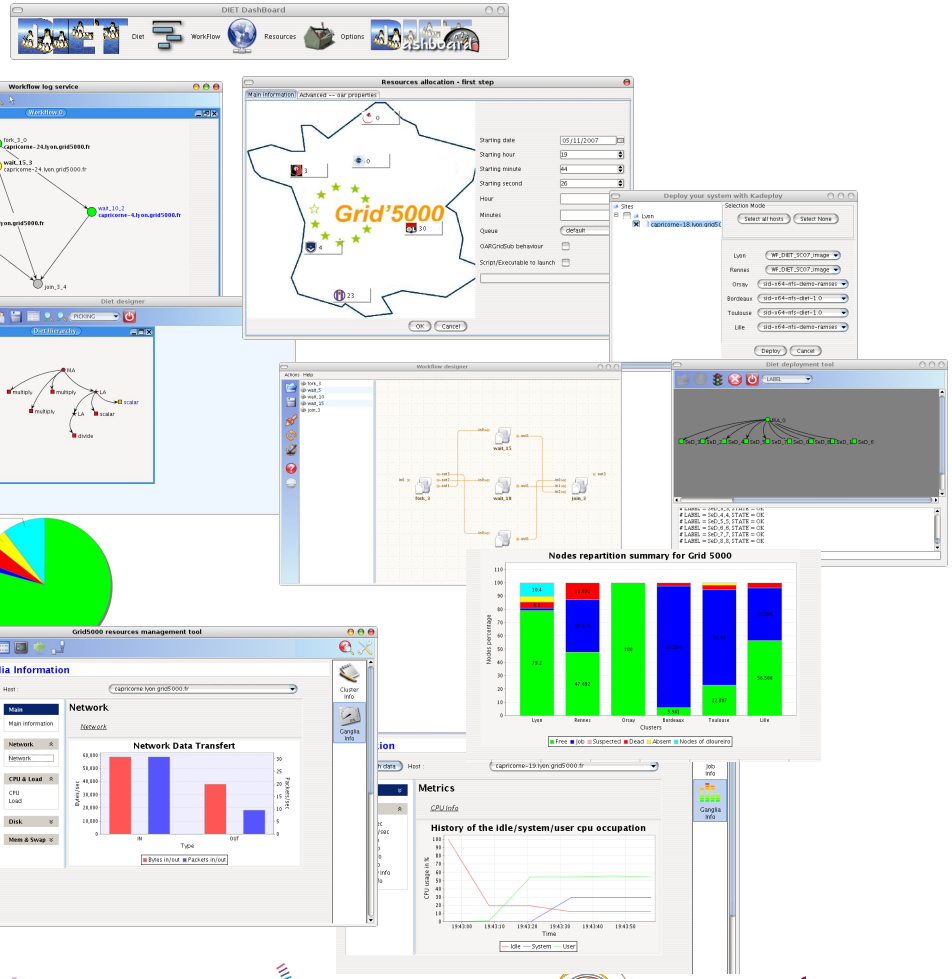


Use case HPC: DIET



Distributed Interactive Engineering Toolbox

GRAAL



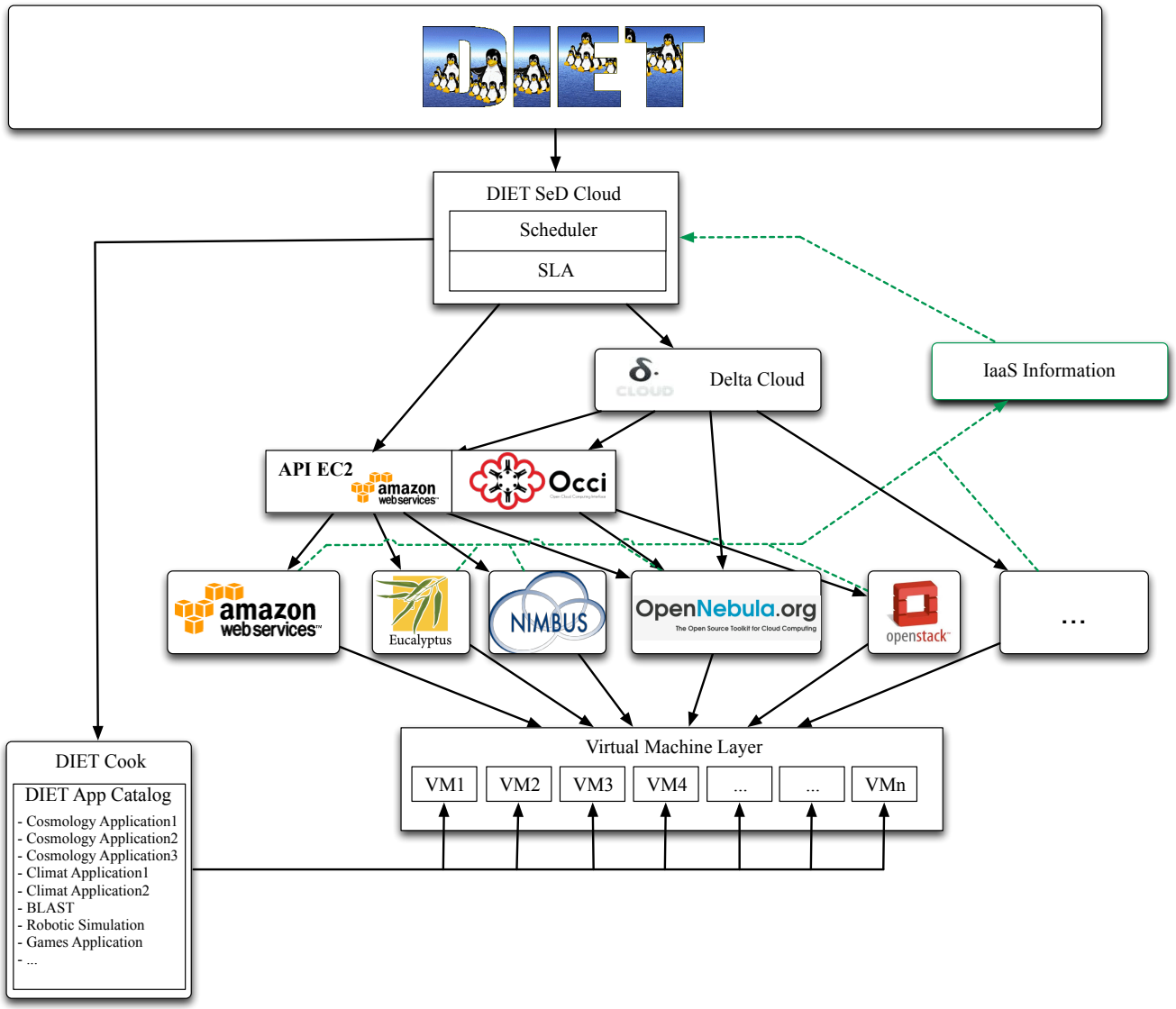
INRIA

CNRS

UNIVERSITÉ DE LYON

LIP

DIET Cloud


DIET
DIET SeD Cloud
Scheduler
SLA
Delta Cloud
IaaS Information
API EC2
amazon web services
Occi
amazon web services
Eucalyptus
NIMBUS
OpenNebula.org
The Open Source Toolkit for Cloud Computing
openstack
...
DIET Cook
DIET App Catalog
- Cosmology Application1
- Cosmology Application2
- Cosmology Application3
- Climat Application1
- Climat Application2
- BLAST
- Robotic Simulation
- Games Application
- ...
Virtual Machine Layer
VM1
VM2
VM3
VM4
...
...
VMn

Conclusion

- Start 04-2012 / End 10-2014
- Seed4C goal: Guarantee end-to-end security of service.
- Up to 80% of problems can be solved with a protected execution and a proper policy enforcement
- A TCB (Trusted Control Plane) within the network: the seed
  - Smart deployment of SEEDs and load balancing
  - Pre-provisioning of security credentials
  - Dynamic association with applications/services
  - SEED form factors and management (Hardware / Software / dedicated VMs / OS component)
- Execution of sensible code: Policy verification, Bootstrap, Isolation
- Assurance: Validation and Certification of host characteristics, Location, etc.
- Design of new elements to interface NoSE and Cloud software