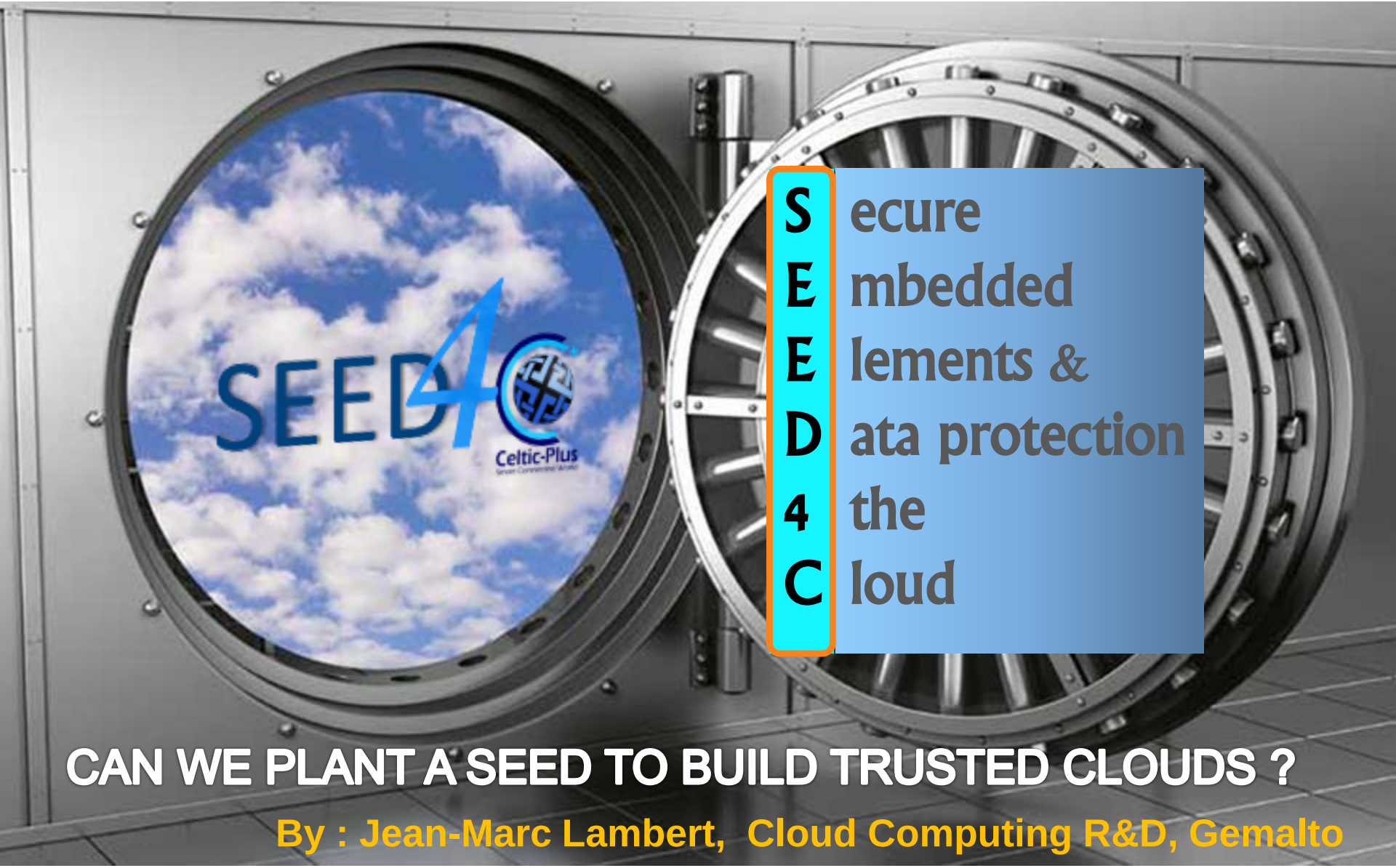


CAN WE PLANT A SEED TO BUILD TRUSTED CLOUDS ?

By : Jean-Marc Lambert, Cloud Computing R&D, Gemalto

http://www.celticplus-seed4c.org/

dgcis direction générale de la compétitivité de l'industrie et des services

Tekes

Gobierno de España · Ministerio de Industria, Energía y Turismo

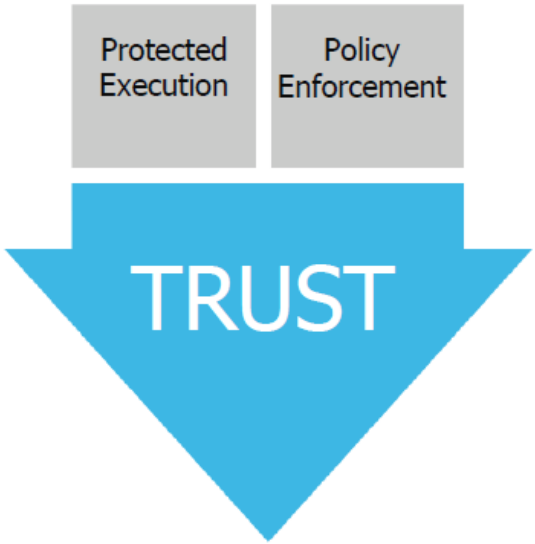
KIAT Korea Institute for Advancement of Technology

Celtic-Plus Smart Connected World

Context

Security of the Cloud is still an roadblock to massive cloud adoption in critical segments.

Customers need trust, and want to keep control of their assets



Need to harden cloud security

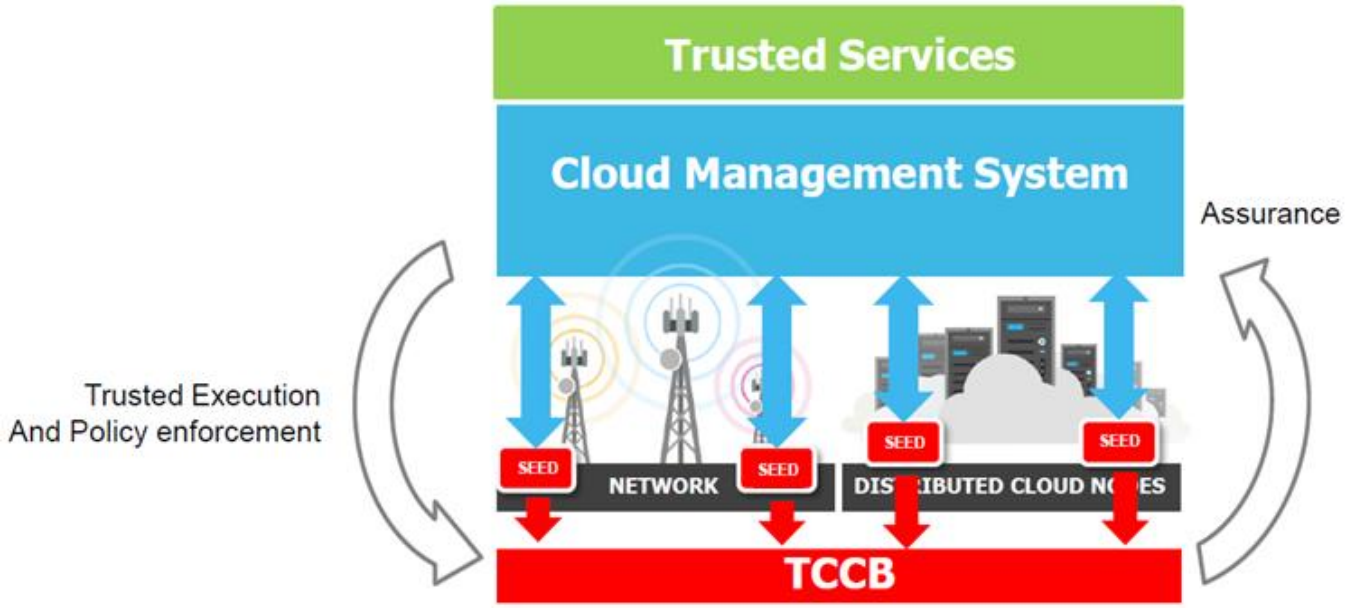
- **Enforce various security policies (e.g., regulation and business policies)**
- **Let customers define & control these policies**
- **Provide evidences of the policy enforcement**

Objectives

⇒ Building a Trusted Cloud Computing Base (TCCB)

Based on

- **A Cloud of minimal Trusted Computing Bases: the SEEDs**
  (Managed by the NoSE : Network of Secure Elements)



Objectives

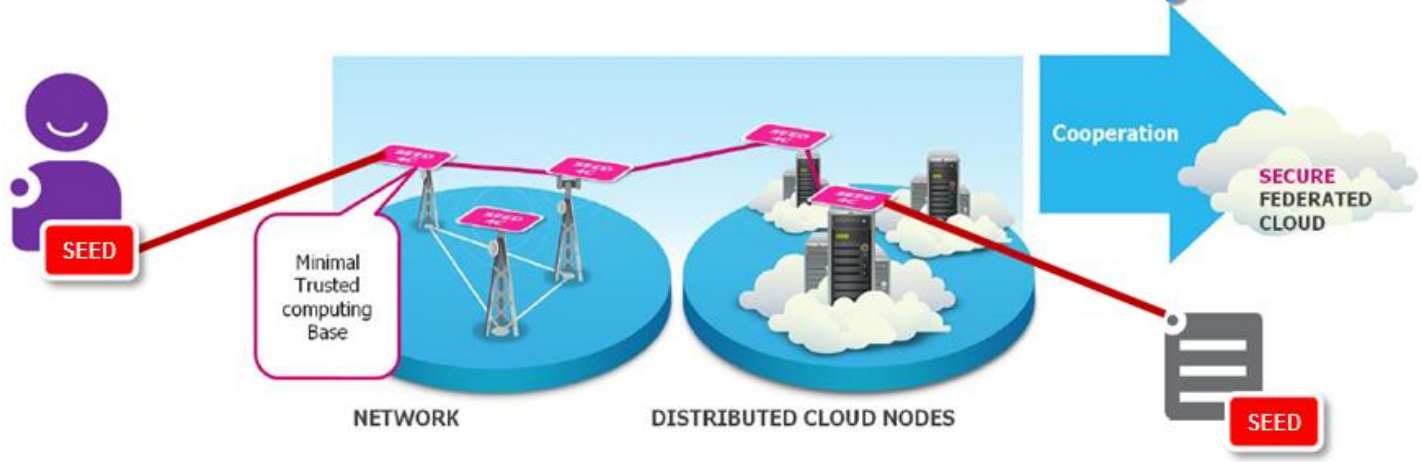
⇒ Building a Trusted Cloud Computing Base (TCCB)

Based on

- A Cloud of minimal Trusted Computing Bases: the SEEDs
  (Managed by the NoSE : Network of Secure Elements)

And

- That can guarantee **end-to-end security** of service



France

Alcatel-Lucent
Gemalto
ENSI Bourges
Inria
Wallix

Finland

Cygate
Mikkelin Puhelin Oy
Nokia Solutions & Networks Oy,
Finceptum Oy
VTT

Spain

Innovalia Association
Nextel
Software Quality Systems (SQS)
Fundación Vicomtech
IKUSI
BISCAYTIK

Korea

SOLACIA

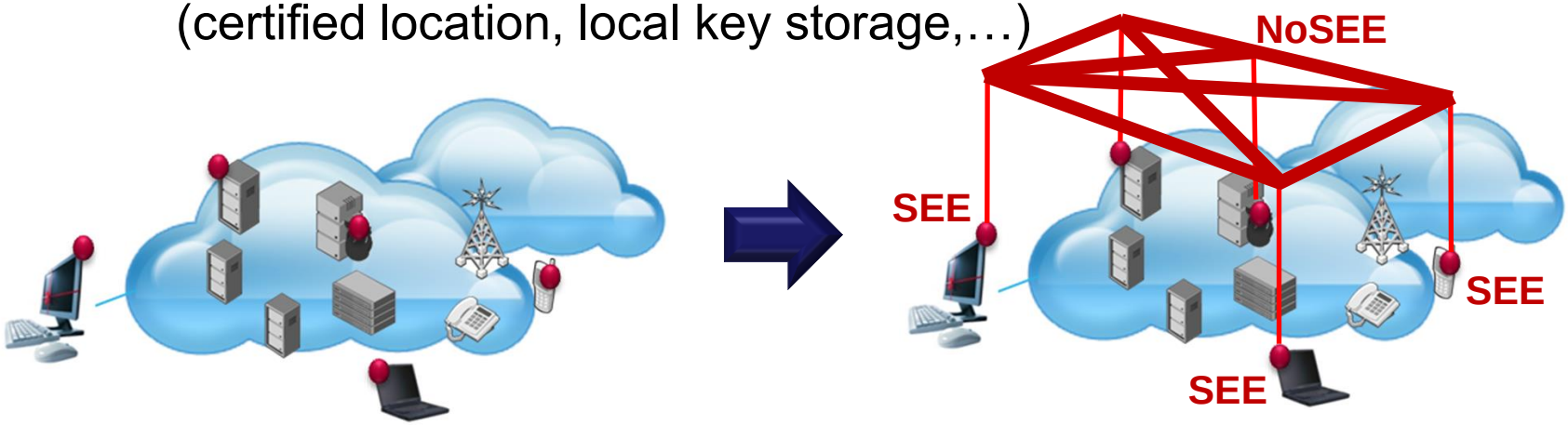
SEED4C: Security Embedded Element and Data Privacy for Cloud

Celtic-Plus
Smart Connected World

SEED4C approach

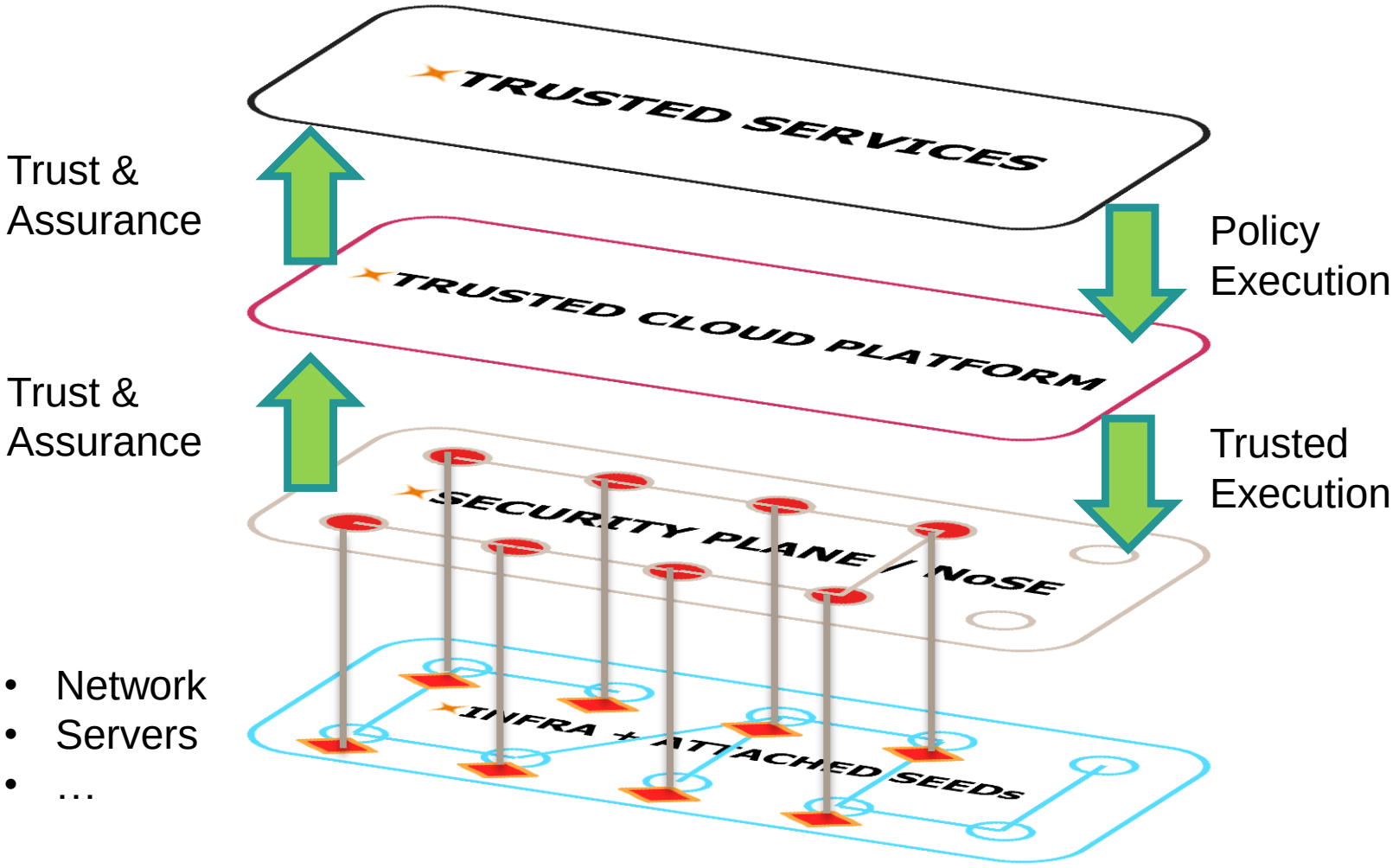
From an isolated security to a coordinated security

- **Secure Element Extended (SEE)**
  - **Store securely** critical data and **execute** securely critical apps
  - Support **multi-tenant data & apps**
- **Network of Secure Element Extended (NoSEE)**
  - **Secure administration** & exchange across cloud nodes.
  - Allow **Tenants** to manage their credentials & trust seeds.
  - Eg. allow critical data to be processed only in secure & compliant VMs (certified location, local key storage,…)



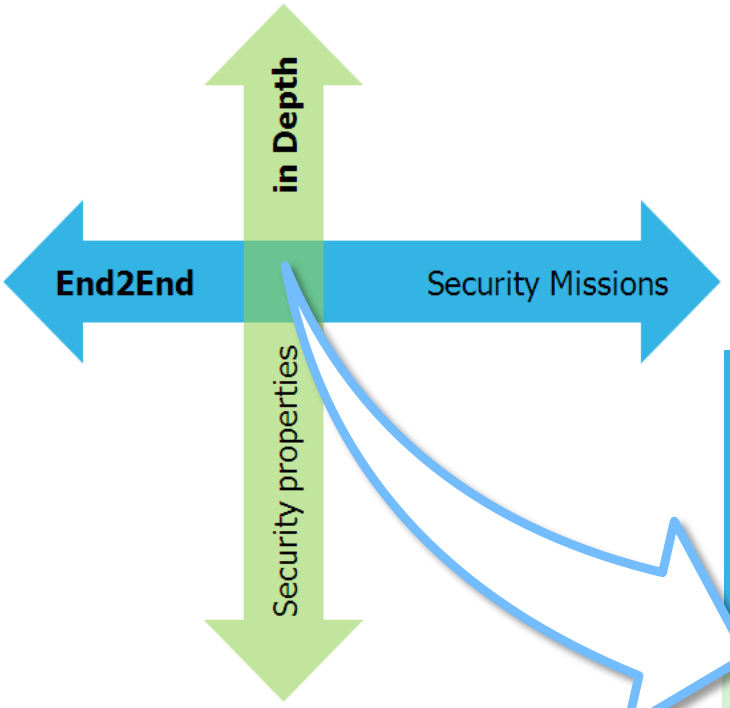
Isolated Security **Coordinated Security**

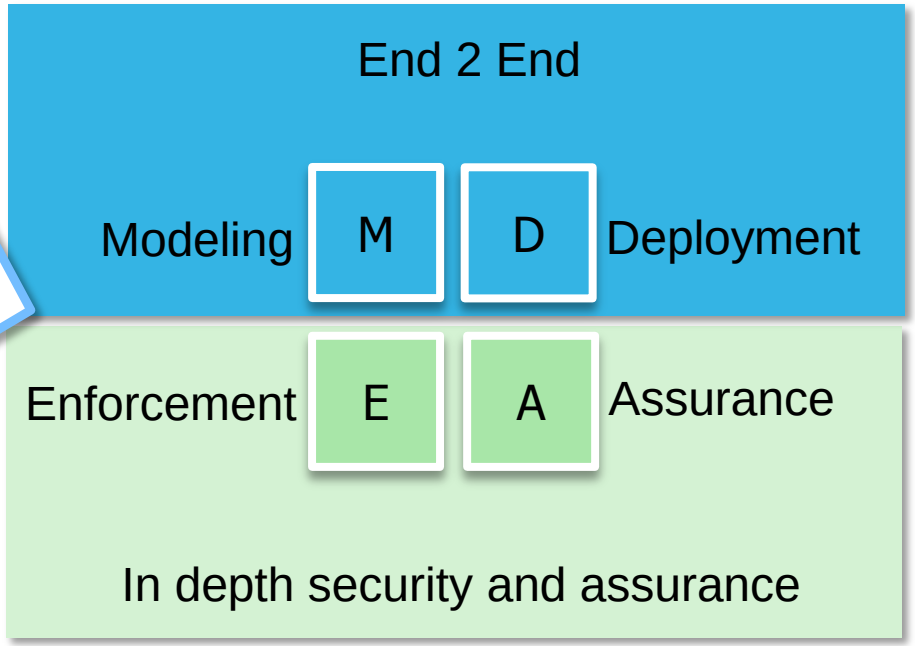
Deliver Trusted Services
in a multi-nodes Trusted Cloud Execution Environment



SEED4C scope of work

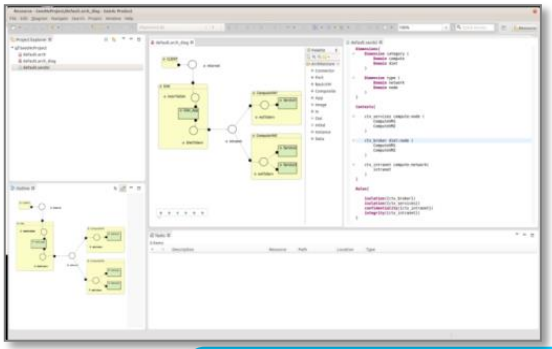
Modeling, Deployment, Enforcement and Assurance

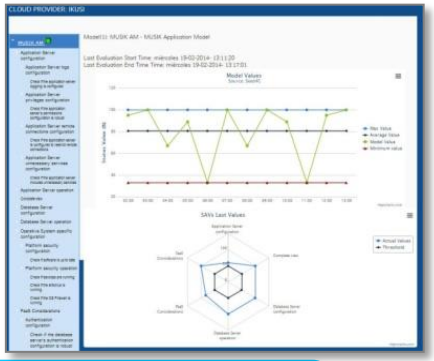




SEED4C process

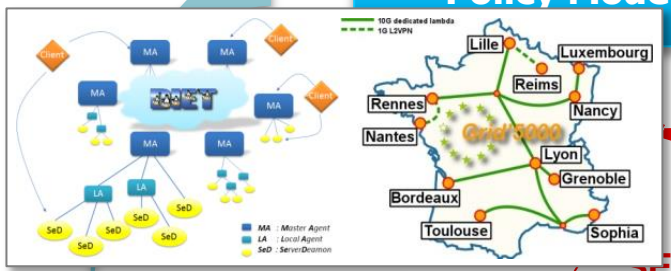
SEED4C Users





Policy Modeling

Policy Assurance



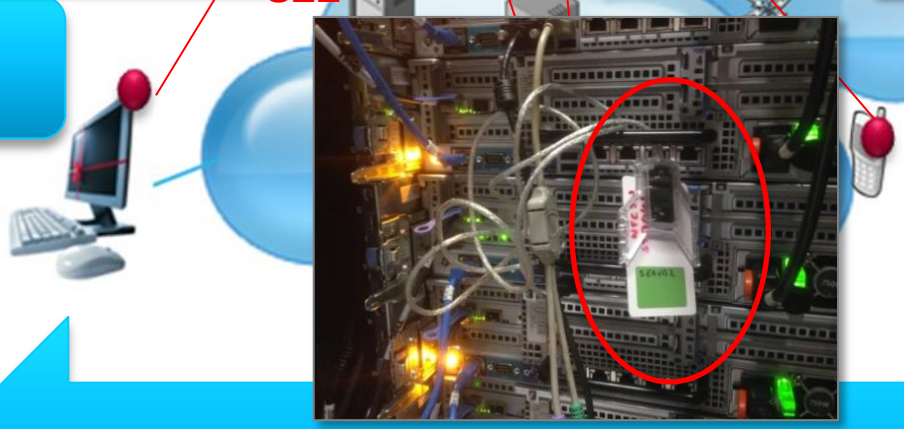
NoSEE

pass	fixed	fail	informational	unknown	total
2	0	2	0	0	4

	Result
Tomcat service running	pass
Tomcat under root user	fail
Tomcat listening on port 80	pass
Tomcat listening on port 8443	fail

App & Policy Deployment

Policy Monitoring



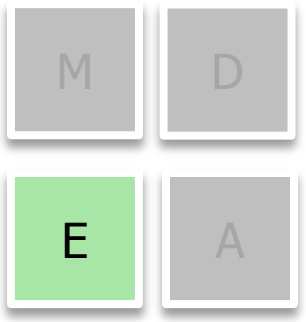
SEE–based Policy Enforcement

SEED4C Celtic-Plus

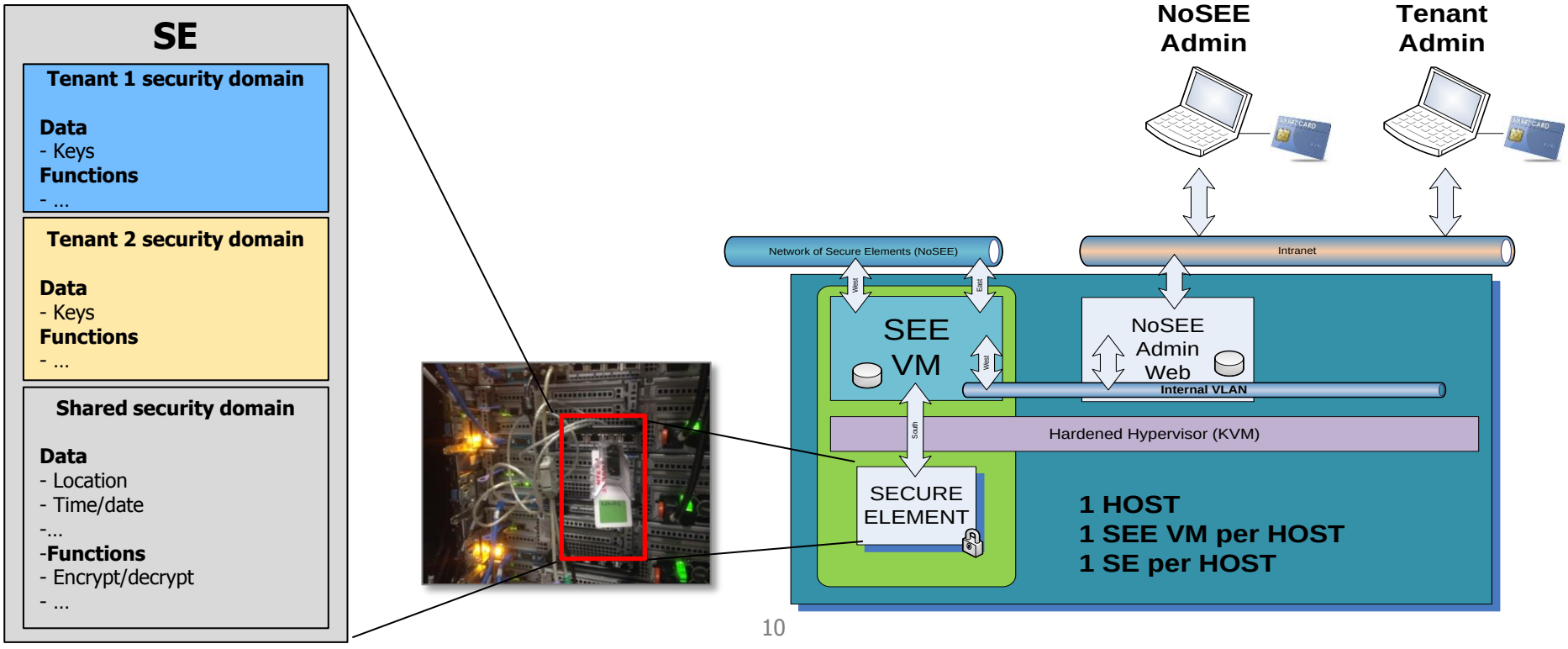
Celtic-Plus Smart Connected World

SEED4C: Enforcement engine

Cooperative security: the SEE model

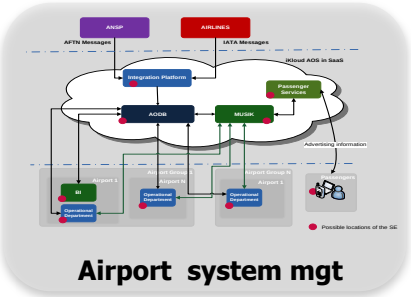


- SE are multi-tenant (isolated security domains)
- SE services offered by a dedicated SEE VM
- **NoSEE Admin**: Manage the attached SE (GP), the allocation of nodes to tenants & mirroring Tenant's security domain into SE(s)
- **Tenant Admin**: Manage security data and function in tenant security domains

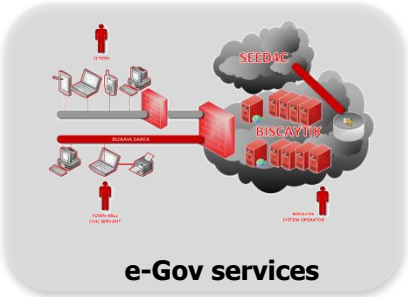


SEED4C Use-cases

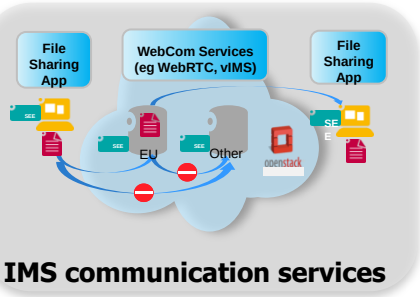
Various types of use-cases at different cloud levels (IaaS, PaaS, SaaS)



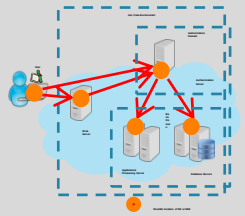
Airport system mgt



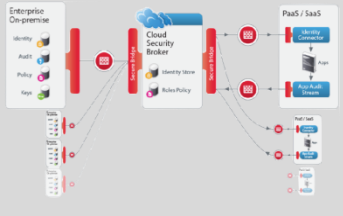
e-Gov services



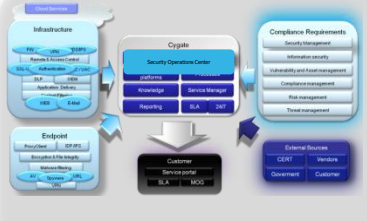
IMS communication services



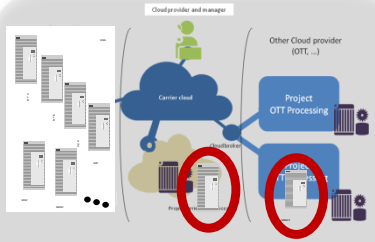
e-Banking



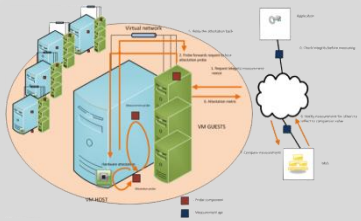
IAM authentication and auditing



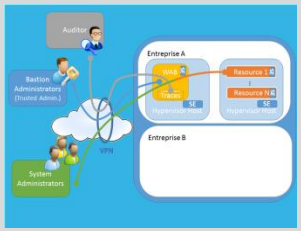
Security monitoring PaaS environment



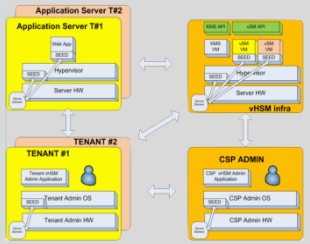
Telco services in the cloud (NFV)



IaaS level security



Administrative access mgt



vHSM + key ceremony

As a Conclusion :

Seed4C provides :

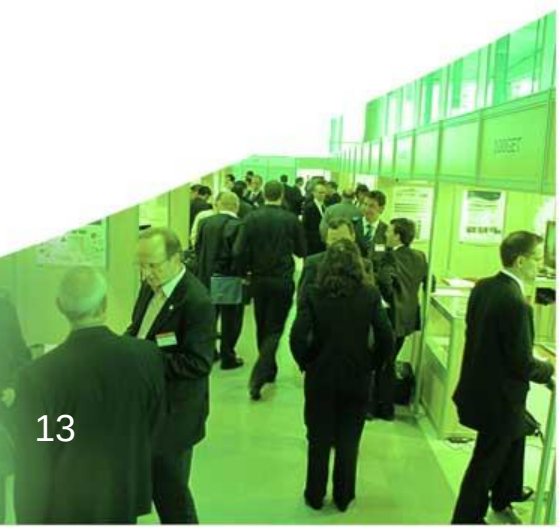
- Tenant's defined Security Policy & Control
- Security aware placement & deployment engine
- Modeling, Deployment, Enforcement and Assurance solution
- Enforced by :
  - The Network of Secure Elements Extended (NoSEE)
  - The Secure Elements physically present in each trustable cloud node.
  - The Assurance Framework providing evidences and allowing continuous monitoring.

Celtic-Plus
Smart Connected World

EUREKA

SEED4C

Celtic-Plus
Smart Connected World



http://projects.celtic-initiative.org/seed4c/