



Cloud Accountability and SLAs: research challenges and opportunities

Dr. Jesus Luna Garcia

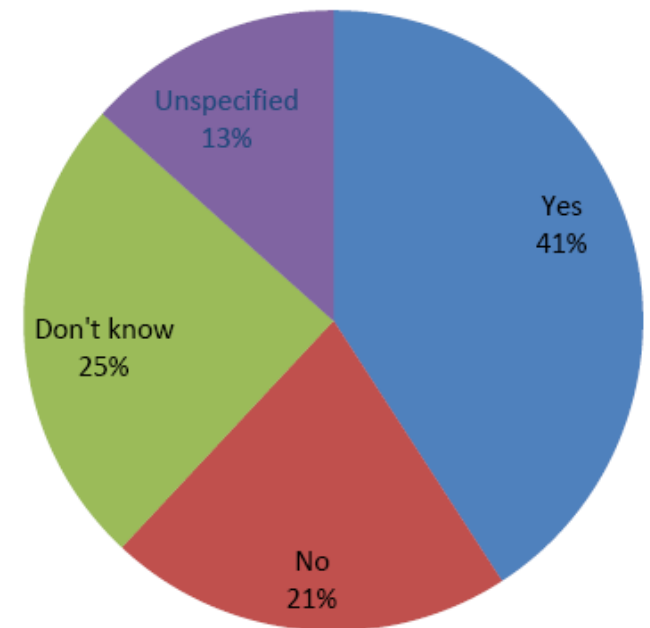
jluna@cloudsecurityalliance.org

Outline

- Cloud SLA's one year ago
- Open Research Challenges:
 - Standardization/certification
 - Accountability
 - SLA management
- Final remarks

One year ago: CCSW'12

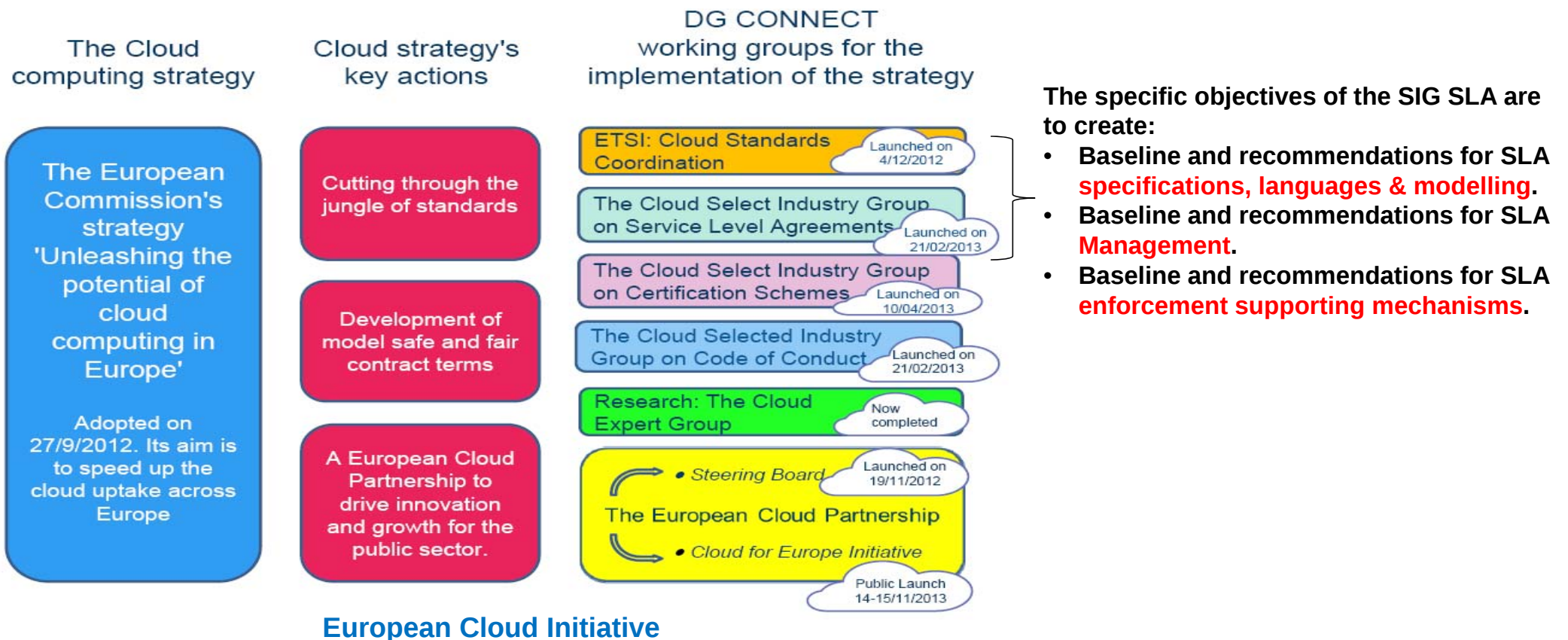
- Specifying **security parameters in Cloud Service Level Agreements (SLA)**.
 - A promising approach for cloud security assurance.
- SLA's in action:
 - ENISA
 - EU FP7 projects
 - Cloud Security Alliance
- **How to quantitatively reason about Cloud SLA's?**



CSPs specifying security in SLAs
(source: ENISA)

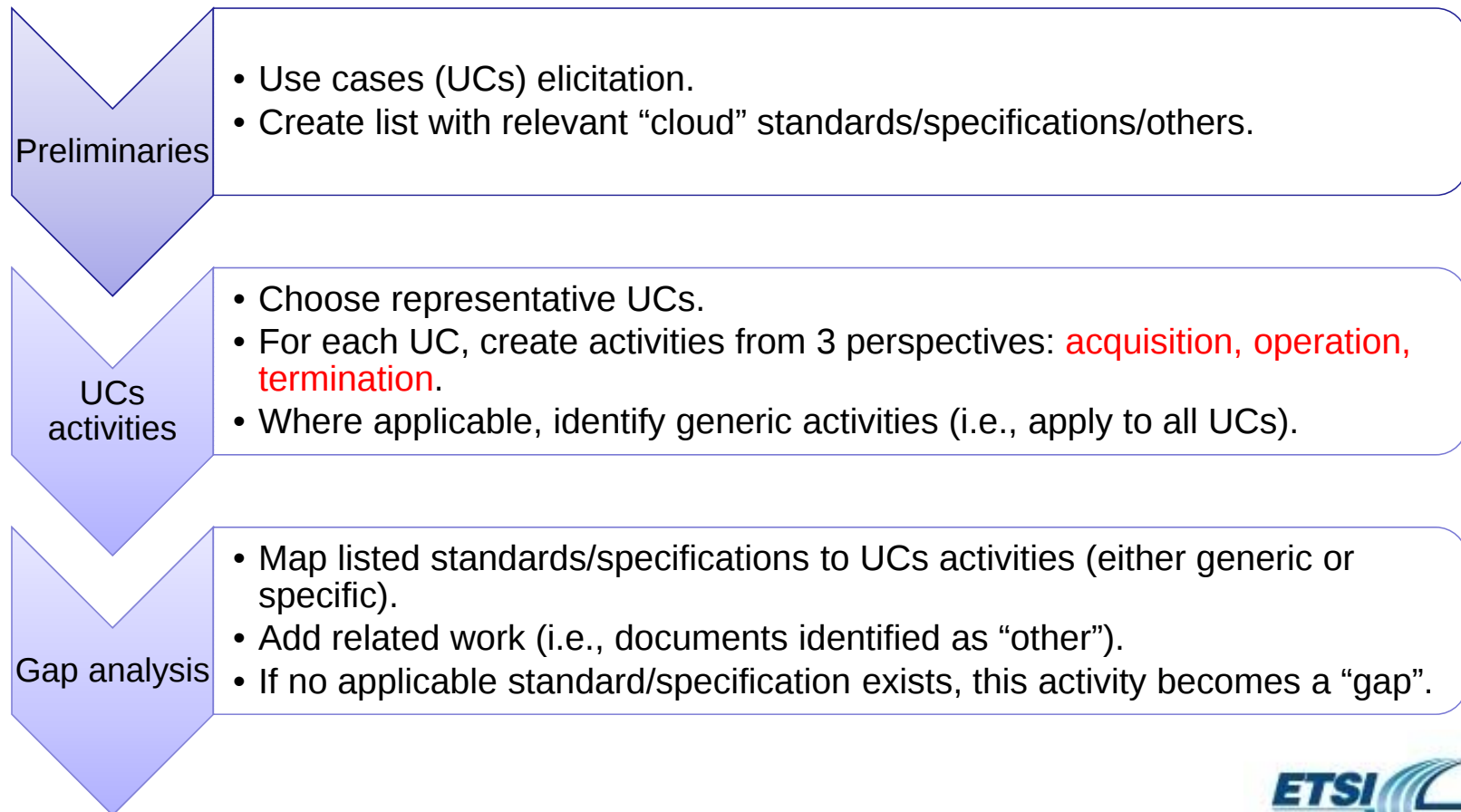
CHALLENGES

European Cloud Initiative



ETSI CSC: cloud standardization gaps

- Focus on **SLA, SEC and IOP**.



ETSI CSC: lessons learned

- No jungle of standards, but jungle of forums:
 - Standards and specifications vs. “related works” (including scientific papers).
- Gap analysis:
 - Lack of standards vs. lack of **cloud** standards.
 - Do identified standards **really** fill the gap?

ETSI CSC: lessons learned

- Gap on SLA models that support common **metrics** and **vocabularies**.
- (Semi-)Automated SLA management:
 - **Reality or fiction?**

Public review of CSC report started Nov-7th.

Standardization and certification

- EU project CIRRUS:
 - Brings together different stakeholders' views, including **research** community.
 - Surveys **emerging and future challenges** for “building the chain of trust”.

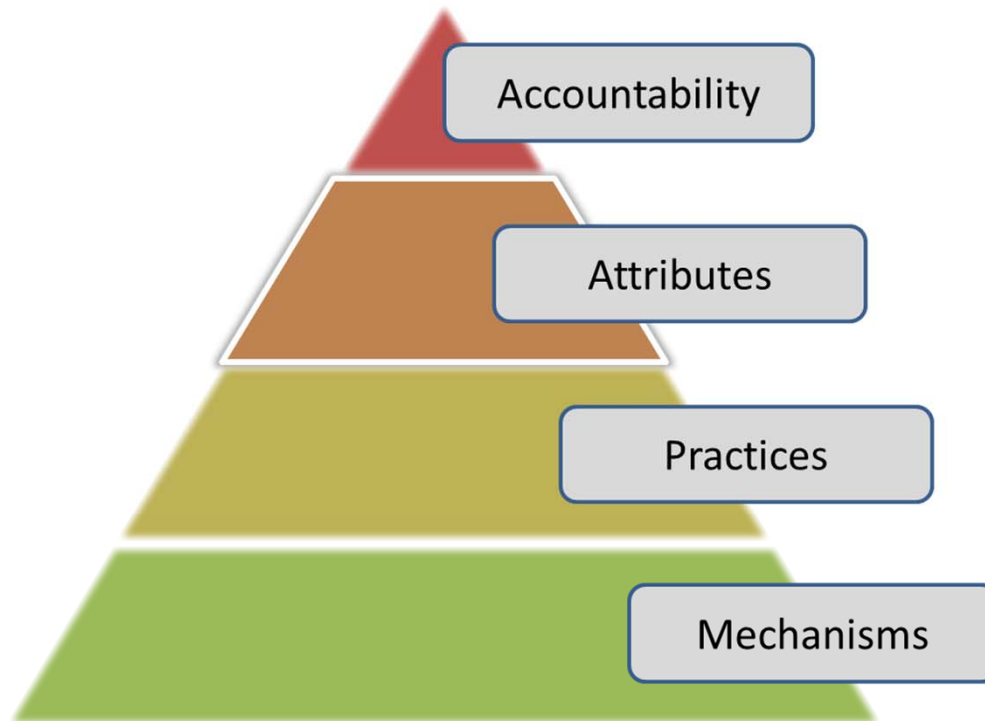
- Identified Cloud SLA challenges:



- SLA's Monitoring-as-a-Service.
- **Cloud federations and cloud brokers**, open new SLA-related challenges e.g., composition, is it time for an “SLA algebra”?
- **Security assurance!**

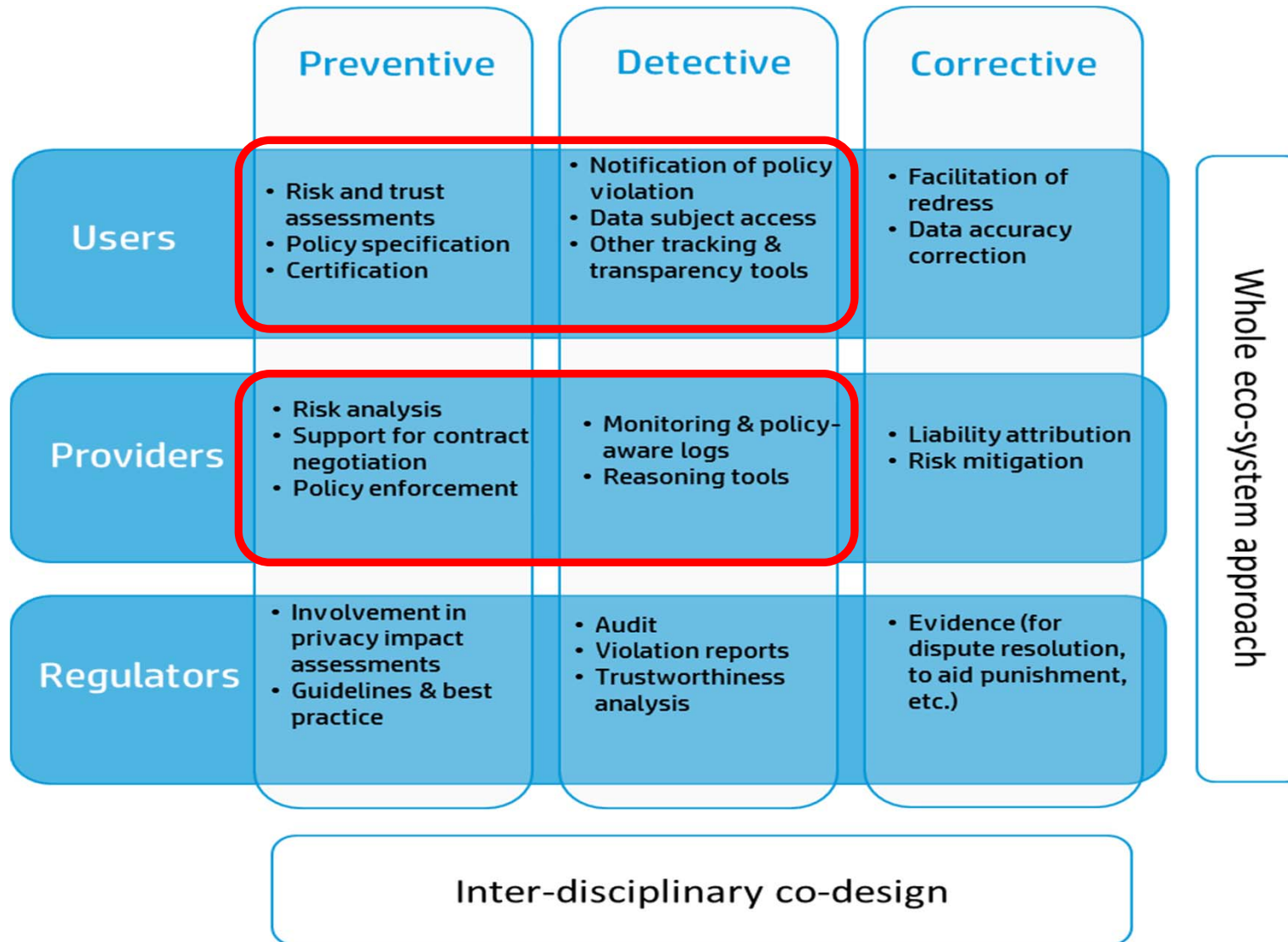
Cloud accountability

- Accountability-based approaches for trust and assurance – EU FP7 A4Cloud.



- Observability
- Verifiability
- Attributability
- Transparency
- Responsibility
- Liability
- Remediation

Conceptual accountability framework

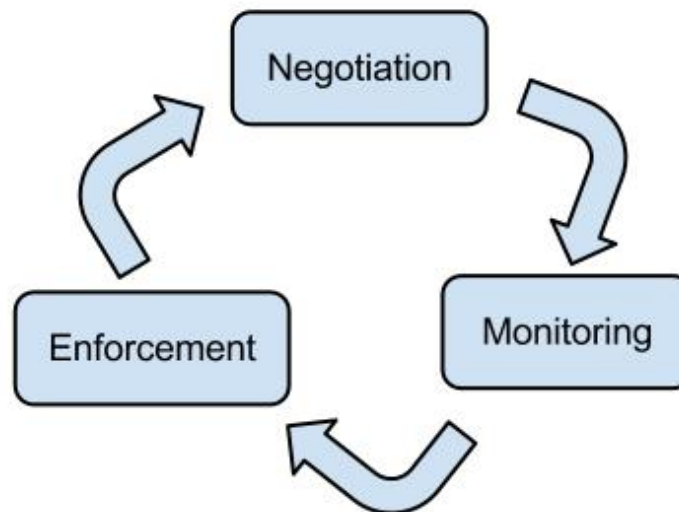


Can SLA's be used to manage accountability in the cloud?

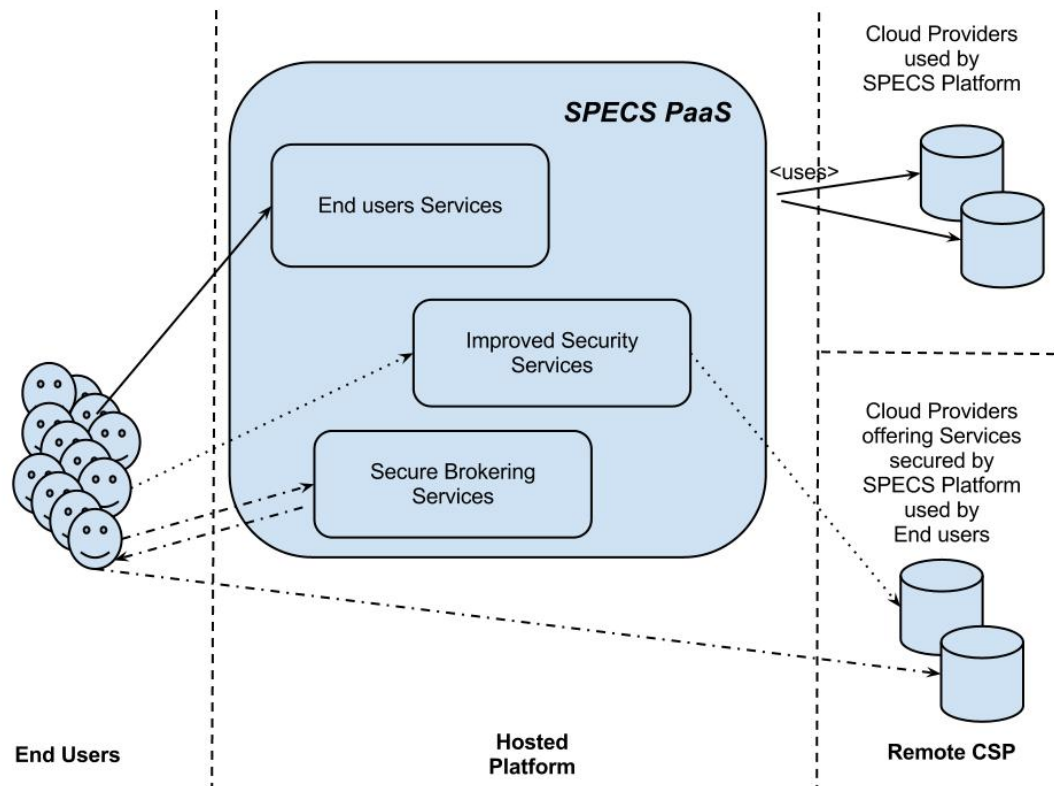
SLA management



- Create, promote and exploit an **open source** PaaS to **offer** and **manage** security features through SLAs.



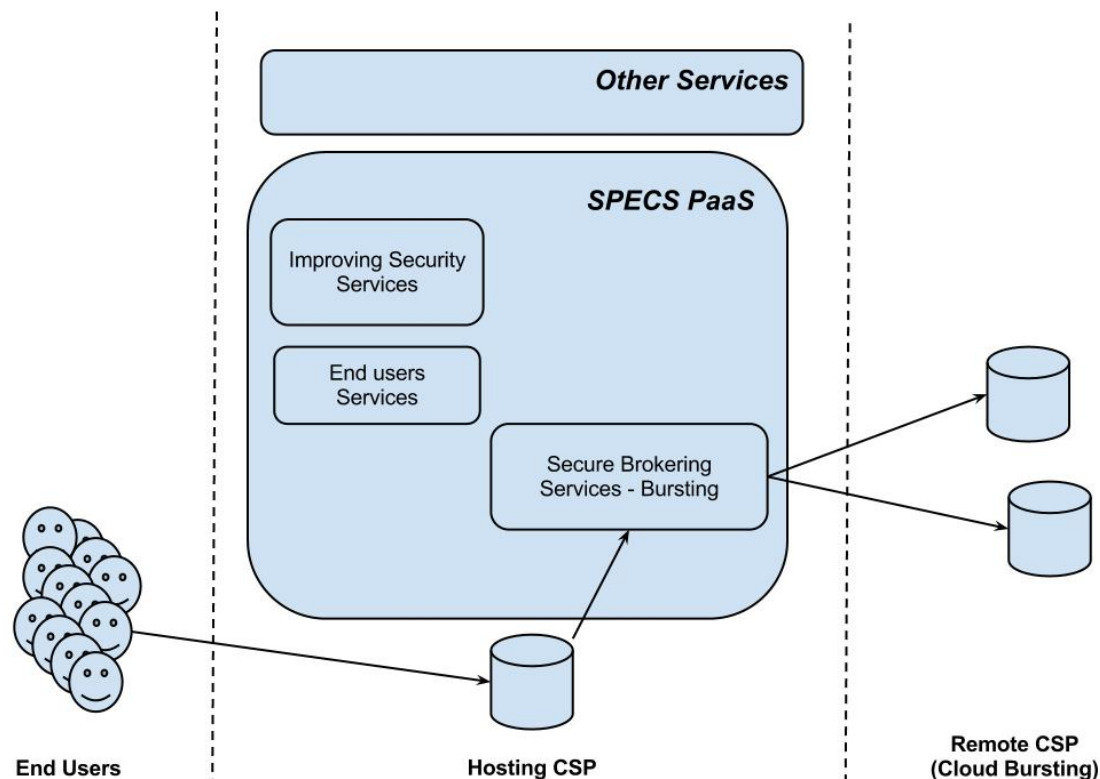
SPECS – PaaS model 1



- Use Case:

- ✓ **Added-value cloud broker**
- ✓ End-user negotiates security with broker
- ✓ Integrates required/new cloud security services into CSP
- ✓ **Continuous SLA monitoring** to offer best available CSP

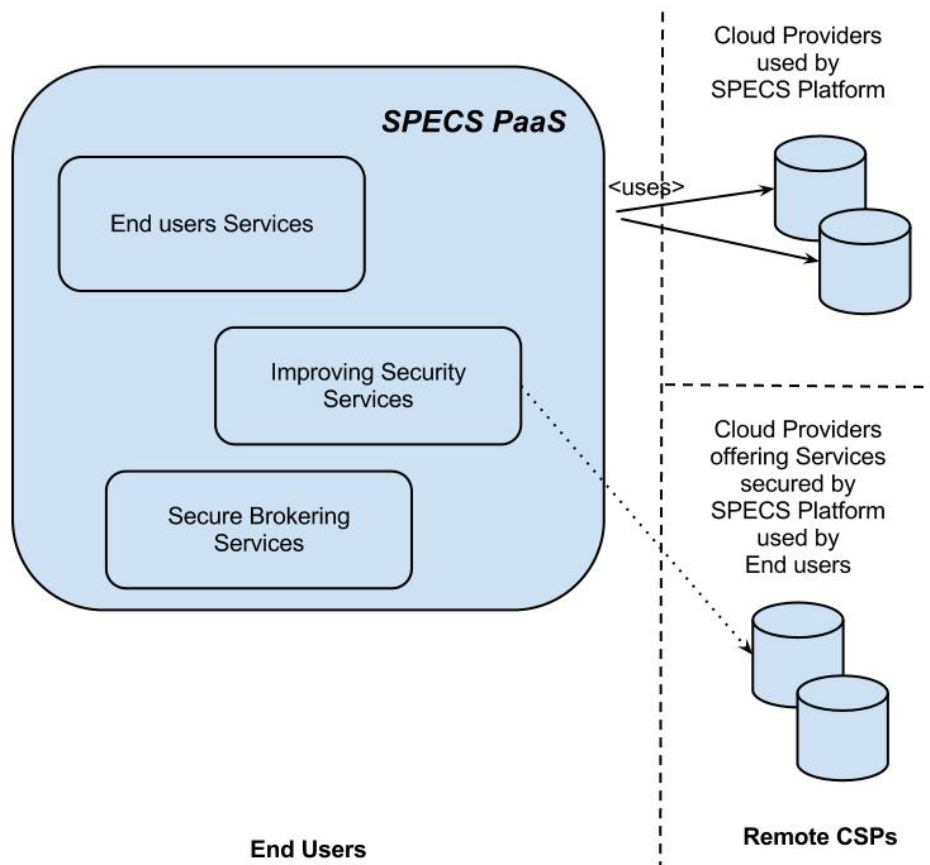
SPECS – PaaS model 2



- Use Case:

- ✓ CSP-managed
- ✓ **Flexible SLAs** offered to the end user
- ✓ Security is **adapted** to end user requirements
- ✓ SLA constantly monitored to react against e.g., cyber incidents

SPECS – PaaS model 3



- Use Case:

- ✓ **User-managed** (possibly a community cloud)
- ✓ User's services benefit from PaaS security services
- ✓ User dashboard to monitor **achieved security levels**

Open Challenges

- SLA (security) Negotiation:
 - Security Aggregation = QoSec (cf., CCSW'12 paper)
 - Quantitative vs. Qualitative vs. Probabilistic security metrics
 - User-centric, trade-offs evaluation
- Continuous SLA Monitoring:
 - Once again, security assurance.
 - Don't reinvent the wheel e.g., extend Cloud Trust Protocol
 - Critical factors: performance, intrusiveness, ...

Open Challenges

- **Automated** SLA enforcement:
 - Guarantee a negotiated SLA/sustained QoSec
 - SLA-based incident management.
- Real-world **validation!**

Final remarks

- **Standardization** (SLAs, vocabularies, metrics).
- **Composition** in the cloud of public services:
 - Cloud brokers everywhere
 - (Secure) SLA composition

Final remarks

- Bridging the (cloud security) gap between **academic and industrial research**
- Hopefully you'll leave with new ideas for CCSW'14