Making SLA's Useful for Security

TECHNISCHE UNIVERSITÄT DARMSTADT

Neeraj Suri

www.deeds.informatik.tu-darmstadt.de

DEEDS Group

Service Level Agreement (SLA)

- "*Contract*" which describes the *Service*, the associated *quality* levels and specifies the *responsibilities* (typically 'soft' formal obligations!) of both the Provider and the Customer. Effectively granted as *QoS*!

Choosing a Cloud Service Provider (CSP)

TECHNISCHE UNIVERSITÄT DARMSTADT

Services (behind the SLA's)

- **Functionality**
- **Performance**
- **Price**
- **Reputation**

❖ **Security?**
From SLA's to SecLA's (Security-LA's)?

DEEDS Group

State of the Art & Practice?

TECHNISCHE UNIVERSITÄT DARMSTADT

- CSPs specifying "*security levels*" associated with their services?
  Very uncommon!

- Semantic mismatch across users (typically non-security expert with informal high level requirements) and CSP (vendor specific specs)?
  Very common!

SecLA's to specify, compare & deliver user-centric security?

DEEDS Group

Key Elements Driving (Useful) SecLA's

TECHNISCHE UNIVERSITÄT DARMSTADT

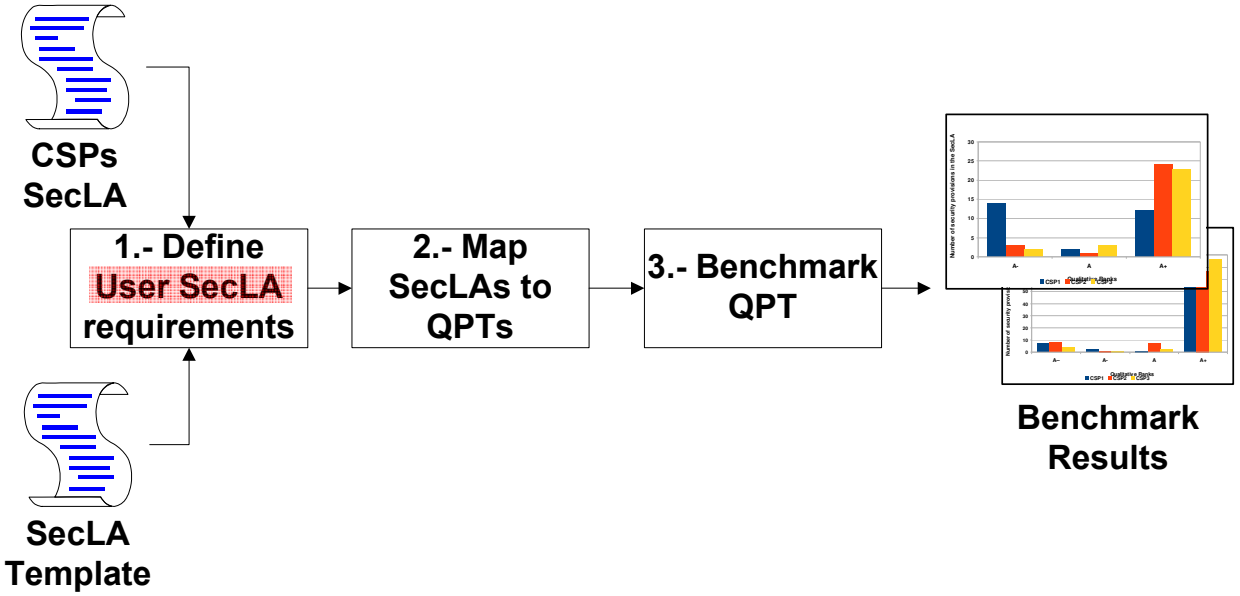
1. **Semantic Brokerage** across User & CSP's SecLA's
2. **Integrated Qualitative and <u>Quantitative</u>** SecLA's
3. **Negotiation** (& Enforcement) via quantitative SecLA's

DEEDS Group

Quantitative Benchmarking [CCSW '12, Secrypt '12]

TECHNISCHE UNIVERSITÄT DARMSTADT

- Quantifying and ranking a Cloud SecLA's security level
  - INPUT: SecLA Template (e.g., from CSA CAIQ, ISO 27001, PCI …)
  - DERIVED INPUT: CSP SecLAs (based on the SecLA Template)
  - DERIVED INPUT: User SecLA

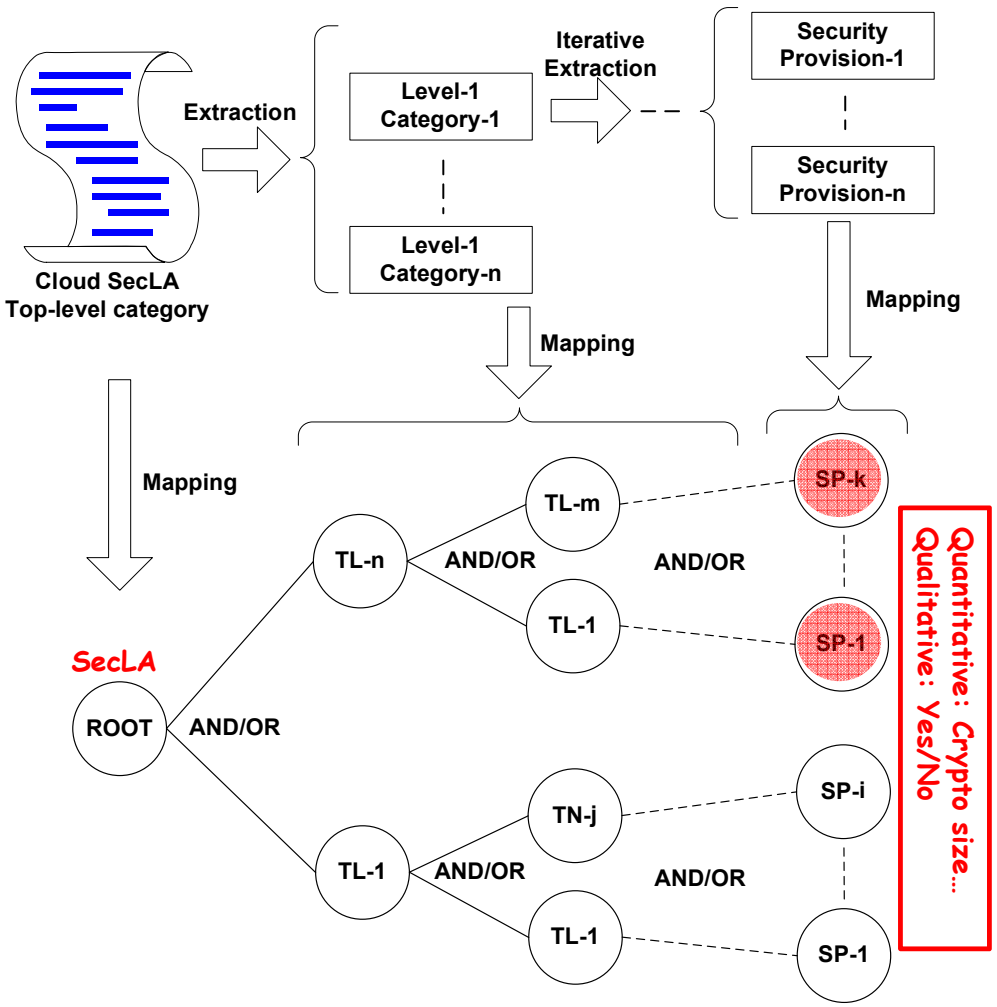


DEEDS Group

Quantitative Benchmarking Methodology

- Mapping SecLAs to Quantitative Policy Trees(QPT)
  - Simple AND/OR or complex (utilizing Cloud SecLA's inherent hierarchical structure)
  - Aggregation + Decomposition!
  - User defined weightings at leaves

➢ Output: 1 User QPT per SecLA

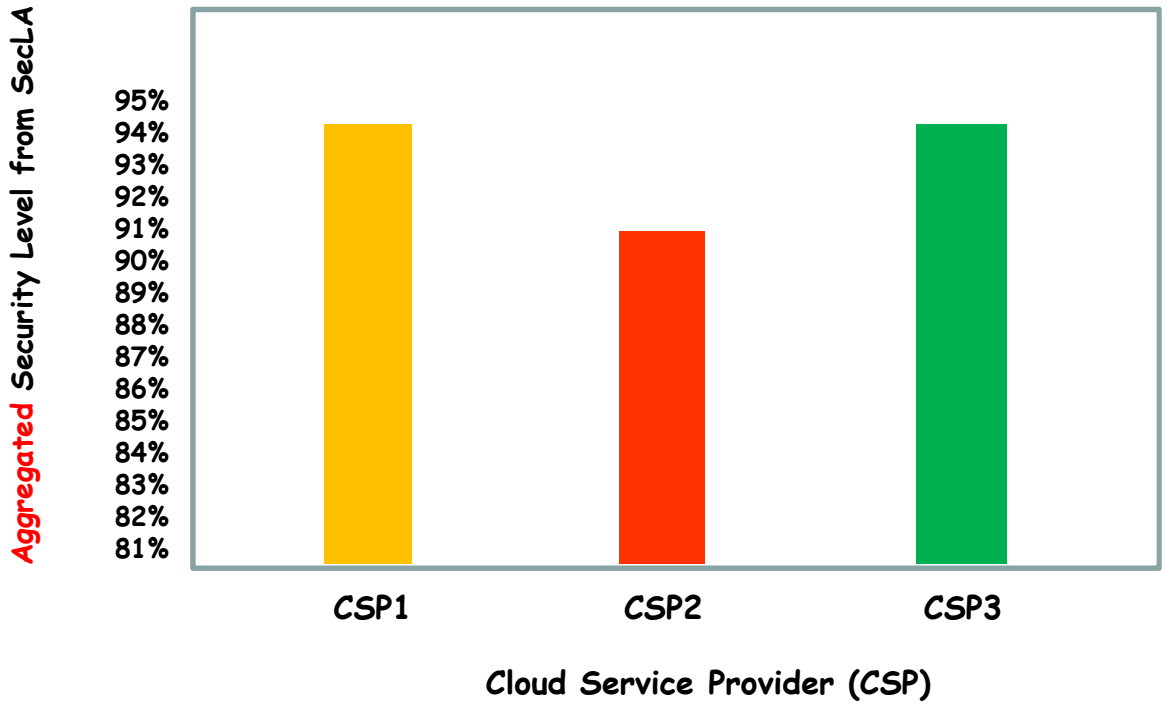


Example Validation: CSP's Match to User's SecLA

TECHNISCHE UNIVERSITÄT DARMSTADT

- **CSP3 ≈ CSP1 > CSP2** … CSA STAR – CCSW'12

  [14 CSP's, 171 Qualitative and 29 Quantitative Security Provisions]



CSP's over/under-provisioning wrt a User's SecLA

	CSP1	CSP2	CSP3
SecLA	0.94	0.91	0.94
CO	0.67	0.92	0.89
DG	0.98	0.97	0.97
FS	1.00	0.91	1.00
HR	1.00	1.00	1.00
IS	0.91	0.88	0.94
LG	1.00	1.00	1.00
OP	1.00	0.91	0.81
RI	0.93	1.00	0.97
RM	1.00	0.70	1.00
RS	0.91	0.96	0.82
SA	0.97	0.79	0.90

DEEDS Group

Quantification as the Basis for SecLA Monitoring, Negotiation and Enforcement

TECHNISCHE UNIVERSITÄT DARMSTADT

The SPECS Project: ***Secure Provisioning of Cloud Services Based on SLA Management***

1. Establishing security trades-offs across CSPs: SecLA negotiation
2. Processes for monitoring and enforcing security levels with CSP's
   ➔ Resource provisioning to maintain SecLA

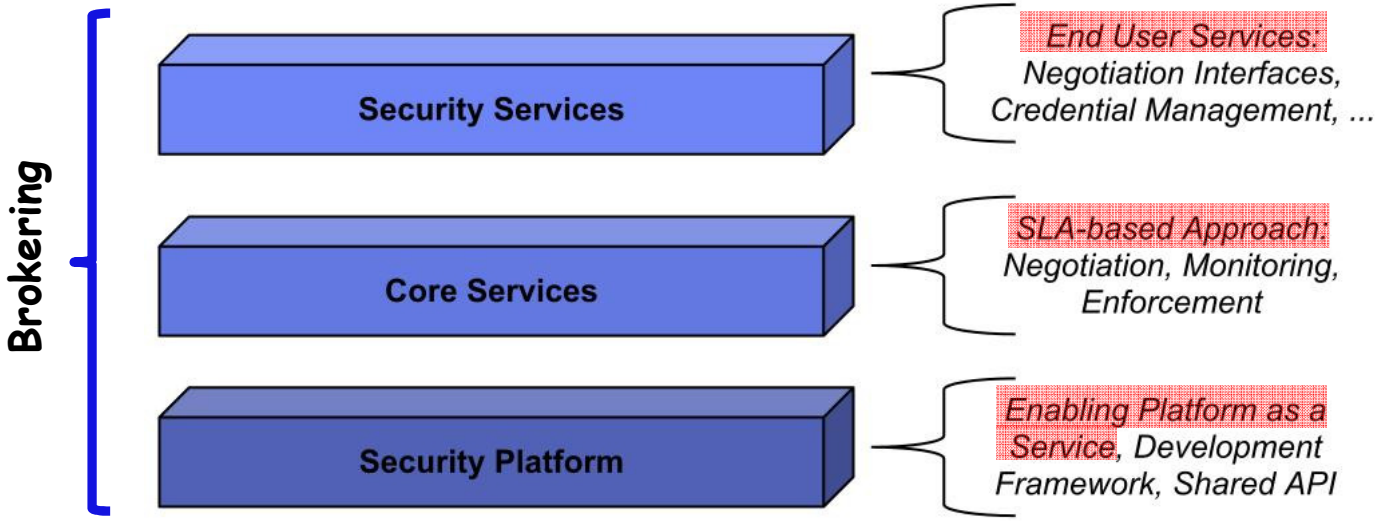
DEEDS Group

The SPECS Stack: Platform-as-a-Service

TECHNISCHE UNIVERSITÄT DARMSTADT

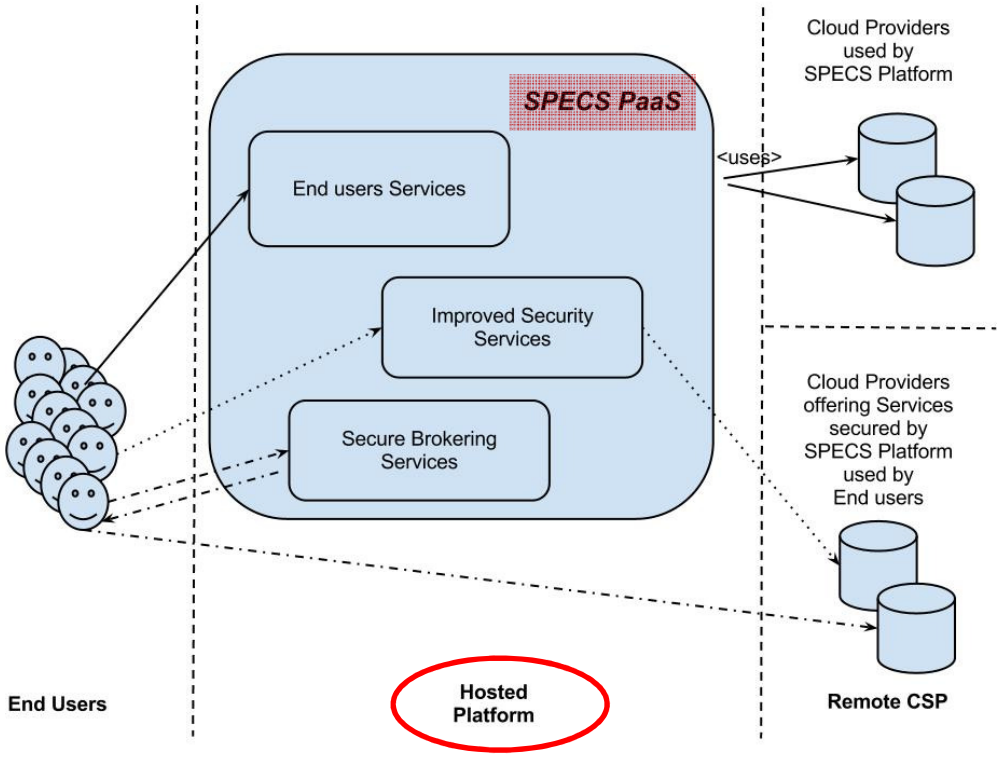
Negotiation ←→ Monitoring & Enforcement to ensure QoSec

- User-centric Cloud SecLA specification of security parameters
- Trade-offs related with offered security in Cloud SecLA
- Reactive mechanisms (re-negotiation, economic & resource provisioning) to maintain desired *Quality of Security!*



DEEDS Group

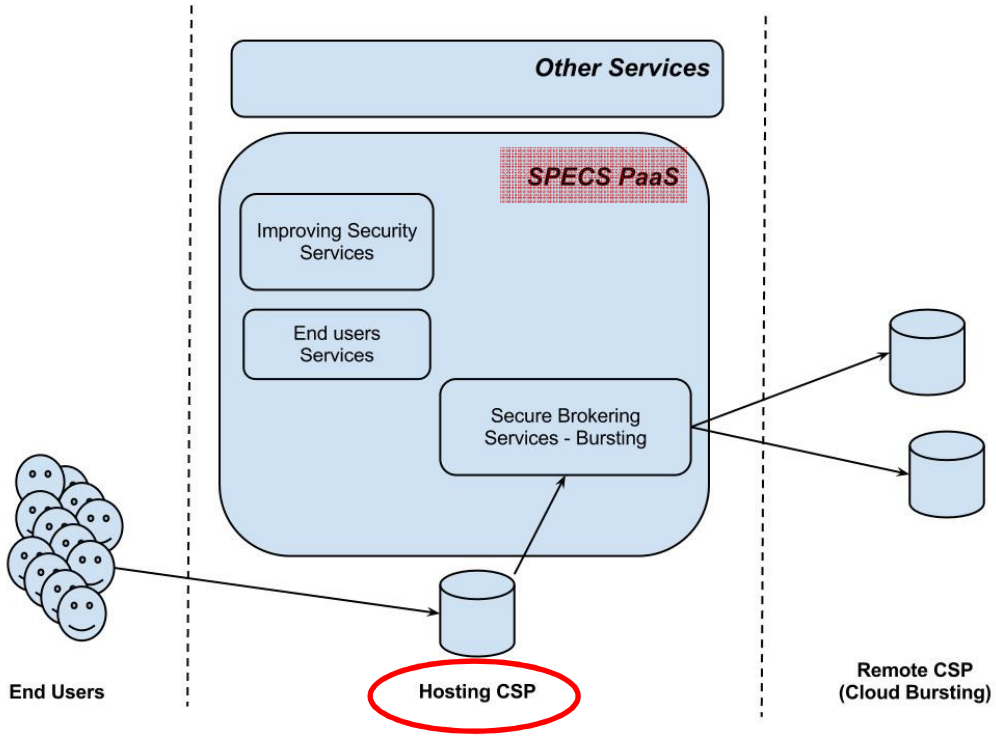
SPECS PaaS Interface/Interaction Model 1



Hosted platform buys/brokers resources from the Cloud

- Discrete SPECS Platform
  - ✓ SPECS as Secure Broker: End-user negotiates security via SPECS broker
  - ✓ SPECS PaaS interfaces on security services with CSPs
  - ✓ Continuous SecLA monitoring to select best available CSP

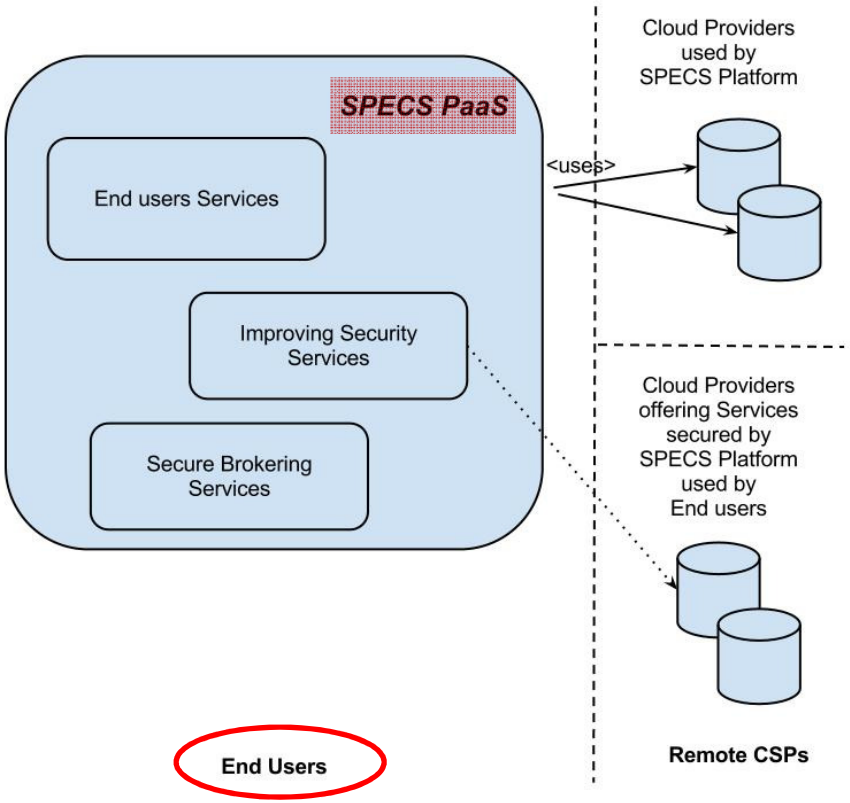
SPECS PaaS Interface/Interaction Model 2



Hosting CSP has own resources

- CSP Hosted Platform
  (Trust chain → trusting the provider!)
  - ✓ Security adapted to end-user requirements
  - ✓ SecLA monitoring to react on security incidents

SPECS PaaS Interface/Interaction Model 3

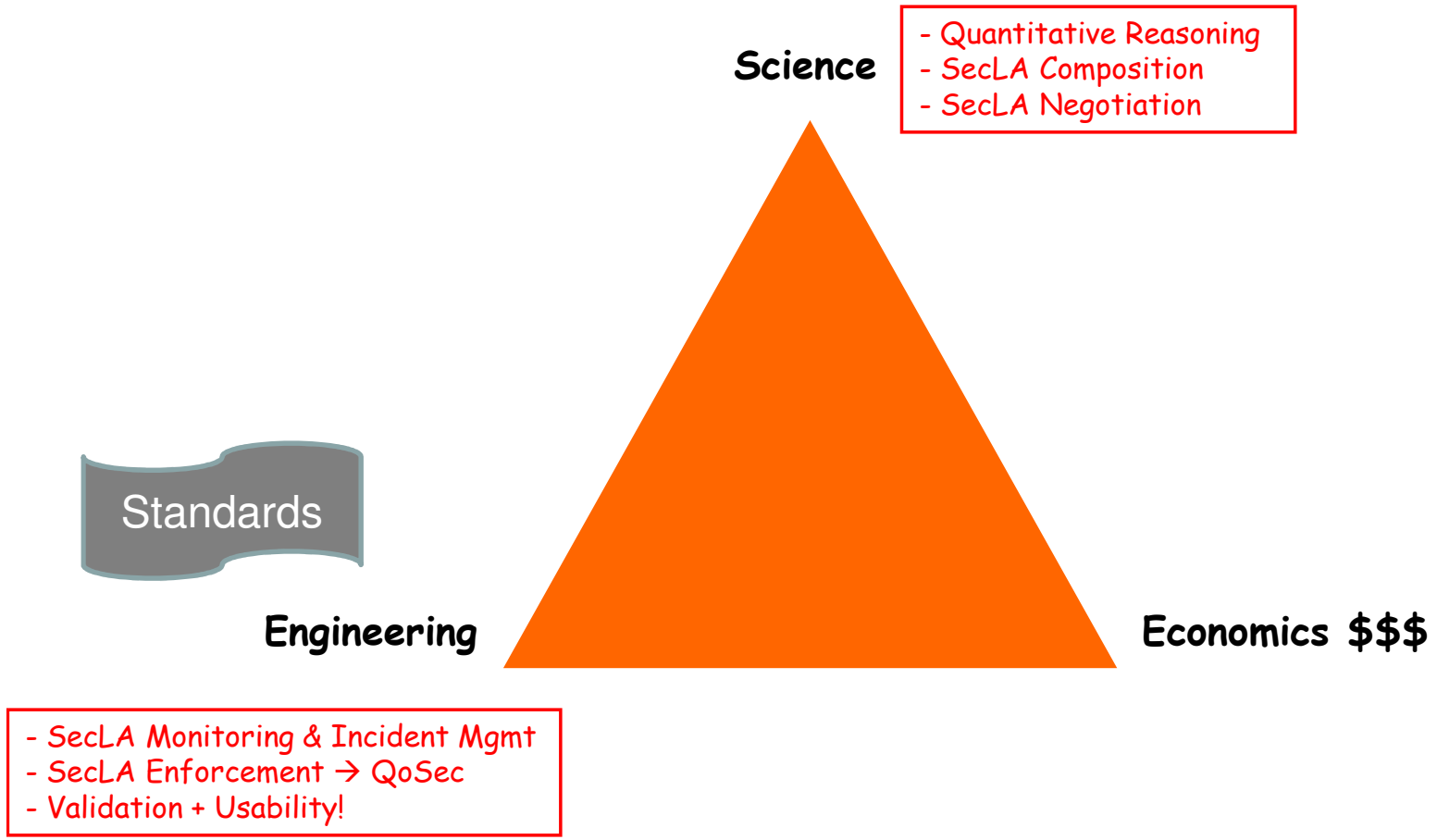


End user buys/brokers Cloud resources via SPECS

- User Managed Cloud
  (User hosts the PaaS platform)
  - ✓ User benefits from SPECS PaaS brokering & secure invocation services
  - ✓ Dashboard to monitor achieved security levels

SPECS SecSLA: Started Nov 1 …Stay Tuned!

TECHNISCHE UNIVERSITÄT DARMSTADT



DEEDS Group