Security Service Level Agreements in the Cloud: The SPECS Framework

Prof. Massimiliano Rak - CeRICT

SPECS Project

Secure Provisioning of Cloud Services based on SLA Management

Outline

- Introduction
  - Project
  - Challenges
  - Security SLAs
  - Mission
- SPECS
  - Models
  - Process
  - Framework
- Results
  - Security SLA
  - Security Metric Catalogue
  - Framework
  - Solution Portfolio
- Demo

SPECS Project

CeRICT, Italy (coordinator)

TUD, Germany

IeAT, Romania

CSA, United Kingdom

XLAB, Slovenia

EISI, Ireland

FP7-ICT-10-610795

Project Start: 1/11/2013
Project Type: STREP
Duration: 30M
Total Funding: 3.5 M
EU Contribution: 2.4 M

Cloud Security Challenges

- **CSP Security Assessment**
  - I made a risk assessment; does my CSP offer all the controls I need to meet my security requirement?
- **Comparison of security offered by CSPs**
  - Many CSPs offer the same functionalities at different costs, how the security changes from one to another?
- **Monitoring CSP Security**
  - My CSP granted me it is applying a lot of security controls, how can I verify it is true? If a security breach happens, how can I be aware of it?
- **Data Protection**
  - Do I respect all data protection regulation? Is my privacy respected?

Security Service level Agreements

Security SLAs are contracts among CSP and CSCs regulating the security level granted over provisioned services

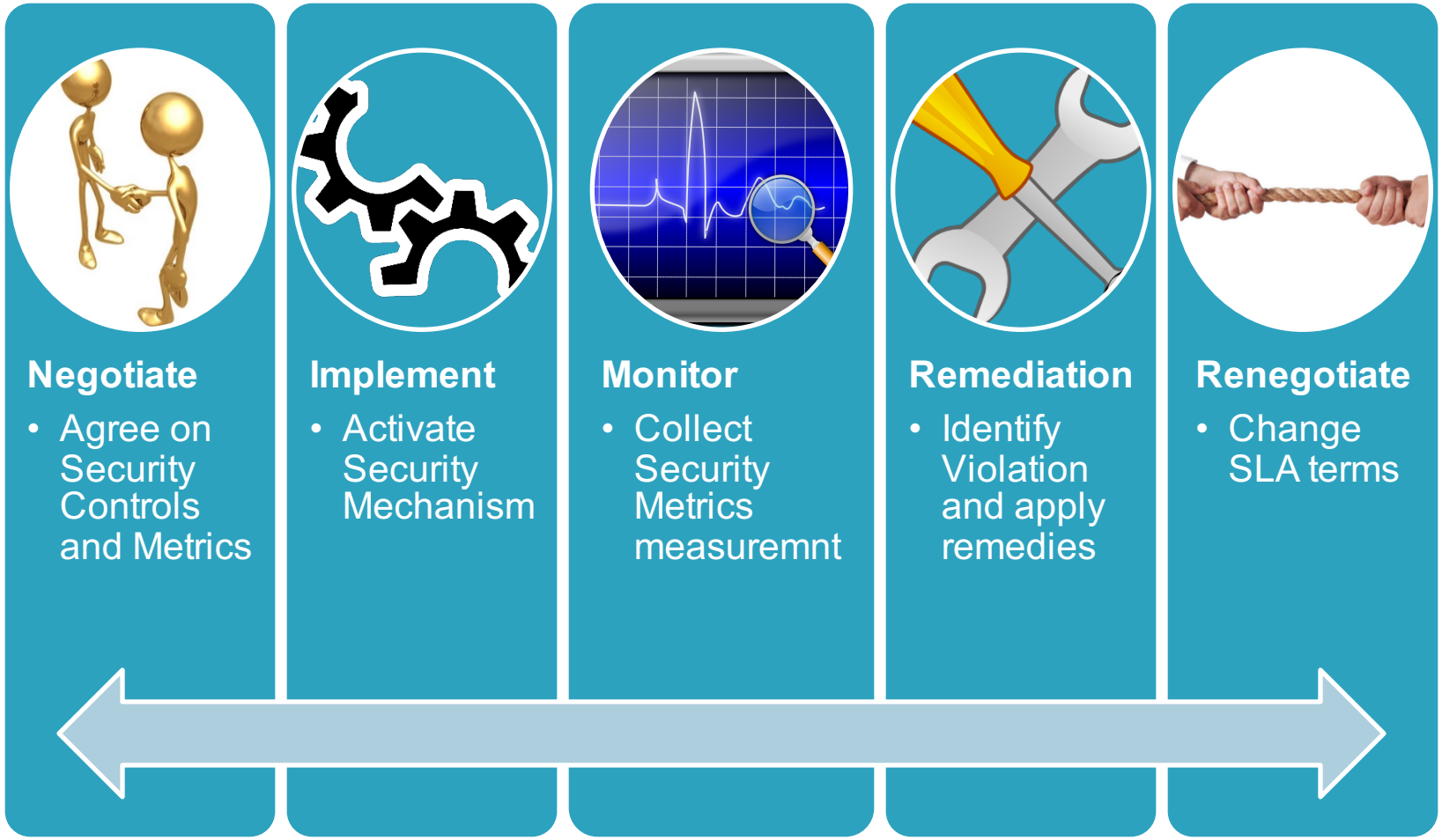
- Open Challenges:
  - identification and representation of security attributes
  - quantification of the security level
  - continuous monitoring of the fulfillment of the SLAs
  - automated enforcement

SPECS Mission

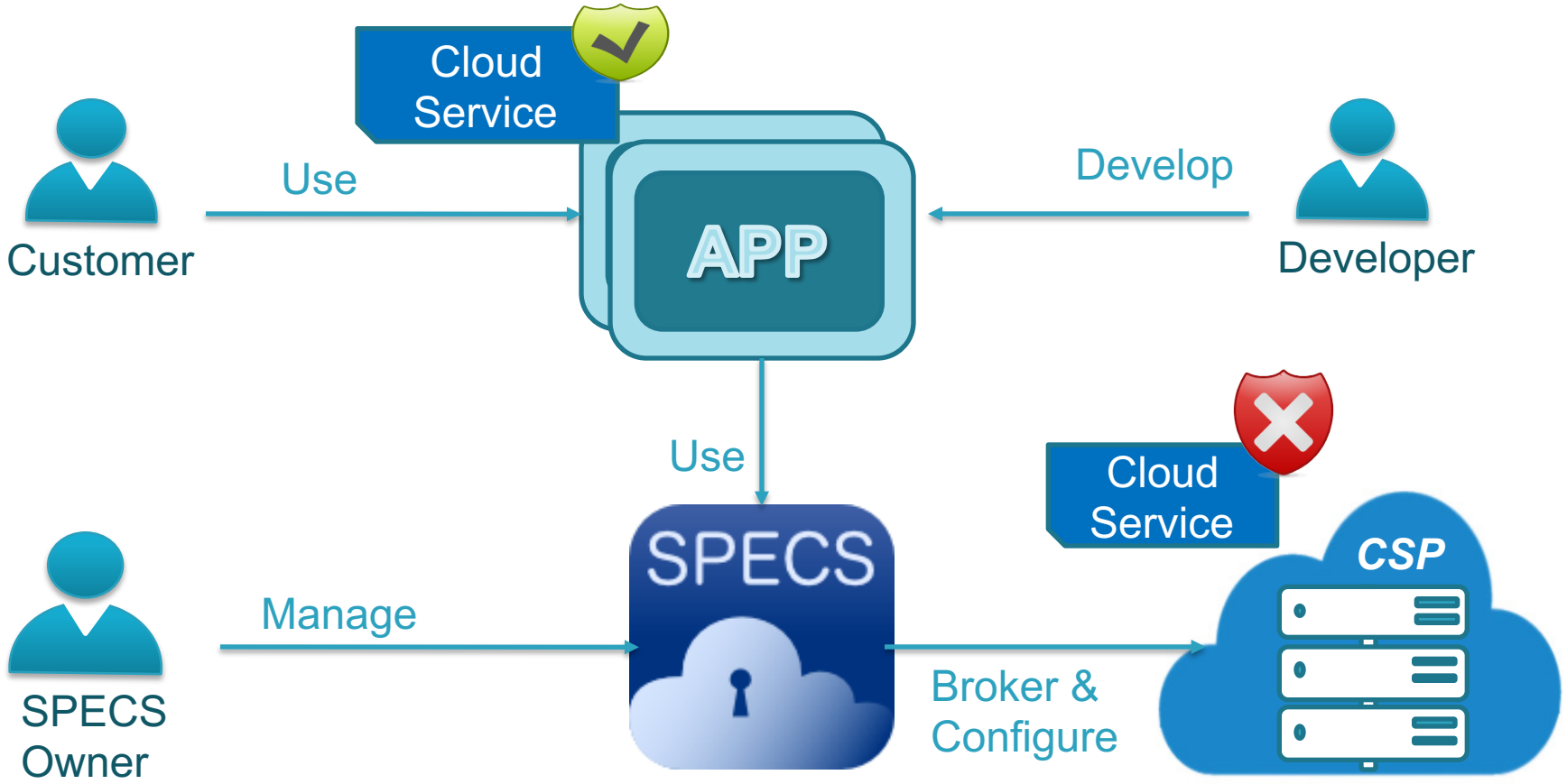
SPECS aims at using Security SLAs to:

- **negotiate Security** among CSC and CSP, enabling Customers to compare CSPs and CSPs to offer security addressing customer specific needs;
- **automatically enforce Security** on services delivered to CSCs according to their requirements.
- enable both CSCs and CSPs to **monitor security** levels and **react** when security is violated

SLA-based cloud Services



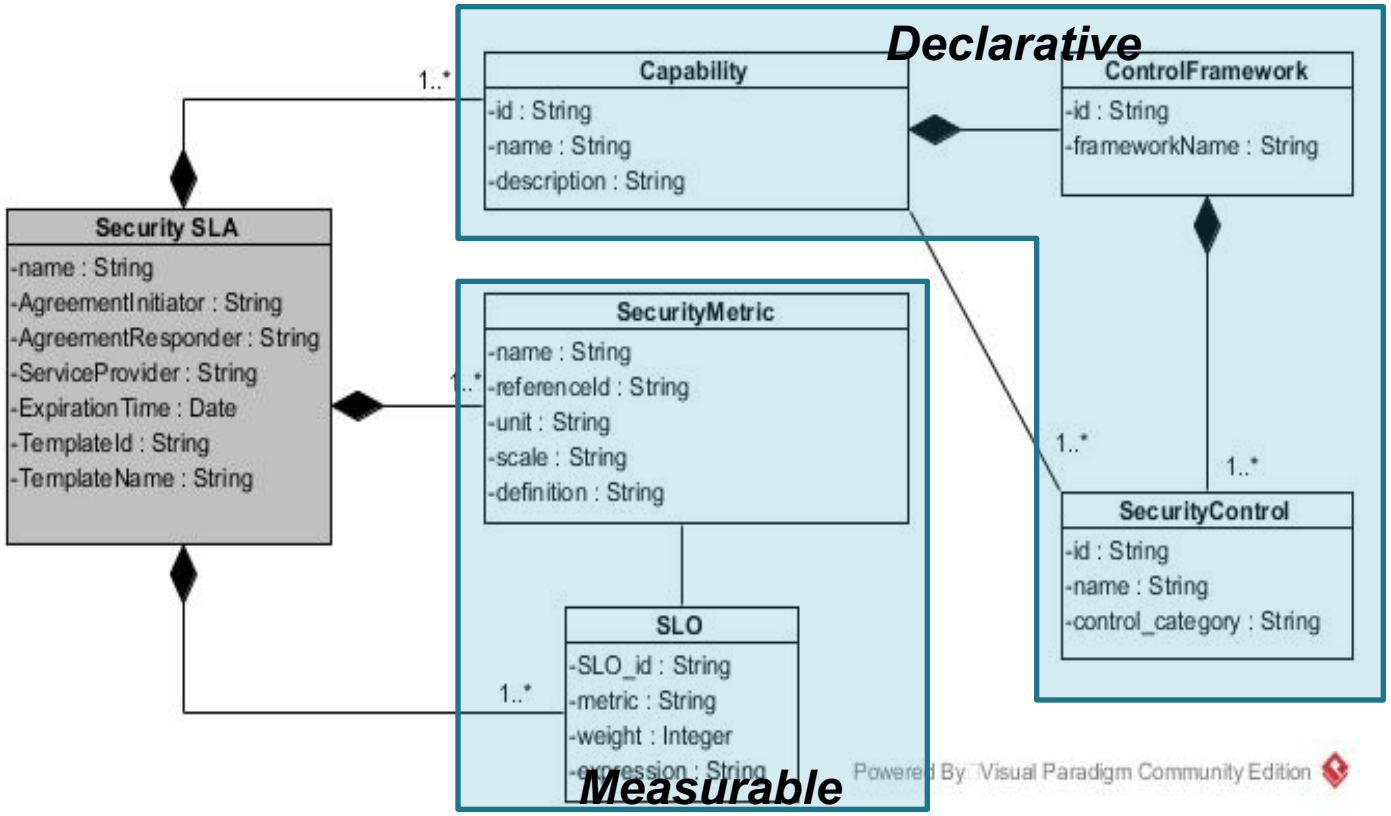
SPECS Model


Cloud Service
Use
Customer
APP
Develop
Developer
Use
Cloud Service
SPECS
CSP
Manage
SPECS Owner
Broker & Configure

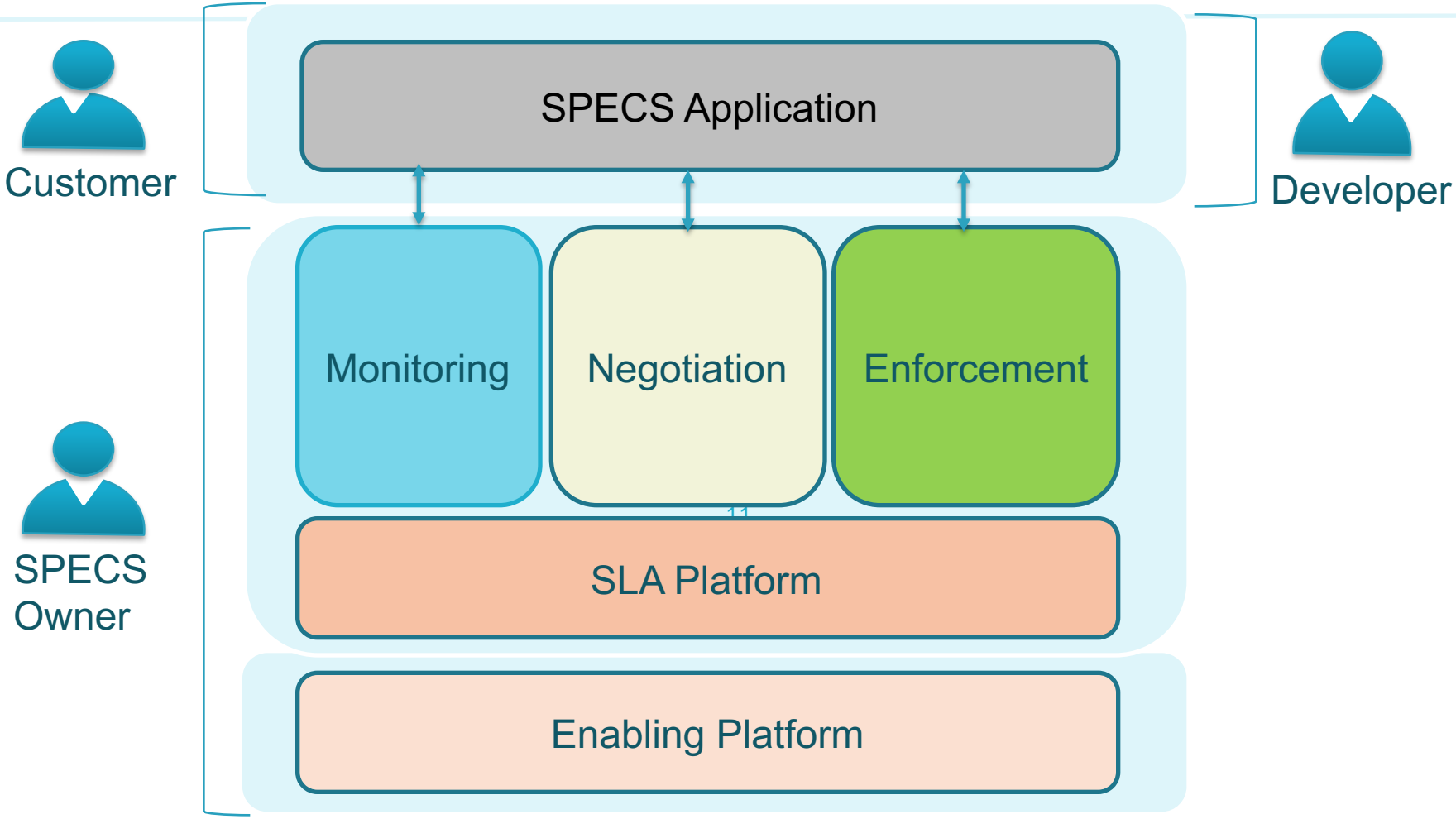
Results: Security SLA Model

- A **Security SLA model** and its **machine readable format** made according to state-of-the art standards (ISO 19086, WS-Agreement, …)
- Security SLA usable according to **standard risk modeling** processes
- Security SLA containing standard and **measurable security metrics** to offer grants (easy for Providers and verifiable by Customers)

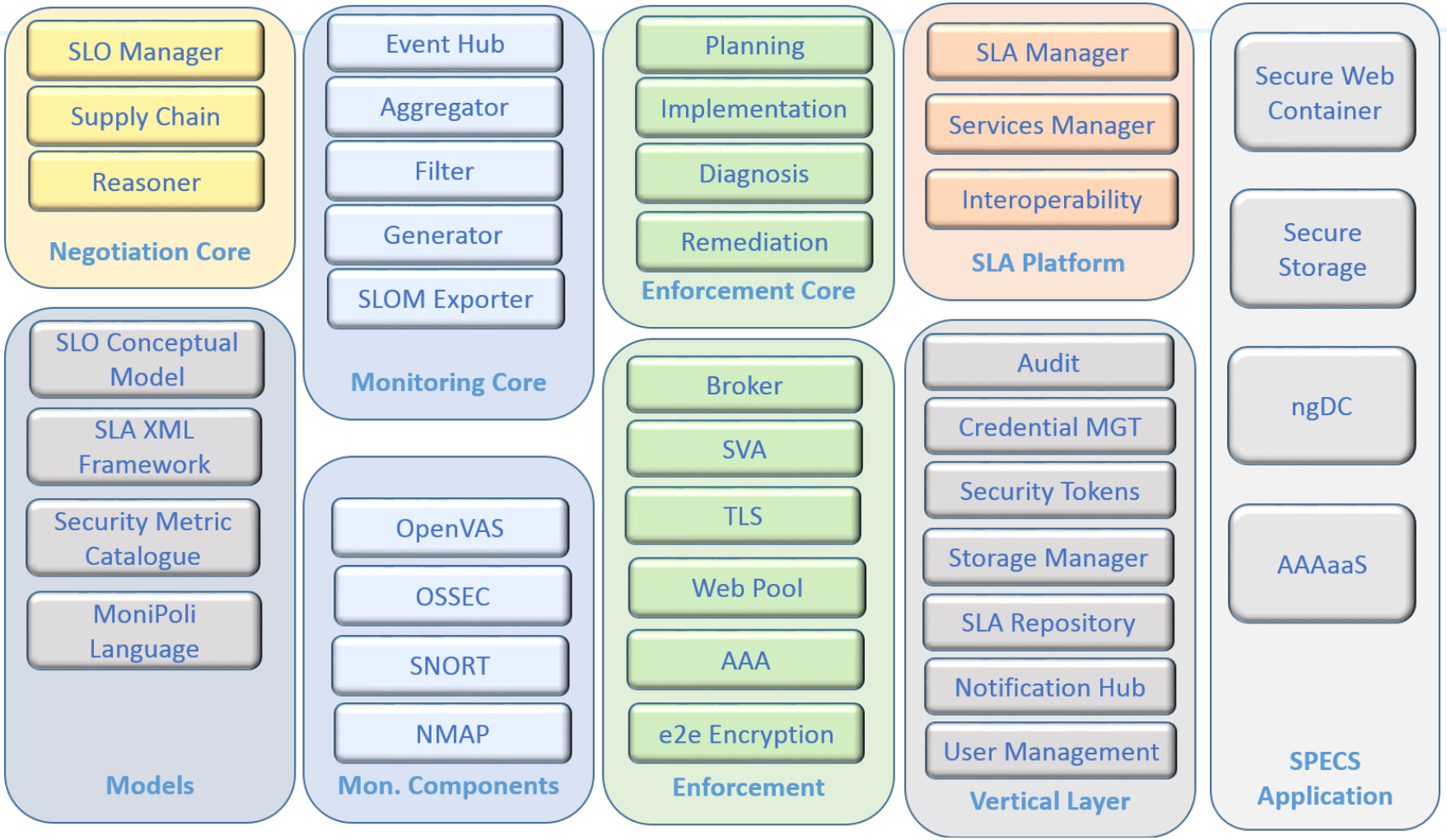
Security SLA Model



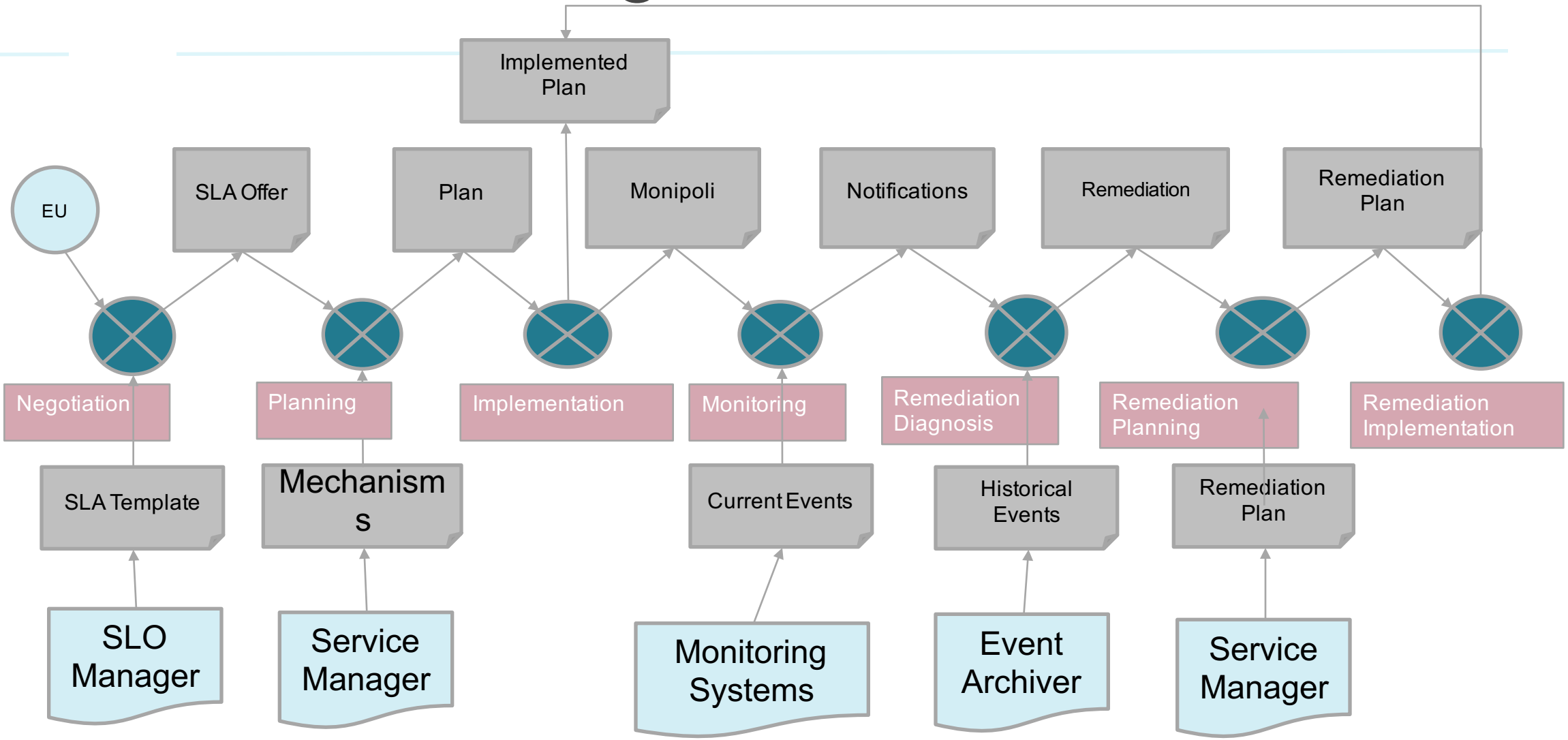
SPECS Framework



Results: SPECS Framework



SPECS SLA Management Process



Results: Security Metric Catalogue

- A Catalogue of security metrics represented according to the latest NIST/ISO standards
- More than 20 security metrics defined in SPECS
- More than 160 security metrics collected from other projects and standard bodies and represented according to SPECS model

Results: SPECS portfolio

- **Secure Web Container**
  - A PaaS offering Web servers preconfigured with TLS, protected against DoS and enriched with Software Vulnerability Assessment

- **STAR Watch**
  - Evaluate and compare CSPs using CSA STAR Repository

- **E2EE**
  - A Storage Service protected with E2E Encryption

- **ViPR+SPECS**
  - A CSP datacenter offering Security SLA on top of EMC ViPR solution

SPECS impact goals

- Support Private and Public Cloud Providers to enhance the security of their service under a signed Security SLA
- Support small Private Cloud Providers (the majority in Europe) to offer more security, and negotiable with customers (more flexibility then big CSP)
- Improve customers' trust in the Cloud

Questions?

References:

SPECS: www.specs-project.eu

Security SLA in WS-Agreement