Usage Control in CONTRAIL Cloud

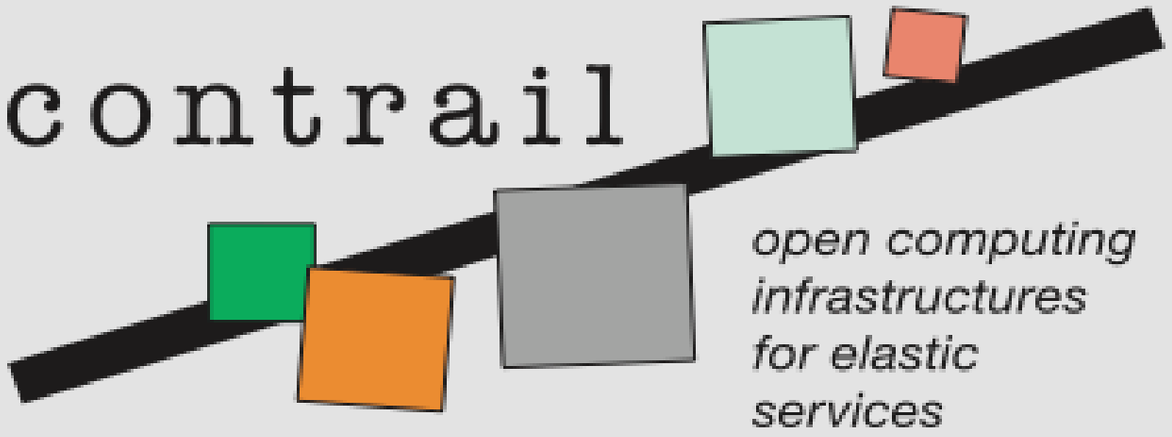
POFI 2011
Pisa, 9 June 2011

Paolo Mori
IIT - CNR

Agenda

- CONTRAIL project
- Usage Control Model
- Security Policy Language
- Usage Control System Architecture

CONTRAIL Project



contrail is co-funded by the EC 7th Framework Programme

Funded under: FP7 (Seventh Framework Programme)

Area: Internet of Services, Software & virtualization (ICT-2009.1.2)

Project reference: 257438

Total cost: 11,29 million euro

EU contribution: 8,3 million euro

Execution: From 2010-10-01 till 2013-09-30

Duration: 36 months

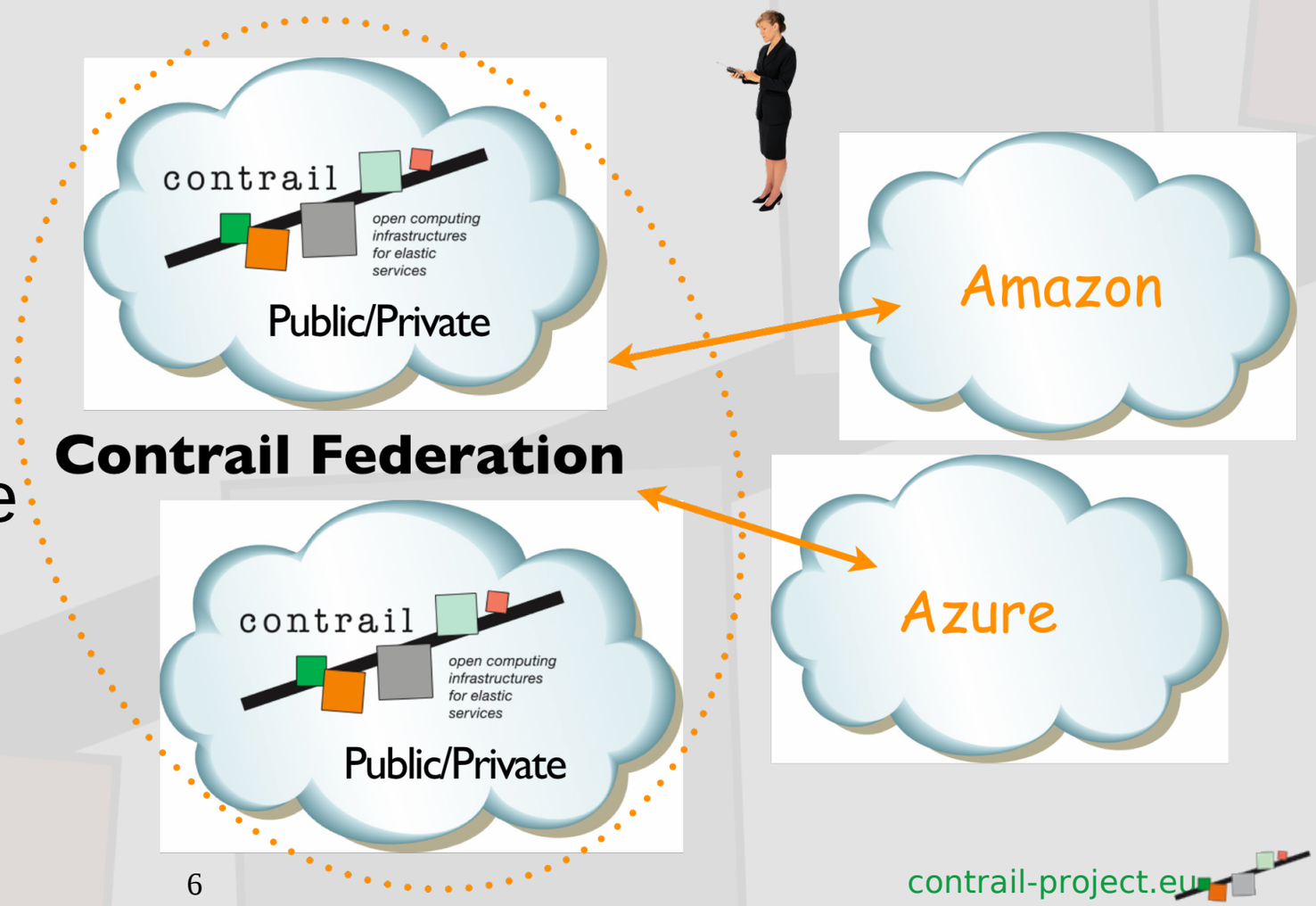
Contract type: Collaborative project (generic)

Objectives

- Design, implement, validate and promote an open source software stack for Cloud federations
- Develop a comprehensive Cloud platform integrating a full IaaS and PaaS offer
- Allow Cloud providers to seamlessly integrate resources from other Clouds with their infrastructure
- Provide trusted Clouds by advanced SLA management
- Break the current customer lock-in situation by allowing live application migration from one cloud to another

CONTRAIL Federation

- A CONTRAIL federation integrates in a common platform multiple Clouds, both public and private
- Coordinates SLA management provided by single Cloud providers
- Does not disrupt providers' business model
- Allows to exploit the federation as a single Cloud



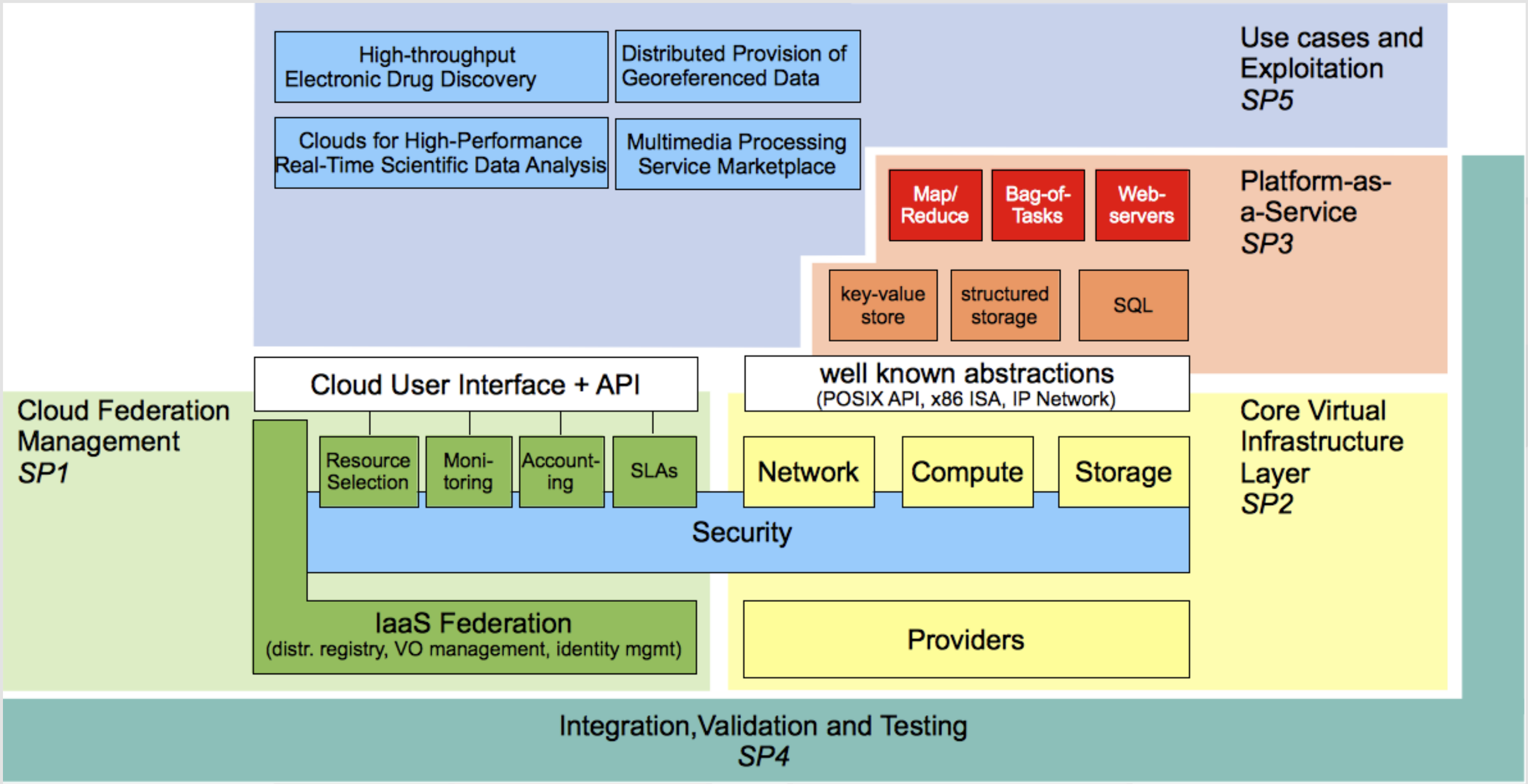
Expected Outputs

- A collection of infrastructure services
  - Virtual Infrastructure Networks
  - Virtual Cluster Platform
  - Globally Distributed File System
- Services to federate IaaS Clouds
  - Identity Management
  - Management of federation policies
  - SLA management
  - Autonomic resource management
- A collection of PaaS services to support Cloud applications
  - High throughput elastic structured storage
  - Automatic set-up and configuration of SQL servers
  - Geographically distributed key/value store

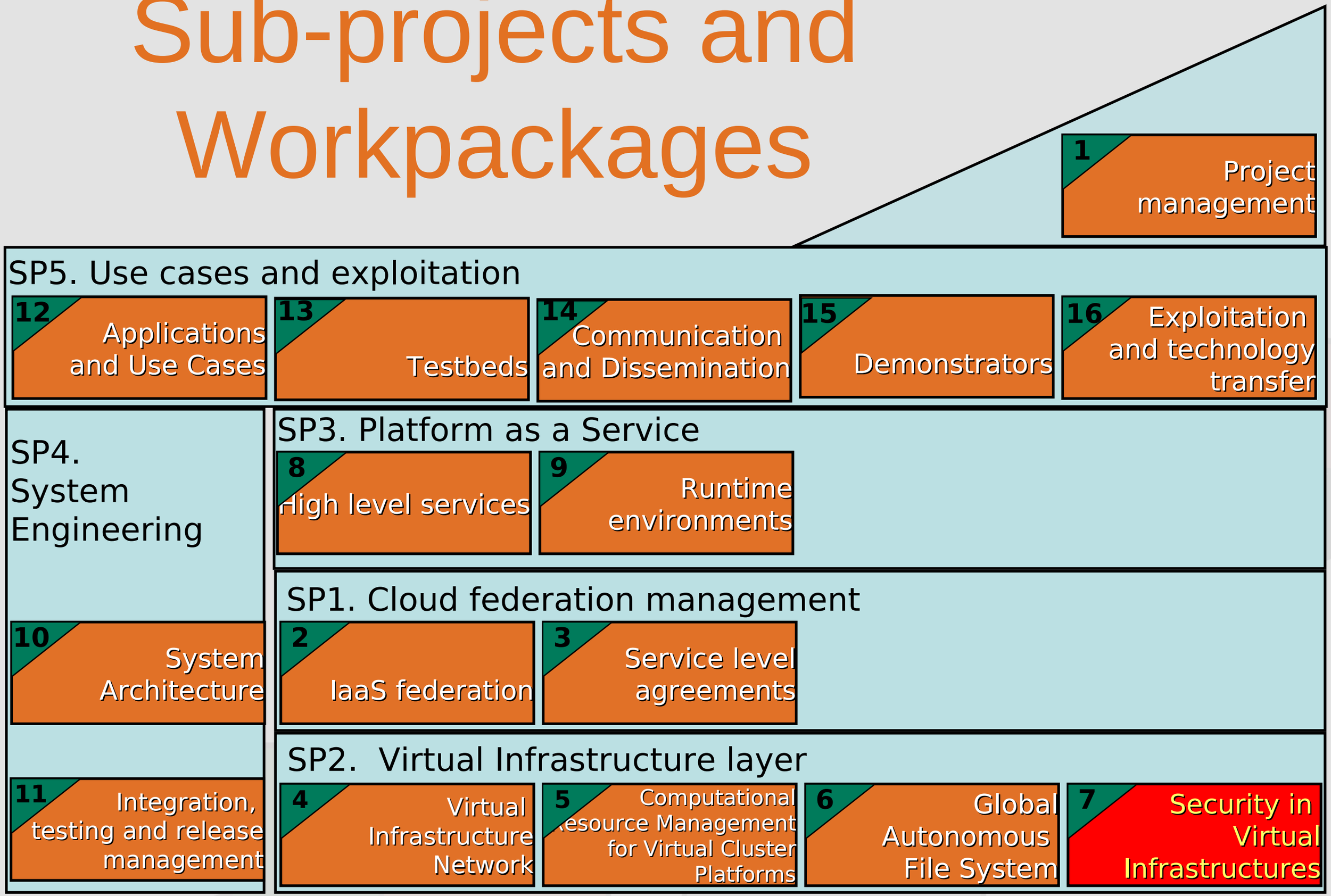
Expected Outputs (II)

- A collection of run-time environments
  - An efficient map-reduce implementation
  - Scalable hosting for service oriented applications
  - Autonomic workflow execution
- A collection of applications
  - Distributed Provisioning of Geo-referentiated Data
  - Multimedia Processing Service MarketPlace
  - Real-Time Scientific Data Analysis
  - Electronic Drug Discovery

CONTRAIL in a Nutshell



Sub-projects and Workpackages



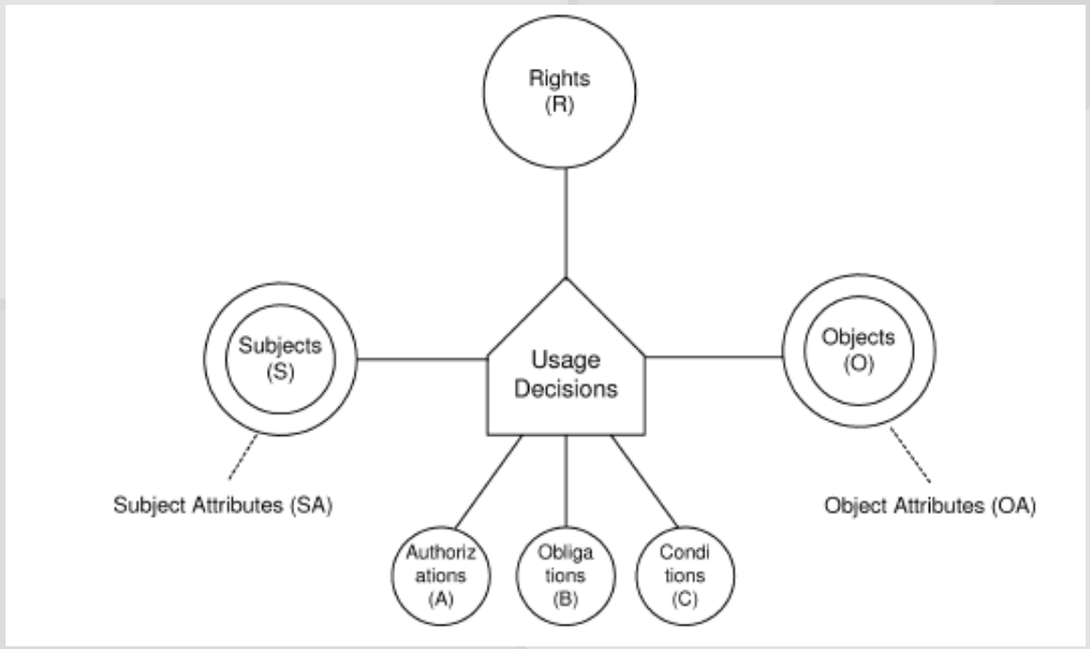
WP7

- Security in Virtual Infrastructure
  - Authentication
  - Usage Control
  - Compartmentalization and Isolation
  - Auditing

Usage Control Model

Usage Control Model

- Defined by R. Sandhu et. al.
  - The UCON Usage Control Model. ACM Trans. on Information and System Security, 7(1), 2004
  - Formal Model and Policy Specification of Usage Control. ACM Trans. on Information and System Security, 8(4), 2005
  - Towards a Usage-Based Security Framework for Collaborative Computing Systems. ACM Trans. on Information and System Security, 11(1), 2008
  - .....
- Main novelties
  - New decision factors
  - Mutability of Attributes
  - Continuity of Enforcement



Example: onGoing Authorization

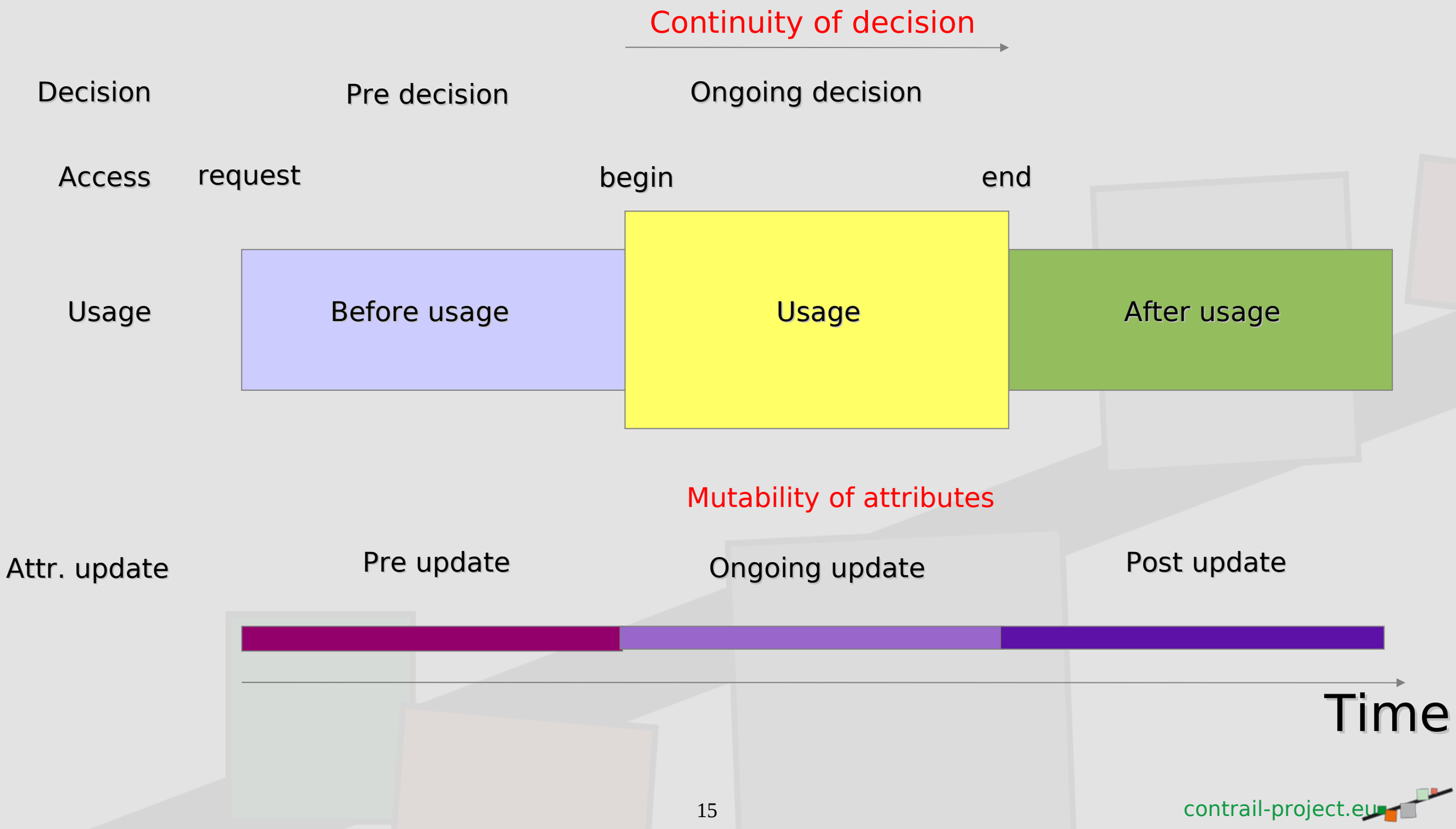
The right is granted without pre decisions, but authorization decisions are made continuously while the right is exercised

authorize(s,o): true
revoke(s,o): (usageNum(o) >10) and (s,t) in startT(o) with t min

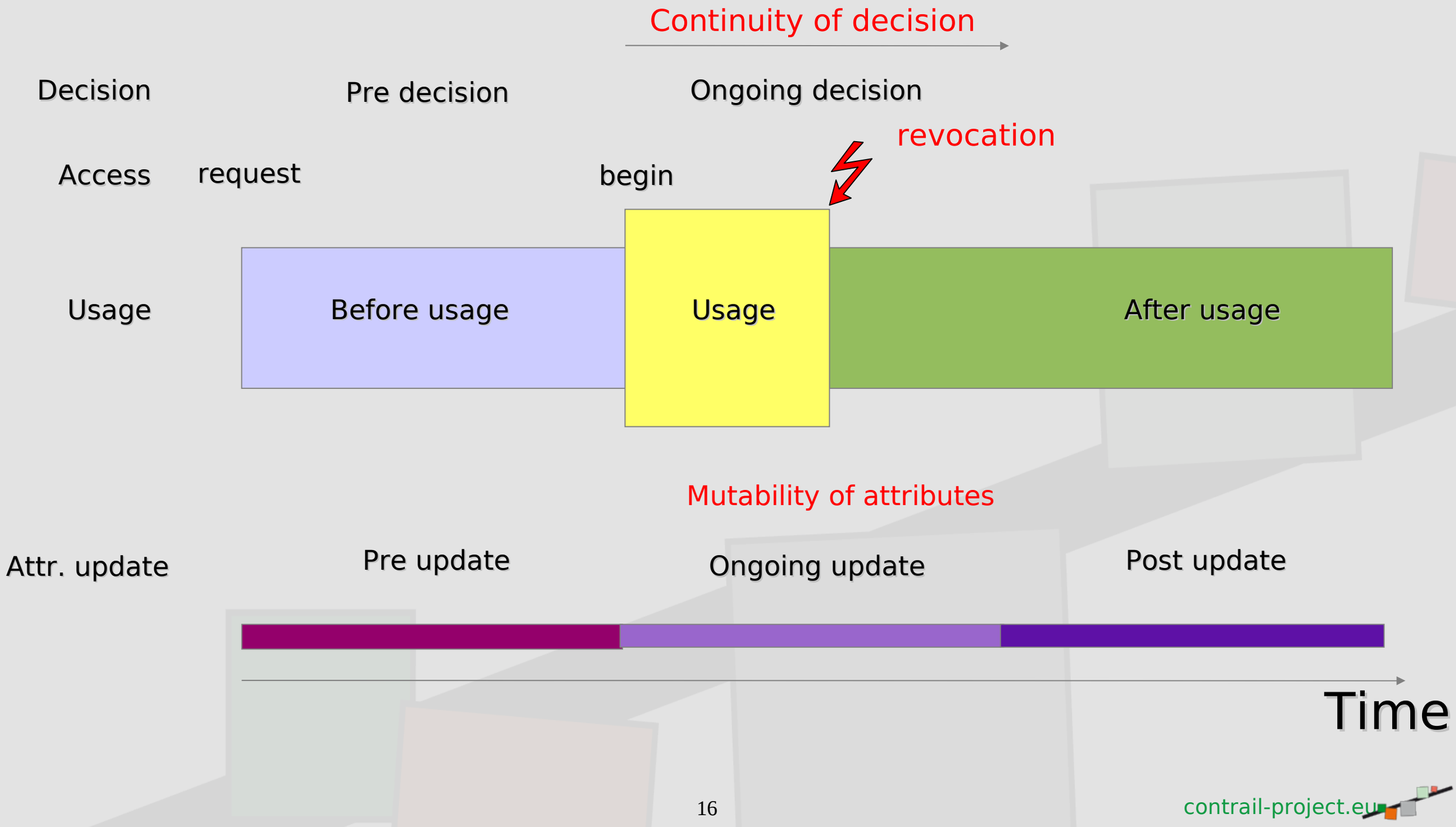
preUpdate(startT(o)): startT(o) = startT(o) U {(s,t)}
preUpdate(usageNum(o)) : UsageNum(o)++

postUpdate(usageNum(o)) : UsageNum(o)--
postUpdate(startT(o)): startT(o) = startT(o) – {(s,t)} where (s,t) in startT(o) with t min

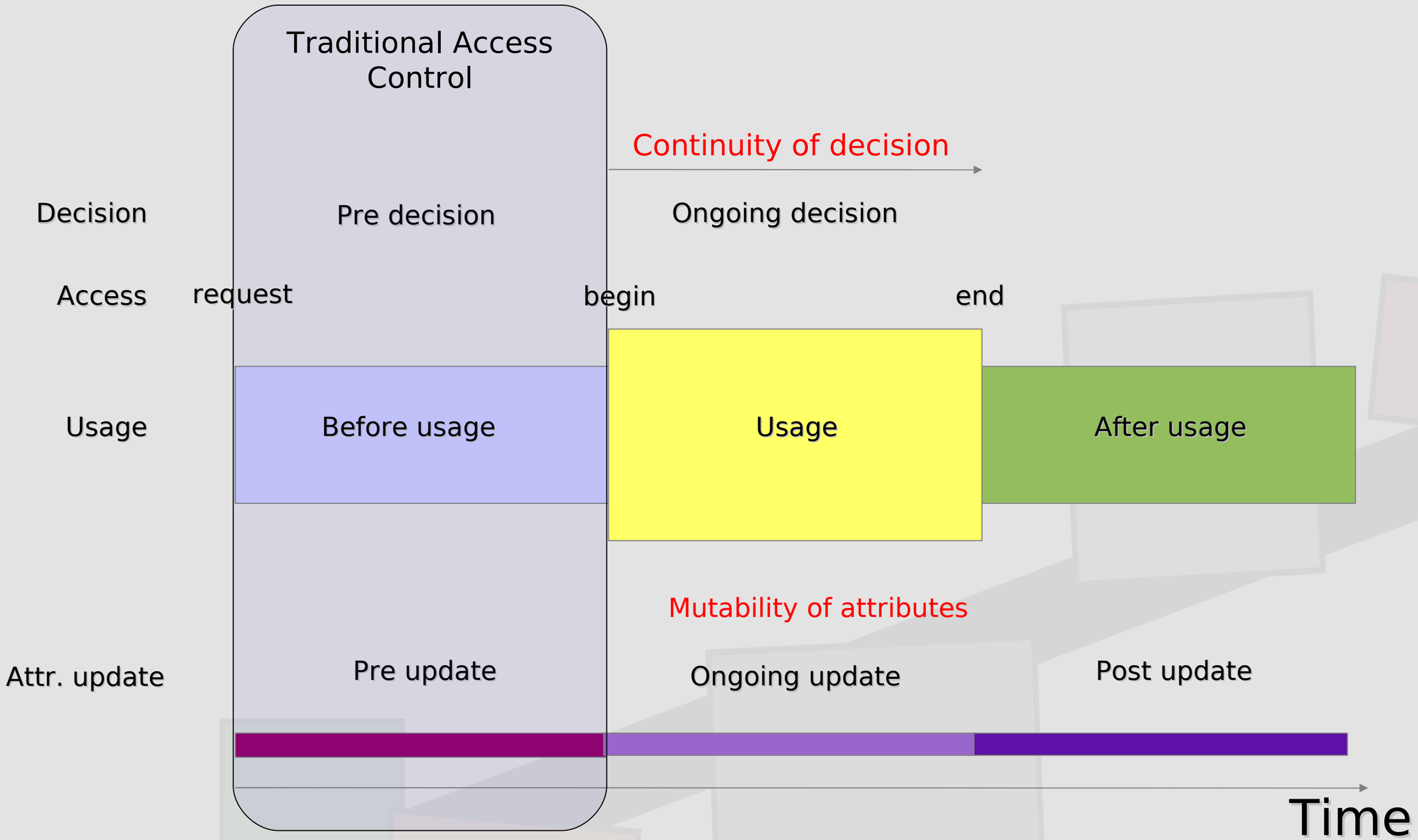
Access VS Usage Control



Access VS Usage Control



Access VS Usage Control



UCON Core Models

Decision Factors	Decision Time	Attributes Update			
		IMMUT	PRE	ONGOING	POST
Auth	PRE	Y	Y	N	Y
	ON	Y	Y	Y	Y
Obbl	PRE	Y	Y	N	Y
	ON	Y	Y	Y	Y
Cond	PRE	Y	N	N	N
	ON	Y	N	N	N

Why Usage Control in CONTRAIL?

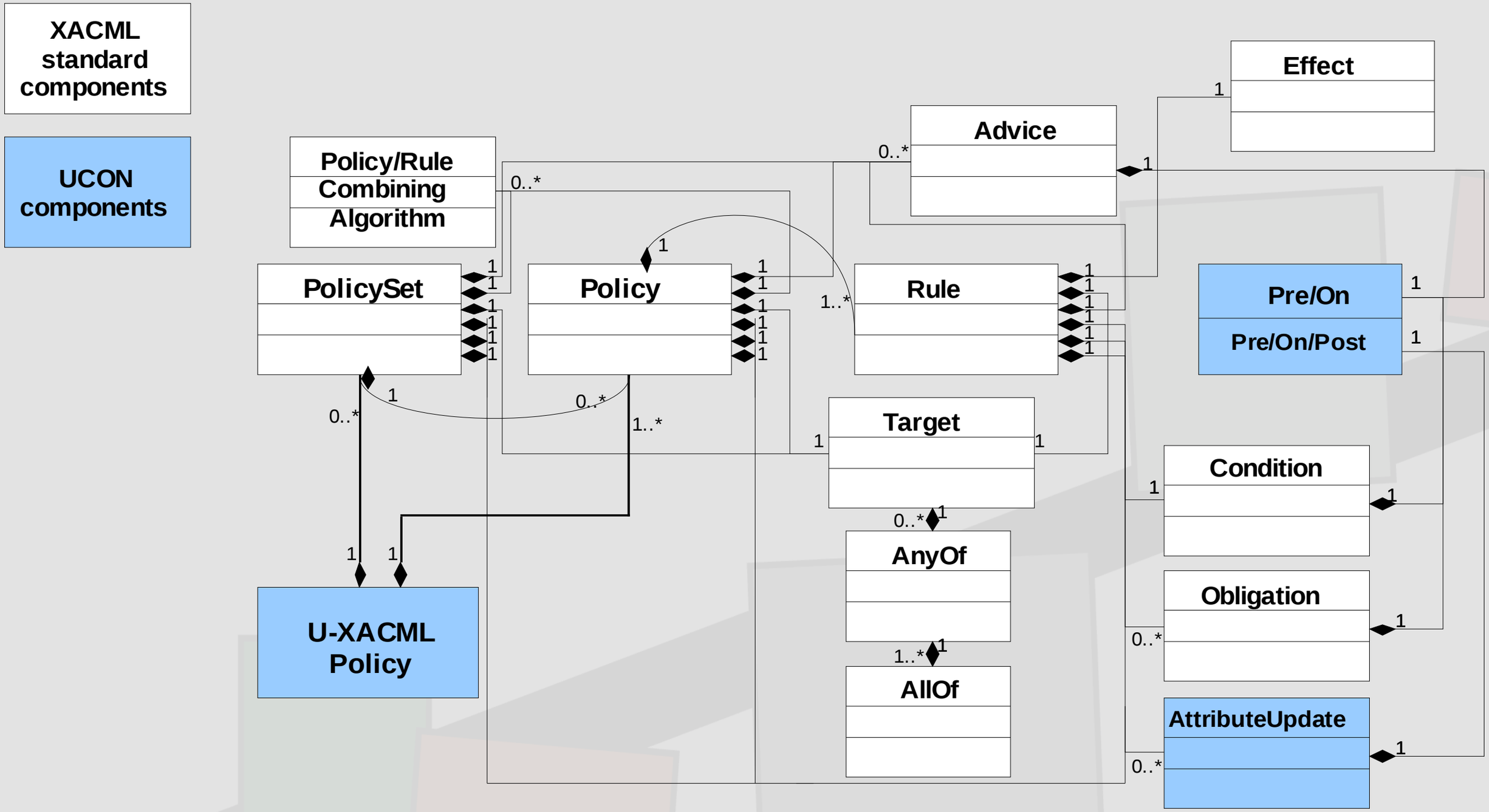
- Accesses to some resources last a long time (hours, days,..)
  - Run a Virtual Machine
  - Mount a Global File System on a Virtual Machine
  - Establish a virtual network connection
  - ...
- The factors that granted the access when it was requested could change while the access is in progress
  - User's reputation could decrease
  - Workload of resources could change
  - ...
- The security policy should be re-evaluated every time that factors change
  - An access that is in progress could be interrupted

Security Policy Language

UCON XACML Security Policy Language

- We are extending XACML language to implement UCON features:
  - Attributes update
  - Continuous control
- Preliminary work:
  - A proposal on enhancing XACML with continuous usage control features. CoreGrid ERCIM WG Workshop on Grids, P2P and Service Computing, 2009

UCON-XACML Policy Schema



Example of UCON-XACML policy

```
<?xml version="1.0" encoding="UTF-8" ?>
- <Policy xmlns="urn:oasis:names:tc:xacml:1.0:policy" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    PolicyId="GeneratedPolicy" RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:ordered-permit-
    overrides">
  + <Target>
  - <Rule RuleId="LoginRule" Effect="Permit">
  + <Target>
  - <Condition FunctionId="urn:oasis:names:tc:xacml:1.0:function:double-greater-than" DecisionTime="2">
    - <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:double-one-and-only">
        <SubjectAttributeDesignator DataType="http://www.w3.org/2001/XMLSchema#double"
          AttributeId="urn:iit:cnr:names:subject:reputation" Issuer="iit.cnr.it" />
      </Apply>
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#double">0.9</AttributeValue>
    </Condition>
  </Rule>
+ <AttrUpdates>
  <Rule RuleId="FinalRule" Effect="Deny" />
</Policy>
```

UCON XACML Security Policy

- CONTRAIL supports security policies at different levels:
  - Federation level
  - Cloud Provider level
  - Interactions through attributes

Usage Control System Architecture

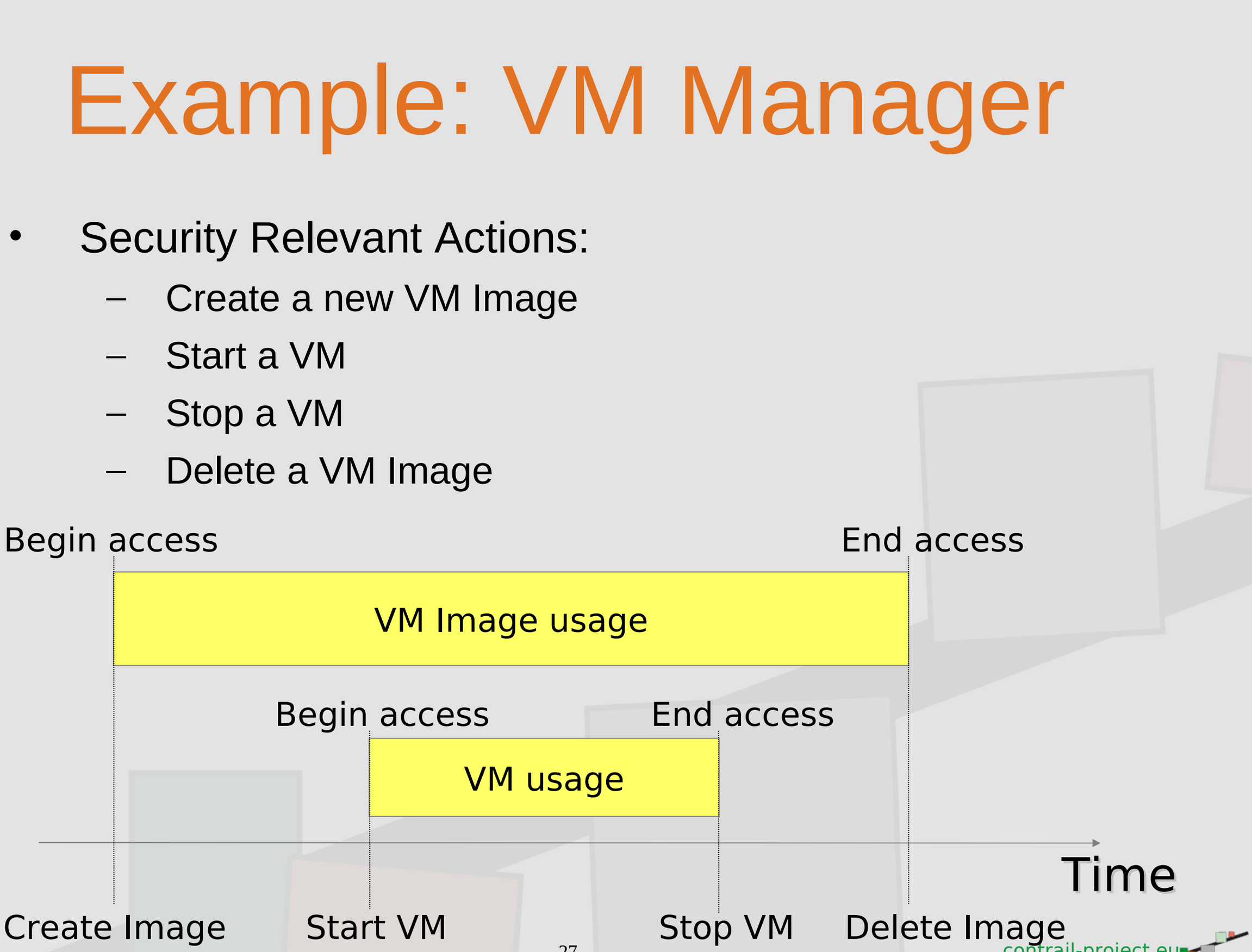
Security-Relevant Actions

- Are the action that are **relevant for system security**
  - Their execution must be controlled by the usage control system

- We are defining the set of security-relevant actions for each component of the CONTRAIL architecture, e.g.:
  - Federation Manager
  - VM manager
  - VIN
  - GAFS
  - VCP
  - …..

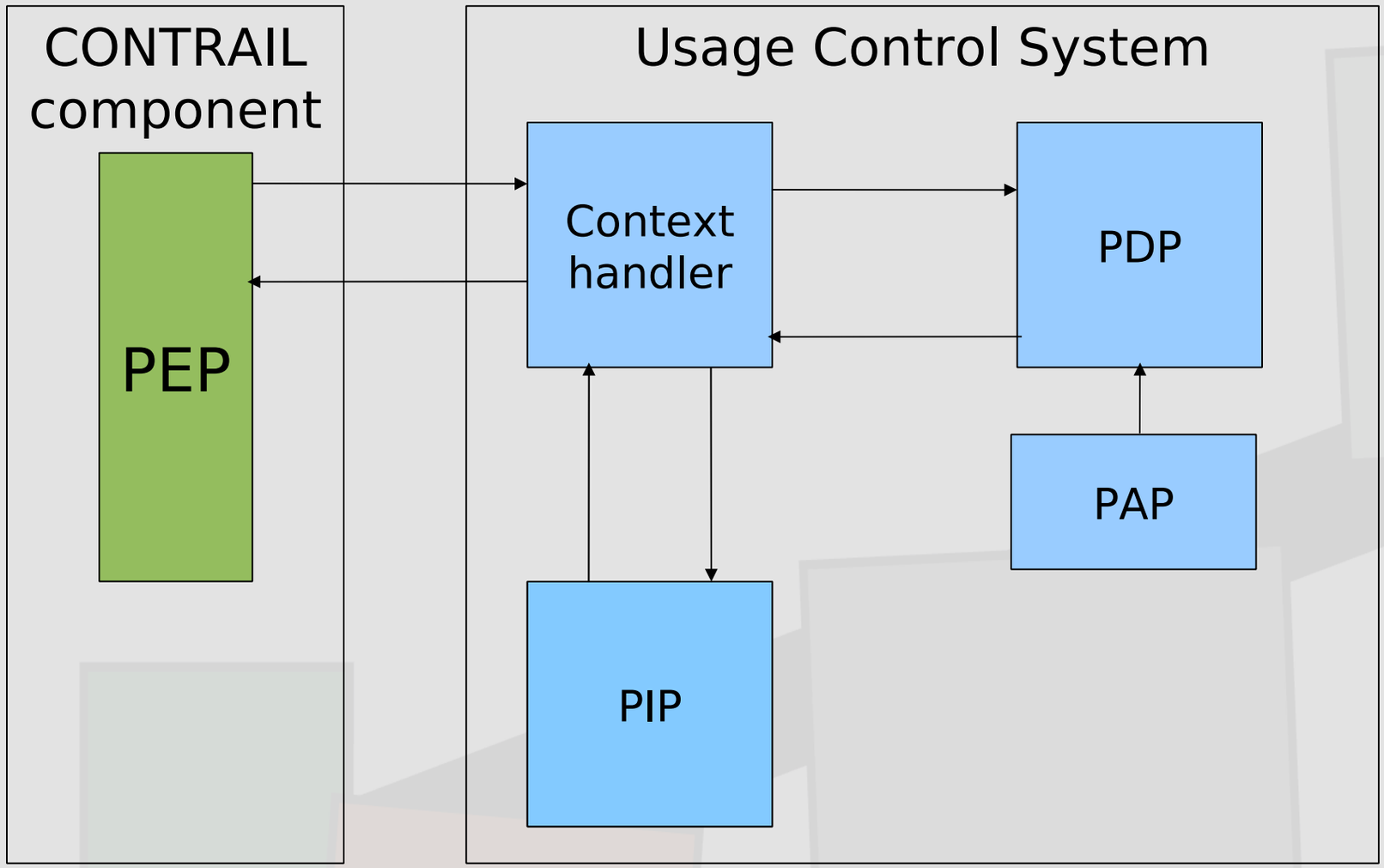
Example: VM Manager

- Security Relevant Actions:
  - Create a new VM Image
  - Start a VM
  - Stop a VM
  - Delete a VM Image



Usage Control System Architecture

- We are extending XACML architecture to deal with continuous policy enforcement

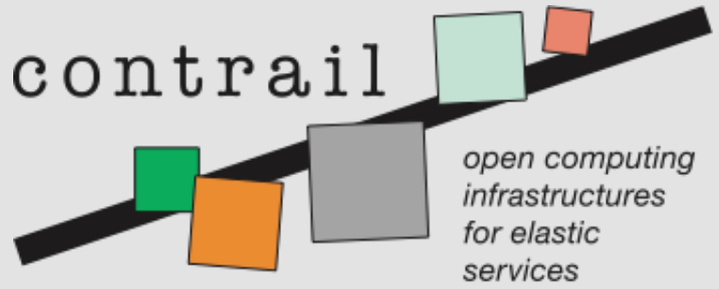


Usage Control System Components

- **Policy Enforcement Point**: intercepts the execution of security-relevant actions
- **Context Handler**: constructs XACML requests for the PDP, retrieves attribute values
- **Policy Decision Point**: evaluates the security policy to determine user's right to execute a security relevant action
- **Policy Information Point**: manages the attributes of users and resources
- **Policy Administration Point**: writes policies and make them available to the PDP

Policy Enforcement Points (PEPs)

- PEPs must be “embedded” in the architecture components that implement the security-relevant action (SRA) to:
  - Intercept the SRAs before their execution and suspend them
  - Ask the PDP to evaluate the security policy and wait for the decision
  - Enforce the decision of the PDP
    - resume the execution of the SRA
    - skip the execution of the SRA
    - …
  - Interrupt the execution of the SRA that is in progress when requested by the PDP
  - Intercept the end of a SRA and communicate it to the PDP



contrail is co-funded by the EC 7th Framework Programme

Funded under: FP7 (Seventh Framework Programme)

Area: Internet of Services, Software & virtualization (ICT-2009.1.2)

Project reference: 257438

Total cost: 11,29 million euro

EU contribution: 8,3 million euro

Execution: From 2010-10-01 till 2013-09-30

Duration: 36 months

Contract type: Collaborative project (generic)