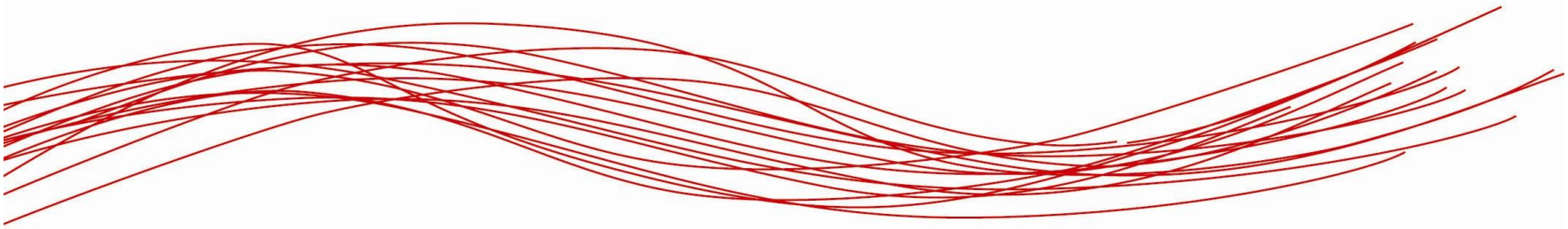
EUROPEAN COMMISSION / European Research Area / 7th Framework Programme

CUMULUS: Overview



G. Spanoudakis (City University)

June 2015

Cumulus

European Commission

Outline

- Overall vision
- Cloud Security – Reference Properties
- Certification Models
- Expected impact

Overall vision

Development of

an integrated framework of models, processes, and tools supporting the certification of security properties of infrastructure (IaaS), platform (PaaS) and software application layer services (SaaS) in clouds.

Use of multiple types of evidence for security assessment including

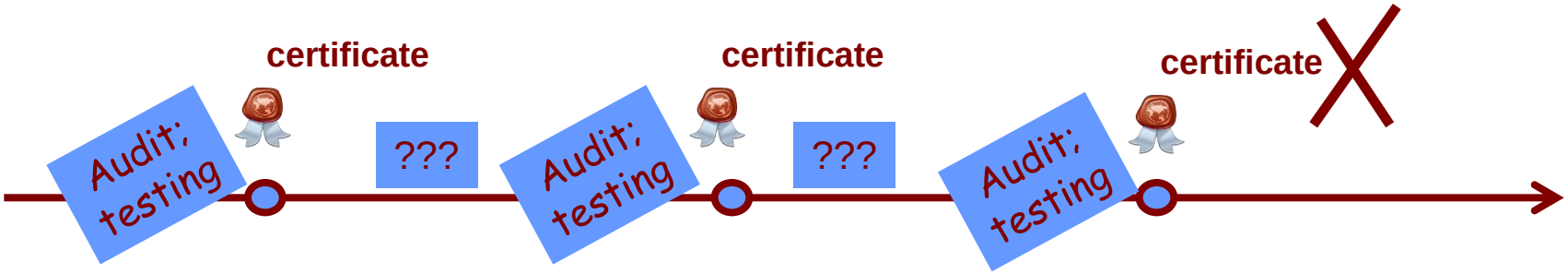
- *testing data*
- *monitoring data*
- *Trusted Computing proofs*

Use of different models for security assessment:

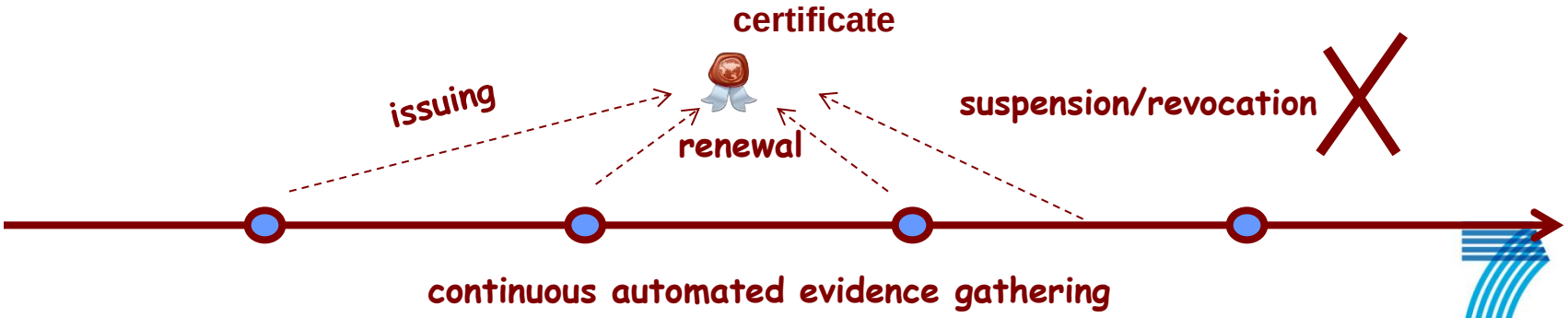
- *hybrid,*
- *Incremental, and*
- *multi-layer security certification.*

Overall Vision (cont'd)

- Present practice (e.g., Common Criteria (CC) a.k.a. ISO/IEC 15408)



CUMULUS approach



Cloud security – Reference Properties

Example Properties

- Tenant isolation on VMs
- External data exchange confidentiality
- Non repudiation of cloud storage services
- Data integrity at rest
  - Only authorised alterations of data are allowed
  - Notifications for any alteration attempt

From a catalogue of 70 property categories (produced by CSA)

Certification Models

- They specify
  - The security property to be certified
  - The target of certification and its environment
  - The evidence (type and extent) that needs to be considered to be able to certify the security property
  - How it will be used to assess the property
  - The life cycle model for certificates

- Consequences

  Certification authorities sign “parametric” certificates, which are based on approved (signed) certification models, and may need to be validated (confirmed) dynamically

  →

  Changes to traditional life cycle model of certificates (e.g., wrt certificate issuing/revocation)

Certification Models (cont'd)

Six types of CMs

- Test based (certification based on static or dynamic testing)
- Monitoring based (certification based on continuous monitoring)
- Trusted Computing (TC) evidence based
- Hybrid models
  - certification based on combinations of raw (i.e., monitoring and test based) evidence
- Incremental
  - Certification based on changes in cloud services
- Multi-layer
  - Certification based on compositions of certificates

Expected impact

Through the CUMULUS framework

- Offer tailorable certification processes and services
- Improve assessment of security properties
- Support continuous automated certification
- Reduce operational costs of certification
  - Make certification accessible to a wider spectrum of cloud service providers
- Improve cloud service clients awareness
- Contribute to standardisation