Bridging the GAP between Software Certification and Trusted Computing for securing Cloud Computing

Vision and short introduction

Safe Society Labs

UNIVERSIDAD DE MÁLAGA

Antonio Maña
Professor. University of Málaga
Scientific director. S2Labs

Motivation

- **Cloud technology still raises concerns**
  - regarding the security, privacy, governance and compliance of the data and software services offered through it
  - despite its appeal from the economic, operational and even energy consumption perspectives.
- **Securing applications and services available through cloud technology is difficult because of:**
  - (i) INTERDEPENDENCE AND DYNAMISM:
    - the provision and security of a cloud service is sensitive to potential interference between the behavior of inter-dependent services in all layers of the cloud stack, as well as dynamic changes in them
  - (ii) LACK OF SUPPORT IN CURRENT PLATFORMS:
    - current cloud models do not include support for trust-focused communication between layers.

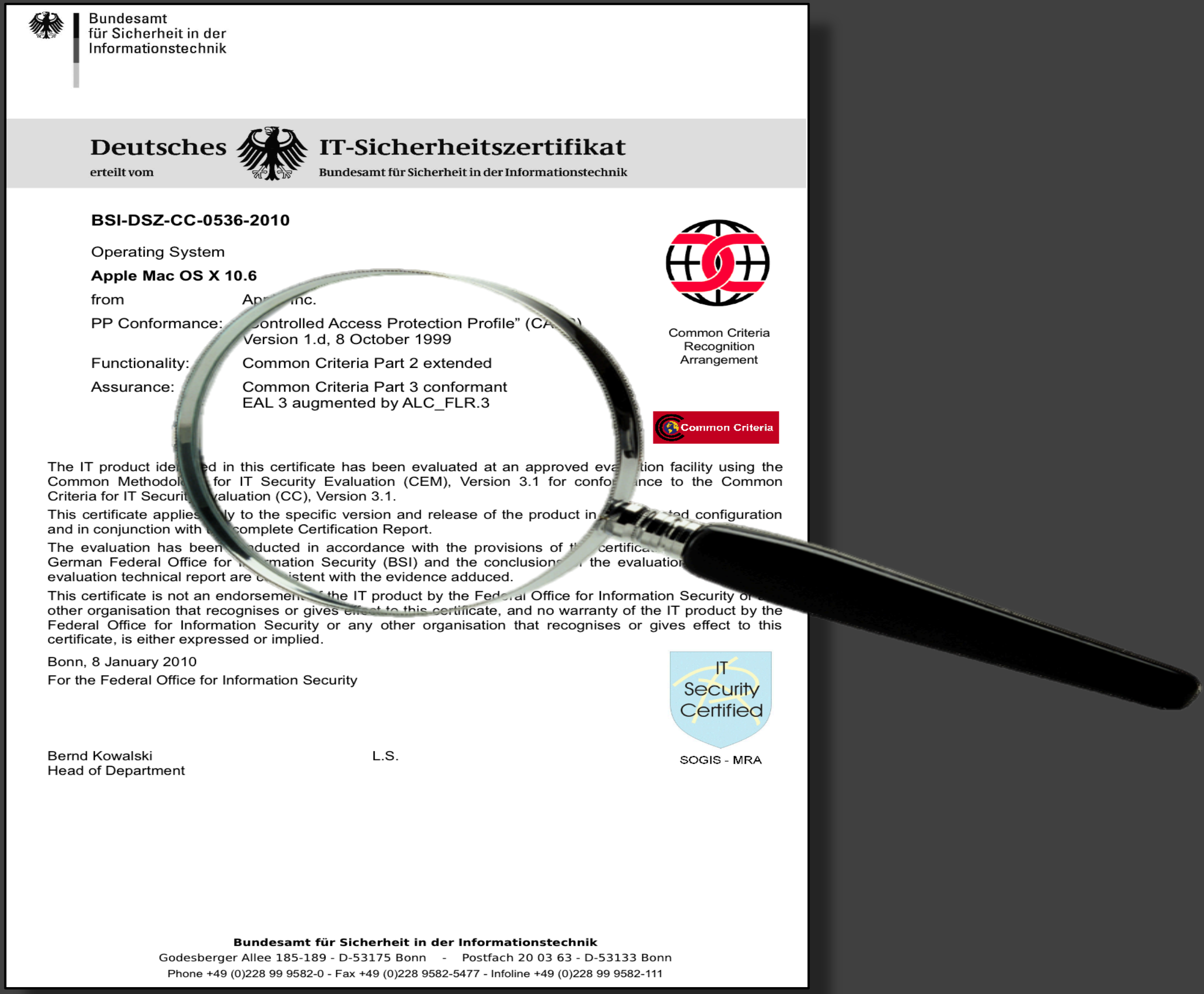
Software Security Certification

- **What is software security certification?**
  - Flavours: Accreditation, Assessment/Evaluation, Attestation/Certification
  - Definition: “the process of evaluating a system to attest its security properties”
- **Why certification is useful?**
  - Certification is a mechanism to increase trust.
  - A certificate is a statement that is authentic and integral

Trust in the certificate issuer + the certificate itself = trust in the certificate subject

Safe Society Labs

An actual Software (CC) Certificate



Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat
erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0536-2010

Operating System

Apple Mac OS X 10.6

from	Ap Inc.
PP Conformance:	ontrolled Access Protection Profile" (CA) Version 1.d, 8 October 1999
Functionality:	Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 3 augmented by ALC_FLR.3

Common Criteria Recognition Arrangement

Common Criteria

The IT product ide ed in this certificate has been evaluated at an approved eva tion facility using the Common Methodol for IT Security Evaluation (CEM), Version 3.1 for confo nce to the Common Criteria for IT Securit valuation (CC), Version 3.1.

This certificate applies ly to the specific version and release of the product in ed configuration and in conjunction with complete Certification Report.

The evaluation has been ducted in accordance with the provisions of t certifica German Federal Office for mation Security (BSI) and the conclusion the evaluatio evaluation technical report are c istent with the evidence adduced.

This certificate is not an endorsemen the IT product by the Fed al Office for Information Security o other organisation that recognises or gives to this certificate, and no warranty of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Bonn, 8 January 2010

For the Federal Office for Information Security

IT Security Certified

Bernd Kowalski
Head of Department

L.S.

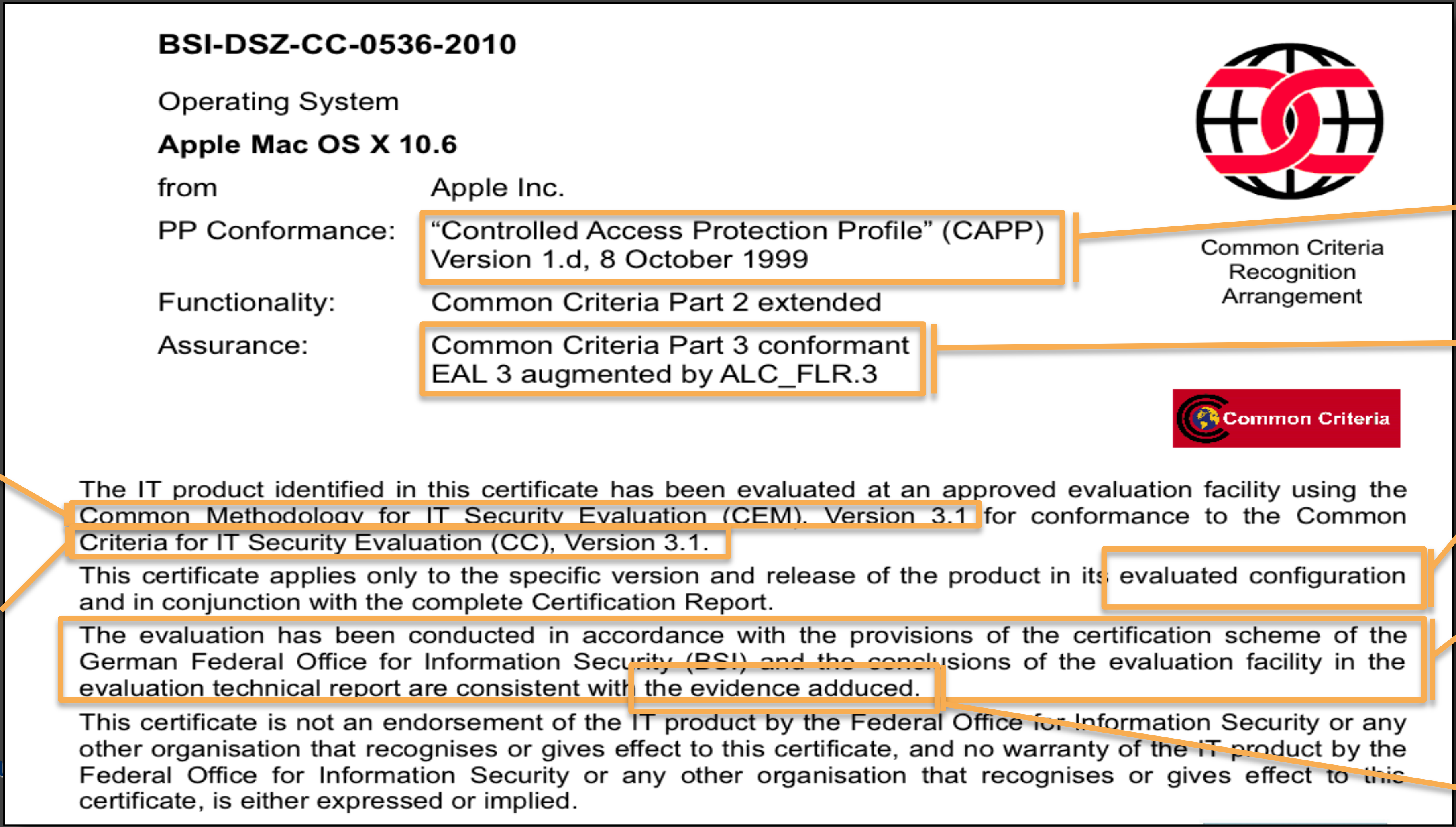
SOGIS - MRA

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 99 9582-5477 - Infoline +49 (0)228 99 9582-111

UNIVERSIDAD DE MÁLAGA

Safe Society Labs

An actual Software (CC) Certificate



BSI-DSZ-CC-0536-2010

Operating System

Apple Mac OS X 10.6

from	Apple Inc.
PP Conformance:	“Controlled Access Protection Profile” (CAPP) Version 1.d, 8 October 1999
Functionality:	Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 3 augmented by ALC_FLR.3

Common Criteria Recognition Arrangement

Common Criteria

The IT product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

This certificate is not an endorsement of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

? ? ? ? ? ? ?

UNIVERSIDAD DE MÁLAGA

Software Security Certification Pros

- Certification
  - Increases Users' trust
  - Attests security properties
- Evaluation done by experts
  - Testing
  - Formal modelling
  - Considerable effort
- Relies on trust
  - In the experts
  - In the certification scheme
- Refers to specific version
  - Changes require re-certification

Software Security Certification Cons

- Certificates
  - Intended for human use
  - Lack machine readable format
  - Lack explicit and precise formulation of security properties
  - Cannot be used for runtime security assessment
- Not suitable for
  - Dynamic environments
  - Highly distributed environments
  - Systems without a central control or controlled ownership
  - Systems modified e.g. by policy decisions
- Don't support
  - Dynamic replacement of components
  - Runtime binding

Current certification schemes do not provide a reliable way to assess the trustworthiness of a composite application at the point of use.

ASSERTs

- ASSERTs are a new type of digital certificates
  - Implemented as a digitally signed SAML-contained XML document
- There are three different types of ASSERTs
  - **Evidence-based Assert (ASSERT-E)**: An ASSERT in which the assessment of the properties is based on the execution of tests.
  - **Model-based Assert (ASSERT-M)**: An ASSERT in which the assessment of the properties is based on the creation and analysis of a formal model.
  - **Ontology-based Assert (ASSERT-O)**: An ASSERT in which the claims about the properties are simply stated by the authority with the support of the ASSERRT Ontology.
  - Interoperability does not compromise security.

ASSERTs

- **ASSERTs are designed to represent software certifications in a way suitable for automated processing**
  - Signed by accredited software certification authorities
  - Used to support the security-based selection of services for integration into security-aware applications
    - thus integrated in service discovery and orchestration processes
- **ASSERTs are designed to support interoperability of certifications produced by different authorities**
  - ASSERT Language relies on the ASSERT4SOA Ontology
  - Interoperability applies to different elements (properties, certification schemes…)
  - Interoperability does not compromise security.

Background Conclusions (I)

- **Software certification**
  - this approach is considered to be an appropriate and robust mechanism for supporting assurance and compliance, but there are two important problems:

    P1. certification has been traditionally targeting humans

    and has not been able to support automated processing of certifications (i.e. verification, selection based on certifications, etc.); and

    P2. certification cannot provide dynamic proofs of the status of a system at runtime

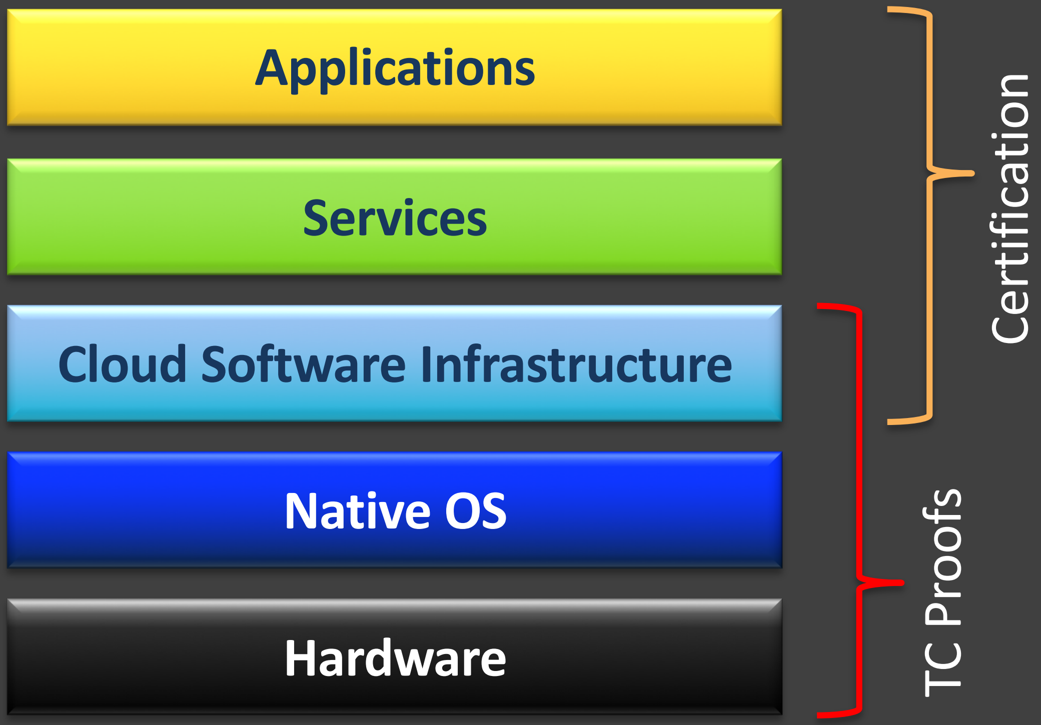
    these are extremely important in a dynamic, heterogeneous and unpredictable scenario such as cloud computing.
- **While recent advances (by ASSERT4SOA project) have solved P1 based on their certificates (a computer-oriented form of certification called ASSERTS); P2 does not currently have a satisfactory solution.**

Background Conclusions (II)

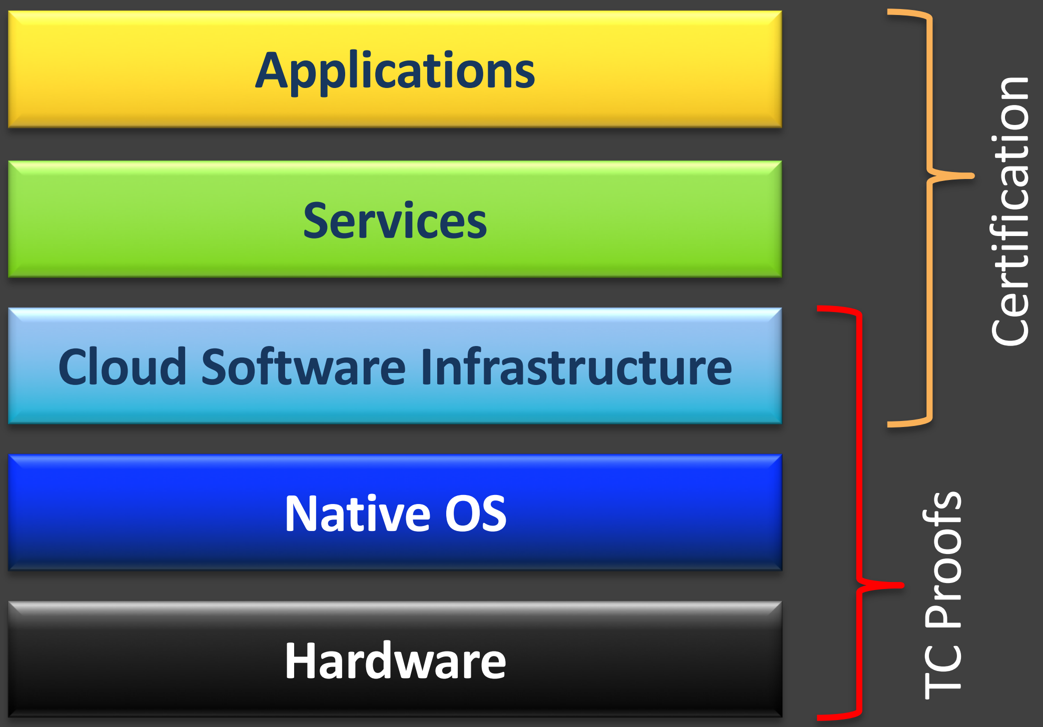
- **Cloud computing architectures are based on a hardware, software and firmware underlying basis that is stable, in the sense that few changes are done in this basis.**
  - However, in the most abstract layers of the software (i.e., applications) changes are produced frequently, different applications are launched in systems sharing resources, resulting in many changes in the system execution stack.
- **Trusted Computing (TC) technologies are well suited to provide proofs of the trustworthiness on the lower level of the cloud stack**
  - starting with the hardware layer, but are not efficient and practical when it comes to dealing with the very dynamic and heterogeneous higher layers (service / application).

Approach (I)

- In the light of the previous discussion, our approach is to use certification for the higher layers, and to link the certificates to proofs produced by TC for the lower layers, thus bridging the gap between these technologies



Approach (II)



Applications

Services

Cloud Software Infrastructure

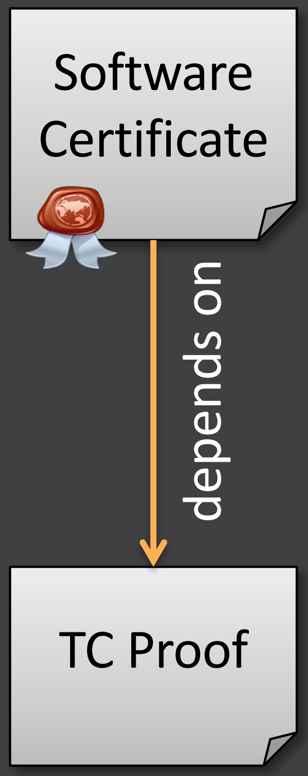
Native OS

Hardware

Certification

TC Proofs

Conceptually



Software Certificate

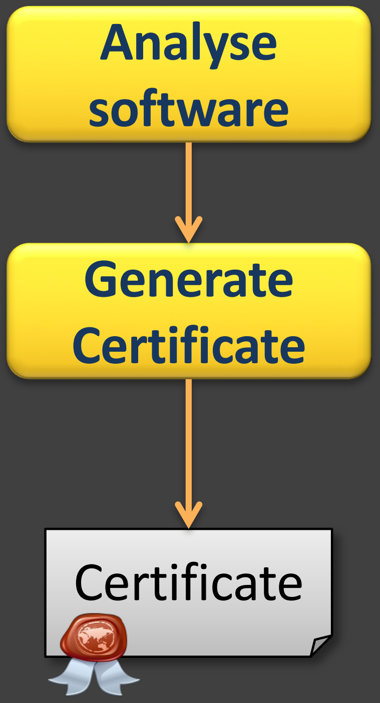
depends on

TC Proof

Approach (III)

Generation

Current certification

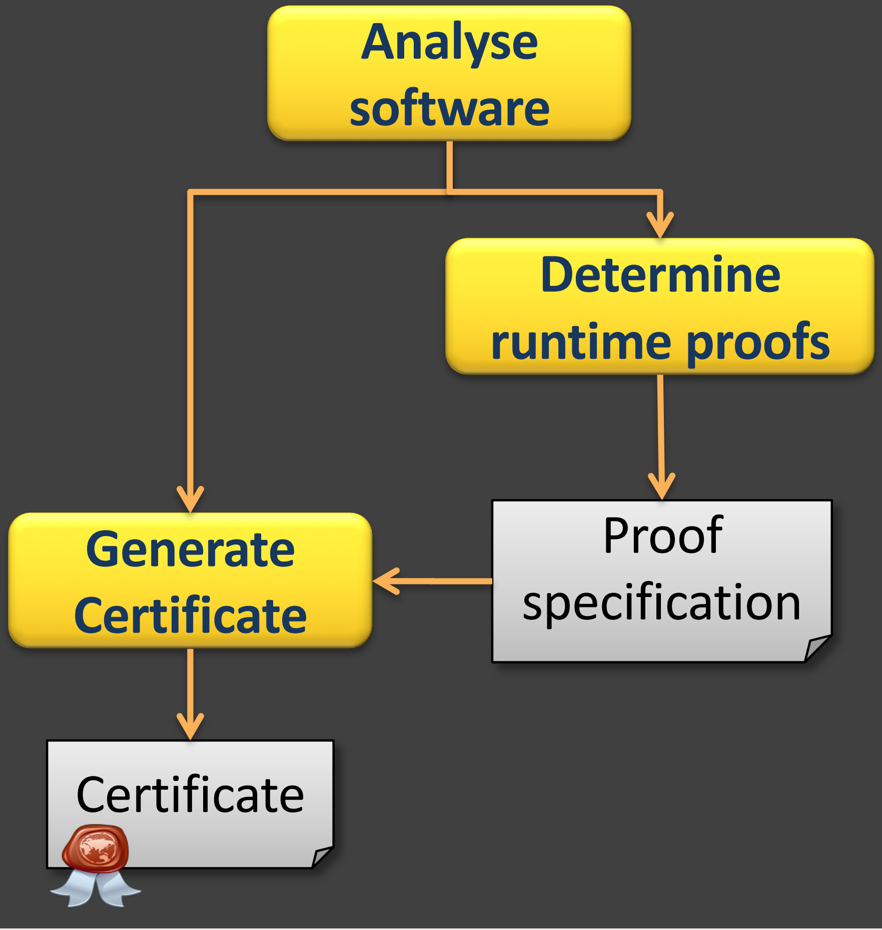


Analyse software

Generate Certificate

Certificate

CUMULUS certification



Analyse software

Determine runtime proofs

Proof specification

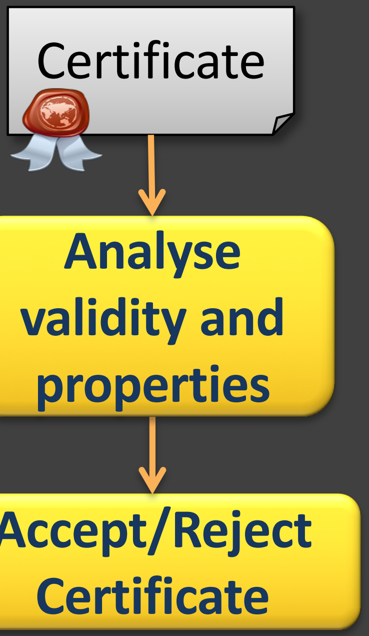
Generate Certificate

Certificate

Approach (IV)

Checking

Current certification

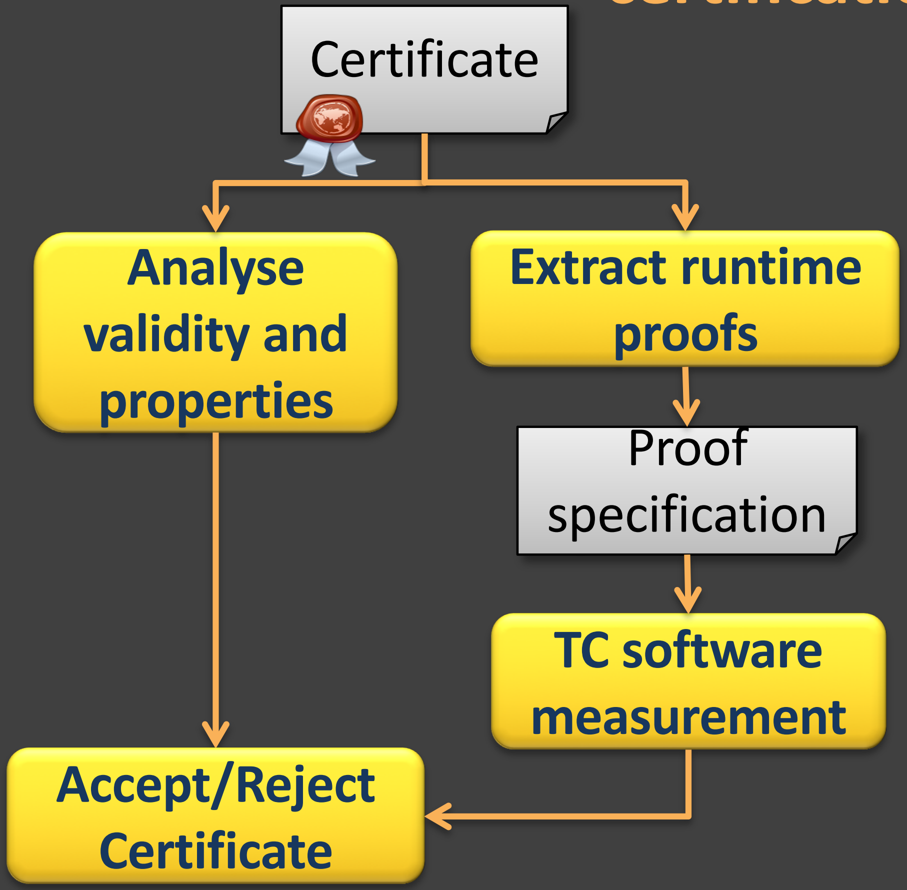


Certificate

Analyse validity and properties

Accept/Reject Certificate

CUMULUS certification



Certificate

Analyse validity and properties

Extract runtime proofs

Proof specification

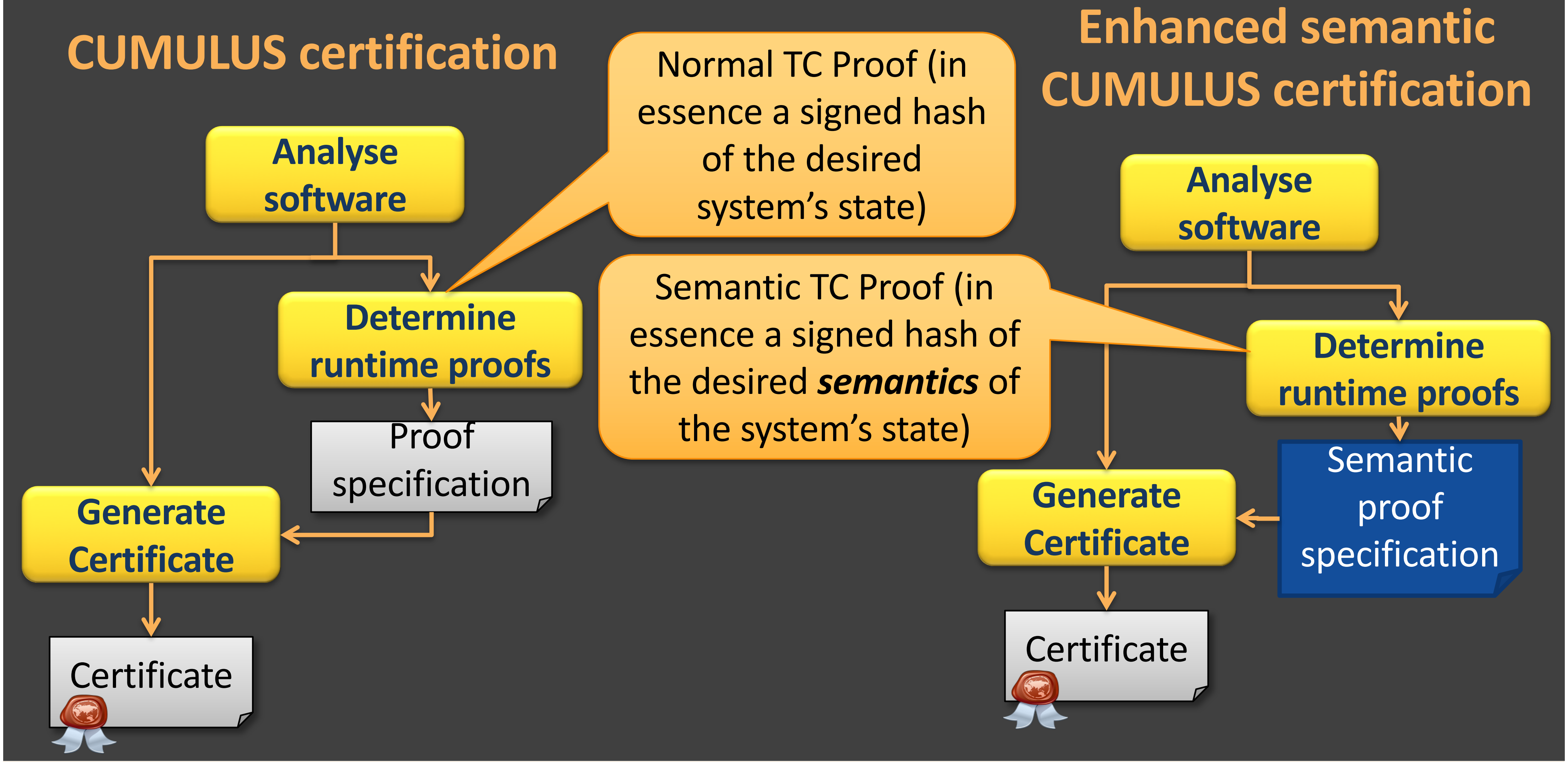
TC software measurement

Accept/Reject Certificate

Can we do better?

- Standard TC Proofs are limited (for this scenario)
  - if a high-level certificate (for instance for a service) refers to a standard TC proof to define the platform state, we would need to issue a different certificate for each valid platform configuration
- We need improvements in
  - flexibility, and
  - interoperability
- Semantic approaches can be the basis for the necessary improvements

Can we do better? (Generation)



CUMULUS certification

Analyse software

Determine runtime proofs

Proof specification

Generate Certificate

Certificate

Normal TC Proof (in essence a signed hash of the desired system's state)

Semantic TC Proof (in essence a signed hash of the desired ***semantics*** of the system's state)

Enhanced semantic CUMULUS certification

Analyse software

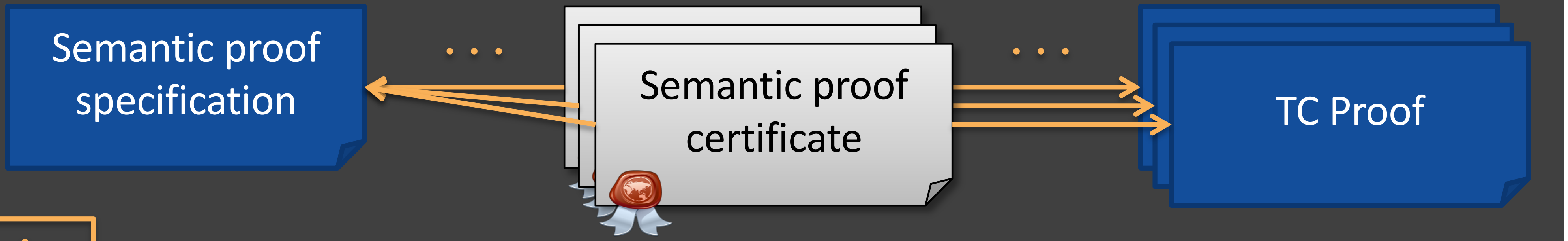
Determine runtime proofs

Semantic proof specification

Generate Certificate

Certificate

Realization of semantic proofs



Semantic proof specification

. . .

Semantic proof certificate

. . .

TC Proof

Contents

- Reference to a semantic identifier +
- Reference to an authority for that identifier

- TC Standard proof +
- Reference to a semantic identifier +
- Signature of the authority for that identifier

- TC Standard Proof

Example

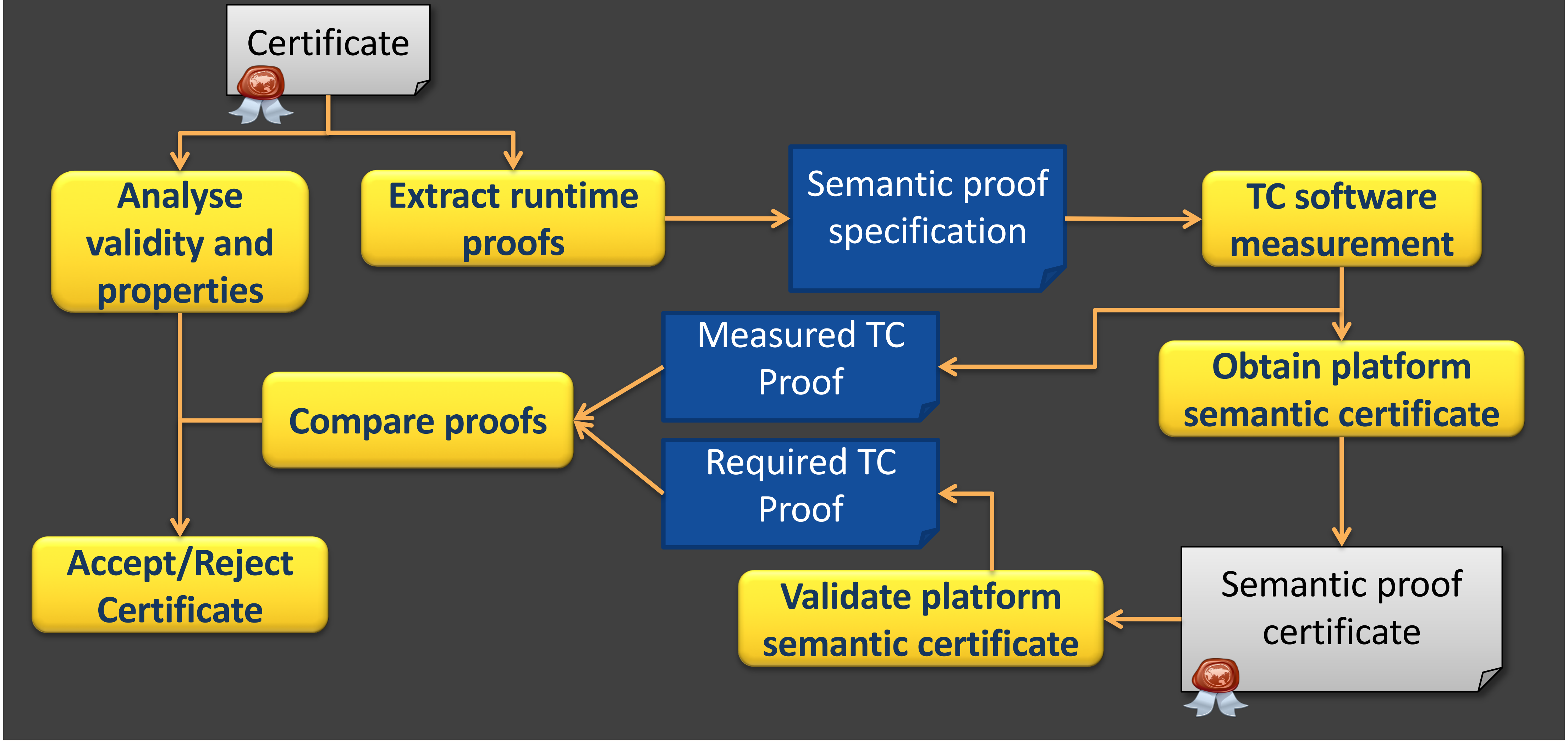
- “Confidential Platform”
- www.commoncriteriaportal.org

- PCR value
- “Confidential Platform”
- Signature of a common criteria authority

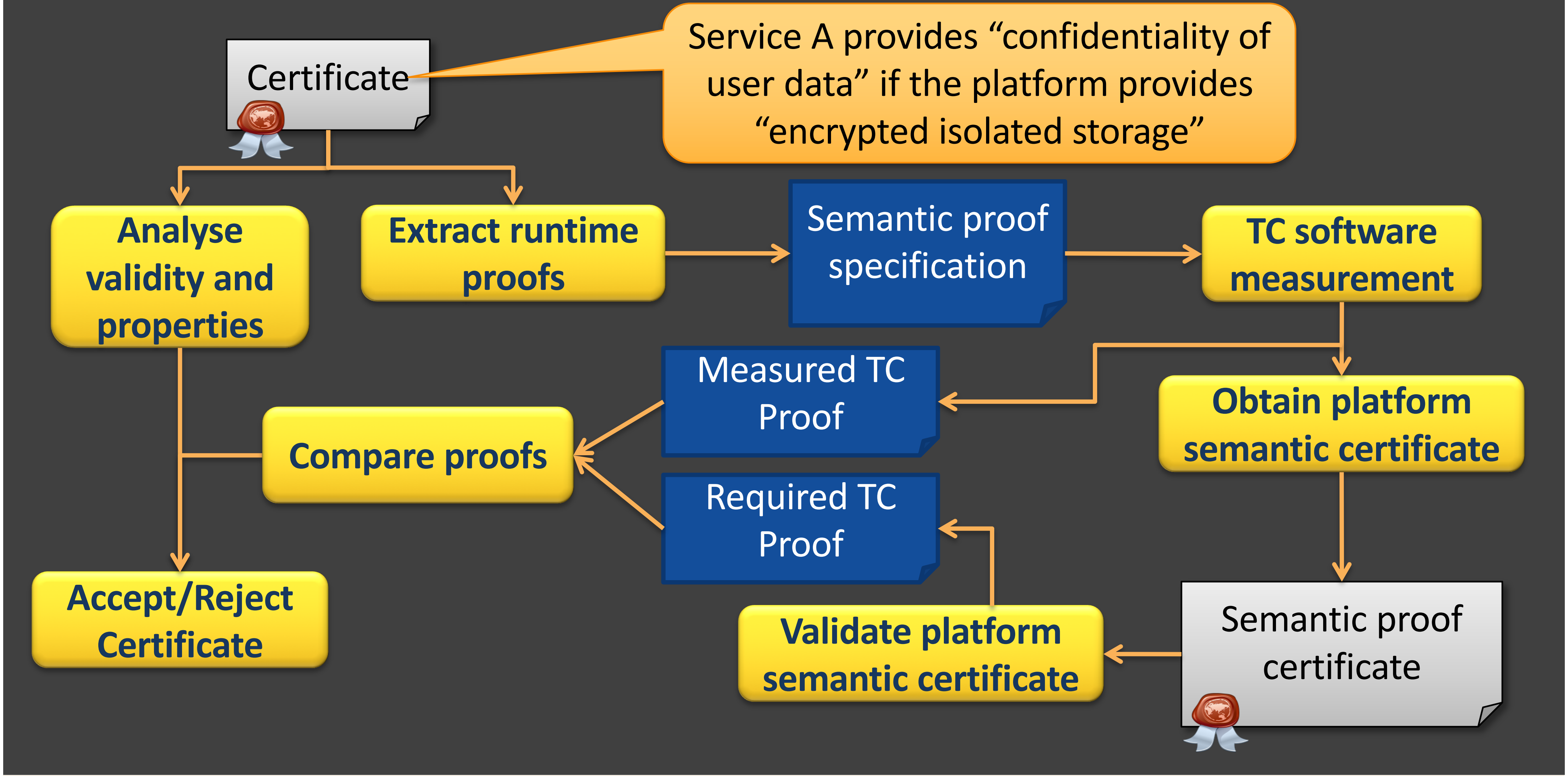
- PCR value

Safe Society Labs

Can we do better? (Checking)

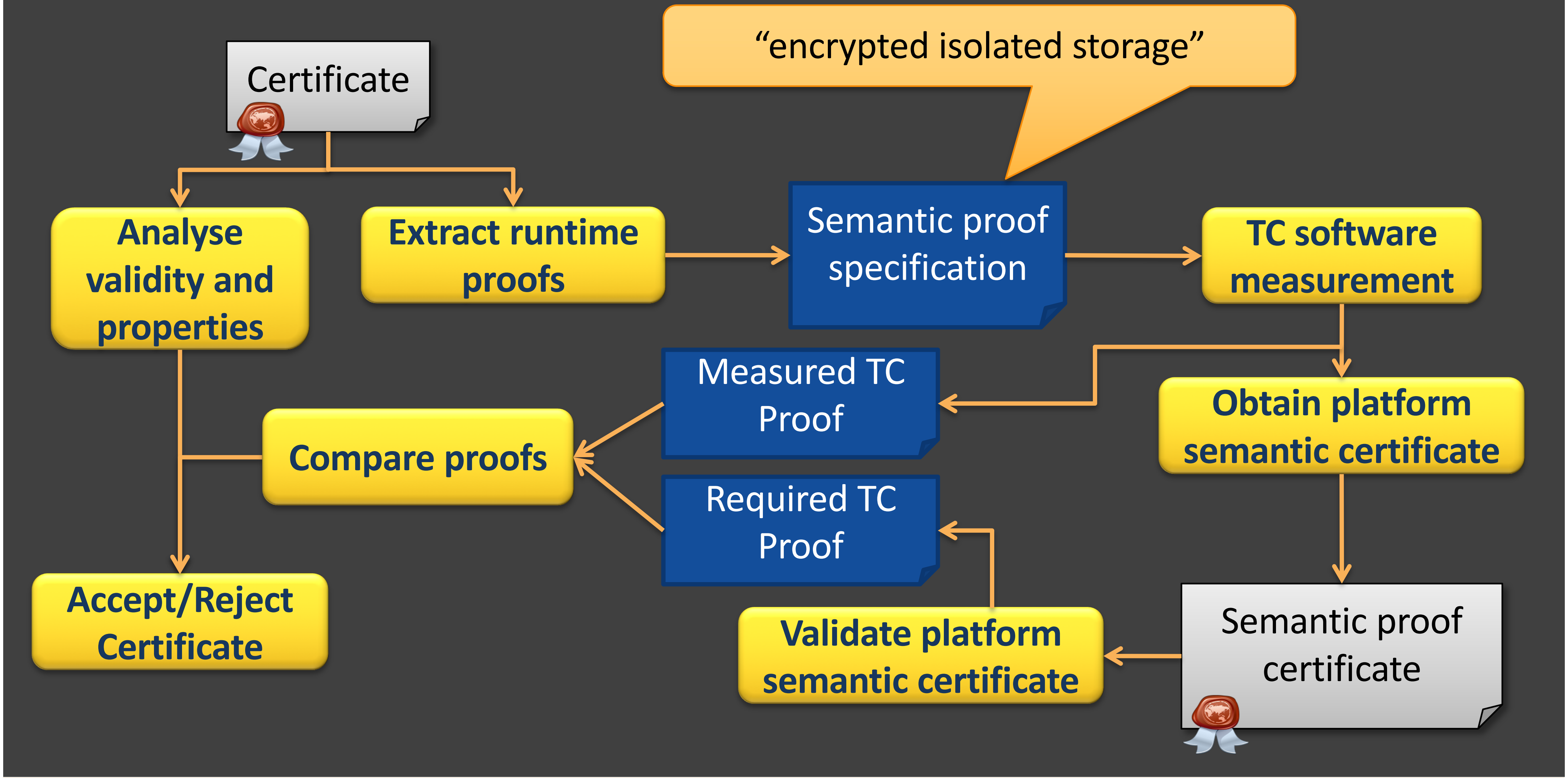

Certificate
Analyse validity and properties
Extract runtime proofs
Semantic proof specification
TC software measurement
Measured TC Proof
Obtain platform semantic certificate
Compare proofs
Required TC Proof
Accept/Reject Certificate
Validate platform semantic certificate
Semantic proof certificate

Can we do better? (Checking)


Certificate
Service A provides “confidentiality of user data” if the platform provides “encrypted isolated storage”
Analyse validity and properties
Extract runtime proofs
Semantic proof specification
TC software measurement
Measured TC Proof
Obtain platform semantic certificate
Compare proofs
Required TC Proof
Accept/Reject Certificate
Validate platform semantic certificate
Semantic proof certificate

Safe Society Labs

Can we do better? (Checking)



Certificate

Analyse validity and properties

Extract runtime proofs

"encrypted isolated storage"

Semantic proof specification

TC software measurement

Measured TC Proof

Obtain platform semantic certificate

Compare proofs

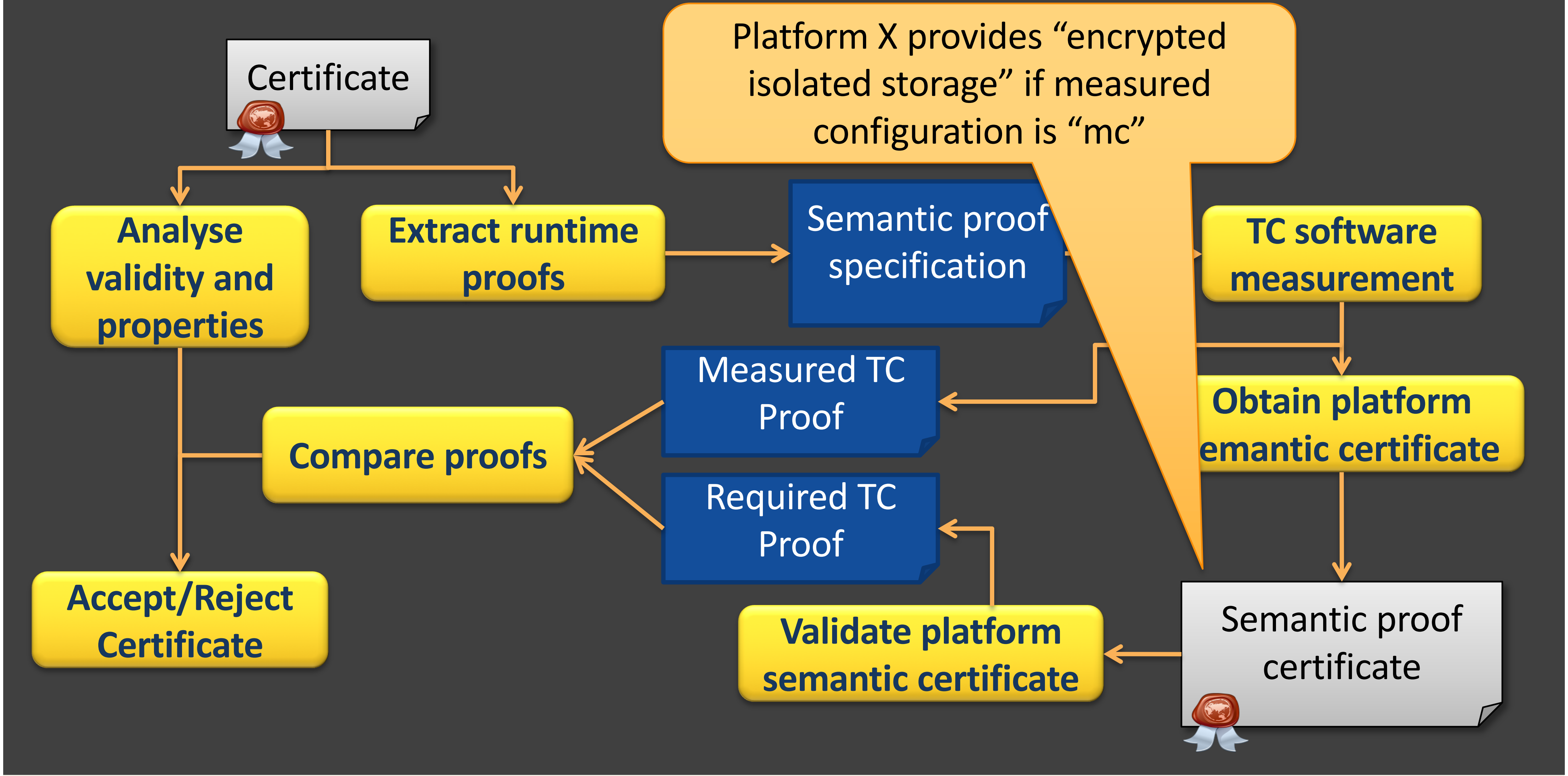
Required TC Proof

Accept/Reject Certificate

Validate platform semantic certificate

Semantic proof certificate

Can we do better? (Checking)



Platform X provides “encrypted isolated storage” if measured configuration is “mc”

Certificate

Analyse validity and properties

Extract runtime proofs

Semantic proof specification

TC software measurement

Measured TC Proof

Compare proofs

Required TC Proof

Obtain platform emantic certificate

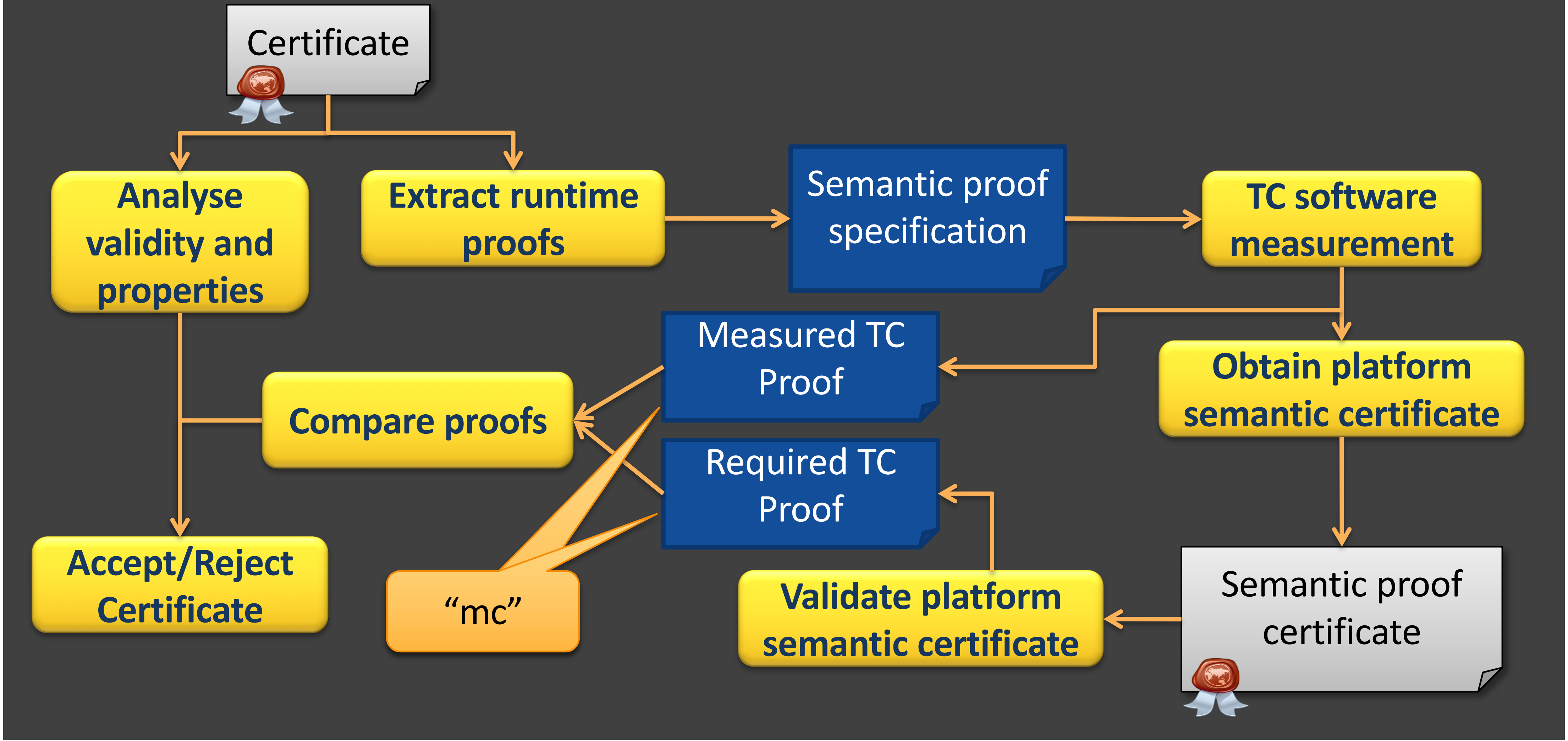
Accept/Reject Certificate

Validate platform semantic certificate

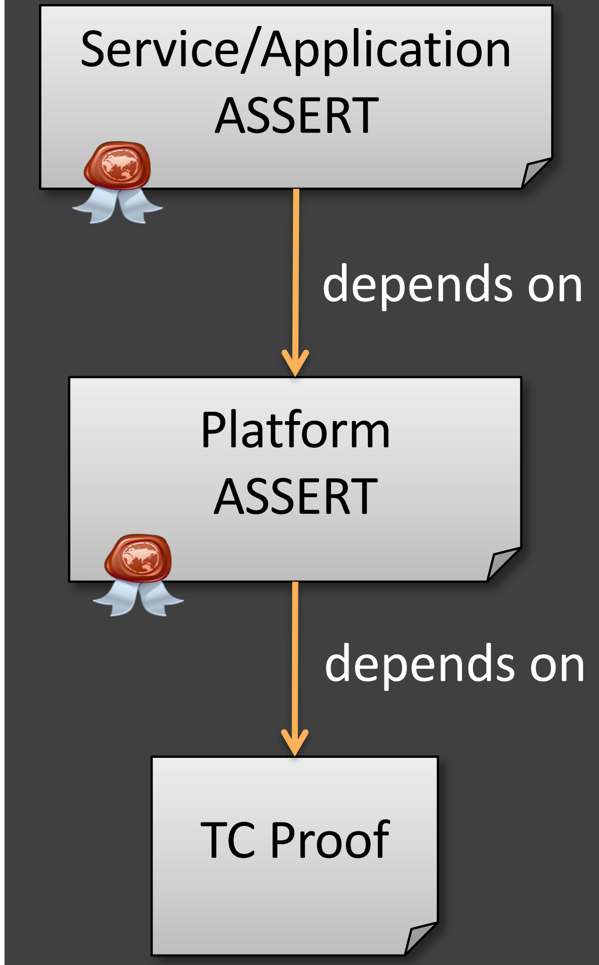
Semantic proof certificate

Safe Society Labs

Can we do better? (Checking)


Certificate
Analyse validity and properties
Extract runtime proofs
Semantic proof specification
TC software measurement
Measured TC Proof
Obtain platform semantic certificate
Compare proofs
Required TC Proof
Accept/Reject Certificate
"mc"
Validate platform semantic certificate
Semantic proof certificate

Summary



Service/Application ASSERT

depends on

Platform ASSERT

depends on

TC Proof

- The proposed scheme can successfully bridge the gap between Trusted Computing and Software Certification by combining the best of both worlds and overcoming their respective limitations
- The concept of ASSERT as a computer-oriented form of certification is also useful for improving the flexibility and practical applicability of TC mechanisms
- This approach can open new application fields for TC
- The approach is based on the results of the ASSERT4SOA project, and will be developed in the CUMULUS project.
- Additionally, an open working group will be established in the Security Engineering Forum

www.securityengineeringforum.org

Bridging the GAP between Software Certification and Trusted Computing for securing Cloud Computing

Vision and short introduction

Trusted Computing Group Meeting, Madrid, June 20th, 2012

Thank you for your attention

Safe Society Labs

UNIVERSIDAD
DE MÁLAGA

Questions?