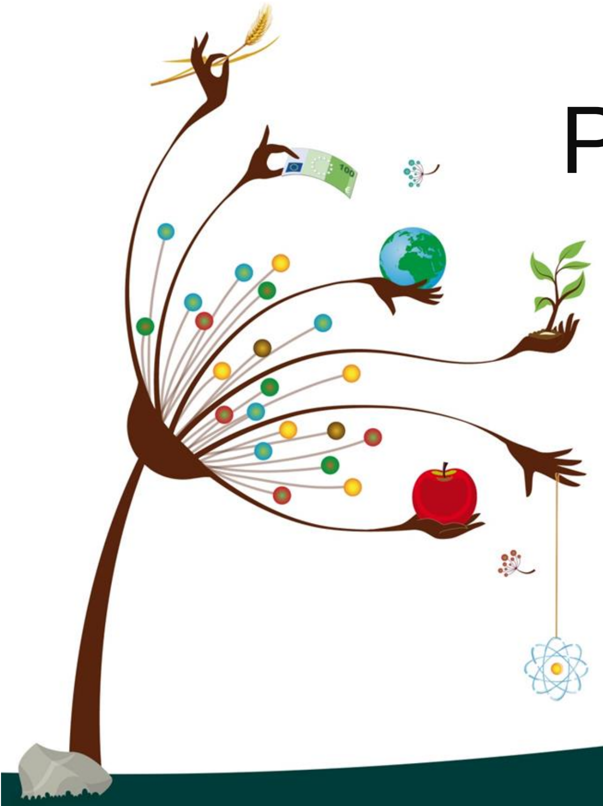
European
Commission

Improving Internet of Things Device Certification with Policy Based Management



Gianmarco Baldini
European Commission
DG.JRC.E3
Gianmarco.Baldini@ec.europa.eu

Joint
Research
Centre

IoT Security

In beginning of 2015, US Federal Trade Commission Chairwoman, Edith Ramirez, laid out in her CES 2015 keynote that heightened security and privacy risks is a major concern facing the IoT that undermine consumer trust.

The proliferation of Internet of Things (IoT) ecosystems is radically affecting the way in which people communicate with their surroundings, transforming current physical spaces into real pervasive environments, in which services and resources can be accessed ubiquitously.

Since this scheme implies that physical objects are being integrated into the Internet infrastructure, they are now vulnerable to attacks and misuse.

Individual security tests can be performed in isolated scenarios but the results are difficult to translate into the real world with acceptable degree of confidence.

Horizon 2020 ARMOUR

The ARMOUR framework for large-scale IoT Security & Trust testing is based on the following principles:

- Focus on dynamic application security testing technologies to target business Logic Vulnerabilities and to ensure the security control.
- Use regression testing techniques and bi-directional traceability between the business and security rules on one hand and the generated tests on the other hand in order to ensure secure dynamic reconfiguration of IoT systems.
- Use as a model-based techniques to describe vulnerability test patterns and security requirements to tackle uncertainty and business logic vulnerabilities, at run-time.
- Provide fully automated security test execution using test execution engine embedded in the test beds and scalable to large-scale IoT systems.
- Define compliance test suite to ensure interoperability between IoT systems and connected Plug'n'Play smart objects.

Security Certification

Certification: “A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system” from NIST SP 800-37

Security Certification in IoT

Security certification in IoT is used to ensure that a product satisfies the required security requirements, which can be both proprietary requirements (i.e., defined by a company for their specific products) and market requirements (i.e., defined in procurement specifications or market standards). In the latter case, these requirements are also defined to support security interoperability. For example, to ensure that two products are able to mutually authenticate or to exchange secure messages.

Security certification has a long history in the defense domain, but could it be applied to Internet of Things ?

There are some know issues in security certification, which are particularly important for IoT.

Known issues for Security Certification with Common Criteria

Issues	Source
Point in time certification. CC certificates a particular version of the product in certain configurations. Any changes to the configuration or any updates to the product that affect the Target of Evaluation (TOE), which is the part of the product that is evaluated, invalidate the certification. This is not a desirable situation, given that products evolve and are updated at a frantic pace and the certification must not be frozen to a specific version of the product.	(Kaluvuri 2014)
The above discussion should have shown how the Common Criteria are not well matched to the needs of the control systems world. At the technical level, a security certification scheme must be able to cope with dynamic systems, dynamic threats and real users working in real organizations. It must complement, rather than conflict with, existing safety certification mechanisms.	(Anderson 2009)
Common Criteria fail to deal satisfactorily with systems that are patched frequently, as operating systems now are; observers of the operating-system patching cycle and vulnerability scene have come to the conclusion that the Common Criteria are no more than a bureaucratic exercise whose costs far outweigh the benefits.	(Anderson 2009)
It is an open question if existing applications might continue running on top of certified, and properly modified of course, products. Assessments should take place to this direction. Re-writing existing application will prove to be a big challenge.	(ENISA 2014)
Re-certification after changes being made in the product is not mandatory, but should be considered case by case.	(ENISA 2014)

ARMOUR approach to address security certification issues in IoT:

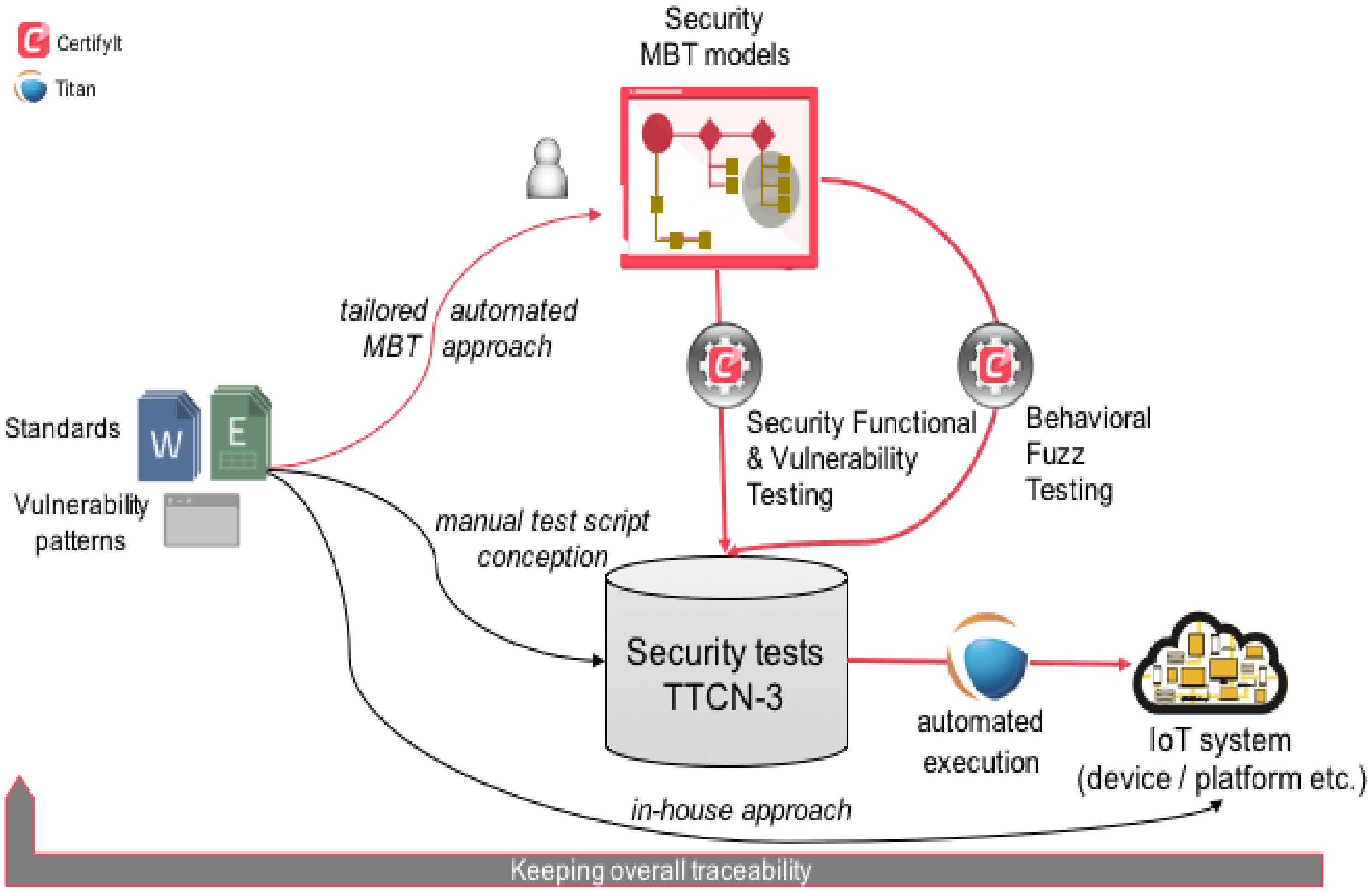
1. Identification of IoT security vulnerability patterns

2. Use of Model Based Testing (MBT)

3. Testing and Test Control Notation (TTCN) v3 language to support security certification for IoT devices

4. Post certification monitoring and action with a Policy based management framework

MBT and TTCN


CertifyIt
Titan
Security
MBT models
tailored
MBT
automated
approach
Standards
Vulnerability
patterns
Security Functional
& Vulnerability
Testing
Behavioral
Fuzz
Testing
manual test script
conception
Security tests
TTCN-3
automated
execution
IoT system
(device / platform etc.)
in-house approach
Keeping overall traceability

Policy Based Management to complement IoT Security Certification

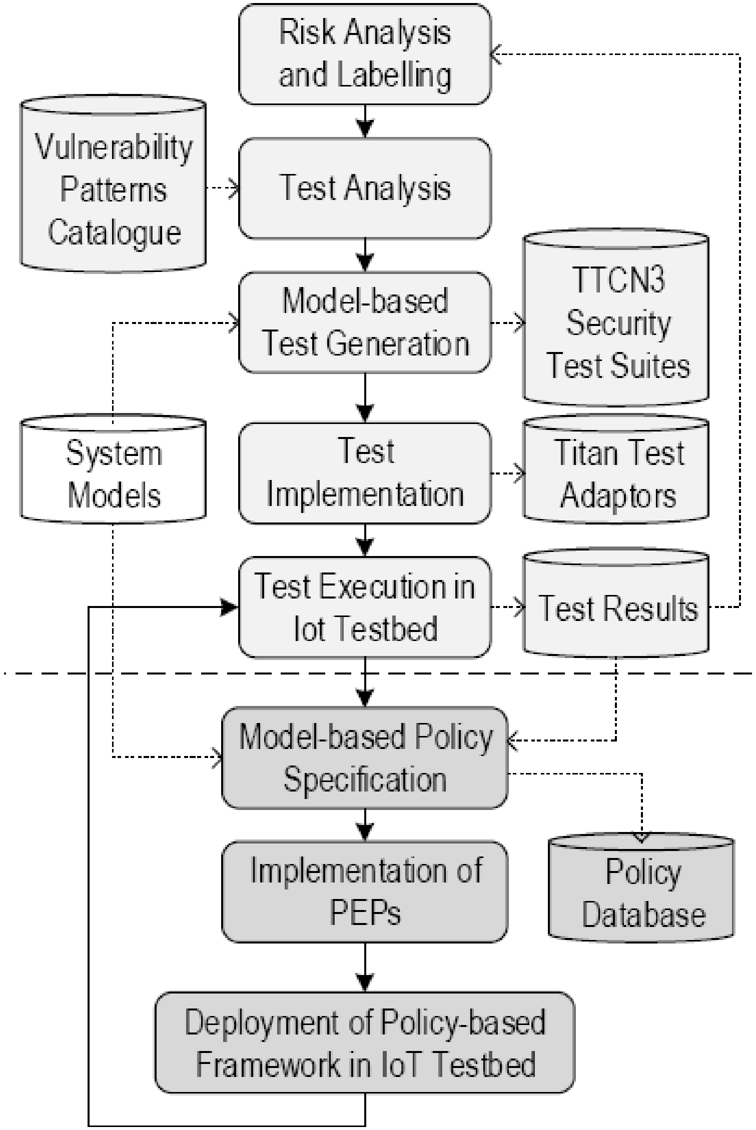
Static Security certification with MBT/TTCN is an important element to build trust in IoT products/systems/applications but would it be enough to support an adequate security coverage for IoT products and systems ?

Security IoT certification may not include the testing of zero-day vulnerabilities and threats, which were not known at the time of security certification.

In addition, IoT applications could also be composed by IoT products, which are not security certified. These products could become the vulnerability of the overall IoT application even if it is mostly built on security certified products.

A complementary (rather than alternative) approach to support IoT lifecycle of products is to introduce a post certification framework for IoT devices. In this approach, a policy based management approach is set up to collect data (management data or traffic data) and define policies, which can be used to identify and correct security threats or testing limitations.

Overall workflow for the proposed approach


Risk Analysis and Labelling
Vulnerability Patterns Catalogue
Test Analysis
Model-based Test Generation
TTCN3 Security Test Suites
System Models
Test Implementation
Titan Test Adaptors
Test Execution in Iot Testbed
Test Results
Model-based Policy Specification
Implementation of PEPs
Policy Database
Deployment of Policy-based Framework in IoT Testbed

SECKIT – Policy Based Management framework

The specification of the security policies is done using the Model-based Security Toolkit (SecKit) defined in the Horizon 2020 iCore project.

The SecKit is an integrated holistic approach for security engineering that defines a collection of metamodels for system design, including security aspects, and runtime components that instantiate these models to manage the system security using a policy-based approach. The system design model considers the structure, behavior, data types, identities, context, rules, trust relationships, threat scenarios for risk analysis, and enforceable countermeasures defined using policy rules to address the identified threats.

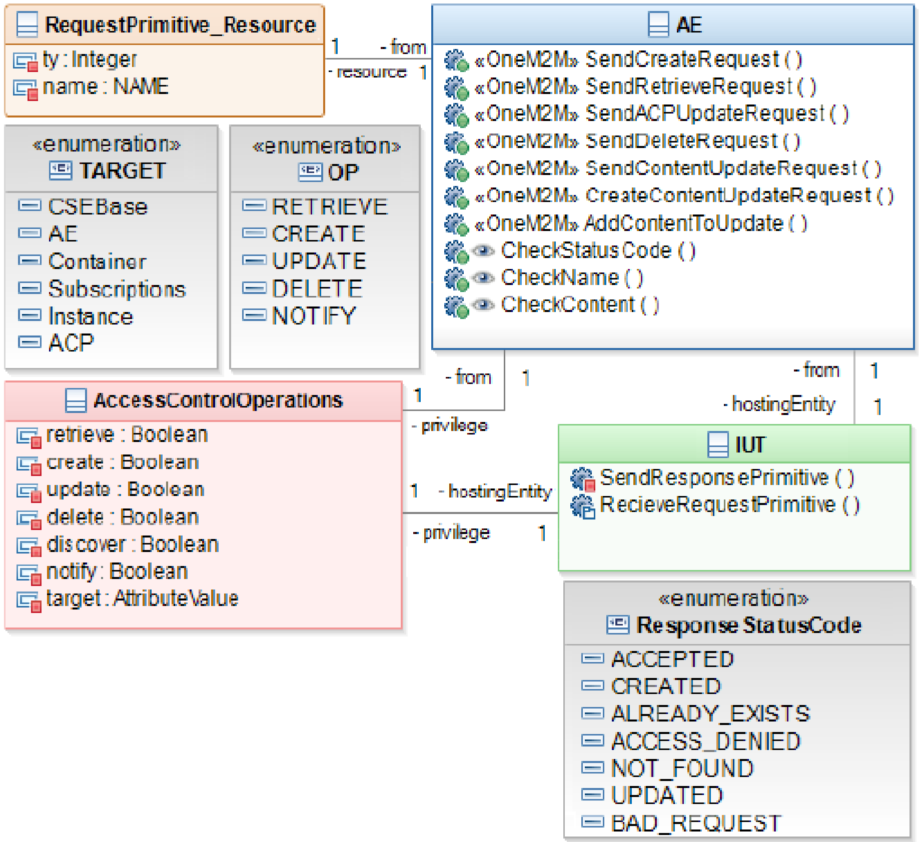
The runtime components dealing with policy rule evaluation and enforcement are respectively the Policy Decision Point (PDP), and technology specific Policy Enforcement Points (PEPs).

Policies are specified in the SecKit policy language using security mechanisms following an Event-Condition-Action (ECA) format: whenever the Event is observed and the Condition evaluates to true, the Action is executed.

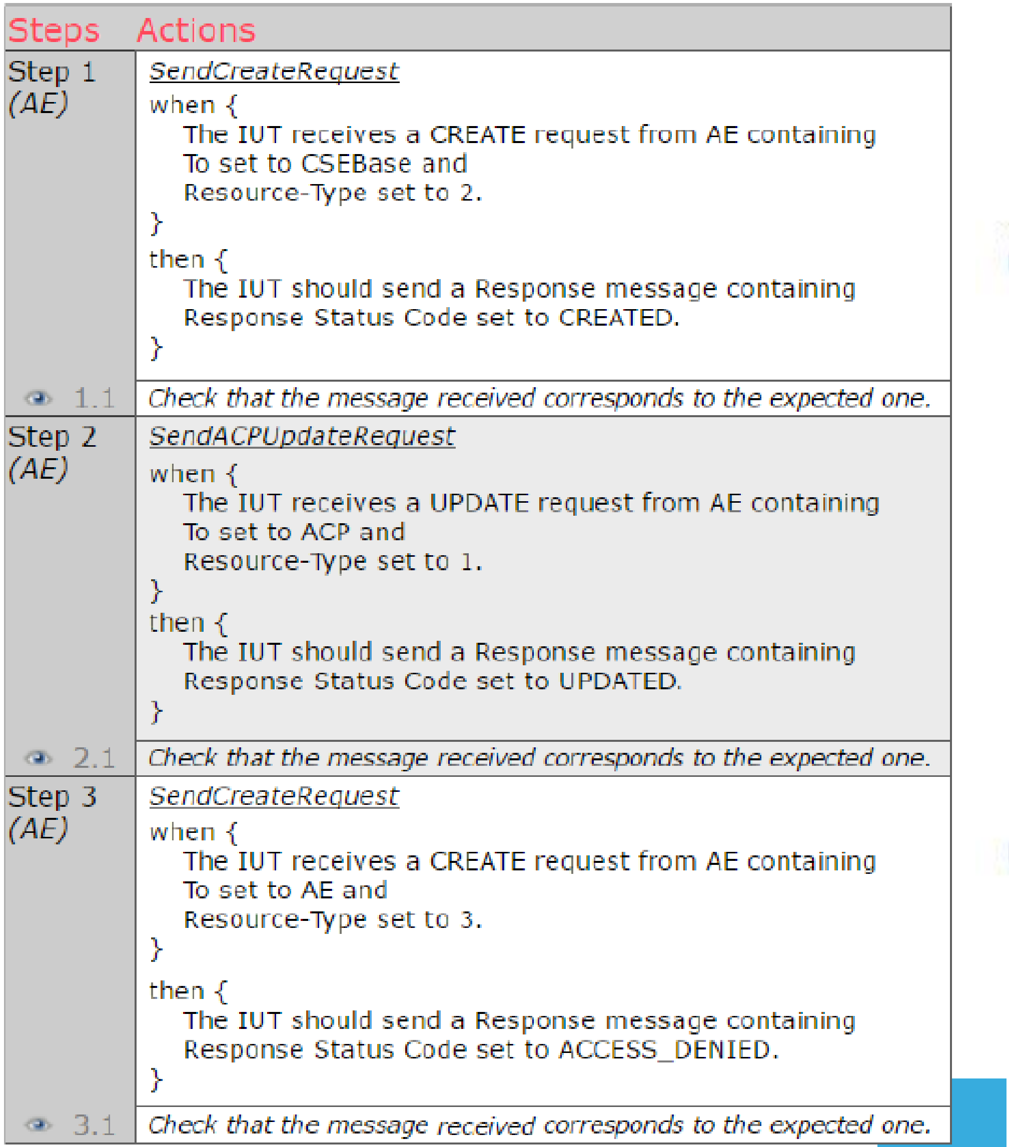
Case Study - oneM2M IoT standard.

The specification of the security policies is done using the Model-based Security Toolkit (SecKit) defined in the Horizon 2020 iCore project.

In the oneM2M specification the authorization function is responsible for controlling access to services and data to authenticate entities according to the provisioned security policies and assigned roles. Security policies are defined as sets of conditions that regulate whether entities are allowed access to a protected resource.



Test steps



Steps	Actions

Step 1
(AE)
	SendCreateRequest
	when {
	The IUT receives a CREATE request from AE containing
	To set to CSEBase and
	Resource-Type set to 2.
	}
	then {
	The IUT should send a Response message containing
	Response Status Code set to CREATED.
	}

1.1	*Check that the message received corresponds to the expected one.*

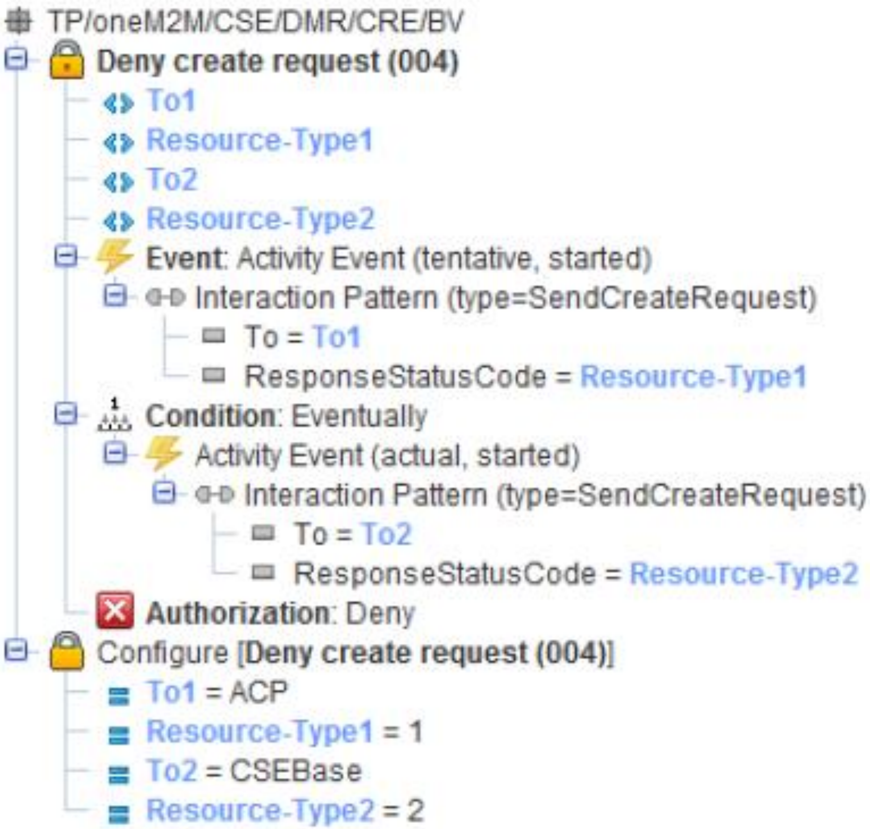
Step 2
(AE)
	SendACPUpdateRequest
	when {
	The IUT receives a UPDATE request from AE containing
	To set to ACP and
	Resource-Type set to 1.
	}
	then {
	The IUT should send a Response message containing
	Response Status Code set to UPDATED.
	}

2.1	*Check that the message received corresponds to the expected one.*

Step 3
(AE)
	SendCreateRequest
	when {
	The IUT receives a CREATE request from AE containing
	To set to AE and
	Resource-Type set to 3.
	}
	then {
	The IUT should send a Response message containing
	Response Status Code set to ACCESS_DENIED.
	}

3.1	*Check that the message received corresponds to the expected one.*

Security Policy



- TP/oneM2M/CSE/DMR/CRE/BV
  - **Deny create request (004)**
    - To1
    - Resource-Type1
    - To2
    - Resource-Type2
    - **Event**: Activity Event (tentative, started)
      - Interaction Pattern (type=SendCreateRequest)
        - To = To1
        - ResponseStatusCode = Resource-Type1
    - **Condition**: Eventually
      - Activity Event (actual, started)
        - Interaction Pattern (type=SendCreateRequest)
          - To = To2
          - ResponseStatusCode = Resource-Type2
    - **Authorization**: Deny
  - Configure [**Deny create request (004)**]
    - To1 = ACP
    - Resource-Type1 = 1
    - To2 = CSEBase
    - Resource-Type2 = 2

Conclusions:

- A new approach is proposed to address the limitations of static security certification.
- A Policy based Management toolkit is used to complement a MBT/TTCNv3 based testing.
- The approach is applied to a case study for access control in a M2M scenario.
- Future developments will address larger case studies and IoT systems

Thank you for your attention.

Joint Research Centre (JRC)
Web: www.jrc.ec.europa.eu