

# Certification of Open Source Software: Foundations, methods and tools

Towards a FP7 Project Proposal

OpenCert 2009

ETAPS - York  
28 March, 2009

# The OpenCert Initiative

[opencert.iist.unu.edu/](http://opencert.iist.unu.edu/)

- Informal network of people from Academia and Industry interested in strengthen the role of open source software and applying FM to its certification
- Discuss on long-term the creation of an international certification authority for open source software, possibly under the umbrella of the United Nations
- Organise the OpenCert Workshops: 2007 (ETAPS, Braga), 2008 (OSS, Milan), 2009 (ETAPS, York)

born at



UNITED NATIONS  
UNIVERSITY

**UNU-IIST**

International Institute for  
Software Technology

# The challenge of Open Source Software

- proved to be popular and **successful over the years** due to its **reliability** and **efficiency**
- high **reputation** of being reliable and cost-effective
- warranty of **technological independence**
- confidence that the open source community could deliver **much more**
- peculiar **development process**

However ...

# The challenge of Open Source Software

- proved to be popular and **successful over the years** due to its **reliability** and **efficiency**
- high **reputation** of being reliable and cost-effective
- warranty of **technological independence**
- confidence that the open source community could deliver **much more**
- peculiar **development process**

However ...

## OSS development weaknesses

It is hard to **objectively assess** the quality of OSS, because

- lack of **standards and methods** to assess the quality of OSS
- and the specific characteristics of OSS **development model**
- OSS projects are **hard to control and to predict** due the lack of central management
- OSS development still falls short of requirements for security and safety-critical systems
- overall quality **depends heavily on the skills and motivation** of the user-developer community
- world-wide code inspection vs intruders

This makes the use of OSS, and its integration within industrial-strength applications, with stringent security requirements, a risk

## OSS development weaknesses

It is hard to **objectively assess** the quality of OSS, because

- lack of **standards and methods** to assess the quality of OSS
- and the specific characteristics of OSS **development model**
- OSS projects are **hard to control and to predict** due the lack of central management
- OSS development still **falls short of requirements for security** and safety-critical systems
- overall quality **depends heavily on the skills and motivation** of the user-developer community
- world-wide code inspection vs intruders

This makes the use of OSS, and its integration within industrial-strength applications, with stringent security requirements, a risk

# Certification of OSS?

*The answer is yes.  
But could you please repeat the question?*

(Woody Allen, 1985)

# Certification of OSS?

*The answer is yes.  
But could you please repeat the question?*

(Woody Allen, 1985)

## Project Goal

To significantly **reduce the risks** involved in using OSS by providing a certification standard for OSS, suitably supported by specific quality assessment, validation and verification methods and technologies.

To **strengthen the role** of open source software in the European IT sector.

# Objectives

- To develop new (and to scale up existing) techniques for **program understanding**, **code analysis**, **software validation** and **formal verification**, and to combine them for quality assessment of open source code.
- To integrate, in a smooth but effective way, such techniques into the OSS peculiar, but quite successful, development process without disturbing its collaborative, distributed and heterogeneous character.

# Objectives

- To propose suitable standards and an independent certification process for OSS, addressing both **functional** and **security** issues.
  - A *quality classification scheme*
  - (in the long term) a *certification authority for OSS*

# Strategy

- Adopt a **problem-driven structure**, identifying, from the outset, a number of case-studies placed by leading IT companies for which reducing the risk associated to OSS components in their own solutions is a major concern.
- Such case-studies will drive the choice of techniques to be developed, provide test data and contribute to the definition of proposals for certification standards and the implementation of the corresponding processes.

# Strategy

- Integration of techniques from four areas, usually applied in isolation: *certification* (at both functional and security levels), *program understanding*, *validation* and *formal verification*.
- Render the project results close to the OSS developing community, in order to get feedback and pave the way for an effective impact of this research effort. A possibility will be to develop and animate an online infrastructure — the **Certification Portal** — in which independently developed analysis and visualisation tools can be inserted and used.

## Context

### Call 5, Objective ICT-2009.1.2

- Reference to OSS: *Objective ICT-2009.1.2* oriented towards the **Internet of Services, Software and Virtualisation**. OSS is mentioned explicitly in target outcome b) (Highly Innovative Service / Software Engineering):

Methods, tools and approaches specifically supporting the development, deployment and evolution of open source software. Investigation into the use of open source approaches for improving service engineering, deployment, management, evolution and take-up.

## Context

### Call 5, Objective ICT-2009.1.2

- The envisaged contribution of OSS, in this specific (but quite broad) context, makes sense if a suitable certification discipline and practice is put forward. This requires, for OSS, the development of
    - Verification and validation methods, tools and techniques assuring the quality of open, large-scale, dynamic service systems without fixed system boundaries, addressing the complete service and software life cycle.
- which is also listed as a main issue in target outcome b).

# Partners

## ... from industry

- MULTICERT, Portugal.

Extensive experience in OSS development and integration, specially in tailored security-related big projects: **electronic postmarking**, **electronic voting**, *digital certification* and OSS security solutions, used in several key projects, namely in the Portuguese Citizen Card, Electronic Passport and Residence Permit.

- Italian Telecom

- ...

## ... from academia

- MINHO UNIVERSITY (PT)

- UNU-IIST (Macau)

- ...

## To do list ...

- Title and acronym
- Refine strategy (cf objective ICT-2009.1.2 is related to the web and services) ...
- Fix consortium
- Start with challenging OSS problems from industry, not just a new research agenda
- Dimension: 6 to 15 participants (minimum 3); 1 to 4 MEuro
- **Deadline: 3 November 2009**