Project Acronym: CUMULUS
Project Title: Certification infrastrUcture for MUlti-Layer cloUd Services
Call identifier: FP7-ICT-2011-8
Grant agreement no.: 318580
Starting date: 1st October 2012
Ending date: 30th September 2015

D7.9 Second Advisory Board Report

AUTHOR(S): R. Menicocci (FUB)
REVIEWER(S): B. Sapio (FUB), M. Junk (IFX), C. Ardagna (UMIL)

Date: 25 July 2014

Summary

Executive Summary **4**
1. Introduction **5**
2. CUMULUS Advisory Board **5**
3. Second Advisory Board meeting **6**
3.1. Organization *6*
3.2. Execution *6*
3.3. Conclusions *6*
Appendix A **8**
Appendix B **10**
Appendix C **14**

List of Tables

Table 1 – CUMULUS AB Members........ 5

Executive Summary

This document reports on organization, execution, and results of the second Advisory Board meeting.

1. Introduction

The objective of deliverable D7.9 is to provide an updated description of CUMULUS Advisory Board (AB) activities, including the results from the second Advisory Board meeting (AB2) held in June 2014.

Chapter 2 briefly introduces the main facts about the CUMULUS AB.

Chapter 3 shortly describes the AB2 agenda and execution and provides the main outputs from the relevant discussions.

Appendix A introduces the AB members who attended at least one of the AB meetings held so far.

Appendix B provides additional information about AB2.

Appendix C reports the joint final comments produced by the advisors attending AB2.

2. CUMULUS Advisory Board

Here we recall the main facts about the CUMULUS AB (refers to D7.8 First Advisory Board Report M12→M13 for full details).

The AB is constituted by 7 international experts representing some of the CUMULUS stakeholders (see the table below).

The AB is coordinated by Massimiliano Orazi (AB Chair, Fondazione Ugo Bordoni (FUB)).

The Consortium meets the AB once per year, to update the advisors on the project progress and receive feedback from them to guide about the ongoing work. The advisors are also included in CUMULUS newsletter mailing list to keep them updated on the project progress.

AB member	Organization	Role	Country	AB Meeting Attendance
Massimo Banzi	Telecom Italia	Industry	IT	AB1, AB2
Michele Bezzi	SAP	Industry	FR	AB1, AB2
Goetz Philip Brasche	Huawei Technologies (Microsoft, at AB1 time)	Industry	DE	AB1
Giacinto Dammicco	Organismo per la certificazione della sicurezza in Italia (OCSI)	Government	IT	AB1
Fabio Martinelli	CNR	Academia	IT	AB1
Siani Pearson	Hewlett Packard	Industry	UK	AB1, AB2
Gunnar Peterson	Artecgroup	Industry	USA	

Table 1 – CUMULUS AB Members

3. Second Advisory Board meeting

In this Section we report the main facts about organization, execution, and outcomes of AB2. Some more details are given in the Appendices.

3.1. Organization

In order to reduce travel costs and maximize CUMULUS Consortium attendance to AB2, we scheduled AB2 in conjunction with a CUMULUS General Meeting. Based also on the availability of advisors, we finally fixed June 4th, 2014 (General Meeting fixed on June 2nd and 3rd, 2014).

FUB (in charge of AB chairing) took care of travels and hotel reservations for the advisors. We organized a social dinner to welcome the advisors.

At the end, we expected to have four advisors attending AB2.

3.2. Execution

AB2 took place in Gargnano (Italy, UMIL historical palace).

Three advisors and eight representatives of CUMULUS partners attended AB2. Notice that 1) at the last minute, one of the advisors communicated he was no longer able to attend, 2) one of the advisors was only able to attend by a Skype audio-video connection, and 3) since the official AB Chair was not able to attend, the role was delegated to the Project Coordinator (PCO).

The main objective of AB2 was to provide the advisors with a view of CUMULUS progress since AB1 (October, 10th, 2013) and this was reflected in the final agenda (see Appendix B).

According to the agenda, the PCO welcomed the AB members and opened the meeting. Then, the Scientific-Technical Coordinator (STCO) gave a general description of the CUMULUS developments covering the current approaches to certification (meta-model, consistent models, and TPM exploitation), engineering support, and validation. Specific presentations gave further details about the aspects introduced by the STCO.

The main references for the presented materials are as follows:

- D2.3 Certification models v.2 (M20);
- D4.2 Tools supporting CUMULUS-aware engineering process v1 - Technical Annex (M20);
- D6.2 Specification of CUMULUS evaluation criteria (M18).

Several interesting aspects connected with the given presentations were discussed with the advisors (see Appendix B and next section). The advisors were also invited to provide their positions about further developments of several specific concepts related to next deliverables (especially, D2.4 Final CUMULUS certification models (M32)).

3.3. Conclusions

At the end of the meeting, the advisors provided some final comments and suggestions (see Appendix C), which are summarized in the following:

- A significant and appreciable general progress has been made since last year;
    - The CUMULUS framework is actually going on in the direction of demonstrating the original project ideas;

- The CUMULUS certification approach fits well within the challenges of cloud-based scenarios, provided that the complexity of the solutions to be realized is adequate for their real usage;
    - Since services are very dynamic and certification may be part of the relevant usage contract, the proposed certification solutions should be very dynamic as well as not to produce unwilled constraints. This aspect should be analyzed in the pilot scenarios in order to possibly identify relevant requirements;
- The consortium should develop a couple of usage/business scenarios where assumptions, stakeholders and technical and business roles are described;
- The consortium should try to align the project outputs with external developments for the cloud domain.

The consortium will take into account the suggestions from the advisors for the next project activities. The third Advisory Board meeting will tentatively take place in June 2015.

Appendix A

Massimo Banzi's research interests span open source software, configuration management and cloud services. He is currently involved with a number of R&D activities in Telecom Italia related to the company public cloud offer. He represents Telecom Italia in the telecommunication industry Technical Management Forum (TMF) on Cloud Services. ***[Massimo attended both AB1 and AB2.]***

Michele Bezzi is a Research Manager at SAP in the Product Security Research team. He received his Master Degree in Physics from the Univ. of Florence in 1994 and his Ph.D. in Physics from the University of Bologna in 1998. He has 10+ years' experience in industrial research. He previously has been contributing to various European projects, (e.g., Assert4SOA, SecCord, Primelife, TAS3, SpikeForce, SensoPac) and he has published 40+ referred papers in various research areas: security, privacy, pervasive computing, neural networks, evolutionary models, complex systems. ***[Michele attended both AB1 and AB2.]***

Goetz P. Brasche is responsible for Microsoft's Cloud Computing Research engagements in EMEA*. He co-founded the European Microsoft Innovation Center (EMIC) which started operations in Aachen in May 2003. Dr. Brasche also initiated the establishment of the Microsoft Embedded Systems Development Center at EMIC in the beginning of 2008 to facilitate an integrated R&D approach of Microsoft in Europe. He represents Microsoft in the Joint Undertaking ARTEMIS where he is on the Steering Board and co-chairs the Chamber of industry members. In his prior roles at EMIC as Director Embedded Systems R&D and Program Director, he was in charge of EMIC's collaborative R&D activities in the fields of »embedded and mobile computing« and EMIC's overall research program management. Dr. Brasche holds a master's degree in Computer Science with a minor in Business Administration and a Ph.D. in Electrical Engineering. He joined Microsoft in May 2003 from Ericsson as Director of Ericsson's partner program for Central Europe which aimed to foster the mobile Internet market through evaluation, design and marketing of promising mobile application and solutions. At Ericsson he was also involved in sales of solutions for the emerging Universal Mobile Telecommunications Systems (UMTS). While at the Ericsson Eurolab Germany, one of Ericsson's major European research centers, he played a decisive role in the development and standardization of mobile communications systems and was in charge of the pilot implementation of one of the first world-wide General Packet Radio Service (GPRS) networks. As research assistant in the Department of Communication Networks at RWTH Aachen University, Dr. Brasche explored various aspects of embedded systems and mobile Internet as early as 1992. In particular, he looked into packet oriented speech and data services for existing and future mobile networks. His numerous publications prove he is knowledgeable in innovation management and embedded mobile communications technologies. The European Microsoft Innovation Center works on collaborative information technology projects that capitalize on Europe's established technology strength and reflect the region's priorities. Working together with academic institutions and industry partners, EMIC concentrates its efforts on software productivity tools, cloud computing technologies, and mobile and embedded systems. An ideal environment for Dr. Brasche to realize his vision of a customer-oriented, open R&D that considerably improves research efficiency and leads to utilizable technology rather than producing dust catchers for the archives. ***[*Goetz is now with Huawei Technologies. Goetz attended AB1.]***

Giacinto Dammicco is a member of the Italian Certification Body of ICT Security (OCSI). Graduated in Electronic Engineering, he has worked for several years as a researcher at the FUB, mainly in the planning and optimization of broadband access networks, producing numerous reports presented at conferences and published in international scientific journals. He also participated in European projects RACE and COST and is member of ASSERT4SOA Advisory Board. Since 2000, he carries out activities in the field of evaluation and certification of ICT security and is member of the Italian Certification Body of ICT Security (OCSI). In this area, he participates in international working groups of the mutual recognition arrangements CCRA and SOGIS. ***[Giacinto attended AB1.]***

Fabio Martinelli, is a senior researcher of Institute of Informatics and Telematics (IIT) of the Italian National Research Council (CNR) and He currently leads the interdepartmental security project of the CNR. He is co-author of more than one hundred of papers on international journals and conference/workshop proceedings. His main research interests involve security and privacy in distributed and mobile systems and foundations of security and trust. He usually teaches at graduate level courses in information security. He founded and chaired the WG on security and trust management (STM) of the European Research Consortium in Informatics and Mathematics (ERCIM) and He is involved in several Steering Committees of international WGs and/or Conferences/workshops. He usually manages R&D projects on information and communication security and he is/has been involved with several roles (including th ecoordinator) in the following FP6-FP7 projects: ANIKETOS, ARTIST2, BIONETS, CONNECT, CONTRAIL, CONSEQUENCE, GRIDtrust, NESSoS, S3MS, SENSORIA. ***[Massimo attended AB1.]***

Siani Pearson is a principal research scientist in the Security and Cloud Lab, at HP Labs Bristol, which is HP's European long term applied research centre. Her current research focuses on accountability, privacy and the cloud and she holds over 50 patents and is author or co-author of well over 100 papers and technical reports in these fields. Siani received an MA from Oxford University in logic, a PhD in artificial intelligence from the University of Edinburgh and was a Research Fellow at Cambridge University before joining HP in 1994. She is a Fellow of the British Computer Society, senior member of IEEE, a Certified Information Privacy Professional/Information Technology, CCSK certified and Vice President of the UK Chapter of the Cloud Security Alliance. She has been editor and co-author of books on Trusted Computing and on Privacy and Security for Cloud Computing, and is associate editor for journals on trust management and on cloud computing. Siani is currently the scientific lead of a major European research project on Accountability for the Cloud (A4Cloud) and is a member of: the steering committees of CSA GRC Stack and IFIP TM 2013; HP Privacy and Data Protection Board; HP security forum; HP cloud security WG; CSA Privacy WG; CSA OCF WG; IEEE Transactions on Cloud Computing Editorial Board; numerous programme committees, including being Program Chair of IEEE CloudCom 2013; the advisory boards of several universities and EU projects. ***[Siani attended both AB1 and AB2.]***

Appendix B

We provide the list of AB2 attendees and a summary of both the given presentations and the relevant discussions.

CUMULUS Consortium	
Rodrigo Diaz (RD)	ATOS SPAIN SA (ATOS)
George Spanoudakis (GS)	CITY UNIVERSITY (CITY)
Renato Menicocci (RM)	FONDAZIONE UGO BORDONI (FUB)
Bartolomeo Sapio (BS)	FONDAZIONE UGO BORDONI (FUB)
Matthias Junk (MJ)	INFINEON TECHNOLOGIES AG (IFX)
Claudio Ardagna (CA)	UNIVERSITÀ DEGLI STUDI DI MILANO (UMIL)
Ernesto Damiani (ED)	UNIVERSITÀ DEGLI STUDI DI MILANO (UMIL)
Francesco Zavatarelli (FZ)	UNIVERSITÀ DEGLI STUDI DI MILANO (UMIL)
CUMULUS Advisory Board	
Massimo Banzi (MBa)	TELECOM ITALIA
Michele Bezzi (MBe)	SAP
Siani Pearson (SP)	HP

The actual agenda was as follows:

- 09:00-09:05 Welcome (B. Sapio (BS), PCO, FUB)
- 09:05-09:20 Overview of project state (G. Spanoudakis (GS), STCO, CITY)
- 09:20-10:00 Scenarios (R. Diaz (RD), ATOS)
- 10:00-10:45 Test based and multi layer certification models (E. Damiani (ED), UMIL)
- 10:45-11:15 *Coffee break*
- 11:15-11:45 Monitoring based and hybrid certification models (G. Spanoudakis (GS), STCO, CITY)
- 11:45-12.30 TPM enabled certification (M. Junk (MJ), IFX)
- 12:30-13:30 Discussion (G. Spanoudakis (GS), STCO, CITY)
- 13:30-14:30 *Lunch*

Overview of project state (GS)

GS introduced the last project developments and reported the main progresses related to the current CUMULUS work (meta-model, basic and advanced certification models, infrastructure, and validation). Apart from some questions clearly related to next presentations (the answers to which were suitably postponed),

- MBe asked about the concept of *Context* included in the CUMULUS meta-model
    - GS explained that Context potentially refers to everything useful to clarify both conditions and assumptions under which the certification process is executed, so that Context provides a reference for the validity of a certificate. For example, Context could include the configuration of the CUMULUS infrastructure;
- SP asked about the current initiatives related to standardization
    - GS announced that CUMULUS is taking over responsibility of a workshop from the CIRRUS project, with the aim of producing recommendations towards ISO 27K.

Scenarios (RD)

RD introduced the pilot scenarios and reported the main development progresses towards their integration within the CUMULUS framework and the consequent validation.

- SP asked for details about CUMULUS roles/actions/support connected to definition/selection and certification of service security properties, especially for pilot scenarios
    - <u>Definition/selection of security properties.</u> RD reported that, for the pilot scenarios, we have manually selected some security properties from the project security property vocabulary. ED added that we have not only selected the security properties but also interpreted and mapped these to service mechanisms. In a real CUMULUS context, we could expect the relevant certification authorities to provide the operational definition of security properties and a service provider to select the security properties to be certified. GS noticed that, in some contexts (like the e-health one), there could be regulation requirements or company policies referring to other security properties. CUMULUS could take this into account by treating the relevant vocabulary as a parameter. He observed that, anyway, providing the relevant certification authorities with automatic tools for the above interpretation and mapping of security properties appears to be too complex;
    - <u>Certification of security properties.</u> RD reported that, for the pilot scenarios, the experimental certification will be done by the CUMULUS framework. ED explained that, in a CUMULUS aware context, the CUMULUS framework could be operated according to several models (under study), including the basic one where an on-line certification authority controls every operation;
- MBe asked for some clarifications about CUMULUS roles/actions connected to certification of service security properties and certificate validity/lifecycle
    - <u>Certification of service security properties.</u> GS clarified that in a real CUMULUS context, the relevant framework could also be used, by a service provider, for self-certification;
    - <u>Certificate validity/lifecycle.</u> GS explained that the certificate produced by the CUMULUS framework could be delivered (and managed) in several ways, also depending on the certificate lifecycle. GS also reported that the framework could execute some certificate validity checks (according to lifecycle specifications), eventually based on TPM proofs, and notify changes to customers;
- MBa asked for some clarifications about the deployments of pilot scenarios

  - RD clarified that real deployments and not only lab ones are used.

Test based and multi layer certification models (ED)

ED reported the last results about the concept of test based certification in CUMULUS. Apart from general comments from advisors (included in the final comments given in Appendix C), there was a specific fruitful discussion, launched by ED, about the approach to be taken to specify the (certificate) lifecycle.

- SP observed that, in order to reach business approval, lifecycle specification should be expressed in simple and significant terms. SP also observed that leaving distinct basic certification models to adopt distinct lifecycle semantics could arise problems (e.g., for the generation of hybrid certification models from the basic ones);
- ED proposed to look for a satisfactory approach can be defined where the users are provided with common simple views of the certificate lifecycle while the needed peculiarities are preserved;
- GS noticed that the concept of external and internal (hidden) state could be used for the lifecycle definition. GS also noticed that, for the definition of external states, both usability and legal requirements could apply;
- ED noticed that a clear visualization of the certificate status could be requested for usability;
- MJ added that, since clear visualization would strictly depend on the specific customer, aspects of this kind are probably out of scope;
- SP suggested to explore the approach where simple views are provided to users along with the possibility of accessing on demand the relevant details about the certificate lifecycle.

Monitoring based and hybrid certification models (GS)

GS reported the last results about the concept of monitoring based certification in CUMULUS, covering also the concept of hybrid certification models including monitoring based evidence. No specific questions came from the advisors, who appreciated the clarity of the presentation.

TPM enabled certification (MJ)

MJ gave an introduction to TPM functionalities and their possible exploitation within CUMULUS. Apart from general questions related to TPM concept and functionalities and general comments from advisors (included in the final comments given in Appendix C),

- SP asked about the connection between testing/monitoring and TPM proofs;
  - MJ answered that TPM proofs finally refers to the integrity of the components supporting the certification activities (these components can possibly be located at both the CUMULUS framework and the provider end);
- SP then asked about the connection between the security properties of the pilot scenarios and TPM;
  - MJ answered that many security properties can benefit from the integrity support offered by TPM;
- SP suggested to analyze cost/advantages for the cloud/service provider to adopt TPM concepts and said that TPM support to certification based on testing/monitoring could be a significant enhancement in the cloud context;
- MBe stressed that the general TPM connection to system integrity should be refined and made more concrete with examples in real world scenarios.

Discussion (GS)

Apart from general comments from advisors (included in the final comments given in Appendix C), there was a general fruitful discussion, launched by GS, about the importance of security certification. MBa was not able to attend part of this final discussion (anyway, his recommendations are included in the final comments given in Appendix C).

- SP reported that the importance of security certification is generally growing, especially for small providers, who cannot rely on some kind of implicit reputation as the big providers (sometimes) can. SP added that security certification is now viewed as clearly related to (and needed for) user service/product acceptance. SP also reported that the concept of provider transparency is getting more important;
- GS noticed that costs are stopping small providers to accept security certification and asked what a reasonable cost could be;
- MBe answered that this depends on the potential revenue of security certification (not so easy to give explicit figures). MBe also said that, in the future, service/product selection could be based on user requirements (cloud provider offer could include different kind of certified services). MBe observed that, for cloud providers, it would be very important to have the possibility of building additional certifications on previous ones;
- GS asked about both the importance of security certification in HP and SAP (MBa was no longer attending the meeting) and if HP and SAP would use security certification even in the absence of regulatory requirements;
- SP reported that HP is an early adopter of security certification (it was the first to execute a CSA self-assessment) and that, for the cloud context, HP would use security certifications even though no regulations enforced that;
- MBe reported that, in SAP, even though security certification is not so important at the moment, it is expected to become that in the near future.

Appendix C

The advisors attending AB2 provided the following final joint comments:

We believe that the concepts and technology of CUMULUS are very relevant for helping address security issues in the cloud. We appreciate the significant progress made since last year, and how the CUMULUS platform is progressing to start to put its pieces together, and demonstrate the original ideas of the project.

The dynamicity of the approach, in particular the Monitoring Certificates, and the usage of Trusted Platform Modules to increase trust, fit well with the challenges of cloud-based scenarios. However, care should be taken that the solutions and the certification processes proposed do not get too complex for real world usage, where services need to be more and more fast, dynamic, easily reconfigured and, since certification may be part of the contract, it is important to keep it as dynamic as the service itself (at least) not to produce unwilled constraints. All these aspects should be tested and improved during the pilots, which may clarify requirements in this regard.

The possibility of having "modular" certification, in which different types of certificates are combined (e.g., a platform certificate issued to the platform provider with one obtained by the service provider) and fast incremental certification (e.g., adding some tests "on-the-fly") are of clear added value to address modern services that can be modular too, dynamically changing and provided in the cloud by multiple providers.

At this stage, we believe that it is important to well define the possible scenarios of usage of CUMULUS, both from a technology and business perspective. We suggest that the consortium develop a couple of usage/business scenarios where assumptions, stakeholders and (technical and business) roles are described. They can be based (even partly) on the existing use cases. Regarding the use cases, although these are clearly relevant, they should be presented highlighting the contribution made to demonstrating CUMULUS technologies and vision. In particular, they should make explicit which parts of the CUMULUS technology will be used, and what scope that would cover. Even if the use cases will not implement all the features of CUMULUS, which is not unusual since CUMULUS is a research project that includes features that address future scenarios, it is important to stress what aspects of CUMULUS are demonstrated with the use cases, and why this is the case.

Finally, we believe that the application of these technologies should be considered and demonstrated within at least some real world scenarios, and that there should be further effort to align the outputs of the project to other external developments, particularly those that are being standardised or starting to be adopted in the cloud domain.

Massimo Banzi, Telecom Italia

Michele Bezzi, SAP Product Security Research

Siani Pearson, Hewlett-Packard Laboratories