SEVENTH FRAMEWORK PROGRAMME	***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***

D6.5 Initial Evaluation Report

AUTHORS: Antonio Álvarez (WELL), Renato Menicocci (FUB), Vittorio Bagini (FUB), Alessandro Riccardi (FUB), Rodrigo Díaz (ATOS), Marina Egea (ATOS), Maria Krotsiani (CITY), Matthias Junk (IFX), Jesús Luna (CSA)

REVIEWERS: Claudio Ardagna (UNIMI), Hristo Koshutanski (UMA)

Summary

List of Figures

List of Tables

Executive Summary

Deliverable D6.5 provides the first report on validation of the CUMULUS Framework. This report covers the first approach considering the validation from the business point of view, the suitability of CUMULUS certification models and processes with respect to users and suppliers, and the validation of the Trusted Computing Proofs within the CUMULUS Framework to check for its applicability based on a Trusted Platform Module (TPM).

1. Introduction

Deliverable D6.5 is envisaged to cover the intermediate results obtained within Task 6.3, devoted to evaluate the CUMULUS Framework. The goal is to check out that what has been made and accomplished so far can: 1) contribute to and enhance the state of the art in the field of certification of cloud services and 2) entail a big leap forward which can be leveraged in the future.

Evaluation is accomplished from different perspectives, which are covered in sections 2, 3 and 4 of this document. Each section is self-contained and starts with an introduction, continues with the explanation of the work performed, and finally gives an outlook and a description of the next steps towards the final version of the deliverable (D6.6, M36).

D6.2 presented the criteria that would be followed to perform the evaluation. These criteria come from the scenarios and requirements presented as a result of Task 6.1 and covered in D6.1. When it comes to apply these criteria, some of them were applied as they were designed, others suffered some modifications, whereas some new criteria arose, as a result of putting evaluation into practice. This is not surprising, since what is descripted in D6.2 is a first approach to such criteria.

Section 2 deals with the evaluation from the business point of view. This section and all the work related is envisaged to gather evidence of the benefits that all the stakeholders involved in the cloud business might obtain from the innovation brought by CUMULUS. It is also desired to gather evidence of the need of security placed by the market in general, what makes very appealing the possibility of adopting a product like CUMULUS to provide the required assurance. Another way to evaluate the soundness of the concept of CUMULUS is by analyzing the contribution that may make to the current landscape of certification metaframeworks. When adopting the technology brought by CUMULUS, companies must also think about the related costs in order to find out whether it makes sense to introduce CUMULUS as a way to improve the security of cloud systems and the certification of such security. This evaluation is, in consequence, mostly based on an ongoing analysis whose status is reported in this deliverable and which will be continued and matured until the end of the project.

Section 3 deals with the evaluation of the certification framework itself. Aspects like usability, representation capability, perceived security, assurance and cost effectiveness are assessed. In order to do so, people outside the consortium were involved and a session took place to collect feedback. This is a first step and from now on to the end of the project at least one more session will take place in order to collect a more detailed and mature feedback. The new version of the architecture, released in D5.3, will be an important input to carry out the collection of this new feedback. Along with this deliverable, all the material produced for this evaluation session including raw results from validators is attached as an annex. The information of this annex is **confidential**, so it is kindly requested to treat it accordingly.

Finally, section 4 deals with the validation of the Trusted Computing proofs. Since the TPM serves as a root of trust in CUMULUS, it must be properly certified so that one can rely on the TPM fulfilling all necessary security requirements. To ensure this, the Common Criteria certification is undertaken and applied to the new TPM 2.0 chip. The corresponding security evaluation of the TPM properties related to CUMULUS requirements is done within CUMULUS.

Task 6.3 will also consider the evaluation of the whole framework from the legal perspective. The result of this evaluation will be provided in the final evaluation report, in D6.6.

2. Business evaluation

D6.2 suggests some evaluation criteria to take into account to perform the validation of the framework from the business perspective, and especially focused on the application scenarios proposed in the project. Below, the criteria are reviewed and the specific application to the scenarios is discussed:

- Criterion 1: *Study which services and layers are going to be certified by CUMULUS*. This service and layers are specified in deliverables D6.3 and D6.4, related to the pilots. During year 3 new security properties will be proposed for certification as a consequence of the development of new hybrid and incremental certification models.
- Criterion 2: *Define the attributes to consider the property as 'verified'*: As it will discussed on this subsection, some widely accepted criteria need to be taken to make the certification process reliable. In response to this demand, we will follow the criteria established in *NSA protection profiles* [18][19][20] , which has been proposed within the consortium. .
- Criterion 3: *Update the service in order to interact with CUMULUS mechanisms*: Both Smart Cities and e-Health scenario have undergone some process aimed at adapting them to interact properly with the CUMULUS Framework. Besides, in order to certify security properties chosen in Criteria 1, some security mechanisms must be in place. In D6.3 and D6.4 the improvements in security that both scenarios have experienced are explained carefully.
- Criterion 4: *Evaluate risks of applying the CUMULUS Framework with respect to costs and security*: Throughout the development of WP6 we have quantified the cost of applying CUMULUS to a couple of pilot scenarios and we have considered the risks that the certification process for certain security properties entail. However, regarding the costs, we could only know them a posteriori, and, as it is stated on the section, these costs are really uncertain when it comes to calculate them in advance. The reason is that the disparity among scenarios is so big that it is really difficult to make estimations basing on previous experiences

Apart from these criteria, we propose some new ones to make the validation more complete:

- Criterion 5: *Analyze how CUMULUS can play a role in the context of certification metaframeworks*. As one of the goals of the project is to contribute to the state of the art of certification, one metric to validate the framework is to obtain convincing arguments about the contribution of CUMULUS to these certification metaframeworks [2][3][11][12][18][19].
- Criterion 6: *Offer arguments for the need of certification of security in the cloud field (including pilots domains), according to market demands*. This is about offering proofs of the market demanding such security and, in consequence, the need of such security being certified to provide assurance.
- Criterion 7: *Offer arguments proofing the benefits different stakeholders can obtain* from the application of the CUMULUS Framework in order to provide assurance about security of cloud services.

This section is structured in the following way:

- Section 2.1 intends to provide an overview on the current practices regarding the certification process, and give a first approach on the role CUMULUS might play in this field.
    - Section 2.1.1 goes through the general considerations of certification. Some key-points about specific requirements a certification process must fulfill are specified. Then, the current approach of certification to the current case of cloud computing is explained, highlighting that cloud-aimed certification can never replace more generic schemes, but rather supplement them.

  - Once a general consideration of what certification is about, and a first approach to how it is applied to cloud computing is provided, section 2.1.2 gives a high-level overview of the current landscape of metaframeworks of certification, analyzing more deeply how a couple of those metaframeworks are applied (CCM applied to CSA OCF and Security Rating Guide). For those particular metaframeworks, the process of evaluating the different cloud assets applying several criteria, and the way the final evaluation result is calculated, are explained. Once this is done, it is analyzed a first approach on how CUMULUS can play a role in the context of certification metaframeworks. This would correspond to Criterion 5. Deliverable D6.6 will cover the work carried out to evaluate CUMULUS from the point of view of this criterion.
  - Finally, once the current certification environment is explained and the likely role CUMULUS could play on it, section 2.1.3 deals with the materialization of the certification process. First, the motivations both public and private organizations may have to undergo a certification process, and the benefits it can bring to them are addressed. These motivations are good reasons clearly supporting the use of CUMULUS, moreover given the fact that can provide automation to such process. Then, some aspects like the time it takes; how the size of the organization, the scope of the certification or the previous experience shape the process; or the typical cost are discussed. Finally, the requirements a person must fulfill to offer certification services playing the role of auditor are also enumerated.

- Section 2.2 provides a set of references demonstrating first the growing demand of security services in the cloud domain and secondly, the need of certification as a way to increase the trust on cloud platform. This includes the contexts of Smart Cities and Health applications, which are particularly relevant, since those two contexts are the ones the pilots are based on. In the particular case of Smart Cities, the possibility of cyber attacks against cloud assets controlling, for instance, public lighting, could provoke blackouts in a whole city with dramatic consequences. This possibility is higher as the Internet of Things paradigm becomes more and more real. Such need of enforcing security requirements will be accompanied by the need of certification providing assurance. This could be a clear business case for CUMULUS, where the framework and infrastructure created within the project can play an important role to develop this new business model and fulfill the need of security against these likely attacks. This corresponds to Criterion 6. In the case of the eHealth, this is also a domain vulnerable to cyber attacks, and due to the critical data managed, requires the highest level of security, however, the main driver for certification in this context would be checking compliance with the legal framework. Consequently, thanks to CUMULUS we can demonstrate, first of all, that the security mechanisms required by law are in place, and secondly, that they are operating as expected.
- Section 2.3 offers a first approach to the analysis of the contribution made by CUMULUS from the point of view of the different stakeholders. Deliverable D6.6 will cover the whole analysis, corresponding to Criterion 7.
  - Section 2.3.1 deals with the business benefits CUMULUS brings to cloud certification providers
  - Section 2.3.2 discusses the impact CUMULUS might have in the activities carried out by cloud auditors.
  - Section 2.3.3 discusses the benefits CUMULUS can bring to cloud providers, along with the problems the adoption of the framework can entail.
  - Finally, section 2.3.4 discusses the vision of the insurances companies protecting the cloud service providers in case of cloud-related incidents originating damages to cloud assets.

2.1. Current practices on certification

2.1.1. General considerations

In an ENISA (European Union Agency for Network and Information Security) [1] study published in 2007 the authors define certification as *the successful conclusion of a procedure to evaluate whether or not a professional activity actually meets a set of requirements* [5]. **The main objective of certification is to inspire trust**. A certification scheme can be defined as *the collection of requirements, procedures and means available for obtaining a certificate*.

Certification often means compliance with a standard. ISO defines an official standard as follows: *document established by consensus and approved by a recognized body, that provides, for common and repeated use, rules guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context* [6]. However, *standards* can also be set de facto, by private actors. By way of illustration, the so-called 'Common Criteria' is a certification scheme where the security level of a product is evaluated according to a set of criteria defined in the international standard ISO/IEC 15408.

Certification as defined in the aforementioned ENISA study, is the final stage of a longer process. This process is usually designated with the term *conformity assessment*. During a conformity assessment a person or a body will evaluate compliance of persons, products and or processes with a given set of requirements. It is important to emphasize that 1) the evaluation and 2) the certification, are not necessarily performed by the same body [4].

Cloud computing is such a new discipline that its standardization and everything related is a tall order in progress nowadays. Included in the aforementioned standardization would be the processes aimed at the certification of the security of cloud services. Europe, in this sense, needs to catch up with other countries where certification is already a part of the cloud strategy such as USA, Singapore, Thailand, China, Hong Kong or Taiwan. They are starting to discern and pave the way to follow. The goal is to make a reliable ISMS (Information Security Management System) to come true. An ISMS is a systematic approach to managing sensitive company information so that it remains secure. It encompasses people, processes and IT systems [4]. The cloud-focused schemes tend to draw upon six existing established standards "families", namely: NIST, ISO, PCI-DSS, COBIT, ITIL and accounting-based standards. None of these six ones provides a general purpose standard for cloud computing, although **the ITU-T has developed a set of high level recommendations for cloud computing** [8]. Most certification schemes are privately run. Industry bodies have had an influential role in their development [9].

As a first step, the work previously accomplished in the field of the certification of information security certification schemes can be leveraged. This work has been developed during previous years much before the emergence of cloud computing. By means of rigorous analysis, organizations like ENISA and related work groups such as CERT-SIG have found out some of the requirements a certification scheme must fulfill when applied to cloud providers. Among others, it could be highlighted that *the certification should be voluntary, never imposed, and driven by industry; should provide the possibility of self-attestation, regardless of the issuing of certificates by an external authority; be technology neutral, be lean and affordable* (nevertheless, this criterion is rather subjective) and leverage global standards as much as possible [2]. With this input, some of the current standards are likely to be applied to the particular case of cloud computing.

The agreement on the need of certification as a key requirement to trust cloud services is clear. Nevertheless so far **the work is made separately** and there are different approaches depending on the countries, even regions within the countries, the kind of sector (public or private) or the working groups. Furthermore, some companies are represented in more than one group and the fact that there **many different approaches with a far from negligible overlap** is quite clear. Given the clear borderless character of cloud computing, it is necessary to converge step by step on a **universal certification view which is compliant with different legislations around the world and is**

inclusive, counting on both big and small companies, as it was highlighted previously. This view **cannot be composed of a single scheme** covering everything. The different security requirements have to be **grouped** properly **in different certification schemes**. This will simplify the certification process for any company, since they will be able to focus on what is really crucial for them. In [2] ENISA highlights that it should be very positive to get 1) a list of existing certification schemes and 2) a metaframework of existing certification schemes detailing the requirements covered by each scheme. This would provide more transparency to costumers and would allow them to map their detailed security requirements to the certification of a provider.

The case of public sector is quite striking. In some cases, rather than placing the security requirements for a provider to be hired in a tender, they elaborate such list of requirements basing on the input obtained by prospective contestants in those tenders. By doing this, the alignment between what providers actually offer and the expectation of the public sector representatives is much more accurate.

It is interesting to highlight ENISA point as for self-attestation. CERT-SIG lists the possibility of **self-attestation as a key principle**. Companies should have this possibility in order to make a certification scheme **affordable for smaller companies** as **no third-party audits would be necessary**. In fact, smaller provider´s circumstances seem not to be taken into account when certification processes are addressed.

Finally, it is important to stress that **cloud specific assessment should never be seen as replacements for certification processes, but a supplement**. For instance, CSA STAR certification assessment (which will be addressed on section 2.1.2) should be seen as part of an ISO 27001 assessment [11] and, in consequence, the scope of ISO 27001 certification must not be less than that of the scope of the STAR Certification.

2.1.2. Metaframeworks of certification

During year 2014, ENISA was working on the creation of a metaframework of security measures for cloud providers [2]. The framework has a tree structure shown in the figure, where there are several domains each of them containing a set of high level security objectives and, in turn, there will be a detailed set of detailed security measures, grouped in sophistication levels. These sophistication levels are necessary so as to be flexible enough to deal with different types of services and different types of customers. ENISA also highlights the importance of not considering a one-dimension rating of security. This is because security can be considered from several points of views: physical security of the infrastructure (especially at IaaS level), security from the point of view of software development or security from the point of view of human resources, to name but a few. Thus, if a one-dimension rating is employed, all these aspects are grouped when they actually need a separate treatment. This need is exactly the same for both providers and customers.

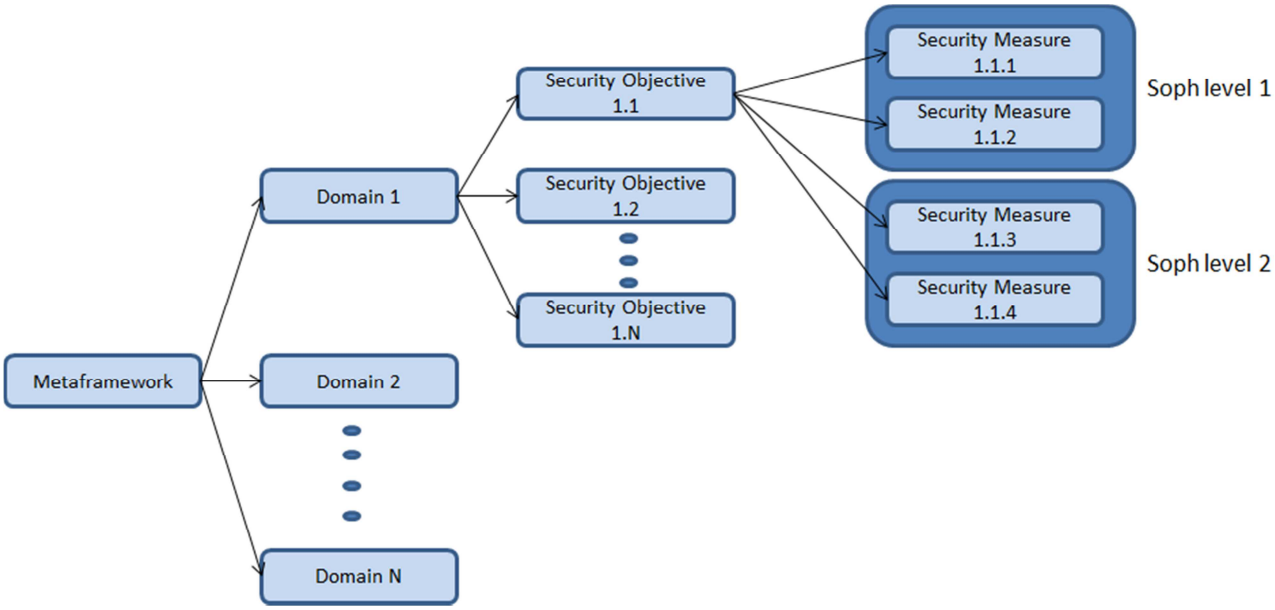

Figure 1. Framework structure

Regardless of how the certification process is set out, it must cover the core Service Level Agreements the organization has with its clients [11].

CCM applied to CSA OCF

A practical example of this kind of frameworks could be CCM (Cloud Control Matrix) [3] which is present at the three levels of the CSA OCF (CSA Open Certification Framework). CCM, in the case of v3.0.1, is a framework structured in 16 domains and composed of 133 controls, which are relevant for cloud [2]. Some of them are to be considered control objectives and others are more detailed technical requirements. The set of controls included in CCM are cloud relevant controls. These controls are also mapped against other rather generic frameworks focused on information security control, and not specifically aimed at cloud, such as ISO 27001:2005 [25], NIST SP 800-53 [26], FedRAMP [27], PCI DSS [28], COBIT v4.1 [29], AICPA Trust Principle, ENISA IAF [30] and the German BSI Cloud Security Catalogue.

Let us see the particular application example of CCM to CSA OCF. The CSA STAR Certification is a rigorous third party independent assessment of the security of a cloud provider. It leverages the requirements of the ISO/IEC 27001:2005 and the CSA CCM and is technology-neutral. It measures the capability levels of the cloud service and assigns a 'Management Capability' score to each of the CCM security domains. It is a management systems standard, which outlines the processes and procedures an organization must have in place to manage Information Security Issues in core areas of the business. The standard does not stipulate how a process should operate.

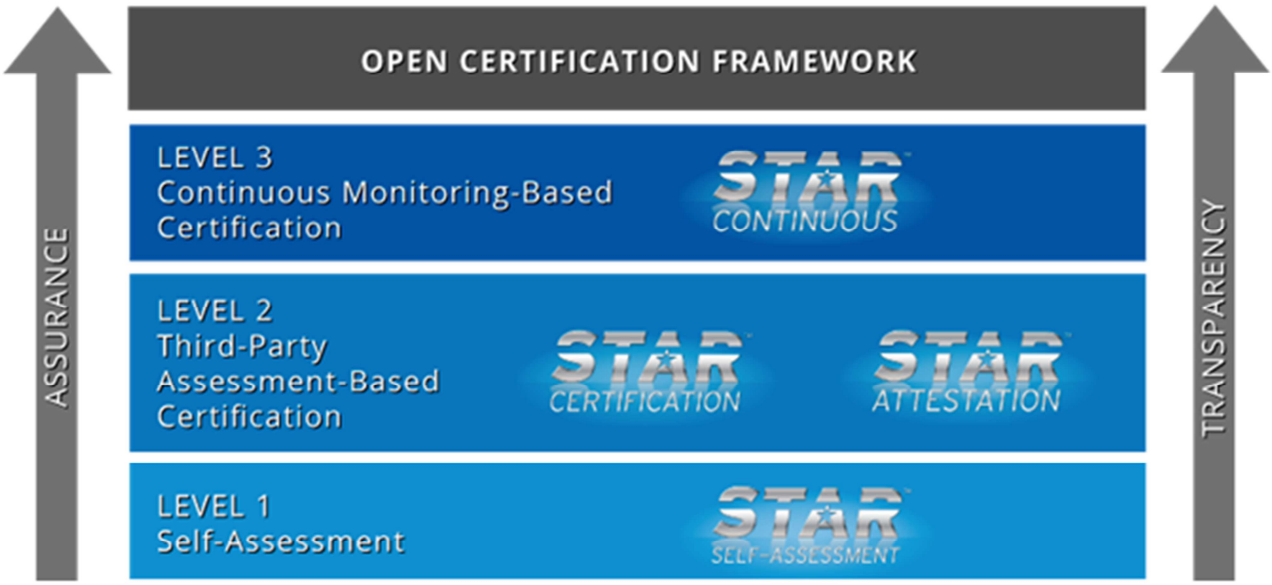

Figure 2. Open Certification Framework

When an organization is audited, a Management Capability Score will be assigned to each of the control areas in the CCM. This will indicate the capability of the management in this area to ensure the control is operating effectively. The management capability of the controls will be scored on a scale of 1-15. These scores have been divided into 5 different categories that describe the type of approach characteristic of each group of scores.

Score	Descriptor
1-3	No Formal Approach
4-6	Reactive Approach
7-9	Proactive Approach
10-12	Improvement Based Approach
13-15	Optimising Approach

Table 1. Scoring of controls

CSA OCF uses 11 out of 16 control areas of CCM. These areas are specified on the table below. Each of them will be awarded a management capability score on a scale of 1-15

CONTROL AREAS
Application & Interface Security
Audit Assurance & Compliance
Business Continuity Management & Operational Resilience
Change Control & Configuration Management
Data Security & Information Lifecycle Management
Data Center Security
Encryption & Key Management
Governance & Risk Management
Human Resources
Identity & Access Management
Infrastructure & Virtualization Security
Interoperability & Portability
Mobile Security
Security Incident Management, E-Discovery & Cloud Forensics
Supply Chain Management, Transparency & Accountability
Threat & Vulnerability Management

Table 2. Control areas considered in CCM to apply to CSA OCF

When assigning a score to a control area the factors to be considered are, namely: Communication and Stakeholder Engagement; Policies, Plans and Procedures, and a systematic approach, Skills and Expertise; Ownership, Leadership and Management; and Monitoring and Measuring. The lowest score against any one of those 5 factors will be the score awarded for the control area. As mentioned before, the score can range from 1 to 15. If a client has a major NCR (Non-Conformance Report) in an area, the maximum possible score will be 6. Once all control areas are scored, the average score will be used to assign the overall level for the client.

In [12] the assessor´s grid with the criteria to evaluate each factor and ascertain the corresponding mark can be found. Also in [12], an example of how an assessor might audit a control area can be read.

Depending on the result of evaluation (average score), a client will either get: Gold Award (more than 9), Silver Award (between 6 and 9), Bronze Award (between 3 and 6) or No Award (less than 3).

Security Rating Guide

Another example of framework will be leveraged to explain on detail the rating process. Security Rating Guide [18] is a framework provided by Leet Security, SL [19] which considers a set of security measurements, classified in 14 areas, namely: Information Security Management Program, Systems Operation, Personnel Security, Facilities Security, Third-party processing, resilience, compliance, malware protection, network controls, monitoring access control, secure development, incident handling and cryptography. These areas will be named as chapters. Every chapter is in turn divided in a number of variable different elements (so-called dimensions, hence the fact of being a multi-dimensional rating system) that should be considered to evaluate the rating of each chapter, namely:

common security measures, security measures regarding confidentiality, security measures regarding integrity and security measures regarding availability. For each element, the conditions needed to achieve each rating level are defined. Five rating levels: A, B, C, D, and E are defined. They are cumulative, so achieving B implies achieving C, D and E. In order to aggregate the rating levels obtained, the formula is the minimum one. This is, when aggregating rating levels the result is the minimum of the levels achieved in each element of the chapter. In turn, the overall rating level is the minimum one obtained among all the chapters (instead of the average as with CCM). Thus, the overall evaluation of the service is based on the weakest component. This rating system has the peculiarity of being applied by the provider itself, who is doing self-assessment, but with the surveillance of Leet Security. This is applied to both the first time the self-assessment is carried out and subsequent modifications. The process is summarized in the table below, where an example is provided.

	DIMENSIONS						
		Common Security Measures	**Security Measures regarding Confidentiality**	**Security Measures regarding Integrity**	**Security Measures regarding availability**	**RATING**	
CHAPTERS	**Information Security Management Program**	B	A	A	B	B	**C**
	Systems operation	A	A	A	A	A	
	Personnel Security	A	A	A	C	C	
	Facilities Security	B	B	A	B	B	
	Third-Party Processing	A	A	A	A	B	
	Resilience	B	A	B	A	B	
	Compliance	A	A	B	A	B	
	Malware protection	B	B	B	B	B	
	Network Controls	A	A	A	A	A	
	Monitoring Access Control	B	B	B	B	B	
	Secure Development	B	A	B	B	B	
	Incident Handling	A	B	A	A	B	
	Cryptography	B	B	B	A	B	

Table 3. Security Rating Guide: process example

CUMULUS in the context of certification metaframeworks

In a recent report from ENISA [22] is introduced the Cloud Certification Schemes Metaframework (CCSM), which maps common security requirements from the European public sector to a set of "security objectives" that should be achieved by suitable Cloud certifications. The CCSM comprises 27 security objectives, derived from the analysis of 29 relevant documents with NIS (Network and Information Security) requirements from 11 countries (United Kingdom, Italy, Netherlands, Spain, Sweden, Germany, Finland, Austria, Slovakia, Greece, Denmark). As mentioned by ENISA's report "…the goal of CCSM is to provide more transparency and help customers in the public sector with their procurement of cloud computing services." [22].

In order to achieve CCSM's main objective, ENISA is in the process of mapping security controls from well-known frameworks[1] (e.g., CSA CCM, and ISO/IEC 27001) to CCSM's security objectives. Given this context, how can Cumulus play a relevant role? A high-level representation of our proposal (to be explained in the rest of this subsection) can be seen in the figure below, where:

1. A set of certification schemes is previously mapped to ENISA CCSM (e.g., CSA OCF and ISO/IEC 27001 as seen in the figure below). This mapping relates security controls from existing certification schemes, to the security objectives defined by ENISA CCSM. The final result shows how well the former are able to cover the requirements for security certifications suggested by ENISA[2].
2. A Cloud Customer from European public sector is trying to select the CSP(s) that better suits its security requirements, by looking at the information published on ENISA's "Cloud Certification Schemes List".
3. Finally, the selected CSP(s) implements Cumulus' certification technology and processes in order to allow the Cloud Customer get assured by continuous/automatic certification of some of ENISA's security objectives from CCSM.

[1] The whole list can be found on ENISA's Cloud Computing Certification website https://resilience.enisa.europa.eu/cloud-computing-certification

[2] At the time of writing this document, ENISA has published a tool that shows the result of the discussed mapping https://resilience.enisa.europa.eu/cloud-computing-certification/list-of-cloud-certification-schemes/cloud-certification-schemes-metaframework

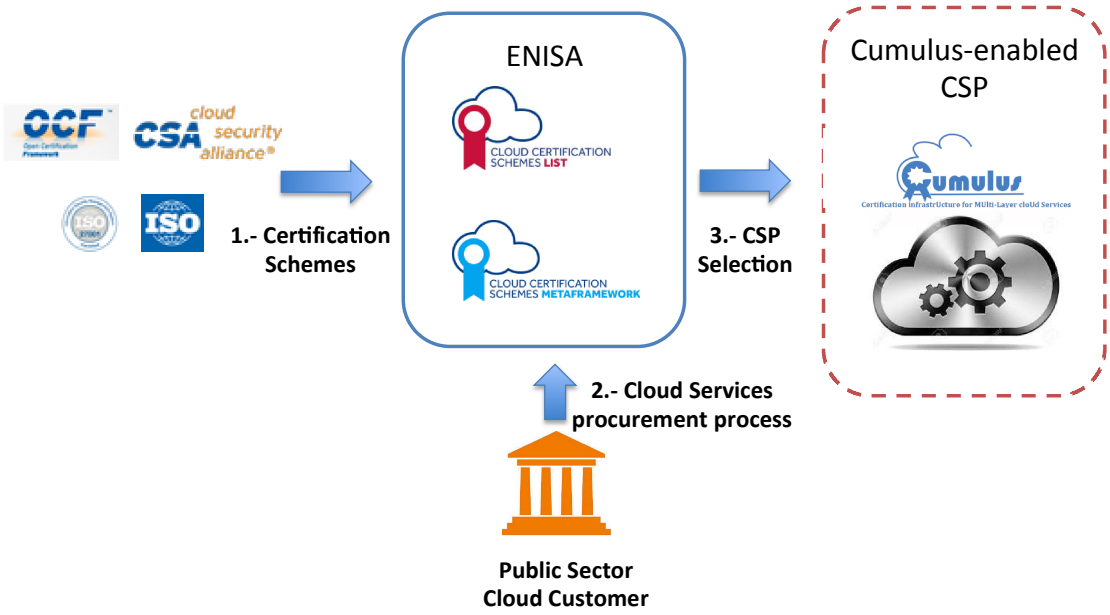

Figure 3. CUMULUS in the context of ENISA CCM

Given the scenario described above, **a proposed validation activity for Cumulus (results to be reported in Deliverable 6.6) will perform a gap analysis between Cumulus' security properties and ENISA CCSM's security objectives**. The goal of this activity is on the one hand to report the **"coverage" that Cumulus does with respect to ENISA CCSM** (i.e., how many of CCSM's security objectives can be certified by Cumulus). On the other hand, a closer examination of the gap analysis' results might help to **better understand the real-world capabilities and limitations of Cumulus** (e.g., most likely, not all CCSM security objectives can be automatically/continuously certified by Cumulus). Overall, obtained results can be also used to **elaborate on the business value that Cumulus might bring to CSP's offering services to the European public sector**.

The validation activity briefly described in this section will use as a baseline the security controls from CSA CCM, because (i) Cumulus security properties have already been mapped to CSA CCM by the technical WPs, and (ii) CSA CCM is part of ENISA certifications list and therefore has a map to CCSM' security objectives. Further information for the gap analysis (e.g., business value associated to covered/not-covered security objectives), will come from leveraging partners experience with CSA Open Certification Framework (as presented at the beginning of this section).

2.1.3. Undergoing the process of certification

Certification focused on cloud was born in a more general context, aimed at information systems in general. Because of that, it is necessary to bear in mind that there are not only cloud focused certification schemes but also more general certification schemes that are at least partly relevant to the delivery of cloud computing services. That is, **the field of cloud computing certification contains both cloud-focused certification schemes and schemes with a wider applicability** (for instance, security, service management or data protection), **which can be adopted to cloud computing**.

Successful cloud certification schemes appear to include the provision of real benefits; relevance; recognition and reputation; transferability and adaptability; transparency. On the other hand, potential shortcomings are: issues related to the adequacy; focus; purpose and complexity of standards; process and administration issues; problems with transparency and public communication, including a lack of awareness; and limitations in the assessment process.

Having said this, it is convenient to think about the motivations leading a company to decide to obtain certification of their cloud systems and in general, to obtain ISMS certification. The reasons can be both internal and external. Undergoing a certification process means to check all the services of the company during the preparation for the certification. This will lead to an **improvement of the quality** (this is also mentioned in section 2.3.3, on the benefits of CUMULUS from the point of view of the cloud provider). Besides, making the system *formal* (by means of certification) greatly improves the ordinary management of security and, in addition, **raises the security awareness of the employees**. From the external point of view, the acquisition of a certificate is a **marketing and competitive advantage** with a good impact both in current and prospective customers (also mentioned in 2.3.3). Moreover, it is more and more common customers driving certification by placing it as a requirement to be fulfilled by a company. Therefore, **meeting customer expectations** is another motivation to undergo a certification process. Finally, another motivation would be certification being a requirement for procurement procedures [4].

In the case of public organizations their motivations have to do with **their awareness of the importance of security** and their **desire to strengthen the confidence of citizens, or of companies collaborating with them**, in the security of IT and data management process. The desire for **security to be integrated throughout their business process rather than be a separate process** is another key factor. In the specific case of health area, some countries remark the requirement of certification of the involved ISMS.

Regarding the time period needed to prepare the company for certification, it is really variable, ranging from 3 to 18 months for private companies and up to 2 years in the case of public organizations. Most companies take between 6 and 12 months. Basically having previous experience in certification speeds up the process since some controls and mechanisms are already implemented, and the staff is familiar to this kind of process. When it comes to a follow-up, this time necessarily diminishes.

The period required for the actual certification process is, on average, a week for private sector and two weeks for public one. Sometimes, this process is split in two stages: the first to review the documented ISMS against the standard and the second to review the implementation of the ISMS within the business and evidence of adherence. Anyway, the size of the organization and the scope of the audit are an important factor to determine this duration. The certificates are usually granted for a three-year period, during which certified bodies need to be annually audited to ensure ongoing compliance with the standards. The certificate can be revoked if the annual audit finds reasons for it.

As for the cost of certification, it does not usually exceed the amount of 10000 €, which is considered in general terms good value for money, in the light of the benefits got from it.

Both public and private sector agree on the positive benefits brought by certification, highlighting that **certification ensures a regular and systematic identification of risks to information security**, and the evaluation and reduction of such risks to an acceptable and feasible degree by means of **suitable security measures**. Certification permits to **audit annually the organization´s good practices**, which requires continuous assessment with the aid of numerous system and process audits and leads to **improvements of the implemented system** and thus **improvements to the organization of work**. Thanks to the calculation of security indicators reflecting the efficiency of the system, **continuous adjustment and further evolution** in line with changing requirements can be achieved. The certification allows the **management of information in a much more rigorous way** than before. The certification also ensures **sustainable security and safety**. Finally, the certification introduces policy access rights to information systems and management of security incidents and vulnerabilities to the surveyed organization [4].

The benefits could be even higher if there were reliable statistics on the number of certificates and certified companies. The bodies issuing certificates are encouraged to keep updated records on certificates that they have issued, on the specific version of products/systems they certified, including information on the validity of the certificates.

Regarding the kind of profiles in charge of running the certification process and eventually authorizing the issuing of the certificates, these change from one organization to another. As an example, in the list below, the requirement an approving assessor must fulfill are enumerated:

- They must demonstrate knowledge of the Cloud Sector
    - Either through verifiable industry experience – this can include though assessing organizations
    - Or through completing CCSK [10] certification or equivalent
- They must be a qualified auditor working a ISO 27006 accredited CB
    - Evidence of conducting ISO 27001 assessments for a certification body accredited by an IAF member to ISO 27006 or their qualifications as an auditor for that organization.
- They must complete the CSA approved course qualifying them to audit the CCM for STAR Certification (This course will be carried out by BSI – British Standards Institute)

2.2. Justifying the need of certification

Despite the growing popularity and technical advances of cloud-based services, **there still exists a confidence gap between the potential stakeholders when it comes to cloud adoption**. While operating and finance personnel are generally excited about cloud because of the variety of powerful services and cost savings available, IT still has its reservations, largely related to **perceptions of cloud security**. For IT departments, the use of cloud can mean a loss of control, increased risk of intrusion or data loss and an aggressive shift in strategy. Also, should any security or privacy problems arise; the responsibility likely will fall back on the individuals responsible for IT.

As presented in the study realized by Accenture and the London School of Economics and Political Science's Outsourcing Unit called "Cloud and the Future of Business; From Costs to Innovation" shows that **IT still sees issues like security and privacy as a barrier to cloud adoption**. The study suggests that data security and privacy together with off-shore data housing and security are perceived to be the most significant risks for cloud.

A lot of research has been done, and is still on going to mind this perception gap. **Cloud-based security services** is an emerging market with rapid growth. It is estimated to rise to $3.1 billion in 2015 and expected to hit $4.13 billion by 2017. Gartner forecasts that two of the top three most sought-after cloud services will be web security services and identity and access management (IAM).

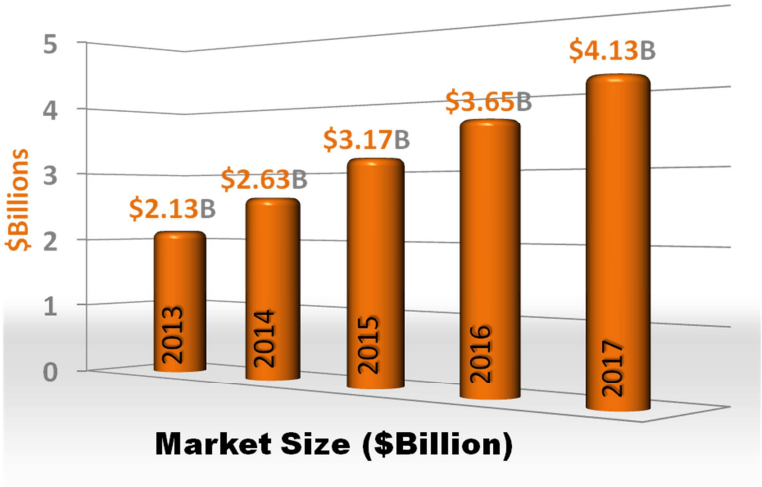

Figure 4. Cloud-Based Security Market Size Forecast (Source Gartner)

Ones of the reasons for this growth is the increasing adoption of Software as a Service (SaaS) applications and other cloud-based services that are encouraging organizations to adopt cloud-based security. Managed Security Services (MSS) are also driving adoption of cloud-based security services among enterprises. MSS delivery models are in turn being affected by demand for cloud-based security services, which is enabling security providers to become de facto MSS players.

Once decided the migration to cloud-based services, questions of security can make or break an IT department, which is why choosing the right provider is one of the most important decisions to make. In order to establish confidence that you will be working with a trusted cloud provider, Gartner suggest asking about security issues, such as, privileged user access, data location, data segregation or for instance, regulatory compliance. **This last one is fully in line with the research done in CUMULUS** since, takes into account the external audits or security certifications that the cloud provider has. So, definitely, to have these certifications can make a substantial difference towards market transformation.

Public cloud providers are not always able to provide the required transparency about the implemented policies, standards, and controls for truly trustworthy and interoperable cloud environments. Sometimes due to technological limitations, but often due to their reluctance to expose their operations. Furthermore, the market lacks independent and credible agents to examine and certify public cloud providers as suitable for the most sensitive information and applications. This lack of transparency and reliable third-party verification is becoming an urgent issue as organizations seek to benefit from better economies of scale by moving processes and services to public clouds. Cloud provider cooperation and transparency inevitably improve with customer demands. For more restrictive services, cloud provider logs and attestations may not be enough. Organizations may ask for means for implementing tools that enable them to observe and measure cloud conditions and activities first-hand. Objective verification, not attestations, will ultimately emerge as the gold standard for ensuring trust in the public cloud.

Certification is considered as a valid answer to the lack of trust in the cloud. For instance, in the context of Trusted Cloud Europe[3], certification comes strongly as a means to increase trust in the cloud. It is still unclear how this certification model should work, for instance the degree to which something is imposed or required and who requires it. What is aimed for EU level is to look at certifications and see what works best.

However, certification is not a panacea, since it costly process, particularly for SMEs, that in the end will have an impact on the cost of the cloud services. To this regard, the framework developed in CUMULUS project will help to automate a continuous certification framework that will help to reduce costs while providing a continuous assessment of the cloud services.

2.3. CUMULUS contribution from the point of view of the main stakeholders

2.3.1. The Cloud Certification Provider perspective

Most commercially available security certifications for the cloud are supported by well-established standards and best practices. As seen in ENISA's Cloud Computing Certification webpage[4] (CCC), the underlying standards/best practices are developed by recognized standardization bodies (e.g., ISO/IEC in the case of 27001), or organizations (e.g., CSA for the Open Certification Framework). These will be referenced as "Cloud Certification Providers" (CCP) in the rest of this section. It is worth to notice that not always a CCP is the same entity that performs the security audit, and actually in many cases there is a clear separation among both activities. For example, in the case of CSA OCF the list of

[3] http://ec.europa.eu/digital-agenda/en/news/trusted-cloud-europe

[4] Please refer to https://resilience.enisa.europa.eu/cloud-computing-certification

certified auditors can be found online[5]. Typically, the CCP will receive a payment (in the form of a royalty) depending on the number of audits performed based on its certification scheme.

The CUMULUS framework brings tangible business benefits for CCP's namely:

- Broaden their portfolio of certification schemes, by offering a "true" **continuous** certification solution. As discussed in Deliverable 7.6, a CUMULUS-based certification is something that customers are willing to pay for.
- Some CCP's sell training services in order to certify auditors on the offered scheme. The CUMULUS framework might allow CSP's to offer **training** services not only to auditors, but also to CSP's willing to integrate/deploy the CUMULUS contributed technology as part of their own services.
- CCP's might find a competitive advantage in offering new certification models suitable for complex cloud architectures. For example, cloud security certifications modeling the behavior of multi-cloud systems like supply chains or cloud federations. To the best of our knowledge, this is a gap at the state of the practice.
- Finally, the time-to-market associated with new CCP versions of existing certification schemes (e.g., adding/removing controls from the underlying standardized frameworks) will be reduced thanks to the systematic approach taken by CUMULUS. These "**incremental certifications**" are not offered by CCP's, just as observed from ENISA CCC.

The next version of this deliverable (D6.6) will further analyze the CCP business benefits discussed above.

2.3.2. The Cloud Auditor Perspective

A cloud auditor is a party that can perform an independent examination of cloud service controls (e.g., security, privacy, performance) with the intent to express an opinion thereon. Audits are performed to verify conformance to standards through a review of objective evidence. A cloud auditor can evaluate the services provided by a CSP such as security controls, privacy impact, and performance. According to ISO/IEC 17789 [7], the audit activity involves:

1. request or obtain audit evidence;
2. conduct any required tests on the system being audited;
3. obtain evidence programmatically, through a set of interfaces provided by the system being audited;
4. redact the evidence, if necessary, in order to protect sensitive information or information subject to regulatory control (e.g., PII);
5. compare the obtained audit evidence against the audit criteria as described by the audit scheme or standard that is being used.

From the activities mentioned above, CUMULUS directly impacts 1 – 3 although in an indirect manner the technological contributions from CUMULUS also will reflect on 4 and 5. **CUMULUS will benefit the cloud security audit function by providing the framework (techniques and tools) to automatically certify a selected set of security properties, directly from the target cloud service**. Furthermore, as required by novel certification schemes like CSA Open Certification Framework (OCF[6]), **CUMULUS will enable continuous certification**. Overall, these aspects will have a direct effect on the following business aspects associated to the audit function:

[5] Please refer to https://cloudsecurityalliance.org/star/certification/#_auditors

[6] Please refer to https://cloudsecurityalliance.org/star/

- Savings through realistic levels of automation: our expectancy is that **cloud auditors will save both time and economic resources thanks to the support provided by the framework/tools developed by CUMULUS**. Ideally, most of the audit activity will have the potential of being automated without losing assurance guarantees, however we expect "realistic" levels of automation to be deployed by the involved parties. For example, some security properties will need still the human component in order to process evidence, like in the case of the physical security controls found on most of currently available certification schemes.
- **New business models based on the Security-as-a-Service paradigm**: a promising audit strategy is to obvert towards the creation of **tools and techniques to reason about the security properties**, as a basis to enable Security-as-a-Service. Such solutions can be offered by independent third parties (brokers/auditors), offering to the end users/regulators monitoring functionalities e.g., to be notified about certifications/SLA violations due to cyber incidents. Some FP7 projects, like SPECS, are building on this, and new H2020 projects starting in 2015 will continue to explore this field.

Intuitively, both incurred savings and development of new business models will result on economic benefits for cloud auditors, which in the short/mid-term should reflect on the rest of involved stakeholders who would **increase notably their competitiveness** (e.g., CSP being charged only by the audit services being consumed, and cyber-insurances lowering prices thanks to the continuous assurance achieved by CSP's). These intuitive notions will be further explored and document in the next (and final) release of this deliverable.

2.3.3. The Cloud Provider Perspective

The increasing importance of cloud computing in the business world is forcing companies to adapt to this new paradigm. The likely loss of competitiveness they might suffer if not doing so is probably the most decisive factor leading them to make the decision. Nevertheless, regardless of this, security issues prevent the business from growing as it could be expected and desired. The demand of security is so high that any company is able to differentiate from competitors by offering such security. This would entail an important advantage.

In this sense, CUMULUS has several positive impacts:

- CUMULUS is somehow a way to encourage companies to implement new security measures. The catalogue of properties is quite appealing for any customer with high concerns of security. CUMULUS put providers on the way to accomplish these implementations.
- CUMULUS automates the evaluation of security and the certification of such security. On top of that, it provides continuous monitoring, a bit concern of the market, as it is shown in the results of questionnaire explained in D7.6.
- Such automation can decrease the number of hours devoted to auditing, and the price the company pays to the auditors.
- The reliability of CUMULUS as an appropriate certification environment could encourage insurance companies (those taking accountability in case of data breaches or the security being compromised) to lower their prices when offering their services. This has a double benefit: it makes the insurance company more competitive and reduces the expenses in this aspect the Cloud Service Provider has to face.
- CUMULUS will also increase cloud trust and transparency, supporting users and providers in their movement to the cloud

The flip side has to do with the adaptations the cloud infrastructure must face in order to be integrated with CUMULUS. Within this project, we have experience as for the number of hours that it takes to

integrate CUMULUS in a couple of specific pilots. Nevertheless, as a result of internal analysis the conclusion says that it is not easily comparable to any kind of pilot. There will be a high uncertainty regarding the effort needed to adapt CUMULUS to a specific cloud infrastructure. This will have an impact in the balance sheet. Besides, as it is stated in D6.2, sometimes parts of the cloud need to be exposed in order to make possible to get evidences to produce the certificate. This is especially meaningful as for testing techniques, where hooks are usually needed. The companies must study this issue before accomplishing the integration of CUMULUS.

Another important risk has to do with the criteria used to consider that a certificate can be issued for a particular security property. These criteria might be considered rather subjective if there are no recognized standards on which the criteria are based. That is why it is necessary, as it is stated in D6.2, to study in depth those standards in order to place properly the metrics and criteria to issue the certificate. In the framework of the project, the criteria that will be studied are compiled in the *protection profiles* by the NSA. These protection profiles have been approved for use by vendors for evaluation of products under the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) and the Common Criteria Recognition Agreement (CCRA). Some *protection profiles* which are relevant for CUMULUS are those for IPSec VPN Clients [18], Enterprise Security Management Identity and Credential Management [19], and Certification Authorities [20]. These profiles, along with others, will be analyzed in order to develop the most rigorous and accurate metrics to decide whether or not issue the corresponding certificate.

2.3.4. The insurance companies and their accountability

Cloud insurance is an approach to risk management in which a promise of finantial compensation is made for specific potential failures on the part of a cloud computing service provider.

A cloud insurance policy protects the cloud provider who is held responsible for a service that was promised but not delivered as well as customers who believe they did not receive promised results. Cloud insurance may be provided as a part of a SLA with the provider or it may be purchased separately through a third-party insurance company. The introduction of liability insurance for Cloud Service Providers is a move towards offering higher levels of data assurance to end user clients.

Cloud insurance can offer compensation for several reasons, such as outages, unintentional data losses or security breaches, to name but a few. Another insurance service is that providing periodical backups, so that the information can never be definitely lost. In [21] a list of reasons to contract this kind of insurances can be checked.

CUMULUS can contribute to make insurance cheaper for cloud providers. If CUMULUS becomes a recognized and trusted tool able to certificate security and provide assurance, insurance companies could offer their protection for a cheaper price to any client counting on CUMULUS to take care of the security of their cloud assets.

Some companies, such as CGI Group, Cloudinsure or MSPA Alliance members provide this kind of services. A study about their pricing and the likely discounts a client could get in case of counting on CUMULUS to provide assurance will be carried out in D6.6.

2.4. Outlook and next steps

The following bullet points analyze the conclusions obtained from each of the evaluation criteria:

- Criterion 1: It has been properly applied to both Smart Cities and eHealth scenario. It can be also applied to any other scenario taking the needed care to analyze the scenario itself and the kind of security that can be certified on it.
- Criterion 2: The *protection profiles*, defined by the NSA, seem to be an appropriate set of criteria to define whether or not a security property is being fulfilled. These criteria will be

studied in depth and applied to the validation for the rest of the project. Deliverable D6.6 will cover these forthcoming outcomes.

- Criterion 3: It has been properly applied to both scenarios, since the needed security mechanisms to make possible the certification of the corresponding security properties have been implemented, making possible such certification. It will continue to be applied for the rest of the project.
- Criterion 4: Regarding the costs of adaptation of the scenario to the framework, the only way to make some estimation is basing on previous experience, what is really difficult since there is not much in common among scenarios. Therefore such estimation in advance of costs, although could be done, would involve a big burden of uncertainty.
- Criterion 5: This criterion and the way to assess it are proposed on this deliverable. Deliverable D6.6 will sum up the work accomplished to perform such assessment.
- Criterion 6: Some references and figures have been provided showing the growing importance of the cloud market and the parallel market appearing with regard to cloud security. This is because security issues are the big threat to the success of the cloud as a new paradigm and as a business actually. CUMULUS is demonstrated to be fully aligned with the market demands and can really provide added value in terms of assurance. Deliverable D6.6 will give room to a deeper analysis by providing more references, outcomes of a more detailed research.
- Criterion 7: A first approach to the analysis of the benefits of CUMULUS from the point of view of different providers has been given. A more detailed work of analysis will be accomplished and reported on Deliverable D6.6. This work will be based on the analysis of bibliography and the interaction from real stakeholders in order to collect firsthand knowledge that may confirm the initial assumptions.

Besides, an overview about the current practices of certification, the way metaframeworks of certification operate and rate cloud services and infrastructures, and practical aspects about how public and private organizations undergo the process of certification and their reasons to do it have been provided within this section.

3. Evaluation of Certification Framework

3.1. Introduction

This section is envisaged to provide the first outcomes regarding the validation of the CUMULUS Framework following a set of concrete criteria, namely: usability, assurance, representation capability, cost effectiveness and security. In order to do this, a validation session, inspired to D6.2 criteria, was held in Rome on January 13rd 2015. In this section we report about design, execution and results of this session.

Along with this external validation, an internal one will be accomplished and reported in D6.6. To do this, the final architecture of the framework, explained in D5.3 (to be released at the same time as D6.5), will be analyzed w.r.t. its alignment with the requirements placed in D6.1. The result will be a traceability matrix which will summarize the achievements and will help to evaluate how much the initial expectations about the features the framework had to offer were fulfilled in the end.

3.2. Session with External Validators

3.2.1. Session Design and Execution

Introduction

The session was designed to be, as much as possible, consistent with the approach defined in [13]. Essentially, we involved external validators, who were requested to answer a questionnaire after being introduced to some aspects of CUMULUS project.

This first session was oriented to collect feedback about CUMULUS from security evaluation/certification experts (also called *respondents*), which is quite natural given the project objectives. We invited validators from Organismo di Certificazione della Sicurezza Informatica (OCSI) (Italian Body for ICT security certification according to the international standard ISO/IEC IS-15408 (or Common Criteria (CC) [15][16][17]) and from FUB. OCSI provided two official certifiers (unfortunately, one of them couldn't join the actual session) and FUB provided three experts of evaluation/certification (selected among people not involved in CUMULUS). In the following, the OCSI expert is denoted as R2 and the FUB experts are denoted as R1, R3 and R4.

Session Design

Based on both availability of validators and session objectives, we decided to have a four hours session to cover, at some extent, all the analyses considered for the CUMULUS framework in [13] (usability, representation capability, perceived security, assurance, cost effectiveness). Accordingly, we discussed both aspects to be presented and corresponding questions to be asked to the validators. Finally, we grouped the selected aspects along with the corresponding questions in four sections and structured the session accordingly.

SESSION SECTIONS

A brief description of the sections follows (some more details are given in table 6) (for a complete view, we refer to the session materials attached to this document):

- CUMULUS Framework (Section I): Introduction to both use cases and corresponding functional and security requirements as given in [23] (with suitable simplifications and special focus on the certifier actor), with corresponding questions from Q-1 to Q-6 (see table 6) supporting the exploration of usability and perceived security (see below);
- CUMULUS Meta Model (Section II): Introduction to both structure and objectives as given in [24] (with suitable simplifications and special focus on how it attempts to capture the basic concepts of a general approach to certification), with corresponding questions from Q-7 to Q-13 (see table 6) supporting the exploration of usability, representation capability, and assurance (see below);
- CUMULUS Test Based Certification Model (Section III): Introduction to both structure and objectives as given in [24] (with suitable simplifications and special focus on how it attempts to capture the basic concepts of test execution in a generic certification process, with emphasis to Common Criteria processes), with corresponding questions from Q-14 to Q-20 (see table 6) supporting the exploration of usability, representation capability, and assurance (see below). Notice that questions from Q-14 to Q-20 are deliberately got, mutatis mutandis, from questions Q-7 to Q-13, respectively, right to validate the two levels of description provided by the Meta Model and by a Certification Model;
- CUMULUS Framework Adoption (Section IV): Introduction to cost and benefit estimation (based on key factors and corresponding raw cost and benefit estimation focusing on the

possible adoption of the CUMULUS Framework in the Common Criteria context), with corresponding questions from Q-21 to Q-24 (see table 6) supporting the exploration of cost effectiveness.

- CUMULUS Monitoring Based Certification Model (Section V): Introduction to both structure and objectives of the monitoring based certification model, with the main focus on how it attempts to capture the basic concepts of the monitoring process and the definition of the different kind of conditions that need to be checked in the certification process.

QUESTIONNAIRE DESIGN

Table 6 provides the list of the questions selected as to be proposed to the validators, along with the corresponding possible answers and the contributed dimension explorations.

We considered only closed-answer questions of two possible types: questions with Yes/No answer (with request for written explanation conditioned on the provided answer) and questions with five level scale answer (Excellent, Good, Neutral, Poor, Very Poor). We decided to provide free text room for each question with five level scale answer so to gather as much feedback as possible from the validators. Moreover, we decided to provide free text room both for each session section and for the overall session so to allow the validators to report any extra relevant comment. The questionnaire was designed so to suitably instruct the validators about their role (for a complete view, we refer to the session materials attached to this document).

EXPLORED DIMENSIONS

It is important to notice that, due to some constraints, we needed to restrict the validation session as to investigate the CUMULUS framework just at a conceptual level. A first constraint was the actual availability of validators, leading to arrange only one validation session, only in the period between the end of 2014 and the beginning of 2015, and taking only half a day. A second constraint was the internal objective to try to contribute as much as possible all the analyses considered in [13]. The third constraint (related to the second one) was the need to introduce in a suitable way a number of concepts related to CUMULUS work. The given constraints suggested both to avoid showing a framework in action and to stay on concepts (many ones, in fact), though suitably presented. The main effects on the session design were:

- Presenting the CUMULUS Framework based just on use cases and corresponding functional and security requirements (as described in [23]);
- Presenting a simplified version of the CUMULUS Meta Model (as described in [24]);
- Presenting a simplified version of the CUMULUS Test Based Certification Model (as described in [24]) with no concrete example instances.
- Presenting a simplified version of the CUMULUS Monitoring Based Certification Model (as described in [24]).

All this produced also:

- A partial satisfaction of the general evaluation criteria (common across all dimensions) given in [13], since we couldn't actually introduce any contextualization to pilot scenarios;
- The need of suitably adapting to the session context the analyses considered in [13] (see the relevant remarks given below).

Usability Analysis Remarks

The designed validation session contributes, though in a non standard way, the usability analysis defined in [13] by covering the aspects of technical quality [13] of CUMULUS Framework

functionalities—as foreseen at requirement levels [23]—and (user) satisfaction [13] about CUMULUS Meta Model and Test Based Certification Model.

As for the technical quality aspect, based on functionalities foreseen at requirement levels, the session enables to:

- Explore both sufficiency [13] and necessity [13] of the reference functionalities (CUMULUS Framework Section, questions Q-1 and Q-2, respectively);
- Gather from the validators a relevant overall rating (through the concept of *completeness*) of the reference functionalities (CUMULUS Framework Section, question Q-3).

As for the (user) satisfaction aspect, the session enables to:

- Gather from the validators a relevant overall rating (through the concept of *easiness of comprehension*) of the reference models (CUMULUS Meta Model Section, question Q-7, CUMULUS Test Based Certification Model Section, question Q-14, and CUMULUS Monitoring Based Certification Model Section Q1).

The main point here is that the analyses enabled by the designed session, even being significant, use only a *conceptual* validation platform (see [13]) and this produces a partial satisfaction of the specific criteria given in [13].

Representation Capability Analysis Remarks

The designed validation session contributes the representation capability analysis defined in [13], since it enables to:

- Explore the ability of the CUMULUS Meta Model to capture the significant aspects of both a generic and a Common Criteria security certification process (CUMULUS Meta Model Section, questions Q-8 (generic process), Q-10 (generic process), and Q-11 (testing in Common Criteria));
- Explore the ability of the CUMULUS Test Based Certification Model to capture the significant aspects of both a generic test based and a Common Criteria security certification (CUMULUS Test Based Section, questions Q-15 (generic process), Q-17 (generic process), and Q-18 (testing in Common Criteria));
- Explore the ability of the CUMULUS Monitoring Based Certification Model to capture the significant aspects of the monitoring based certification process (CUMULUS Monitoring Based Certification Model Section Q2-5);
- Gather from the validators an overall rating of the ability of the CUMULUS Meta Model and Test Based Certification MODEL and Monitoring Based Certification Model to capture the significant aspects of security certification of cloud services (CUMULUS Meta Model and Test Based Certification Model Sections, questions Q-9 and Q-16, respectively, and Monitoring Based Certification Model Section Q6);

There are no particular remarks for this analysis.

Perceived Security Analysis Remarks

The designed validation session contributes the perceived security analysis defined in [13], since it enables to:

- Explore the completeness of the security functionalities foreseen at requirements level for the CUMULUS Framework (CUMULUS Framework Section, questions Q-4 and Q-5);
- Gather from the validators an overall rating of the security level that stems out from the CUMULUS Framework security requirements (CUMULUS Framework Section, question Q-6).

Also the perceived security analysis enabled by the designed session, even being significant, uses only a *conceptual* validation platform (see [13]) and this produces a partial satisfaction of the specific criteria given in [13].

Assurance Analysis Remarks

The designed validation session contributes the assurance analysis defined in [13], since it enables to:

- Analyze if the current definitions of the CUMULUS Meta Model and Test Based Certification Model could affect negatively the assurance of the certification processes described according to them (CUMULUS Meta Model Section, questions Q-12; CUMULUS Test Based Certification Model Section, questions Q-19);
- Gather from the validators positions about if/how introduce in the CUMULUS Meta Model and Test Based Certification Model any component/rule explicitly related to the assurance of the certification processes described according to them (CUMULUS Meta Model Section, questions Q-13; CUMULUS Test Based Certification Model Section, questions Q-20).

The main point here is that the assurance analysis enabled by the designed session, even being significant, uses only the CUMULUS Meta Model and the CUMULUS Test Based Certification Model (to collect possible requirements for their refinement) and this produces a partial satisfaction of the specific criteria given in [13].

Cost Effectiveness Analysis Remarks

The designed validation session, as with other dimensions considered, focuses on a conceptual level but it covers all the specific criteria given in [13].

The presentation includes a list of key factors apparently relevant for a cost effectiveness analysis of the adoption of the CUMULUS Framework within a security certification process. For these key factors, a raw estimation for the specific case of the Common Criteria certification process is also included. Table 5 reports a synthesis of the considered key factors along with the corresponding raw estimation (for a complete view, we refer to the session materials attached to this document).

Key cost factor	**Raw estimation for Common Criteria**
Identification of the certification process steps to be automated	LOW
Certification Model definition and CUMULUS Framework integration	HIGH
Training	LOW
Key benefit factor	
Increase in speed	MEDIUM
Increase in uniformity	MEDIUM
Increase in repeatability	HIGH
Reuse of defined Certification Model	MEDIUM

Table 4. Synthesis of the cost effectiveness analysis presented to the session with external validators

The session contributes the cost effectiveness analysis in [13], since it enables to:

- Gather a feedback from the validators regarding the completeness of the aspects considered as costs and benefits factors for cost effectiveness analysis (CUMULUS Framework Adoption Section, question Q-21);

- Gather the validators opinion about the accuracy of the raw estimation on costs and benefits of the adoption of the CUMULUS Framework in a Common Criteria certification process (CUMULUS Framework Adoption Section, questions Q-22 and Q-23);
- Obtain an overall rating of the cost effectiveness of the CUMULUS Framework adopted in a Common Criteria certification process (CUMULUS Framework Adoption Section, question Q-24).

#	Text	Possible Answers	Explored Dimensions	Reference Section
Q-1	Are the functionalities foreseen in the CUMULUS Framework sufficient? If not, please explain.	Yes No	Usability	CUMULUS Framework (I)
Q-2	Are the functionalities foreseen in the CUMULUS Framework all necessary? If not, please explain.	Yes No	Usability	CUMULUS Framework (I)
Q-3	How would you rate the completeness of an actual CUMULUS Framework implementing the foreseen functionalities?	Excellent Good Neutral Poor Very Poor	Usability	CUMULUS Framework (I)
Q-4	Are the security functionalities foreseen in the CUMULUS Framework sufficient? If not, please explain.	Yes No	Perceived Security	CUMULUS Framework (I)
Q-5	Are the security functionalities foreseen in the CUMULUS Framework all necessary? If not, please explain.	Yes No	Perceived Security	CUMULUS Framework (I)
Q-6	How would you rate the level of security of an actual CUMULUS Framework implementing the foreseen security functionalities?	Excellent Good Neutral Poor Very Poor	Perceived Security	CUMULUS Framework (I)
Q-7	How do you rate the easiness of comprehension of the CUMULUS Meta-Model?	Excellent Good Neutral Poor Very Poor	Usability	CUMULUS Meta Model (II)
Q-8	Is the CUMULUS Meta-Model adequate to represent the key aspects of security certification? If no, please, specify.	Yes No	Representation Capability	CUMULUS Meta Model (II)
Q-9	How do you rate the CUMULUS Meta-Model completeness in capturing the key aspects of security certification of cloud services?	Excellent Good Neutral Poor Very Poor	Representation Capability	CUMULUS Meta Model (II)
Q-10	Does the CUMULUS Meta-Model need to be reduced/extended/refined? If yes, please, specify.	Yes No	Representation Capability	CUMULUS Meta Model (II)
Q-11	Does the CUMULUS Meta-Model miss any key aspect of test activities occurring in CC approach to security certification? If yes, please, specify.	Yes No	Representation Capability	CUMULUS Meta Model (II)
Q-12	Does the CUMULUS Meta-Model limit, in any way, the assurance that can be obtained by certification processes specified according to it? If yes, please, specify.	Yes No	Assurance	CUMULUS Meta Model (II)

Q-13	Should the CUMULUS Meta-Model include an explicit coverage of the concept of assurance? If yes, please, provide possible reasons for that.	Yes No	Assurance	CUMULUS Meta Model (II)
Q-14	How do you rate the easiness of comprehension of the CUMULUS Test Based Certification Model?	Excellent Good Neutral Poor Very Poor	Usability	CUMULUS Test Based Certification Model (III)
Q-15	Is the CUMULUS Test Based Certification Model adequate to represent the key aspects of security certification? If no, please, specify.	Yes No	Representation Capability	CUMULUS Test Based Certification Model (III)
Q-16	How do you rate the CUMULUS Test Based Certification Model completeness in capturing the key aspects of security certification of cloud services?	Excellent Good Neutral Poor Very Poor	Representation Capability	CUMULUS Test Based Certification Model (III)
Q-17	Does the CUMULUS Test Based Certification Model need to be reduced/extended/refined? If yes, please, specify.	Yes No	Representation capability	CUMULUS Test Based Certification Model (III)
Q-18	Does the CUMULUS Test Based Certification Model miss any key aspect of test activities occurring in CC approach to security certification? If yes, please, specify.	Yes No	Representation Capability	CUMULUS Test Based Certification Model (III)
Q-19	Does the CUMULUS Test Based Certification Model limit, in any way, the assurance that can be obtained by test based certification processes specified according to it? If yes, please, specify.	Yes No	Assurance	CUMULUS Test Based Certification Model (III)
Q-20	Should the CUMULUS Test Based Certification Model include an explicit coverage of the concept of assurance? If yes, please, provide possible reasons for that.	Yes No	Assurance	CUMULUS Test Based Certification Model (III)
Q-21	Does the costs/benefits analysis miss any key aspects? If yes, please specify.	Yes No	Cost Effectiveness	CUMULUS Framework Adoption (IV)
Q-22	Does the costs/benefits estimation underrate any key factors? If yes, please specify.	Yes No	Cost Effectiveness	CUMULUS Framework Adoption (IV)
Q-23	Does the costs/benefits estimation overrate any key factors? If yes, please specify.	Yes No	Cost Effectiveness	CUMULUS Framework Adoption (IV)
Q-24	How would you rate the benefit of an actual CUMULUS Framework capable to automate the execution of tests in a CC certification process?	Excellent Good Neutral Poor Very Poor	Cost Effectiveness	CUMULUS Framework Adoption (IV)
Q1	Do you think that CUMULUS Monitoring Based Certification Models (MBCMs) are capable of representing comprehensively continuous security certification processes for cloud services security?	No, not at all Yes, but in less than 25% of cases that I can think of Yes, in about 25-49 % of cases that I can think of Yes, in about 50-74 % of cases that I can think of Yes, in about 75-90 % of cases that I can	Usability	CUMULUS Monitoring Based Certification Model (V)

		think of Yes, in excess of 90% of cases that I can think of		
Q2	Do you think that the assertion rules specified as part of a CUMULUS Monitoring Based Certification Model are capable of representing accurately and effectively the continuous collection of evidence required for the assessment of security properties and/or the effectiveness of control mechanisms realising these properties in the cloud?	No, not at all Yes, but in less than 25% of cases that I can think of Yes, in about 25-49 % of cases that I can think of Yes, in about 50-74 % of cases that I can think of Yes, in about 75-90 % of cases that I can think of Yes, in excess of 90% of cases that I can think of	Representation Capability	CUMULUS Monitoring Based Certification Model (V)
Q3	Do you think that the life cycle models specified as part of a CUMULUS Monitoring Based Certification Model are capable of representing effectively the processes of collecting evidence, and generating and managing certificates based on it?	No, not at all Yes, but in less than 25% of cases that I can think of Yes, in about 25-49 % of cases that I can think of Yes, in about 50-74 % of cases that I can think of Yes, in about 75-90 % of cases that I can think of Yes, in excess of 90% of cases that I can think of	Representation Capability	CUMULUS Monitoring Based Certification Model (V)
Q4	Do you think that the evidence sufficiency conditions that may be specified as part of a CUMULUS Monitoring Based Certification Model (number of events, period of monitoring, expected behaviour of target of certification) are capable of representing effectively the circumstances under which the evidence collected would be enough to make a decision about issuing a certificate or otherwise?	No, not at all Yes, but in less than 25% of cases that I can think of Yes, in about 25-49 % of cases that I can think of Yes, in about 50-74 % of cases that I can think of Yes, in about 75-90 % of cases that I can think of Yes, in excess of 90% of cases that I can think of	Representation Capability	CUMULUS Monitoring Based Certification Model (V)
Q5	Which of the following parts of CUMULUS Monitoring Based Certification Models, do you think that it would be difficult for someone with expertise in cloud security to specify even after training?	None Assertions expressing the collection of evidence for security properties/anomalies Evidence sufficiency conditions Life cycle models	Representation Capability	CUMULUS Monitoring Based Certification Model (V)
Q6	Are there any key elements/requirements that continuous security certification	Yes No	Representation Capability	CUMULUS Monitoring Based Certification Model

	processes for cloud services should address but CUMULUS Monitoring Based Certification Models fail to cover?			(V)

Table 5. Questions proposed for the session with external validators

Recommendations for Future Sessions

Based on the remarks given before, possible future validation sessions involving security evaluation/certification experts could be extended so to:

- Use more concrete validation platforms
  - Involve architecture design and/or component implementation;
- Consider a more significant coverage of the relevant dimensions
  - For usability analysis, possibly include also efficiency and learnability aspects [13];
  - For assurance analysis, possibly include also instances of Certification Models;
- Cover advanced concepts of CUMULUS Framework
  - Exploit knowledge acquired by validators already involved.

SESSION EXECUTION

The session started with a presentation of the session structure and objectives, followed by an introduction to the relevant aspects of CUMULUS. Then, according to the planned duration, each section was executed, taking about 15 to 30 minutes for slide presentation and about 15 minutes for questionnaire answering. Further details were given to meet requests from validators (to clarify presented concepts and/or proposed questions). Where needed, the validators were requested to clarify their answers to the questionnaire.

3.2.2. Session results

INTRODUCTION

This section reports an analysis of the results of the validation sessions with external validators. Consistently with [13], given the session context, a quantitative analysis is not so significant, so the analysis follows a qualitative approach, where the main objective is to extract from the validator feedback (filled questionnaires) as many as possible recommendations and suggestions to guide the next CUMULUS activities.

Accordingly, both answers and comments from the validators are first discussed question by question. The more relevant suggestions and recommendations emerged from the discussion are then summarized at the end of the section.

Validation results

Table 7 provides the raw answers of the validators to the questions proposed to them, while in the next subsections the answers to each question are discussed in detail along with the relevant comments provided by the validators (for a complete view of the feedback from validators, we refer to the session materials attached to this document).

#	R1	R2	R3	R4
Q-1	Yes	Yes	No*	Yes*
Q-2	Yes	Yes	Yes	Yes
Q-3	Neutral*	Excellent	Excellent	Good
Q-4	Yes	Yes	No*	Yes
Q-5	Yes	Yes	Yes	Yes
Q-6	Neutral	Good	Good	Excellent
Q-7	Neutral*	Good	Neutral*	Neutral*
Q-8	Yes	Yes	Yes	N/A
Q-9	Neutral*	Neutral*	Good	N/A*
Q-10	No	No	No	No*
Q-11	No	No	Yes*	No
Q-12	No	No	No	No
Q-13	N/A*	No*	Yes*	*Yes
Q-14	Good*	Good	Neutral*	Excellent
Q-15	Yes	Yes	Yes	Yes
Q-16	Neutral*	Neutral*	Good	Excellent
Q-17	N/A*	No	Yes*	No
Q-18	Yes	No	No	No
Q-19	No	No	No	No*
Q-20	No	No	Yes*	No
Q-21	Yes*	No	Yes*	No
Q-22	No	No	No	No
Q-23	No	No	No	No
Q-24	Neutral*	Good	Poor	Poor
Q1	>90%	>90%	>90%	>90%
Q2	N/A*	>90%	>90%	>90%
Q3	>90%	>90%	>90%	>90%
Q4	N/A*	>90%	>90%	50-74%
Q5	Assertions	None	Assertions	Evidence Sufficiency Conditions
Q6	Yes*	No*	Yes*	No*

Table 6. Raw results of the responders to the questionnaire. Answers enriched by significant comments (see below) are asterisked (the reader can retrieve all validators´comments by checking the annexes attached to this deliverable).

Usability analysis

CUMULUS FRAMEWORK SECTION

Questions Q-1, Q-2 and Q-3 referred to the CUMULUS Framework section and, as explained in Section 3.2.1, aimed at supporting usability analysis (see table 6) through analyzing the technical quality of the CUMULUS Framework foreseen functionalities.

The feedback from the validators was fully positive (once the comments from the validators have been analyzed (see below) and can be summarized as follows:

- All the respondents with one exception (R3) agreed that the functionalities foreseen in the CUMULUS Framework are sufficient (see raw answers to Q-1 in table 6);

- All the respondents agreed that the functionalities foreseen in the CUMULUS Framework are all necessary (see raw answers to Q-2 in table 6);
- All the respondents with one exception (R1) rated Excellent or Good the completeness of an actual CUMULUS Framework implementing the foreseen functionalities (R1 rated such completeness Neutral) (see raw answers to Q-3 in table 6).

The answers that seemed to be critical were especially analyzed, looking at the motivations provided by the validators and directly interacting with them. It turned out that such answers finally do not affect the technical quality of the CUMULUS Framework foreseen functionalities, for the following reasons:

- R3 motivated the negative answer to Q-1 by explaining that an integrity check for the evidence collected from the cloud system could be useful. Anyway, such integrity check is already considered in the requirements for CUMULUS Framework, although implicitly. This point, which was not highlighted during the session due to the limited time available for the presentation, can be detailed as follows:
    - The CUMULUS Framework is foreseen to provide for the evidence collection session the security protections that are specified in the corresponding certification configuration (Requirement 6019.SEC of [23]). These security protections (motivated by possible attacks to the connection between CUMULUS Framework and a Cloud System) may include protection of integrity of the evidence since it has been collected in the Cloud System. Once acquired, the collected evidence is part of an evidence collection trace that is stored by the CUMULUS Framework (Requirement 3015.FUN of [23]). The CUMULUS Framework is foreseen to maintain the integrity of each evidence collection trace (Requirement 6020.SEC of [23]);
- R1 interpreted completeness in Q-3 as not limited to the objectives of the CUMULUS Framework (and especially to the automatic execution of a CUMULUS certification process), but extended to a generic certification process that is partially delegated to the CUMULUS Framework by a human certifier. Based on this, R1 motivated the Neutral rating in the answer to Q-3 by commenting that such a completeness depends on how much of a generic certification process can be actually delegated to the CUMULUS Framework by a human certifier.

The overall positive feedback received should just be completed with a general recommendation to not underrate the needs of the human certifiers that will use the CUMULUS Framework. This concern was especially felt by R4, as detailed below:

- In a comment to Q-1, though giving a positive answer, R4 anyway pointed out that a certifier would like to have documentation on the available services, on how to use those services and on inputs to be provided to the interfaces;
- In an extra comment to the CUMULUS Framework section, R4 stressed that a certifier expects help from the CUMULUS Framework, and not extra work to be done.

CUMULUS META MODEL SECTION

Question Q-7 referred to the CUMULUS Meta Model section and, as explained in Section 3.2.1, aimed at supporting usability analysis (see table 6) through (user) satisfaction about CUMULUS Meta Model.

At a first sight the feedback from the validators seemed to be critical, since only R2 rated Good easiness the of comprehension of the CUMULUS Meta Model that was instead rated Neutral by all the

other respondents (see raw answers to Q-7 in table 6). Anyway, the impact of these prevailing Neutral answers has been reduced by looking at the motivations provided by the validators and directly interacting with them. After such analysis, it turned out that only one of the respondents who gave Neutral ratings (R4) actually raised doubts on the overall comprehension of the CUMULUS Meta Model, and this position was motivated with the difficulty to find a parallel with the usual Common Criteria evaluation work done by R4. On the other hand, the Neutral ratings by R1 and R3 were based on single specific aspects that do not actually affect the (user) satisfaction about CUMULUS Meta Model. These were, respectively:

- For R1, the overlapping between the type of Evidence and the type of Certification Model;
- For R3, the lack of uniformity with the vocabulary used by security standards as the Common Criteria.

CUMULUS TEST BASED CERTIFICATION MODEL SECTION

Question Q-14 referred to the CUMULUS Test Based Certification Model section and, as explained in Section 3.2.1, aimed at supporting usability analysis (see table 6) through (user) satisfaction about CUMULUS Test Based Certification Model.

The feedback from the validators was essentially positive, since all the respondents with one exception (R3) rated Excellent or Good the easiness of comprehension of the CUMULUS test based Certification Model (see raw answers to Q-14 in table 6). R1 especially pointed out that all is relatively clear, except what the element ToC (Target of Certification [24]) exactly specifies. Only one respondent (R3) gave a Neutral answer, which anyway was motivated by the fact that R3 did not deem himself as an expert in model description and not by negative considerations on the CUMULUS Test Based Certification Model.

CUMULUS MONITORING BASED CERTIFICATION MODEL SECTION

Questions Q1 refer to the CUMULUS Monitoring Based Certification Model section and aimed to support usability analysis and user satisfaction about CUMULUS Monitoring Based Certification Model.

The overall feedback from the validators was essentially positive, however they stated that there were some of the elements difficult and a bit complex to understand in order to define some elements.

Assurance analysis

CUMULUS META MODEL SECTION

Questions Q-12 and Q-13 referred to the CUMULUS Meta Model section and, as explained in Section **¡Error! No se encuentra el origen de la referencia.**, aimed at supporting assurance analysis (see table 6).

The feedback from the validators was essentially positive and can be summarized as follows:

- All the respondents agreed that the CUMULUS Meta Model does not limit in any way the assurance that can be obtained by certification processes specified according to it (see raw answers to Q-12 in table 6);
- Actually all the respondents with one exception (R3) did not agree that the CUMULUS Meta Model should include an explicit coverage of the concept of assurance (see raw answers to Q-13 in table 6 plus the observations below).

As for Q-12, all the positive answers were basically motivated by the very high level of the description provided by the Meta Model.

When answering to Q-13, two respondents (R3 and R4) seemingly agreed that the CUMULUS Meta Model should include an explicit coverage of the concept of assurance but only R3 actually agreed and motivated this with the need for comparison of certified products. A direct interaction with the respondent clarified that R4 actually did not agree. In fact R4 explained in a comment to Q-13 that nothing more can be done at the Meta Model level, since the relevant values to determine assurance are set at the Certification Model level. Also R2 did not agree and explained in a comment to Q-13 that an explicit coverage of assurance by the Meta Model is not necessary, provided that the actual Certification Models cover in some way the concept. Finally, R1 did not answer, but actually did not agree. In fact, in a comment to Q-13, R1 assumed that the assurance concept is somehow included in the element Security Property and explained that, under this assumption, there is no need of an explicit coverage of assurance in the Meta Model.

CUMULUS TEST BASED CERTIFICATION MODEL SECTION

Questions Q-19 and Q-20 referred to the CUMULUS Test Based Certification Model section and, as explained in Section 3.2.1, aimed at supporting assurance analysis (see table 6).

The feedback from the validators was essentially positive and can be summarized as follows:

- All the respondents agreed that the CUMULUS Test Based Certification Model does not limit in any way the assurance that can be obtained by certification processes specified according to it (see raw answers to Q-19 in table 6);
- Actually all the respondents with one exception (R3) did not agree that the CUMULUS Test Based Certification Model should include an explicit coverage of the concept of assurance (see raw answers to Q-20 in table 6).

As for Q-19, R4 just pointed out in a comment that the assurance is probably limited only by how the CM is instantiated.

As for Q-20, all the respondents that answered No pointed out in their comments that the provided assurance may be somehow derived from the contents of the Certification Model. On the other hand, R3 justified his Yes answer as that to Q-13, with the fact that an explicit coverage of assurance is needed for comparison of certified products.

Representation capability analysis

CUMULUS META MODEL SECTION

Questions Q-8, Q-9, Q-10 and Q-11 referred to the CUMULUS Meta Model section and, as explained in Section 3.2.1, aimed at supporting representation capability analysis (see table 6).

The feedback from the validators was essentially positive and can be summarized as follows:

- All the respondents except one (R4) agreed that the CUMULUS Meta Model is adequate to represent the key aspects of security certification (see raw answers to Q-8 in table 6);
- Only one of the respondents (R3) rated Good the CUMULUS Meta Model completeness in capturing the key aspects of security certification of cloud services. Two other respondents (R1 and R2) rated it Neutral and R4 did not answer (see raw answers to Q-9 in table 6);
- All the respondents agreed that the CUMULUS Meta Model does not need to be reduced/extended/refined (see raw answers to Q-10 in table 6);
- All the respondents except one (R3) agreed that the CUMULUS Meta-Model does not miss any key aspect of test activities occurring in CC approach to security certification (see raw answers to Q-11 in table 6).

The answers that seemed to be critical were especially analyzed (especially those to Q-9), looking at the motivations provided by the validators and directly interacting with them. It turned out that such answers do not substantially affect the representation capability of the CUMULUS Meta Model, based on the observations that follow.

As for Q-8, R4 did not answer and pointed out in a comment that it is not clear how the Meta Model could represent actual evaluation activities.

As for Q-9, the impact of the Neutral ratings is reduced by the motivations provided for them. In fact, in their comments to Q-9, R1 motivated the rating with a single specific aspect (to R1, it all depends on how the element ToC [24] is defined) and R2 by an alleged poor knowledge of cloud systems security. Finally R4 did not answer, but in direct interaction explained to have several doubts on the concept of Meta Model itself (this is consistent with other answers by R4 to questions about the Meta Model, e.g., Q-8).

In a comment to Q-10, R4 pointed out that the Meta Model could just be made easier to understand (this is consistent with other answers by R4 to questions about the Meta Model: see, e.g., Q-7). Moreover, in an extra comment to the CUMULUS Meta Model section, R3 suggested that the addition of extra information that permits composition of ToCs [24] may simplify the certification of complex ToCs.

In the comments to Q-11, the No answers were all basically motivated by the very high level of the description provided by the Meta Model; on the other hand, R3 motivated his Yes answer by specifying that in the Meta Model the strength of security functions is missing. Anyway, since the strength of security functions is a possible metrics for penetration tests, it may be covered within the CUMULUS Test Based Certification Mode, especially by the element Test Metrics.

CUMULUS TEST BASED CERTIFICATION MODEL SECTION

Questions Q-15, Q-16, Q-17 and Q-18 referred to the CUMULUS Test Based Certification Model section and, as explained in Section 3.2.1, aimed at supporting representation capability analysis (see table 6).

The feedback from the validators was essentially positive and can be summarized as follows:

- All the respondents agreed that the CUMULUS test based Certification Model is adequate to represent the key aspects of security certification (see raw answers to Q-15 in table 6);
- Half of the respondents rated Excellent or Good the CUMULUS test based Certification Model completeness in capturing the key aspects of security certification of cloud services, whereas the other half rated it Neutral (see raw answers to Q-16 in table 6);
- Half of the respondents agreed that the CUMULUS test based Certification Model does not need to be reduced/extended/refined (see raw answers to Q-17 in table 6);
- All the respondents except one (seemingly R1, but actually R3 (see observations below)) agreed that the CUMULUS Meta-Model does not miss any key aspect of test activities occurring in CC approach to security certification (see raw answers to Q-18 in table 6).

The answers to Q-16, Q-17 and Q-18 that seemed to be critical were especially analyzed, looking at the motivations provided by the validators and directly interacting with them. It turned out that such answers do not substantially affect the representation capability of the CUMULUS Test Based Certification Model, based on the observations that follow.

In the comments to Q-16, the respondents who gave Neutral ratings (R1 and R2) gave motivations that reduce the impact of such rating. In fact, R1 motivated her answer with the fact that it is difficult to "force" significant specifications without limiting the possible cases, but also noted that this problem is common to any model, whereas R2 motivated her answer by an alleged poor knowledge of cloud systems security.

As for Q-17, R1 did not take a position, giving in a comment essentially the motivation that the time provided was not sufficient to give a satisfactory answer. Finally, only one respondent (R3) answered Yes and, recalling their comment to the CUMULUS Meta Model section, specified that the CUMULUS Test Based Certification Model could be refined by adding some information to permit the composition of ToCs [24], thus simplifying the certification of complex ToCs.

As for Q-18, all the respondents except (seemingly) R1 answered No. Anyway, direct interaction with the respondents clarified that R1 answered Yes by mistake, whereas R2 answered No but actually thought that some aspect was missing. In fact, in a comment to Q-18, R2 pointed out that the CUMULUS Test Based Certification Model does not seem to cover aspects as test coverage and depth. As for this comment, it may be noted that the CUMULUS Test Based Certification Model does not explicitly address these aspects, but nevertheless provides a way to specify them (as much as they can be adapted to the context of cloud services) through the element Test Metrics.

CUMULUS MONITORING BASED CERTIFICATION MODEL SECTION

Questions Q2-6 referred to the CUMULUS Monitoring Based Certification Model section and aimed at supporting representation capability analysis (see table 6).

The overall feedback from the validators was that the Monitoring Based Certification Model is able to represent the key aspects of the monitoring based certification process. However, there were some comments whether the monitor can detect any changes that might occur in a service that is being monitored and certified, in order to adapt the certification process according to them. This comments lead to the necessity of having the incremental certification process, which will be covered in the CUMULUS project. Finally, some certifiers also proposed to combine the monitoring-based certification process with a test-based process, to check that no changes have occurred in the service that is being certified, which leads to the necessity for a hybrid certification process.

Perceived security analysis

CUMULUS FRAMEWORK SECTION

Questions Q-4, Q-5 and Q-6 referred to the CUMULUS Framework section and, as explained in Section 3.2.1 , aimed at supporting perceived security analysis (see table 6).

The feedback from the validators was essentially positive and can be summarized as follows:

- All the respondents except one (R3) agreed that the security functionalities foreseen in the CUMULUS Framework are sufficient (see raw answers to Q-4 in table 6);
- All the respondents agreed that the security functionalities foreseen in the CUMULUS Framework are all necessary (see raw answers to Q-5 in table 6);
- All the respondents with one exception (R1) rated Excellent or Good the level of security of an actual CUMULUS Framework implementing the foreseen security functionalities (R1 rated such completeness Neutral) (see raw answers to Q-6 in table 6).

As for Q-4, R3 motivated the negative answer in a comment by pointing out that an integrity check for evidence provided by the cloud system could be useful. This motivation is the same given by R3 for his answer to Q-1 and has been discussed when reporting the answers to Q-1.

As for Q-5, R3 in a comment just raised some doubts about the scope and the purpose of non-repudiation and on its meaning from the point of view of the cloud system owner. Actually, the CUMULUS Framework is foreseen to assure the non-repudiation of Certification Results (Requirement 6014.SEC of [23]). The purpose is to provide support to resolution of disputes about the fact that a given certification result has been originated in the CUMULUS Framework. Therefore, from the point

view of the cloud system owner, non repudiation is a protection in possible disputes with a Certifier that uses the CUMULUS Framework.

As for Q-6, R4 in a comment pointed out that security requirements should be transparent for the certifier, to avoid complicating the work to be done. Finally, R1 motivated their Neutral answer with the comment that it is impossible to answer if an actual implementation is not available. These answers seem to notify that the overall security level perceived by the validators for the considered conceptual Framework level is good, and to suggest to extend the analysis to a more concrete Framework.

It is relevant for perceived security also the extra comment of R3 to the CUMULUS Framework section, noting that the separation of privileges between Administrator and Auditor may relax the assumptions to be done about the Administrator, which in this way would be controlled at some extent by the Auditor. Even if this sounds as a good suggestion, since it is not about one of the main objectives of the project it seems that a possible revision of the requirements and assumptions would be not necessary in this case.

Cost effectiveness analysis

CUMULUS FRAMEWORK ADOPTION SECTION

Questions Q-21, Q-22, Q-23 and Q-24 referred to the CUMULUS Framework adoption section and, as explained in Section 3.2.1, aimed at supporting cost effectiveness analysis (see table 6).

When answering to Q-21 two of the respondents indicated that the analysis could miss a key factor. R1 identified this missing factor as the "cost of preparing automation tools/framework" but recognizing that it could be included (as it actually is) in the cost of preparing appropriate CMs and integrating the CUMULUS Framework in a given certification process. R3, on the other hand, underlined that CUMULUS view does not explicitly consider a distinction between the evaluation and the certification process, which is a basic distinction in a Common Criteria certification process. R3 highlighted that the CUMULUS Framework best fit into the CC evaluation process, but should consider as a key cost factor the interaction between the Certification Body and the Evaluation Facility. After a direct interaction with the respondent he recognized that the missing cost was indeed present in the factor taking into account the definition of CMs and the integration of these in the CUMULUS Framework. To better clarify the importance of the aspects considered, R3 suggested, for a possible future estimation (that could be done for example for a second validation session), to split the relevant key factor and to estimate separately the cost of defining CMs and the cost of integrating them in a certification process.

When answering to Q-22 and Q-23 all the respondents agreed that the raw estimation provided in the presentation rated in a correct way (neither underrated nor overrated) all the identified key factors. These positive answers confirm the results of the raw estimation: even if an important factor to be considered is the cost of generating new CMs, this cost could be in a long-term phase mitigated by the reuse of other CMs already generated and moreover other benefits factors like the increase in speed, uniformity and repeatability of certification results would have an important impact in overall cost effectiveness of adopting the CUMULUS Framework.

When answering to Q-24, two of the respondents rated as good the benefit coming from the automation of a part of the CC certification process that could be provided by a tool like the CUMULUS Framework. On the other hand R1 expressed a neutral opinion justified by the fact that the advantages of adopting a tool like the CUMULUS Framework are relevant only if a good reuse in the definition of CMs is possible. Another respondent (R3) considered as Poor the overall benefit of adopting the CUMULUS Framework in a CC process since the time saving would be very low. Both these comments seems to be strictly related to the peculiarities of the CC certification process since in this process a huge part of the work done by an evaluator is "manual" (e.g. analysis of documental evidence) and it is difficult to automate and reuse. This seems to be confirmed also by the additional comment provided by R4 stating that the initial overhead of setting up an appropriate CM for a CC certification process

seems to be high. In this sense, even if adopting the CUMULUS Framework in a CC certification process would bring limited advantages as of today, considering a different and more cloud-oriented certification process or even a modified CC process adapted to the cloud context needs, the cost effectiveness of the CUMULUS Framework would considerably increase.

Three of the respondents also provided general comments to this section. R1 suggested that also part of the document revision that is done during a CC evaluation could be automated (e.g. by verifying the presence of given paragraphs/sections) thus suggesting that the CUMULUS Framework functionalities could be extended and consequently the raw estimation could be revised by considering also this point. Even though the suggested automation cannot be readily included in the CUMULUS scope, it makes some sense in that the CUMULUS Framework could provide automatic tools for assessing, at some extent, some kind of correctness (e.g., the syntactical one) of the artefacts it processes (e.g., of the CM instances). Moreover, R2 suggested that the tools provided by CUMULUS could be used also in the automation of tests done in a standalone non-cloud context. From this point of view, R4 added that his rating regarding the adoption of the Framework (i.e. Q-24) has not fully taken into consideration the cloud nature of the context analyzed. Once considered the context R4 noticed that the overall benefit would be even better.

General comments to the session

Only one respondent gave a general comment to the overall session by stating that the CC certification could be adapted to be automated in a more significant portion but also recognized that this seems to be out of CUMULUS scope.

The validators also provided interesting comments during the session by asking questions about the project and specifically about the topics presented in the slides.

One of this comments was about the Meta-Model (MM) asking the rationale behind the fact that the MM does not share the same terminology with the CC for similar concept like the ToC (Target of Certification, MM term [24]) and TOE (Target Of Evaluation, CC term [15]). After a more precise and detailed description of the ToC and even other concepts, the validators understood that since there isn't a perfect overlapping between the concepts in MM and CC world, the project has deliberately chosen a different term in order to avoid to create confusion and misunderstandings.

Another comment from the validators was about the fact that they considered very difficult to answer to some questions (e.g., the ones about adequateness of the CUMULUS Framework functionalities) without interacting with a concrete tool and without knowing more specific details about how the project has implemented the requirements that it has specified. This could be a good suggestion for the design of a possible second validation session in order to gather a more significant feedback from the validators.

3.3. Outlook and next steps

The session produced a set of suggestions from the validators that are of two main kinds: suggestions for guiding the rest of the CUMULUS project development and suggestions for improving possible future validation sessions.

As far as the first kind of suggestions is concerned, the validators provided the following advices:

- It could be useful to foresee an explicit coverage of the assurance concept within the Certification Model in order to ease the comparison of two different certified services;
- It could be useful to consider the composition concept that is used in the Common Criteria when defining advanced Certification Models like the multilayer ones;
- The CUMULUS Framework could consider to provide support for syntactical checks of Certification Model instances.

Regarding the second kind of suggestion, the validators provided the following advices:

- The definitions of the key factors identified as relevant for the cost effectiveness analysis could be refined;
- The session could involve a more concrete analysis of the CUMULUS Framework so to allow the validators to get a deeper understanding of its capabilities.

The project will try to take advantage as much as possible of these suggestions to improve the quality of both the CUMULUS Framework and possible future session for its validation, which should be designed considering also the recommendations given in Section 3.2.1.

4. TC Proofs Evaluation

4.1. Introduction and recapitulation from D6.2

As explained in the specification of CUMULUS evaluation criteria [13], Infineon undertakes a Common Criteria certification of its new TPM 2.0 chip. The corresponding security evaluation of the TPM security properties related to CUMULUS requirements is done within CUMULUS.
In the TPM 2.0 Protection Profile (PP) [14], the following requirements have been selected as CUMULUS validation criteria:

- **Cryptographic Security Functional Requirements (SFR)**
  The support of new cryptographic functions and the flexible usage of cryptographic algorithms facilitates the use of the TPM in CUMULUS scenarios and in the certification infrastructure.
- **Measurement and Reporting SFR**
  The TPM measuring and reporting functions are crucial to assure the integrity of CUMULUS components. The new TPM V2.0 support for more than one bank of PCRs adds additional flexibility.
- **Security Assurance Requirements (SAR)**
  The SARs describe the measures to be taken during development and evaluation of a product to assure compliance with the claimed security functionality. With respect to the evaluation of security properties related to CUMULUS requirements, the evaluation process and artefacts must comply with the SARs.

4.2. Overview of CC certification of Infineon TPM

Security evaluation is a crucial part of the Common Criteria (CC) certification process. The following figure illustrates the three main parties involved in the certification process and the process steps.

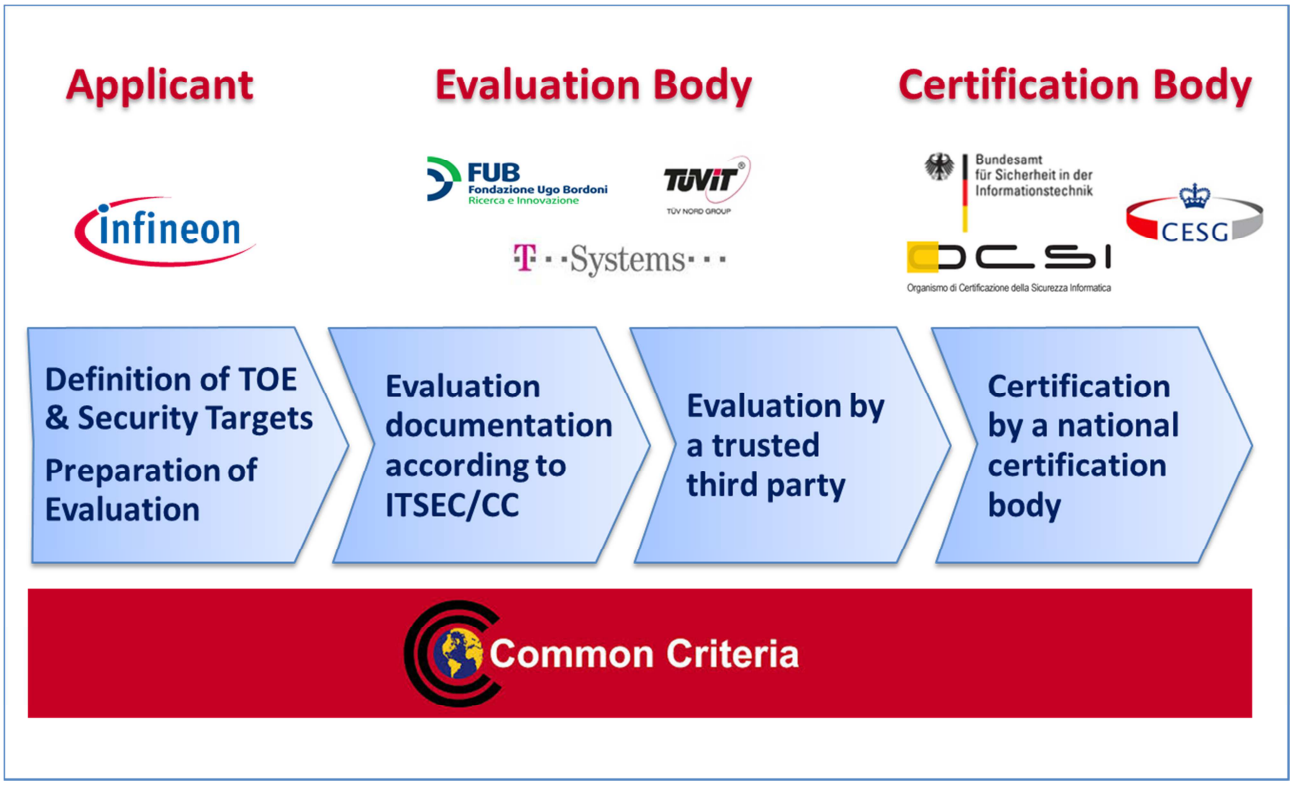

Figure 5. Common Criteria Certification Process

With respect to the TPM 2.0 certification, Infineon Technologies AG is in the role of the applicant. Infineon develops all artefacts necessary for the security evaluation, which includes developing and executing test cases related to the evaluation criteria and writing comprehensive documentation. The applicant's effort and costs exceed Infineon's planned effort in CUMULUS WP6 by far. On the other hand, not all properties covered in the security evaluation are CUMULUS specific. Therefore the work in CUMULUS task 6.3 focusses only the validation criteria listed in section 4.1.
CC defines seven Evaluation Assurance Levels (EAL) which determine the depth and rigor of an evaluation, [15] [16] [17]. Each EAL corresponds to a precisely defined set of security assurance requirements (SARs) covering the complete development of a product, with a given level of strictness, ranging from EAL1, which stands for functionally tested, up to EAL7, meaning formally verified, designed and tested. The following figure depicts the seven levels.

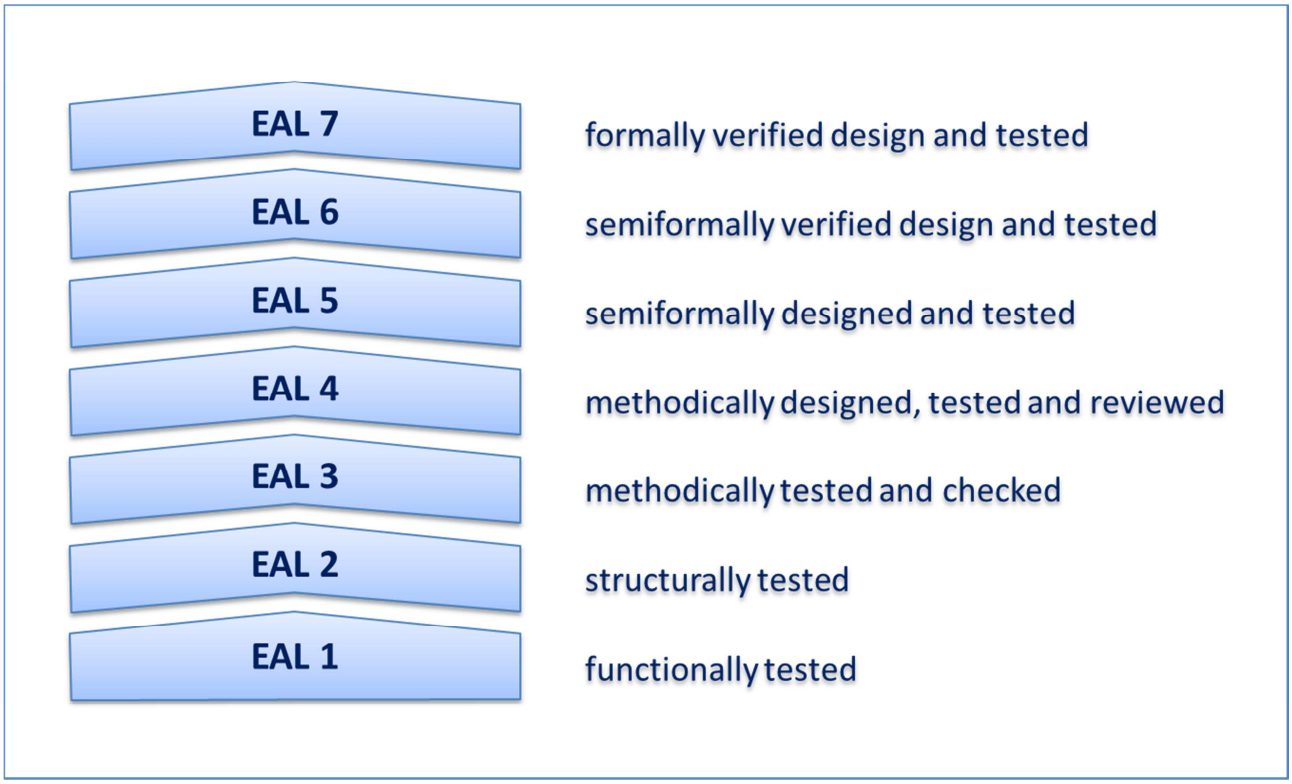

Figure 6. Common Criteria Evaluation Assurance Levels

To meet specific objectives for a given product category to be certified, an assurance level can be augmented by one or more additional SARs. In the EAL notation this augmentation is indicated by a '+' suffix, e.g. "EAL 4 augmented" is noted as "EAL 4+".
In CC Version 3.1 the targeted level of vulnerability analysis and attack potential is specified additionally for security products providing cryptographic functions (called "strength of function" or SOF in earlier CC versions). This corresponds to the minimum effort necessary to successfully attack the underlying security mechanisms. Possible values are basic, enhanced-basic, moderate and high.

The following figure explains the EAL notation, including augmentation and level of vulnerability analysis.

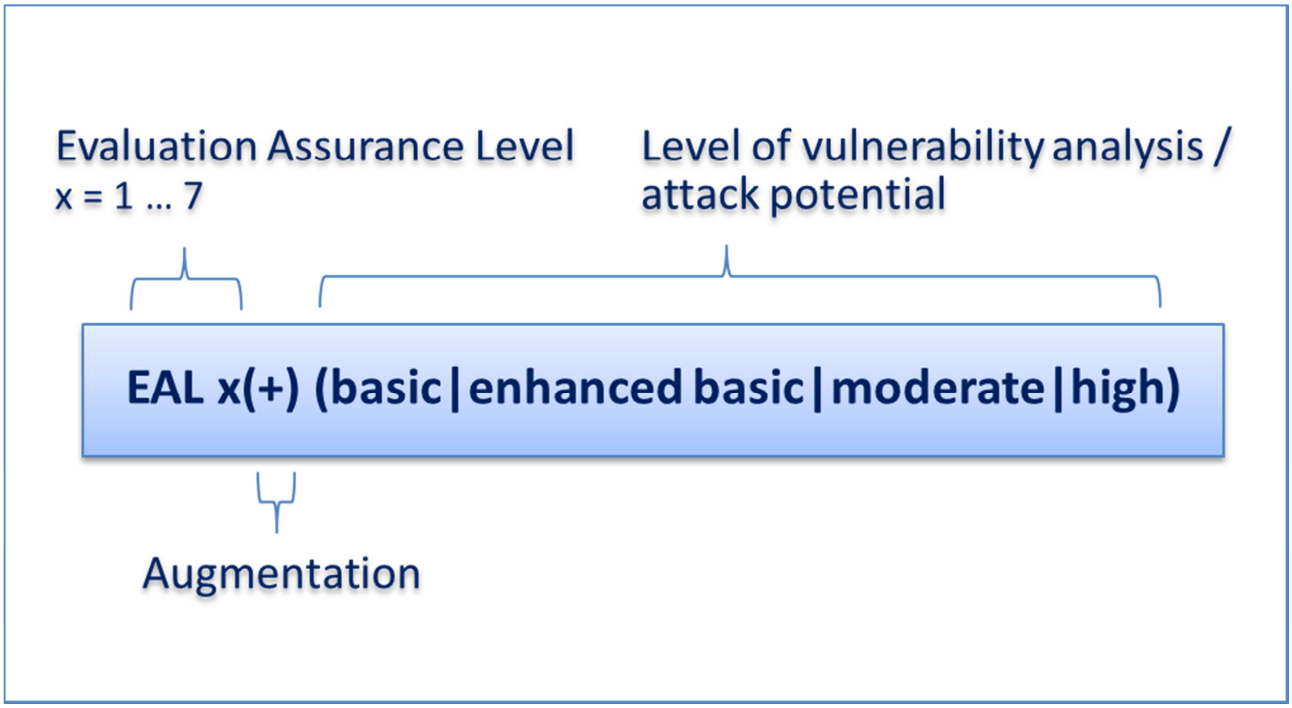

Figure 7. Evaluation Assurance Level Notation

The assurance level targeted by CC TPM 2.0 certification is **EAL 4+ moderate** (according to CC Version 3.1 Revision 4, [15] [16] [17]), which means:

- Methodically designed, tested and reviewed
- Augmented with specific additional SARs required for TPM certification (ALC_FLR.1 and AVA_VAN.4, see [13])
- The evaluator performs penetration testing, to confirm that the potential vulnerabilities cannot be exploited in the operational environment for the Target of Evaluation (TOE). Penetration testing is performed by the evaluator assuming an attack potential of Moderate (AVA_VAN.4, see [13]).

Typical characteristics for this assurance level are approximately 3000 pages of technical documentation and certification duration of 9 to 12 months.

Note that other Infineon products based on the same family of security ICs as the new TPM 2.0 chip are certified to higher assurance levels than EAL4.

4.3. Performed work and achieved results

When the specification of CUMULUS evaluation criteria [13] was written in the beginning of 2014, the release of the TPM 2.0 PP was expected in the second quarter of the same year. As of today, a public review version of the PP has been available for several months, but no released version. The review version does not have any changes concerning the validation criteria relevant for CUMULUS (see section 1.1), and there is no indication that the PP review process will lead to such changes. As a consequence the CC evaluation related work at Infineon could be started nearly as planned originally.

The following tasks have been performed by Infineon in order to define the TOE and Security Targets (ST) and to prepare the evaluation to be executed by an accredited evaluation body:

- Development of tests necessary for the evaluation

- Execution of all tests necessary for the evaluation
- Development of all certification documentation necessary to start the evaluation

In general the first feedback from the evaluation body indicates that the TOE (the new Infineon TPM 2.0 chip) can meet the requirements to be CC certified according to the aimed EAL.

4.3.1. TPM 2.0 Security Evaluation Test Tool

Infineon has developed a TPM 2.0 Security Evaluation Test Tool which covers all the requirements defined in the PP. In particular, for each SFRs listed in [13] a test case has been written. Also all SARs listed in [13] which are relevant for testing, have been considered in the design and implementation of the TPM 2.0 Security Evaluation Test Tool. The tests are integrated in Infineon's continuous build and delivery framework which means that they are fully automated and executed whenever the chip's embedded TPM software is built.

Prior to the start of the TPM 2.0 security evaluation at the authorized evaluation body, all CC related tests have been executed with success.

The following table provides an overview of CUMULUS relevant tests executed by Infineon to prepare CC security evaluation.

Requirement Category	Test Tool	Test Tool Component	Status
Cryptographic SFR	TPM 2.0 Security Evaluation Test Tool (newly developed by IFX, fully automated test execution)	TPM 2.0 Crypto tests	100% test cases executed with success
Measurement and Reporting SFR	TPM 2.0 Security Evaluation Test Tool (newly developed by IFX, fully automated test execution)	TPM 2.0 Measurement & Reporting tests	100% test cases executed with success
Security Assurance Requirements (SAR)	Considered in the design and implementation of the TPM 2.0 Security Evaluation Test Tool		

Table 7. Overview of CUMULUS relevant tests

4.3.2. Cryptographic Security Functional Requirements

The following table shows the mapping of cryptographic SFR and test cases, and the test execution status.

SFR ID	SFR	Test Case	Test Execution Status
FCS_RNG.1	Random number generation	Random number generation	Succeeded
FCS_CKM.1/PK	Cryptographic key generation (primary keys)	Generation of primary keys	Succeeded
FCS_CKM.1/RSA	Cryptographic key generation (RSA keys)	Generation of RSA keys	Succeeded
FCS_CKM.1/ECC	Cryptographic key generation (ECC keys)	Generation of ECC keys	Succeeded
FCS_CKM.1/SYMM	Cryptographic key generation (symmetric keys)	Generation of symmetric keys	Succeeded
FCS_CKM.4	Cryptographic key destruction	Key destruction	Succeeded
FCS_COP.1/AES	Cryptographic operation (symmetric encryption/decryption)	AES encryption and decryption	Succeeded
FCS_COP.1/SHA	Cryptographic operation (hash function)	Hash value calculation	Succeeded
FCS_COP.1/HMAC	Cryptographic operation (HMAC calculation)	HMAC calculation	Succeeded
FCS_COP.1/RSAED	Cryptographic operation (asymmetric encryption/decryption)	RSA encryption and decryption	Succeeded
FCS_COP.1/RSASign	Cryptographic operation (RSA signature generation/verification)	RSA signature generation and verification	Succeeded
FCS_COP.1/ECDSA	Cryptographic operation (ECC signature generation/verification)	ECC signature generation and verification	Succeeded
FCS_COP.1/ECDAA	Cryptographic operation (ECDAA commit)	DAA signature generation	Succeeded

FCS_COP.1/ECDEC	Cryptographic operation (decryption)	Decryption of ECC key	Succeeded

Table 8. TPM V2.0 Cryptographic SFR

4.3.3. Measuring and reporting Security Functional Requirements

The following table shows the mapping of Measurement and Reporting SFR and test cases, and the test execution status.

SFR ID	SFR	Test Case	Test Execution Status
FDP_ACC.1/M&R	Subset access control (measurement and reporting)	M&R access control	Succeeded
FDP_ACF.1/M&R	Security attribute based access control (measurement and reporting)	M&R access control by security attribute	Succeeded
FMT_MSA.1/M&R	Management of security attributes (measurement and reporting)	M&R management of security attributes	Succeeded
FMT_MSA.3/M&R	Static attribute initialization (measurement and reporting)	M&R static attribute initialization	Succeeded
FCO_NRO.1/M&R	Selective proof of origin (measurement and reporting)	M&R proof of origin	Succeeded

Table 9. TPM V2.0 Measurement and reporting SFR

4.3.4. Security Assurance Requirements

The following table shows how the Security Assurance Requirements (SAR) are handled during TPM 2.0 security evaluation.

Assurance Class	Assurance components	Implementation	Evaluation
ADV: Development	ADV_ARC.1 Security architecture description	SLB9665_ARC.doc	Done by IFX
	ADV_FSP.4 Complete functional specification	SLB9665_FSP.doc	Done by IFX
	ADV_IMP.1 Implementation representation of the TSF	SLB9665_IMP.doc	Done by IFX
	ADV_TDS.3 Basic modular design	SLB9665_TDS.doc	Done by IFX

AGD: Guidance documents	AGD_OPE.1 Operational user guidance	SLB9665_AGD.doc	Done by IFX
	AGD_PRE.1 Preparative procedures	SLB9665_AGD.doc	Done by IFX
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation	Development_Prod-uction.doc SLB9665_CMS.doc SLB9665_ALC.doc	Done by IFX
	ALC_CMS.4 Problem tracking CM coverage	Development_Prod-uction.doc SLB9665_CMS.doc SLB9665_ALC.doc	Done by IFX
	ALC_DEL.1 Delivery procedures	Development_Prod-uction.doc SLB9665_ALC.doc	Done by IFX
	ALC_DVS.1 Identification of security measures	SLB9665_ALC.doc	Done by IFX
	ALC_LCD.1 Developer defined life-cycle model	Development_Prod-uction.doc	Done by IFX
	ALC_FLR.1 Basic flow remediation	SLB9665_ALC.doc	Done by IFX
	ALC_TAT.1 Well-defined development tools	Development_Prod-uction.doc SLB9665_ALC.doc	Done by IFX
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims	SLB9665_SecTar.doc	Done by IFX
	ASE_ECD.1 Extended components definition	SLB9665_SecTar.doc	Done by IFX
	ASE_INT.1 ST introduction	SLB9665_SecTar.doc	Done by IFX
	ASE_OBJ.2 Security objectives	SLB9665_SecTar.doc	Done by IFX
	ASE_REQ.2 Derived security requirements	SLB9665_SecTar.doc	Done by IFX
	ASE_SPD.1 Security problem definition	SLB9665_SecTar.doc	Done by IFX
	ASE_TSS.1 TOE summary specification	SLB9665_SecTar.doc	Done by IFX
ATE: Tests	ATE_COV.2 Analysis of coverage	SLB9665_ATE.doc	Done by IFX
	ATE_DPT.2 Testing: security enforcing modules	SLB9665_ATE.doc	Done by IFX
	ATE_FUN.1 Functional testing	SLB9665_ATE.doc	Done by IFX
	ATE_IND.2 Independent testing - sample	Single Evaluation Report ETR-Part AVA	Done by Evaluation Body

AVA: Vulnerability assessment	AVA_VAN.4 Methodical vulnerability analysis	Single Evaluation Report ETR-Part AVA	Done by Evaluation Body

Table 10. Security Assurance Requirements for the TOE

4.3.5. TPM Security Evaluation Documentation

The following documents have been developed to prepare CC security evaluation.

Document	Content & Purpose	Volume	**Confidentiality**	Author(s)
SLB9665_2.0 Security Target	Definition of the security requirements of the product	60 pages	Public (as soon as certification is completed)	Infineon
SLB9665_2.0 Functional Specification	Definition of the TOE Security Functionality Interfaces	50 pages	Confidential	Infineon
SLB9665_2.0 Security Architecture	Definition of the Security Architecture	120 pages	Confidential	Infineon
SLB9665_2.0 Literature_ Reference	Definition of the used Literature and References	20 pages	Confidential	Infineon

Table 11. TPM Security Evaluation Documentation

The following documents will be available after the security evaluation.

Document	Content & Purpose	Volume	**Confidentiality**	Author(s)
SLB9665_2.0 Test Documentation	Definition of the TOE Test procedures	50 pages	Confidential	Infineon
SLB9665_2.0 TOE Design	Definition of the Design of hardware and firmware	180 pages	Confidential	Infineon
SLB9665_2.0 Guidance Documentation	Definition of the TOE User Guidance	10 pages	Confidential	Infineon
SLB9665_2.0 AIS20 Developer evidence for the DRNG	Definition of the TOE DRNGs	30 pages	Confidential	Infineon
SLB9665_2.0 Life-cycle Support	Definition of the TOE life cycle	15 pages	Confidential	Infineon
SLB9665_2.0 Configuration Management	Definition of the TOE configuration management	15 pages	Confidential	Infineon
SLB9665_2.0 Implementation	Definition of the TOE implementation and generation processes	50 pages	Confidential	Infineon
Production and Development	Definition of the TOE development, production,	70 pages	Confidential	Infineon

	test and delivery processes			
Protection Profile PC Client Specific TPM	Definition of the TOE Security Requirements	110 pages	Public	Trusted Computing Group

Table 12. Documentation after evaluation

The following documents will be available after the CC certification.

Document	Content & Purpose	Volume	**Confidentiality**	Author(s)
Protection Profile PC Client Specific TPM	Definition of the TOE Security Requirements	110 pages	Public	Trusted Computing Group
SLB9665_2.0 Security Target	Definition of the security requirements of the product	60 pages	Public	Infineon
Certification Report BSI-DSZ-CC-0965-2015 for SLB9665_2.0	Certification report of the Bundesamt für die Sicherheit in der Informationstechnik	40 pages	Public	Bundesamt für die Sicherheit in der Informations-technik

Table 13. Documentation after CC certification

4.4. Outlook and next steps

As of January 2015, Infineon plans to complete the TPM 2.0 security evaluation in the first half-year of 2015. Subsequently, the Common Criteria certification will be undertaken. An update and final version of this evaluation report will be provided in D6.6.

5. Annexes

This deliverable is presented along with some **confidential** annexes related to the validation session hosted in Rome in January 13th and analyzed in section 3. These annexes are the following:

- A presentation covering an overview of the CUMULUS Project, and going into detail for the following matters: CUMULUS Framework, CUMULUS Meta Model, CUMULUS Test Based Certification Model and CUMULUS Adoption Costs and Benefits.
- A questionnaire on the topics covered by this presentation
- A presentation on the CUMULUS Monitoring Based Certification Model.
- A questionnaire on the topics covered by the second presentation.
- The feedback collected from the validators

References

[1] ENISA: European Union Network Information Security Agency: https://www.enisa.europa.eu/

[2] Marnix Dekker, Dimitra Liveri: *Certification in the EU Cloud Strategy*. ENISA. November 2014.

[3] CCM: Cloud Control Matrix: https://cloudsecurityalliance.org/research/ccm

[4] ENISA: *Security Certification Practice in the EU. Information Security Management Systems – A case study*. October 2013.

[5] C.Casper, A.Esterle: *Information Security Certification. A Primer: People, Products, Processes*. ENISA. December 2007

[6] ISO: *Glossary of terms and abbreviations used in ISO/TC Business Plans.* http://isotc.iso.org/livelink/livelink/fetch/2000/2122/687806/Glossary.htm?nodeid=2778927&vernum=0

[7] *Information Technology — Cloud Computing — Reference Architecture*. ISO/IEC 17789. 2014.

[8] International Telecommunications Union: *Recommendation ITU-T Y.3501 Cloud Computing framework and high-level requirements. Series Y: Global Information Infrastructure, Internet Protocol Aspects and Next-Generation Networks*. May 2013

[9] Monica Lagazio, David Barnard-Wills, Rowena Rodrigues, David Wright: *Certification Schemes for Cloud Computing. European Comission*. DG Communications Networks, Content & Technology. 2014

[10] Certificate of Cloud Security Knowledge: https://cloudsecurityalliance.org/education/ccsk/

[11] Cloud Security Alliance: *Requirements for bodies providing STAR Certification*. 2012

[12] Cloud Security Alliance: *Auditing the Cloud Control Matrix. Guidance Document*. August 2013

[13] D6.2 Specification of CUMULUS evaluation criteria – Project CUMULUS Grant agreement no.: 318580 (FP7-ICT-2011-8)

[14] Protection Profile for PC Client Specific TPM, Family 2.0, Draft Revision 0.21 (Public Review Version), June 2014, Trusted Computing Group, Incorporated

[15] Common Criteria for Information technology Security Evaluation, Part 1: Introduction and general model, September 2012, Version 3.1 Revision 4, CCMB-2012-09-001

[16] Common Criteria for Information technology Security Evaluation, Part 2: Security functional components, September 2012, Version 3.1 Revision 4, CCMB-2012-09-002

[17] Common Criteria for Information technology Security Evaluation, Part 3: Security assurance components, September 2012, Version 3.1 Revision 4, CCMB-2012-09-003

[18] Information Assurance Directorate: *Protection Profile for IPSec Virtual Private Network (VPN) Clients v1.1*. December 2012

[19] ESM Protection Profile Technical Community: *Standard Protection Profile for Enterprise Security Management Identity and Credential Management*. October 2013.

[20] National Information Assurance Partnership: *Protection Profile for Certification Authorities. May* 2014.

[21] MSP Alliance: *10 Reasons to buy cyber liability insurance*. Available on: http://www.mspalliance.com/wp/wp-content/uploads/2008/11/Cyber10Reasons.pdf

[22] ENISA: *Cloud Certification Schemes Metaframework.* November 2014. https://resilience.enisa.europa.eu/cloud-computing-certification/cloud-certification-schemes-metaframework

[23] D6.1 Specification of pilot scenarios and requirements – Project CUMULUS Grant agreement no.: 318580 (FP7-ICT-2011-8)

[24] D2.3 Certification models v.2 – Project CUMULUS Grant agreement no.: 318580 (FP7-ICT-2011-8)

[25] ISO/IEC 27001:2005: *Information technology, security techniques, information security management systems, requirements*. 2013

[26] NIST Special Publication 800-53: *Security and Privacy Controls for Federal Information Systems and Organizations*. April 2013

[27] FEDRAMP Public Website: http://cloud.cio.gov/fedramp

[28] Payment Card Industry Data Security Standard: *Requirements and Security Assessment Procedures*. Version 2.0. October 2010.

[29] IT Governance Institute: COBIT Framework v4.1

[30] ENISA: *Information Assurance Framework*. November 2009