MEDINA: Improving Cloud Services trustworthiness through continuous audit-based certification

Leire Orue-Echevarria [1], Jesus Luna Garcia [2], Christian Banse [3] and Juncal Alonso [1]

[1] *TECNALIA, Basque Research and Technology Alliance (BRTA), Parque Científico y Tecnológico de Bizkaia, Astondo bidea,700, E-48160 Derio, Spain*
[2] *Robert Bosch GmbH, Postfach 30 02 20 , 70442 Stuttgart, Germany*
[3] *Fraunhofer AISEC, Lichtenbergstraße 11, 85748 Garching near Munich, Germany*

Abstract

One of the reasons of the still limited adoption of Cloud Computing in the EU is the EU customers' perceived lack of security and transparency in this technology. Cloud service providers (CSPs) usually rely on security certifications as a mean to improve transparency and trustworthiness, however European CSPs still face multiple challenges for certifying their services (e.g., fragmentation in the certification market, and lack of mutual recognition). In this context, the EU Cybersecurity Act (EU CSA) proposes improving customer's trust in the European ICT market through a European certification scheme (EUCS). The proposed cloud security certification scheme conveys new technological challenges including the notion of automated monitoring for the whole supply chain, which needs to be solved in order to bring all the expected benefits to EU cloud providers and customers. In this context, MEDINA proposes a framework for supporting a continuous audit-based certification for CSPs based on EU CSA's scheme for cloud security certification. MEDINA will tackle challenges in areas like security validation/ testing, machine-readable certification language, cloud security performance, and audit evidence management. MEDINA will provide and empirically validate sustainable outcomes in order to benefit EU adopters.

Keywords

cloud certification scheme, Cybersecurity Act, continuous auditing, continuous certification, smart contracts, certification language

1. Introduction and motivation

Despite the conspicuous benefits to customer's trustworthiness in cloud services, which result from leveraging recognized security certifications (just as evidenced by the EU Cybersecurity Act (EU CSA)), it is also true that European cloud providers currently face multiple challenges to certify their services. Take for example the European Commission's study SMART 2016/0029 "Certification schemes for cloud computing" led by TECNALIA [3], which shows that the market penetration of the cloud security certification is rather uneven. ISO 27001-based certifications are leading the market, despite being a generic IT systems management standard and not focusing solely on cloud services. The above-mentioned study has analysed the market penetration of international certification schemes (e.g., ISO, Cloud Security Alliance, …), Member States' schemes (e.g., Germany's BSI C5, Spain's Esquema Nacional de Seguridad – ENS), private initiatives (e.g., Zeker online, EuroCloud), public-private initiatives (e.g. Trusted Cloud) and cross-border initiatives (e.g., ESCloud) in 50 Cloud Service Providers (CSPs). The conclusions demonstrate a big fragmentation in the domain of existing certification schemes.

First workshop on trustworthy software and open source, March 23-25, 2021, Virtual Conference
EMAIL: Leire.Orue-echevarria@tecnalia.com (L.Orue-Echevarria) ; Jesus.LunaGarcia@de.bosch.com (J. Luna Garcia), christian.banse@aisec.fraunhofer.de (C. Banse) , juncal.alonso@tecnalia.com (J. Alonso)
ORCID: 0000-0002-0648-4689 (L. Orue-Echevarria); 0000-0002-9244-2652 (J. Alonso);

In addition to the evident fragmentation in cloud security certification schemes, the EC study also highlighted the diverse focus of the different security controls in current certification schemes.

The final challenge that European cloud providers face when seeking a certification is the selection of the conformity assessment method (CAM). Several different CAMs exist at the state of practice such as self-assessment, evidence-based, ISO-based, and ISAE 3402. Each of these CAMs also have different scopes. While ISO mainly assesses if security measures are defined and put in place at a certain point of time, ISAE evaluates the efficiency of the implemented controls in a period of time, usually six months.

The conspicuous lack of cloud-specific security certifications, in addition to the existing market fragmentation (scope, methodologies), hinder transparency and accountability in the provision of European cloud services. Both issues ultimately reflect on the level of customer's trustworthiness and adoption of cloud services in Europe.

In an effort to solve some of the challenges depicted above, the EU Cybersecurity Act (EU CSA, approved in June 2019) in its Title III gives ENISA the mandate of defining and implementing a European security certification scheme for ICT products, processes and services for three different levels of assurance (low, substantial, and high). Being cloud computing one of the identified EU CSA priorities, Articles 54 (j) and 57 (9) propose the possibility of deploying a high-assurance, evidence-based and continuous certification of European cloud providers. Despite the evident benefits of EU CSA's principles for the European market and cloud customers, currently there are no concrete cloud certification frameworks nor tools for implementing any of those proposals.

To overcome this situation, the main objective of the MEDINA European research project [14] is to provide a holistic framework that enhances cloud customers' control and trust in consumed cloud services, by supporting CSPs (IaaS, PaaS and SaaS providers) towards the successful achievement of a continuous certification aligned to the EU Cybersecurity Act (EU CSA). Such certification should fulfill the requirements of the EU cloud security certification scheme in their basic, substantial and high assurance levels. The proposed framework will be comprised of tools, techniques, and processes supporting the continuous auditing and certification of cloud services where security and accountability are measurable by design. As the MEDINA framework is leveraged into a cloud supply chain, it will support continuously assessing the efficiency and efficacy of security measures to ultimately achieve and maintain a certification.

The rest of this paper is structured in the following manner: Section 2 introduces an overview of the related state of the art and the progress that MEDINA expect to provide to each topic. Section 3 details the MEDINA approach for Cloud Security Continuous Certification and section 4 oversees the future work in MEDINA.

2. Introduction and motivation

In the last years, several projects and initiatives have worked in research areas of interest for continuous certification of security in Cloud Services. Table 1 shows an overview of the main challenges identified after the analysis of the current state of the art per area of interest, considering national and/or international initiatives, and highlighting the main scientific advances that MEDINA will bring.

Table 1
State of the art analysis

Topic and related works	Current state-of-the-art (SOTA)	Expected progress beyond the SOTA
Cloud security certification schemes and conformity assessments [26], [3]	• Fragmented certification schemes. • Partial coverage of relevant cloud security controls.	• MEDINA framework supports the homogenization of certification schemes, by aligning to the EU CSA.

	• Wide variety of conformity assessment methods.	• Framework fully covers security controls from relevant standards and good practices. • MEDINA leverages conformity assessment methodologies proposed to EU CSA
Continuous assessment, audit and certification [22], [18], [10], [19], [8]	• Static cloud security configurations, i.e., forced by traditional audits, cannot adapt to a changing threat landscape. • Lack of KPIs and techniques for measuring cloud security efficiency/efficacy. • Trustworthiness of evidences, and automation are missing in current cloud certification processes. • Non-technical measures are not quantifiable and thus currently hard to assess continuously	• Toolset supporting EU CSA's cloud certification processes, including automation (smart contracts), accountability and trustworthiness. • Risk-based MEDINA's framework supports CSPs in adapting security configuration at run-time/design-time, in a certifiable manner. • Contribution of a repository containing TOMs, metrics and security KPIs derived from internationally accepted control frameworks. • New techniques to analyse the semantic of documents and process descriptions to address non-technical and organisational controls
Policies for certification language [27], [28], [6], [5], [29], [21]	• Limited scope of existing tools on new computing paradigms such as serverless computing • Existing static code analysis techniques are not adopted to the needs of gathering evidences in a certification context • Non-technical measures are not quantifiable and thus currently hard to assess continuously • Auditors lack real-world experience on continuous certification	• Provision of a broad spectrum of evidence gathering techniques for technical measures, such as security assessment of cloud workloads, containers and serverless functions • Analysis of data flows of cloud applications using code property graphs on incomplete source code • Machine-learning and NLP to analyse the semantic of documents and process to address non-technical or organisational measures • Validation of techniques based on real-world audit practices
Economic and risk aspects of certification [16], [15], [30], [2], [11], [31], [12], [7]	• Lack of (economic) analysis for evaluating the cost-benefit of security certifications, and related cybersecurity risks.	• MEDINA framework for quantitative risk-assessment for cloud security certification. • Contribution of validated cost-benefit analysis

	• No CSP guidance for selecting risk-assessment methodologies for purposes of cloud certification. • Entry barrier for small EU CSPs, which face costly setup of security configurations to achieve a certification.	to ensure the cost-effectiveness of the selected countermeasures. • The MEDINA framework will also help to compare various security system configurations to support CSPs in their certification efforts. • Provide support re-evaluate the CSP security configuration at run-time, thus ensuring continuous adaptability of the certification.

3. MEDINA approach

The MEDINA approach is depicted in Figure 1 MEDINA approach for continuous Cloud Services certification against the EU Cloud Certification Scheme (EUCS). It describes the lifecycle of continuous Cloud security certification, from the definition of the security controls and metrics to the continuous auditing of the evidences. Such lifecycle can be summarized as follows:

1. Define a catalogue of metrics associated to technical and organizational measures out of the MEDINA catalogue (e.g., based on EUCS [4]). This repository of metrics (Key result 1- [KR1]) and measures entails a clear definition of the technical and organizational measures (TOMs) relevant for cloud service providers. The repository also includes the corresponding security metrics (both quantitative and qualitative) for security requirements/TOMs such as those related to system security and integrity, operational security, business continuity and incident management.
2. Select controls: Taking into consideration the CSPs risk appetite following a risk-based approach and the chosen assurance level, the CSP shall select the implementing TOMs and related metrics for all security controls considering its risk appetite. MEDINA offers a tool-supported risk-based approach [KR2] to select the appropriate controls aligned with the overall risk "appetite" of the organisation. This will be based on a risk self-assessment tool and will help to identify the core assets of the service (considering all involved stakeholders), help to value them and identify the relevant threats. Furthermore, the framework will be improved to propose an (near) optimal security configuration to ensure the optimal coverage of security risks. After that, assets of the cloud service and relevant IT threats shall be identified, and additional implementing TOMs proposed [KR2]. MEDINA proposes a tool-supported methodology for the selection of additional controls and associated TOMs, which address the concrete needs of a CSP taking into consideration both its risk appetite and requested certification's assurance level.
3. Specify the certification language: currently certification schemes are expressed using natural language. MEDINA proposes to transform this certification language into a machine-readable expression [KR3], by using NLP, including aspects such as scope of the certification, assurance level and conformity assessment method. For a lean and seamless trait d'union between what is required by official documents of the European Commission in terms of certification to the definition of the machine-readable certification language [KR3] MEDINA intends to develop:

- A procedure to semi-automatically translate Natural Language (NL) certifications terms and conditions, as they appear on official documents like, e.g., the Cybersecurity Act, into a Controlled Natural Language (CNL) [9];
- A tool to edit, tune and revise semi-automatically generated CNL, to manually improve the translation and verify the generated statements;
- A component to map the CNL to a runtime-enforceable Domain-Specific Language (DSL) that can be used by assessment tools to check the compliance status of the stated certification terms and conditions.

4. Collect and evaluate evidences, continuously and automatically audit: Once the scope of the certification scheme is established, the evidences need to be collected [KR4] at cloud service as well as code level, both at design and at operation time, that is, during the whole lifecycle of the cloud service. The collected evidences need to be ensured that no one has tampered with them and are trustworthy. MEDINA refers to Distributed Ledger Technologies (DLT)-based that manage evidence (e.g., on a private blockchain) based on additional information about the deployed or to-be-deployed services. Moreover, these evidences are continuously evaluated [KR5] and the risks continuously monitored and updated [KR6], in order to have a secure operational service certifiable through the selected conformity assessment method.
5. Achieving continuous certification is the process of continuously evaluating whether appropriate evidence is collected [KR4] that supports the fulfilment of individual controls of a certification target. MEDINA aims to greatly reduce this effort by providing quantitative measures for both the target as well as the evidence. Since evidence is collected as a set of measurable metrics (e.g., by measuring the value 256 of the metric key-size, simple Boolean expressions such as key-size => 128 in the certification target can be employed), MEDINA is able to validate whether a measurement result fulfil the certifiable requirement or not [KR5].

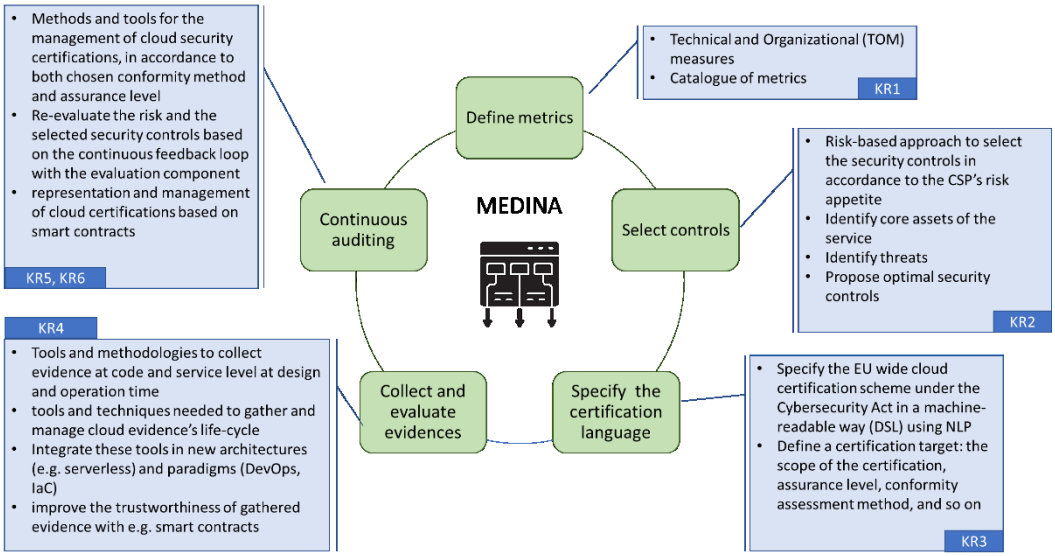

Figure 1 MEDINA approach for continuous Cloud Services certification against the EU Cloud Certification Scheme (EUCS).

Summarizing from the table above (Table 1) and the approach presented here it can be concluded that no initiative or commercial solution fully covers the objectives of MEDINA.

4. Use cases

The MEDINA framework will be validated in two use cases:

1. European Certification of Multi-cloud backends for IoT Solutions, provided a big industrial player such as Bosch. This use case will deploy a set of IaaS and PaaS services, commonly used for IoT backends, in at least three public CSPs (e.g., Microsoft Azure, AWS, and Fabasoft). This case includes managed Kubernetes clusters, transactional SQL databases, raw virtual storage, virtual networks, virtual machines (e.g., as jump hosts), and serverless PaaS (e.g., functions). Furthermore, widely used "support" PaaS will be also deployed e.g., virtual hardware security modules (HSM), log repositories, application gateways, and network security groups/firewalls-as-a-service. Those PaaS components will be orchestrated to mock-up and IoT service based on the company's industrial experience. Having a measurable, holistic, and end-to-end view of the security measures (TOMs) implemented in such a complex cloud ecosystem becomes essential for the certification process of the supply chain. Beyond its usage for the European certification, the continuously achieved levels of security transparency bring

a huge benefit to the internal processes of the organization providing the IoT solution e.g., security governance, security benchmarking, measurable efficiency and efficacy of implemented TOMs, and enablement of secure DevOps.

2. Continuous Audit of SaaS Solutions for the Public Sector: this use case provided by Fabasoft aims to provide a high level of automation to the current audit process of a SaaS provider in alignment to the EU CSA, with particular focus on continuous audit-based certification. At the state of practice, for a good number of requirements in current certification schemes (e.g., BSI C5, SOC2, ISO 20017, etc.), several CSPs already collect evidence automatically by using monitoring tools, log files, internal versioning and the likes. However, this generated evidence cannot, to date, be evaluated and audited automatically (continuously) due to the lack of standardized processes and tool chains. Furthermore, there is no clear definition of what "real evidence" is (i.e., evidence that auditors consider trustworthy for certification purposes), when it is automatically produced. The tools and techniques proposed by MEDINA will be validated in this use case, taking into consideration the objectives and Key Results expected from the project.

5. Conclusions and future work

This paper presented the proposed MEDINA approach to support current challenges in the continuous security certification of Cloud Computing services. MEDINA proposes to increase the trustworthiness of the Cloud Services and Cloud Service Providers through a framework of methods, mechanism and tools supporting continuous cloud security certification, through trustworthy evidence-management methods. The project started in November 2020 and will last 36 months. Currently the reference architecture for the MEDINA framework is being designed, and the first versions of the methods and prototypes will be ready during 2021.These initial versions will be validated by two European Cloud Providers which are part of the MEDINA consortium, Robert Bosch GmbH and Fabasoft.

Acknowledgements

This work has been partially funded by the European project MEDINA (Horizon 2020 research and innovation Programme, under grant agreement no 952633).

References

[1] M. Anisetti, C.A. Ardagna, E. Damiani, N. El Ioini, F. Gaudenzi, Modeling time, probability, and configuration constraints for continuous cloud service certification, Computers & Security. 72 (2018) 234–254.

[2] R.M. Blank, A. Secretary, Guide for Conducting Risk Assessments, 2011.

[3] European Commission. Directorate General for Communications Networks, Content and Technology., Fundación TECNALIA RESEARCH & INNOVATION., Certification schemes for cloud computing: final report., Publications Office, LU, 2018.

[4] European Union Agency for Cybersecurity, EUCS – Cloud Services Scheme, n.d.

[5] A. Fantechi, A. Ferrari, S. Gnesi, L. Semini, Requirement Engineering of Software Product Lines: Extracting Variability Using NLP, in: 2018 IEEE 26th International Requirements Engineering Conference (RE), 2018: pp. 418–423.

[6] A. Ferrari, G. Gori, B. Rosadini, I. Trotta, S. Bacherini, A. Fantechi, S. Gnesi, Detecting requirements defects with NLP patterns: an industrial experience in the railway domain, Empir Software Eng. 23 (2018) 3684–3733.

[7] J. Großmann, F. Seehusen, Combining Security Risk Assessment and Security Testing Based on Standards, in: F. Seehusen, M. Felderer, J. Großmann, M.-F. Wendland (Eds.), Risk Assessment and Risk-Driven Testing, Springer International Publishing, Cham, 2015: pp. 18–33.
[8] D. Knoblauch, C. Banse, Reducing Implementation Efforts in Continuous Auditing Certification Via an Audit API, in: 2019 IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), IEEE, Napoli, Italy, 2019: pp. 88–92.
[9] T. Kuhn, A Survey and Classification of Controlled Natural Languages, Computational Linguistics. 40 (2014) 121–170.
[10] I. Kunz, P. Stephanow, A Process Model to Support Continuous Certification of Cloud Services, in: 2017 IEEE 31st International Conference on Advanced Information Networking and Applications (AINA), IEEE, Taipei, Taiwan, 2017: pp. 986–993.
[11] M.S. Lund, B. Solhaug, K. Stølen, Model-Driven Risk Analysis, Springer Berlin Heidelberg, Berlin, Heidelberg, 2011.
[12] S.N. Matheu-García, J.L. Hernández-Ramos, A.F. Skarmeta, G. Baldini, Risk-based automated assessment and testing for the cybersecurity certification and labelling of IoT devices, Computer Standards & Interfaces. 62 (2019) 64–83.
[13] I. Matteucci, M. Petrocchi, M.L. Sbodio, CNL4DSA: a controlled natural language for data sharing agreements, in: Proceedings of the 2010 ACM Symposium on Applied Computing - SAC '10, ACM Press, Sierre, Switzerland, 2010: p. 616.
[14] MEDINA, MEDINA Security framework to achieve a continuous audit-based certification in compliance with the EU-wide cloud security certification scheme - Annex 1, DoA Part B, 2020.
[15] T. Mikolov, I. Sutskever, K. Chen, G. s Corrado, J. Dean, Distributed Representations of Words and Phrases and their Compositionality, Advances in Neural Information Processing Systems. 26 (2013).
[16] N.M. Müller, D. Kowatsch, P. Debus, D. Mirdita, K. Böttinger, On GDPR Compliance of Companies' Privacy Policies, in: K. Ekštein (Ed.), Text, Speech, and Dialogue, Springer International Publishing, Cham, 2019: pp. 151–159.
[17] E. Schmieders, A. Metzger, K. Pohl, A Runtime Model Approach for Data Geo-location Checks of Cloud Services, in: X. Franch, A.K. Ghose, G.A. Lewis, S. Bhiri (Eds.), Service-Oriented Computing, Springer Berlin Heidelberg, Berlin, Heidelberg, 2014: pp. 306–320.
[18] P. Stephanow, N. Fallenbeck, Towards Continuous Certification of Infrastructure-as-a-Service Using Low-Level Metrics, in: 2015 IEEE 12th Intl Conf on Ubiquitous Intelligence and Computing and 2015 IEEE 12th Intl Conf on Autonomic and Trusted Computing and 2015 IEEE 15th Intl Conf on Scalable Computing and Communications and Its Associated Workshops (UIC-ATC-ScalCom), IEEE, Beijing, 2015: pp. 1485–1492.
[19] P. Stephanow, K. Khajehmoogahi, Towards Continuous Security Certification of Software-as-a-Service Applications Using Web Application Testing Techniques, in: 2017 IEEE 31st International Conference on Advanced Information Networking and Applications (AINA), IEEE, Taipei, Taiwan, 2017: pp. 931–938.
[20] P. Stephanow, M. Moein, C. Banse, Continuous Location Validation of Cloud Service Components, in: 2017 IEEE International Conference on Cloud Computing Technology and Science (CloudCom), 2017: pp. 255–262.
[21] I.K. Tanoli, M. Petrocchi, R. De Nicola, Towards automatic translation of social network policies into controlled natural language, in: 2018 12th International Conference on Research Challenges in Information Science (RCIS), IEEE, Nantes, 2018: pp. 1–12.
[22] I. Windhorst, A. Sunyaev, Dynamic Certification of Cloud Services, in: 2013 International Conference on Availability, Reliability and Security, IEEE, Regensburg, Germany, 2013: pp. 412–417.
[23] F. Yamaguchi, N. Golde, D. Arp, K. Rieck, Modeling and Discovering Vulnerabilities with Code Property Graphs, in: 2014 IEEE Symposium on Security and Privacy, 2014: pp. 590–604.
[24] [24] J. Zhang, N.M. El-Gohary, Semantic NLP-Based Information Extraction from Construction Regulatory Documents for Automated Compliance Checking, J. Comput. Civ. Eng. 30 (2016) 04015014.
[25] P. Zhou, Ontology-based information extraction from environmental regulations for supporting environmental compliance checking, 2015.

[26] “Unleashing the Potential of Cloud Computing in Europe,” EC, 2012.
[27] OSCAL, (n.d.).
[28] OWL - Semantic Web Standards, (n.d.).
[29] Natural Language Toolkit — NLTK 3.5 documentation, (n.d.).
[30] PAe - MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, (n.d.).
[31] Self-Assessment Tools | CyberSecurity Observatory, (n.d.).