The AssureMOSS security certification scheme

Ákos Milánkovich
akos.milankovich@search-lab.hu
Search-Lab Ltd.
Budapest, Hungary

Gergely Eberhardt
gergely.eberhardt@search-lab.hu
Search-Lab Ltd.
Budapest, Hungary

Dávid Lukács
david.lukacs@search-lab.hu
Search-Lab Ltd.
Budapest, Hungary

ABSTRACT

In the AssureMOSS project we aim to improve the security of MOSS (Multi-party Open Software and Services), which faces challenges of increasing complexity, high-frequency update cycles and high costs of evaluation. In this quest we will create a methodology to evaluate and certify MOSS projects regularly to improve and maintain a higher level of security in those projects. We aim to make the methodology and tools related to this effort open source for the benefit of the open projects.

As a first step, this document presents the state of the art in security certification through showing the most popular and relevant – from the point of view in AssureMOSS – certification schemes. Moreover, as some shortcomings of these schemes are presented, we present the motivation behind the creation of the AssureMOSS scheme was necessary. In AssureMOSS we concentrate on the domain of MOSS, where constant recertification caused by the rapid release cycles of a product would cause extreme overhead in the budget and for developers as well if they need to maintain a documentation suitable for security evaluation. The AssureMOSS scheme would fill a void in the cloud- and microservices domain by employing the concept on delta evaluation in a lightweight certification scheme. Building on the capabilities of the AssureMOSS tools and implementing the methodology of the hereby presented AssureMOSS scheme we will build on the DeltAICert tool, which will be able to help the work of security evaluators by automating the security evaluation and certification process via delta evaluation, which concentrates the evaluation effort on the changes between the certified and new version of the target of evaluation (ToE).

CCS CONCEPTS

• **Security and privacy → Security requirements**; **Trust frameworks**.

KEYWORDS

Delta, security, certification, scheme, microservices, MOSS

ACM Reference Format:

Ákos Milánkovich, Gergely Eberhardt, and Dávid Lukács. 2022. The AssureMOSS security certification scheme. In *The 17th International Conference on Availability, Reliability and Security (ARES 2022), August 23–26, 2022, Vienna, Austria.* ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3538969.3543804

ARES 2022, August 23–26, 2022, Vienna, Austria

ACM ISBN 978-1-4503-9670-7/22/08…$15.00
https://doi.org/10.1145/3538969.3543804

1 INTRODUCTION

This paper introduces the AssureMOSS scheme, developed in the AssureMOSS project [3] which uses the concept of delta evaluation to provide a more economical security certification methodology. The requirements of the scheme are defined for MOSS with microservices-based architecture.

We discuss how we build on existing standards (subsets of their requirements), best practices and topic of research to create a new scheme, which makes automatic certification possible. The scheme aims to improve the efficiency of security evaluations by automating the evaluation of changes introduced to the ToE after a full manually assisted evaluation. Subsequent evaluations can be fully automated or require significantly lower effort from human experts, as the AssureMOSS tools will be able to gather indicators and evidence about the occurred changes that can be used to make the security assessment based on the rules the first evaluation defined. The scheme incorporates risk assessment as well, which can even be real-time in case runtime monitoring of the ToE is provided. The validity of the certification would dynamically respond to newly discovered vulnerabilities or incidents. The paper is structured as follows: Section 1 introduces the context of certification schemes and initial motivation. Section 2 of the document describes the popular and relevant certification schemes along with showing their strengths and weaknesses in a comparison and assessment, introducing the need for the AssureMOSS scheme. Section 3 describes the AssureMOSS scheme by introducing the methodology, the requirements, and the certification life cycle. Section 4 shows the next steps.

2 IT SECURITY CERTIFICATION SCHEMES

2.1 Certification schemes landscape

This chapter introduces certification concepts and processes, particularly to industry-standards and EU-derived solutions. Many of them are globally accepted by regulators and authorities or it was created by them. The schemes presented here were selected based on popularity and relevance to the concepts the AssureMOSS scheme uses.

In the summary of this section, we are giving a general overview about the concepts and processes of these schemes and show the motivation behind the need of the new AssureMOSS scheme.

2.1.1 Common Criteria. As the most well-established internationally accepted general security certification scheme, the Common Criteria serves basis for many other certification schemes as well. It layed the ground as a framework to evaluate a wide range of

products and services. The Common Criteria for Information Technology Security Evaluation (CC) [6] is an international standard (ISO/IEC 15408) used for declaring and validating the security level of a product in computer security. It was developed and defined based on the CTCPEC, TCSEC and the ITSEC in 1994 by the government of the Netherlands, France, Canada, Germany, the UK, and the USA. With the help of the CC certification which imply an objective evaluation of a device, system, or any other kind of IT product to ensure that it fulfils a well-defined bunch of security relevant requirements. With CC it is easier to avoid re-evaluations for products that were devoted to international markets.
During a CC evaluation several Key Concepts [6] shall be considered:

- **Target of Evaluation (ToE)**: specifies the exact product (device or system) which is the subject of the evaluation process for a CC certification.
- **Protection Profile (PP)**: a document which defines and details a separate standard set of security requirements and secure implementation objectives for a product or a specific type of product or system (like firewalls, digital signature, or intrusion detection systems).
- **Security Target (ST)**: a document which contains information and details about the exact security properties and the correct operational environment of the ToE. As it was stated at the PP description, many times an ST may claim conformance with one or more PPs.
- **Security Functional Requirements (SFRs)**: details those functionalities that the evaluated product will provide. As a base CC provide a base list of standard functionalities that the different kinds of products are able to provide.
- **Security Assurance Requirements (SARs)**: [8] expressed in a PP or in a ST. Quality assurance requirement, which verifies the development and evaluation processes to ensure compliance with the related security functionalities.
- **Evaluation Assurance Level (EAL)**: As a result of a CC evaluation, an assurance level called EAL [7] shall be specified, which defines the tasks and methods how the TOE shall be tested, and it shows the thoroughness of the evaluation as well. Each EAL level defines which assurance components from the related class shall be fulfilled. The different EAL levels:
  - EAL1 Functionally Tested
  - EAL2 Structurally Tested
  - EAL3 Methodically Tested and Checked
  - EAL4 Methodically Designed, Tested, and Reviewed
  - EAL5 Semiformally Designed and Tested
  - EAL6 Semiformally Verified Design and Tested
  - EAL7 Formally Verified Design and Tested

The maximum EAL that a product can gain is EAL7. The higher the EAL level is the more stringent the evaluation were. However, basically EAL levels do not show the security level of the specific product or system, rather it measures the scale and scope to which the security of the product or system was tested. This means that an EAL4 evaluation compared to EAL1 has a wider scale of security evaluation with a more comprehensive set of security requirements on which the ToE must pass. Obviously, with a higher EAL level the required effort grows together with the price and the duration of the evaluation. At the time of writing altogether more than 1500 products are CC certified in 14 different categories. In [6], an estimation of the efforts and the costs can be observed, stating that an EAL 1 certification required about 33-72 man-days and associated costs of 27.000-74.000€. EAL 5 required approximately 121-238 man-months and 97.000-241.000€, which illustrates how complex and resource-intensive is the certification process for CC. The AssureMOSS scheme aims to provide a more lightweight approach in terms of expert effort and costs.

2.1.2 CSPN. In AssureMOSS we aim to provide a more lightweight approach in terms of complexity and costs compared to Common Criteria. The Certification de Sécurité de Premier Niveau (First Level Security Certification) [7] was defined by the French Natianal Cybersecurity Agency (ANSSI , Agence Nationale de la Sécurité des Systèmes d'Information) with the intention to make it as the lightweight version of the Common Criteria (CC). The CSPN scheme is suitable for evaluating hardware and software components/products. ANSSI defined the following possible technical domains [1] that the evaluated product should be associated with. During CSPN evaluations 3 actors (optionally 4) are involved to the certification process. The first is the sponsor who provides the product together with its security target and documentation. The second is the evaluation facility who is licensed for the technical domains to evaluate the products for the CSPN. The third one is the ANSSI's certification body who makes the drafts for the evaluation criteria and the generic method for the CSPN together with methods for certain types of products. If it possible the developers of the product (the 4th actor) are also submitted to the evaluation. As discussed in [7], the base intention of the CSPN just in case of the CC is to ensure that the security services declared by a product are achieved. However, on average the success rate of the CSPN evaluations is about 50%. The main raison behind this is that the developers still not give enough attention to security and not intents to provide a comprehensive security in the design. Therefore, often a CSPN evaluation comes before a CC evaluation to reduce the effects of an inappropriate security consideration of the product and to prepare it for a CC evaluation. With this it is possible to reduce the costs of a CC evaluation even more than 20%. As a more lightweight approach compared to CC, CSPN still needs an effort of at least 2 months for evaluation and certification.

2.1.3 EUCC. AssureMOSS aims to reuse evaluation results from previous assessments and move towards a more affordable way of certification compared to CC. The candidate EUCC scheme (Common Criteria based European candidate cybersecurity certification scheme) [12] is the result of the request made in 2019 from the European Commission in accordance with the Article 48.2 of the Cybersecurity Act [13]. As a solution ENISA (European Union Agency for Cybersecurity) established an Ad Hoc Working Group (AHWG with participation of leading cybersecurity experts and members of the European Cybersecurity Certification Group (ECCG)) to support the composition of the EUCC scheme which is intended to be the successor of the currently existing schemes which serves under the SOGIS MRA (Senior Officials Group Information Systems Security Mutual Recognition Agreement). The EUCC basically focuses on the cybersecurity certification of the ICT (Information Communication

Technology) products – any kind of product that somehow creates, stores, transmits, receives, or works with information in any other possible way than in a digital manner (e.g., security dedicated products like encryption devices or signature devices or products with security functionalities like bank cards, routers, and even medical devices). Due to that it is not just usable with different type of products, but with sector specific products also, it is rather a kind of a horizontal scheme. The scheme is generally based on the Common Criteria (see [6]) and the first "draft" version was published on July 02, 2020 [12] for a month-long consultation period to gain feedback from all the interested parties. After all the feedbacks were taken into consideration and were implemented into the scheme causing some major modification the v1.1.1 version of the candidate EUCC scheme was published on May 25, 2021 [10], which is the latest version at the time of the writing this document. All the ICT products which are devoted to take place in the European Union Internal Market may be covered by EUCC and shall comply with the next 2 conditions: First: contain significant and important set of security functional requirements (description in [6] and [7]) Second: aiming to fulfill the "substantial" or "high" assurance levels of the CSA (CyberSecurity Act) [13] Despite that the EUCC does not offer the lower or a base level of assurance levels which means less rigorous security requirements as well as requires less security evaluation evidence, with the two assurance levels ("substantial" and "high") the EUCC can submit a considerable amount of collection of the claiming security requirements. The scheme contains the same assurance classes as the CC has. It is also possible just like in the case of CC scheme to establish Protection Profiles to reflect relevant security requirements and these PPs may also be applicable or reference standers for some stakeholders. With the EUCC it is allowed to have composite product certification (certifying an application on top of a certified platform or certifying a platform on top of a certified IC) in order to lower the price of the certification process, which is also the goal of the AssureMOSS scheme. The EUCC scheme concentrates on IoT products and not directly applicable for MOSS.

2.1.4 EUCS. Moving away from protection profiles, the AssureMOSS scheme is concentrating on microservices-based architecture, which can have common elements (and requirements) with cloud services. The EUCS (European Cybersecurity Certification Scheme for Cloud Services) [11] is similar to the EUCC and it was published first on December 22, 2020 with the aim to have a specialized certification scheme for the Cloud Services. After the publication of the first "draft" version [11] the ENISA (European Union Agency for Cybersecurity) also give an almost 2 month long public consultation period for the interested parties to submit their modification proposal and to send their feedback. At the time of writing this document, the scheme has no newer version published. In conceptual contrast to the EUCC the EUCS scheme has 3 assurance levels: the "Basic", the "Substantial" and the "High" levels. The lowest level is the "Basic" level which corresponds to the "basic" assurance level of the EUCSA (specified in EUCSA's Article 52(5) [13]). The base intention of the Basic assurance level is to "minimise the known basic risks of incidents and cyberattacks". It also aims to meet with the common security requirements on services for non-critical data and systems. The depth of this level shall comprise resistance against an attacker with limited skills and limited resources retrying known vulnerabilities and shall contain only review and scrutiny activities of the coherence and the completeness of the design and processes documentations to ensure that the technical and organizational proposals and measures are satisfied together with the requirements of a fully automated test against simple and known vulnerabilities and automated compliance checks by the CSP (Cloud Service Provider). Thanks to the above mentioned three assurance levels, the EUCS scheme covers a wide range of security requirements aiming to improve the Internal Market conditions and to increase the level of security among cloud services. The EUCS certification scheme [11] offers two assessment methods describing how to verify that a cloud service complies with the related requirements of the EUCS. It also offers a detailed list of the documents that shall be made public as part of the certification in order to help users to find the information which they need for making a thoughtful decision. We have analyzed the requirement list of the EUCS and were inspired by them in cases of the requirements related to the environment of the ToE. We also assessed the number of requirements that are automatable completely (by using the output of a tool/script) and partially (in case a human assessment was made for the requirement, the changes can be automatically assessed based on the previous results). As the statistics in Table 1 show, according to our assessment only 2% of the EUCS requirements is completely automatable, and 11% is partially automatable. In the AssureMOSS scheme we aim for at least partial automation for all the requirements.

Table 1: EUCS automation statistics

Statistics	No. requirements
Automation possible partially	59
Automation not possible	461
Complete automation possible	13

2.1.5 MASVS. AssureMOSS aims to collect a list of requirements relevant for microservices, which share common properties (and requirements) with securing mobile applications. The Mobile App Security Requirements and Verification Standard [20] was defined and composed by OWASP (Open Web Application Security Project – a non-profit foundation whose base intention is to improve the software security). The fundamental idea behind the MASVS was that to have a well-defined set of security related requirements to establish a baseline security for mobile application. It is an important part of the MASVS that it mostly focusing on the client-side security and just tangentially focusing on the server-side if one of the requirements demands it. MASVS [20] defines three (3) security levels the L1 (Standard Security), the L2 (Defense-in-Depth) and the R (Resiliency Against Reverse Engineering and Tampering). Only the requirements of the V8 class define the level R. Mobile apps can be verified against L1 or L2 level while the MASVS-R can be complimentary for both levels. As a suggestion from OWASP all the mobile application should implement the L1 security level, while those apps that have functionalities like purchasing options or just work with more confidential or sensitive data, information and/or functionalities (e.g., banking apps or healthcare related apps)

shall apply to MASVS-L2 level. The MASVS-R level is suggested to be chosen in addition if the app shall protect intellectual property and/or the apps works within a specific environment where it is required to store sensitive information and data on the phone, or some of them must be hardcoded. In case of gaming applications, the MASVS-R level can also be relevant to be resistant against cheating and modding. The AssureMOSS scheme follows the structuring of requirements according to MASVS.

2.1.6 CLS. The notion of labeling appears in AssureMOSS via the resilience level. The resilience level will represent the combined risks associated with the parts and the whole of the assessed software and associate a level of trust to the ToE. A similar approach of differentiated levels of trust was expressed in levels in the following lightweight scheme. The Cybersecurity Labelling Scheme [9] was the result of the initiative under Safer Cyberspace Masterplan to make Singapore's cyberspace more secure and to raise the cyber hygiene levels. The scheme is owned and managed by the Cybersecurity Centre (CCC) under the ambit of the Cyber Security Agency of Singapore (CSA) . The label of the CLS would implicate the level of the security of the network-connected smart devices. The main aim of the CLS is to enhance the consciousness in the field of cybersecurity with making the security relevant provisions more transparent for the customers and to help them making better judgement and choice in purchasing products which have better security by the help of the information based on the cybersecurity labels. The CLS has four cybersecurity levels. Only the 3rd and 4th level require the involvement of an independent 3rd party evaluation laboratory, while the first two level of the scheme requires assessment and appraisal from the developer's side. The overall picture of the four levels:

- Tier 1 (Baseline requirements)
- Tier 2 (Lifecycle requirements)
- Tier 3 (Software binary analysis)
- Tier 4 (Black box penetration test)

The scheme is currently voluntary, but it will be monitored to determine if it would be feasible and suitable to make it mandatory for IoT devices, and it is only recognized in Singapore at the time of writing of this document. The successfully achieved labels are valid until the manufacturers support their devices with security updates, but a maximum of 3 years long. However, it could be revoked earlier in case of a security breach or if any misbehavior has been found in the completed tier assessments or some misuse of the labels happens. This idea is also reflected in the AssureMOSS scheme.

2.2 Other relevant projects

Beside the schemes described above which are the most common ones, some other security certification schemes and approaches are available or is in the design phase like (Cybersecurity Certification Framework [16]). However, most of them are conceptually planned for a specific group of products (e.g., IoT devices) and do not focus on the certification of OS software. Moreover, the automation possibilities during the certification process are also not in the focus of these schemes. As we found there are only a few possibilities for the certification of open-source products. The main reason behind this can be that most of the certifications are expensive and usually hold for at least a few months. In the "Certification of Open-Source Software – A Scoping Review" research [14] which summarized the available research about the certification of the OS projects together with the issues, approaches, and solutions for it, showed that only a very few research deals with this topic. It also highlighted some differences and problems between the OS software and the closed source software certification. Among many others the main difference was that the evolution OS projects are much more dynamic and not as linear as the closed ones. The AssureMOSS scheme aims to support this dynamic nature of development of OS software by delta evaluation. Delta certification has been a returning concept, discussed in international CC conferences as well [2] as a possible way to reduce evaluation costs and time by emphasizing the importance of reuse in the evaluations. They introduce more reuse scenarios:

- Trivial reuse: Developer assurance of no changes
- Simple reuse: Evaluator determines no changes
- Common reuse: Evaluator focus on identified changes
- Complex reuse: Combining or reusing results from different sources

However, they are not able to automate the process of reuse as the scheme itself prevents this possibility. The AssureMOSS scheme on the contrary will entirely embrace the delta evaluation concept by automating simple reuse, common reuse and complex reuse scenarios. Microservices also have relevant certification schemes. For example, the Government of the UK issued the DWP SS-028 Security Standard - Microservices Architecture [2] which lists requirements related to microservices deployed in the Authority estate. These requirements may be too restrictive for general-purpose software with microservices-based architecture. Other security related projects which also aim to propagate and improve security and safety of the different kind of software and hardware products are also available. Most of these projects are free and were designed to be easily usable and if it was possible some level of automation was also taken into consideration during the design phase. However, most of these projects and ideas are rather just a set of best practices and recommendations or guidelines about how to make a product more secure, and they are not issuing any certification. Therefore, they are rather good for the developers or the communities who develop and maintain the products than to grow the awareness and trust of the end users in the security of the products. CIS Benchmarks™ : is a non-profit independent organization with a global community of cybersecurity experts. Their main objective is to create more trust in security for the people and businesses as well. As a result, at the time of writing of this document they have more than 100 configuration guidelines over more than 25 product families containing security best practices and hardening guidelines/recommendations to secure specific IT systems and data. Based on the CIS docker benchmark [5] which contains two hardening levels for the docker and host Linux system, the recommendations are indicated as "Automated" or "Manual" which show that the implementation of the recommendation can be done automatically or requires any manual step(s). Each recommendation is mapped with the relevant CIS Controls which is a general set of suggested (best) practices to secure a wide range of software systems and different types of devices. The default outcome of the assessment of the recommendations of a specific

benchmark is a table showing which of the specific recommendation was set correctly and which were not. The AssureMOSS scheme will use CIS benchmark results in requirements related to Docker and Kubernetes.

2.3 Summary

Certification is a strictly defined process to evaluate and testify that a product (software, hardware, combination of these) meets a certain set of requirements. In the IT security domain, there are various certification schemes aimed at different types of ToE (Target of Evaluation). The most recognized IT security certification scheme is Common Criteria (also known as ISO/IEC 15408 [6]), which can be customized by Protection Profiles to be applied to different classes of ToE, e.g.: smart meters, smart cards, biometric devices, etc. Common Criteria (CC) is considered to be a "heavyweight" certification scheme. Although it is accepted by many countries, there is public criticism against its costly preparation and evaluation process and the fact that most of the assessment is done on the documentation. Other popular schemes, e.g.: CSPN [1], CLS [9] are created with the aim to provide a more lightweight approach to certification compared to CC. Search-Lab also defined an evaluation scheme called SCL developed as part of the VESSEDIA [23] EU project for IoT devices [22]. The European Union tasked ENISA to create certification schemes considering the Cyber Security Act. EUCC and EUCS were in candidate stage at the time of writing and would be rooted from Common Criteria for IoT and cloud services respectively. Table 2 summarizes the key aspects and differences compared to the AssureMOSS scheme of the schemes presented in this section.

In the context of MOSS, where continuous development and rapid release cycles are trending in software development, a constant recertification of a product would cause extreme overhead in the budget and for developers work as well. The AssureMOSS scheme would fill a void in the cloud- and microservices domain by employing the concept on delta evaluation. To evaluate a new ToE, at first, a full evaluation would be required against the ToE, which would build up a model of the evaluation by creating associations among requirements, evidence, and tests. Then, in case there are changes to the ToE (i.e., a new commit or release was published), based on the classification of changes and the built model, the requirements can be evaluated in a significantly more efficient way. The evaluator would immediately know that a certain change would require to reassess only a subset of requirements relevant to the change. Moreover, the AssureMOSS scheme will be designed to contain requirements for which changes can be automatically evaluated based on the output of the AssureMOSS tools. The combination of these two methods will significantly reduce the evaluation time required for subsequent changes after a first full human-assisted evaluation was performed. In the AssureMOSS scheme no document and process auditing-based assessment is required which would result in lower effort needed from developers and evaluators as well. Instead, we concentrate on static analysis and penetration testing activities which would lead to improved results compared to document-based assessment. The scheme is designed to serve results for the first evaluation in weeks (depending on the complexity of the ToE) compared to months standard in Common Criteria-like schemes. The delta evaluation on changes can be fully automatic, delivering results in minutes after a commit was issued if employed in CI/CD, which is unique among the schemes. The AssureMOSS scheme is not a standard as compared to other schemes, however, by using it on many open-source project it can gain traction and increased adaptivity could lead to acceptance in the development and security community as well. The scheme is designed for MOSS with microservice-based architecture compared to general or cloud services schemes. The validity period of the AssureMOSS certificate is lower compared to the certification schemes we described. This is because the AssureMOSS scheme is considering the higher pace of software development in MOSS and the higher dependability on third party code would introduce more risks in terms of resilience, therefore a lower validation period is suggested. As a unique feature of the AssureMOSS scheme compared to the ones described is that the validity period can even be dynamic, meaning that in case a ToE is continuously monitored, and a security incident happens, it may lower the Resilience level of the ToE resulting in a lower validity period or even an expired certificate. The AssureMOSS scheme aims to provide solutions for the challenges identified during the analysis of existing schemes and current research (as described in Section 2) according to Table 3.

3 ASSUREMOSS SCHEME

As the conclusion of the previous section suggested, there is a need for a lightweight and automatable certification in the context of MOSS (Multi-party Open Software and Services) This chapter introduces the AssureMOSS scheme and describes in detail the different aspects, such as purpose, applicability, methodology, requirements, certificate management of the scheme. The concepts used in this paper are defined according to Table 4 in the scheme.

3.1 Scope and purpose

The AssureMOSS scheme is a lightweight and automatable certification in the context of MOSS. It is lightweight, as it does not require extensive documentation-based and process-auditing steps in the assessment, instead it automates the evaluation process by using numerous tools (including tools developed in the AssureMOSS project) and comparing the changes (delta) among certified and evaluated versions of the target. The AssureMOSS scheme requires initial manual evaluation by experts and subsequent evaluations are automatable in case of minor changes to extend the certification validity for a new version of the target. The scheme is suitable for integration into the rapid software development cycle. The purpose of the AssureMOSS scheme is to elevate the overall security, resilience, and awareness of open-source projects by providing the necessary tools and opportunity to automatically certify software that changes rapidly.

3.1.1 Applicability. The AssureMOSS scheme – and the AssureMOSS project – demonstrates the capabilities best when applied on software built with microservices architecture. The scheme was also designed with the vision that builds on the strengths of the AssureMOSS tools. The scheme also includes requirements which are applicable to a wider range of software and services and can

Table 2: Summary of the Certification schemes

Scheme	Accepted standard	Required effort	Applicable to MOSS	Automation potential	Document-based	Pentesting	Static analysis	Supports delta eval.	Validity period
CC	Yes	High	Yes, with an appropriate PP	Low	All EAL level	All EAL level	>EAL1	No	5 years
CSPN	Yes	Medium	No	Low	<Phase 6	>Phase 6	>Phase 4	No	5 years
EUCC	No*	High	No	Low	All	Each level, based on CC	Yes	No	5 years
EUCS	No*	High	No	Low	All	From Substantial level	Yes	No	3 years
MASVS	No	Medium	No	Low	No	All levels	Optional	No	-
CLS	Yes	Medium	No	Low	<Tier2	>Tier 3	Yes	No	3 years
AssureMOSS	No	Low	Completely	High	No	Yes	Yes	Yes	1 year

Table 3: Challenges and solutions

Challenge	Description	AssureMOSS solution
Security evaluation of microservices	The main target of the AssureMOSS tools are microservices, the number of applicable schemes designed for this topic is low.	The AssureMOSS scheme is designed to focus on software implemented using microservices-based architecture.
Dynamicity of development	Development of MOSS requires adaption of new solutions quickly, support for interchangeable components, rapid release cycles.	The AssureMOSS scheme support integration into CI/CD processes and designed to be fully automated with delta certification approach.
Dynamicity of attacks	Some certification schemes provide a valid certificate for up to 5 years, which is plenty in the security domain as attacker methods are constantly evolving and due to the nature of MOSS these may cascade in the developed software. A new vulnerability in a component of many is likely to be found soon after certification.	The AssureMOSS scheme is designed to support monitoring to make adjustments in the resilience level and revoke the certificate if necessary. Maintenance of the scheme is also designed to be yearly.
Overhead of current approaches	The existing approaches are usually expensive, slow and complex, requiring formal documentation and processes. It could potentially imply the developercannot afford the certification costs, or the delay for the release of the software in the market.	The AssureMOSS provides a lightweight approach which does not require the audit of documentation and processes and relies on automation.
Required effort from evaluators	Most schemes require effort from developers to maintain documentation. Security evaluators need to assess this documentation, and even the development process itself beside the ToE.	The AssureMOSS scheme encourages automation by the requirements and the concept of delta evaluation minimizes the required effort for recertification.
Tool support	Tools would be required to make automation possible	The AssureMOSS tools will be able to provide the toolset (including static (SAST) and dynamic (DAST) analysis tools, DeltAICert and the ResilienceTool) required to automate the evaluation based on the AssureMOSS scheme.

be utilized to provide continuous certification for the rapid development in a fast-paced agile environment. To certify a MOSS, the AssureMOSS scheme requires (read-only) access to the source code repository to be triggered by new versions of the ToE and check out the project for analyzing the source code and configuration files. The scheme does permit conformity self-assessments, as there is no certification body established for enforcing quality and correctness of the assessments based on the scheme. The AssureMOSS project suggest that the evaluation and certification activities should not be carried out by the same organization that developed the ToE. It is advised rather for the developer of the ToE to contract a third party who can make an independent security analysis using the AssureMOSS scheme and tools. This third party can generate a valid certificate if all the requirements were assessed to be passing and sufficient evidence can be shown to support this claim.

Table 4: Definitions

Concept	Definition	Source
Assessment	The process that outputs a verdict (pass/fail/inconclusive) about a requirement concerning the ToE. One or more pieces of evidence can support it.	
Evaluation	Series of assessments based on requirements against the same ToE.	
Evidence	Supporting material that answer to the specific question(s) raised by the requirements of a certification scheme.	
Indicators	Quantifiable metrics that can be used to assess the risks associated with the ToE.	
Certification	A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system	FIPS 200 (1)
Risk	Effect of uncertainty on objectives, a positive or negative deviation from what is expected.	ISO 31000
Risk assessment	The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.	CNSSI-4009 (4)
Threat	Any circumstance or event with the potential to adversely impact organizational operations, organizational as-sets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.	FIPS 200 (1)
Vulnerability	A weakness of an asset or group of assets that can be exploited by one or more threats	ISO 27000

3.2 Certification types

This section shows the two different types of the certification: baseline and delta. Baseline certification is mandatory and a prerequisite for enabling automation for delta certification.

3.2.1 Baseline certification. The AssureMOSS scheme defines baseline certification as the first type of certification which is mandatory in the scheme. The baseline certification lays down the baseline of the evaluation process and is required to be conducted by human security evaluators. As a first step, the AssureMOSS and third-party tools provide their outputs automatically, then a human evaluator defines the rules that are required to extract evidence from these outputs. The rules will be reusable on a newer instance of the evidence in case of a delta evaluation and certification. After the rules have been applied, the evaluator makes the assessment on the evidence based on the requirements. The assessment must be stored and included in the report for the evaluation. If all the requirements pass, the certification should be granted for the ToE. Baseline certifications are usually followed by delta certifications in case a new version of the ToE is released. However, if the validity period has expired or an incident is detected the certificate can only be earned after a new baseline certification.

3.2.2 Delta certification. In the AssureMOSS scheme delta certification is an automated process. To provide delta certification, the type of change in the ToE must be determined automatically. The following two change categories are introduced in the scheme: 1. Minor changes: automated tests can determine whether the requirements still pass based on automatic evidence extraction and/or comparison with previous baseline evidence. 2. Major changes: automated tests fail to conclude on the results, previous evidence differs in key aspects. Major changes imply to continue certification with manual assessment. Delta certification requires at least one previously passing baseline certification. The delta certification consists of all the same requirements as the baseline certification. In case the evidence collection, automation, and assessment rules – defined during baseline certification – could not run or produce conclusive results, the delta evaluation should be handed over for human assessment for the failing requirements.

3.3 Requirements

The assessment of the scheme is based on checking all the requirements of the scheme. The evaluator (or an automated tool) may decide and prove with evidence, that a certain requirement has either failed, passed or not applicable to the ToE. The goal of the requirements is to cover the most important security-relevant topics relevant in a security evaluation of MOSS software in a way that their assessment can be fully (a tool is directly providing evidence for the requirement) or partially (via delta evaluation: comparing to a previously certified version) automated. Compared to certification schemes in the previous section the AssureMOSS scheme covers the same topics, focusing on automation and omitting documentation and procedure-based assessment. The following requirements were derived from automatically verifiable requirements and best practices based on OWASP microservices [19], OWASP Kubernetes [18], MASVS [20], CIS benchmark for Kubernetes [4], CIS Benchmark for Docker [5], NIST [17], EUCS [11]. The AssureMOSS requirements consists of general requirements related to the overall security of the ToE and more detailed requirements about some key aspects of implementation. A subset of the requirements was selected from other certification schemes mentioned above (marked in the table of requirements), others were building on the outputs of the AssureMOSS tools. The following requirement categories were considered:

- Architecture: corresponds to general and design choices.
- Data storage and privacy: handles how sensitive data is managed.

- Cryptography: deals with algorithms and keys used for cryptographic operations.
- Authentication and session management: considers user roles, authentication methods and session management implementation.
- Communication: restricts module to module and module to third-parties' communication methods via network interfaces.
- Code quality and build settings: requires hardening and best practices.
- Environment: describes deployment configuration.

The requirements are related to a predefined scope They should be assessed according to their designated scopes as described below:

- Global scope: should be assessed with the whole ToE in scope
- Component scope: should be assessed for every system component (i.e., docker container) individually

The AssureMOSS scheme's requirements are available on GitHub at [21].

3.4 Indicators

Indicators are mainly used for risk assessment in the AssureMOSS scheme aiding human evaluators to obtain a general and intuitive assessment of the tested artefact. Some of the indicators can be also used to answer the requirements (as marked in the requirements description tables above). Indicators are useful for giving empirical support for evaluators to assess ToE-associated risks that can be used directly or indirectly for certification. Indicators are produced by AssureMOSS and third-party tools and processed by EU-VRi's ResilienceTool, which will calculate a final Resilience Level for the project. Indicators are metrics that can be derived by an algorithm based on information from the artefact itself or by observing and/or interacting with the artefact in runtime. Indicators can be numerically represented (with continuous or discrete numbers) and can be scaled to fall between minimum and maximum values. Indicators can be combined and organized into a hierarchical structure depending on each other according to an algebraic calculation function.
Proposed indicators include:•Code quality impressions; Security best practices; Dependencies; Technical leverage [15]

3.5 Evidence

Evidence is supporting material that answer to the specific question(s) raised by the requirements of a certification scheme. Evidence can take various forms e.g.: source code snippets, (parts of) runtime logs, network captures, output of the artefact, results of a static or dynamic analysis tools, etc., even some indicators can be used directly as evidence (e.g., CVE scores for found vulnerabilities). Evidence can be combined to support the argument of the assessment for the requirements. In the AssureMOSS project evidence are produced by various tools and processed by Search-Lab's DeltAICert tool and/or human evaluators.
Evidence sources include: Modelling outputs; Source code; Static analyzers (PMD, Spotbugs, SonarQube, CIS, etc.); Dynamic analyzers (runtime log, network traffic, configuration).
For every piece of evidence the following metadata has to be collected: Creation date; Corresponding ToE (identified with commit hash); Generation method; Evidence hash.
Storage of evidence with the guarantee to maintain their integrity must be provided by e.g., storing the SHA-1 hashes of the evidence files.

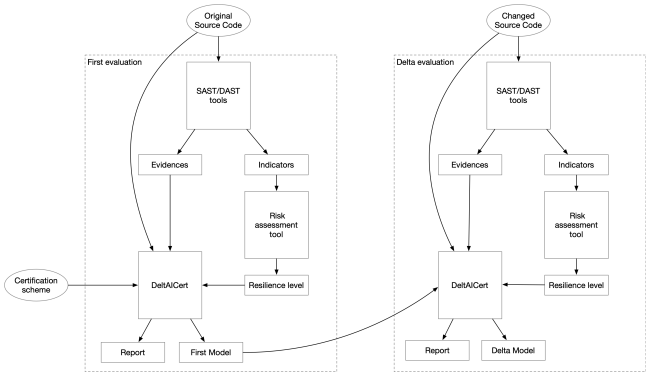

Figure 1: Delta evaluation workflow

3.6 Automation

The Resilience tool collects the indicators produced by AssureMOSS and third-party tools, then calculates the Resilience Level used in the AssureMOSS scheme to determine the certificate validity period based on the associated risks coming from first- and third-party components. The DeltAICert tool to be developed by Search-Lab will employ the AssureMOSS scheme and delta certification by analyzing changes among a certified and modified version of a ToE (Target of Evaluation). Helping human evaluators by automatically comparing changes in source code and evidence generated by AssureMOSS (and probably other 3rd party) tools and matching these to requirements according to a selected certification scheme. DeltAICert aims to automate changes-based delta evaluations as much as possible. In case the evidence did not change among versions, the associated requirements should be accepted. Figure 1 shows the high-level workflow of the delta evaluation.

During the assessment of requirements, automation is achieved by comparing previous passing and failing cases of evidence with the current evidence of the ongoing evaluation. DeltAICert and the AssureMOSS tools can be implemented as a service, which can be integrated with the CI/CD processes of companies. Human assessment can augment the automated process in the baseline certification and in case automation is not capable of making the assessment for a certain requirement. To further automate the evaluation and certification process by leveraging knowledge from other evaluations, DeltAICert will be able to import and export evaluations (in terms of evidence and certification results) for the components it has already assessed. These partial results can be reused in a subsequent evaluation. For example, if company A develops a product, which is certified by AssureMOSS, and company B uses it as a component of their system, then the evaluation of company B's software can be sped up by reusing the evaluation and certification results for the component company A developed.

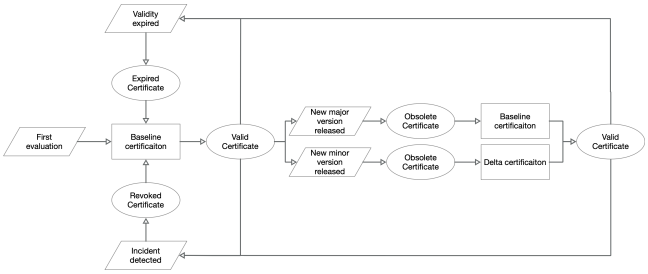

Figure 2: Certification life cycle

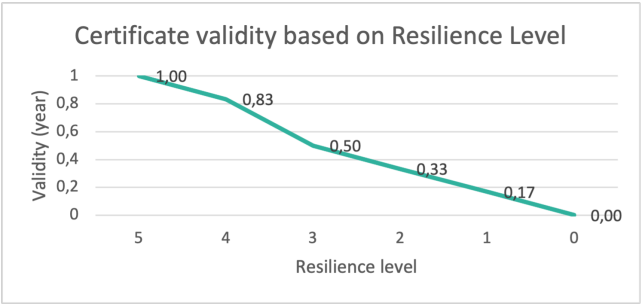

Figure 3: Certificate validity period based on Resilience Level

3.7 Certificate management

This section describes the management of the certification schemes. It shows how the AssureMOSS certification can be obtained, validated, or revoked, how it is maintained and what form can it take to show that the ToE is certified.

3.7.1 Certification life cycle. The certificate can be created by a manual baseline evaluation or an automated delta-evaluation. A certificate can be in one of the following states:

- Valid: the certificate is active and should be accepted
- Invalid: the certificate is not valid, should be rejected
- Expired: invalidation triggered by expiration of validity period
- Revoked: invalidation is triggered by an incident
- Obsolete: invalidation is triggered by releasing a new version of the ToE

Figure 2 summarizes the certificate life cycle.

3.8 Certificate validity

The maximum period of validity of the certificates shall be one (1) year. The validity period was defined based on the rapid nature of software development nowadays and the constant evolvement of standards, and the capabilities of threat actors. The value of the Resilience Level calculated by the Resilience Tool (Developed in the AssureMOSS project by EU-VRi with the purpose of live monitoring of indicators to determine associated risks) based on the indicators can lower the validity period of the AssureMOSS certificate according to Figure 3.

3.8.1 Certification scheme maintenance. The AssureMOSS scheme itself should also be updated in a scheduled and triggered way as well. The maintenance of the certification scheme does not invalidate previously issued certificates, as the risks associated with the resilience level already embrace the concept of aging. The following maintenance tasks must be performed to keep the certification scheme up to date:

- Scheduled maintenance: The evaluators using the scheme must yearly update assessment rules related to best practices.
- Triggered maintenance: in case a standard is updated, the evaluators must update the assessment rules related to the changes

(e.g., a new NIST standard was published).

3.8.2 Report content. As the final step of the certification process, a report (PDF file) must be generated, which summarizes the results of the evaluation, to give feedback to the developers and managers of the ToE. The report must contain the following elements:

- Certificate (in case all requirements passed)
- Management summary with result statistics (number of passed and failed requirements).
- List of requirement-based assessments with relevant parts of evidence. In case of human evaluation was required, it must be stated.
- List of evidence file hashes for the requirements.

3.9 Provisioning

Evaluators may use the following standard as for the general rules related to vulnerability disclosure: ISO/IEC 29147 Information technology - Security techniques - Vulnerability disclosure. The certifier entity shall maintain a record system in accordance with the requirements of the applicable accreditation standard ISO/IEC 17065 or ISO/IEC 17025 for its activity.

4 CONCLUSIONS AND FUTURE WORK

This document presented the AssureMOSS scheme which aims to improve the efficiency of security evaluations of MOSS by employing the concept of delta evaluation and automation. The set of covered topics and their associated requirements were developed by building on existing standards and best practices in the field of software using microservices-based architecture. The final list of requirements may be refined and as the project matures; influenced by the indicators and evidence that the tools under development will be able to provide. DeltAICert will be developed during the AssureMOSS project and will automate the use of the AssureMOSS scheme as described to improve the efficiency of security evaluators' work. A pilot task within the AssureMOSS project will demonstrate the capabilities of the tools by employing the AssureMOSS scheme and DeltAICert on a selected project to show how a change detected by the modeling tools are able to influence the certification and give the developers useful feedback related to the discovered issue. Validation of the concept and the DeltAICert tool will be organized with student experiments.

ACKNOWLEDGMENTS

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 952647.

REFERENCES

[1] ANSSI. 2020. CSPN - Criteria for evaluation in view of a first levele security certification. https://www.ssi.gouv.fr/uploads/2015/01/anssi-cspn-cer-p-02-criteres_pour_evaluation_en_vue_d_une_cspn_v4.0-en.pdf
[2] T.D.James Arnold. 2006. Common Criteria: Delta Evaluation. https://www.commoncriteriaportal.org/iccc/7iccc/t1/t1201130.pdf
[3] AssureMOSS. 2021. AssureMOSS website. https://assuremoss.eu/en/
[4] CIS. 2022. Benchmark for Kubernetes. https://www.cisecurity.org/benchmark/kubernetes/
[5] CIS. 2022. CIS Docker Benchmark. https://www.cisecurity.org/benchmark/docker/
[6] Common Criteria. 2017. Common Criteria for Information Technology - Part 1: Introduction and general model. https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf
[7] Common Criteria. 2017. Common Criteria for Information Technology - Part 2: Security functional components. https://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R5.pdf
[8] Common Criteria. 2017-04. Common Criteria for Information Technology - Part 3: Security assurance components. https://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R5.pdf
[9] CSA. 2021-04. Cybersecurity Labelling Scheme (CLS) Publication No. 2 - Scheme Specifications.
[10] ENISA. 2020. EUCC Scheme draft version. https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme
[11] ENISA. 2020-12-22. EUCS – Cloud Services Scheme. https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme
[12] ENISA. 2021. EUCC Scheme. https://www.enisa.europa.eu/news/enisa-news/crossing-a-bridge-the-first-eu-cybersecurity-certification-scheme-is-availed-to-the-commission
[13] EU. 2019-04-17. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act. http://data.europa.eu/eli/reg/2019/881/oj
[14] Eirini Kalliamvakou, Jens Weber, and Alessia Knauss. 2016. Certification of Open Source Software – A Scoping Review. In *Open Source Systems: Integrating Communities*, Kevin Crowston, Imed Hammouda, Björn Lundell, Gregorio Robles, Jonas Gamalielsson, and Juho Lindman (Eds.). Springer International Publishing, Cham, 111–122.
[15] Fabio Massacci and Ivan Pashchenko. 2021. Technical Leverage in a Software Ecosystem: Development Opportunities and Security Risks. https://doi.org/10.48550/ARXIV.2103.03317
[16] Sara Nieves Matheu Garcia, José Hernández-Ramos, and Antonio Skarmeta. 2019. Toward a Cybersecurity Certification Framework for the Internet of Things. *IEEE Security and Privacy* 17 (05 2019), 66–76. https://doi.org/10.1109/MSEC.2019.2904475
[17] NIST. 2022. Cryptographic Standards and Guidelines. https://csrc.nist.rip/Projects/Cryptographic-Standards-and-Guidelines
[18] OWASP. 2022. Kubernetes security. https://cheatsheetseries.owasp.org/cheatsheets/Kubernetes_Security_Cheat_Sheet.html
[19] OWASP. 2022. Microservices security. https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/Microservices_security.md
[20] OWASP. 2022. Mobile Application Security Verification Standard (MASVS. https://github.com/OWASP/owasp-masvs
[21] SLAB. 2022. AssureMOSS scheme. https://github.com/assuremoss/Assuremoss_scheme
[22] VESSEDIA. 2018. D4.2 - VESSEDIA approach for security evaluation.
[23] VESSEDIA. 2019. VESSEDIA. https://vessedia.eu