CS3 MESH4 EOSC

Connecting European Data

Project acronym: CS3MESH4EOSC

Deliverable D2.4: **Implementation of security policies and procedures**

Contractual delivery date	31-12-2021
Actual delivery date	19-08-2022
Grant Agreement no.	863353
Work Package	WP2
Nature of Deliverable	R (Report)
Dissemination Level	PU (Public)
Lead Partner	SWITCH
Document ID	CS3MESH4EOSC-21-017
Authors	Renato Furter, Ron Trompert, David Antos, Holger Angenent, Hugo Gonzalez Labrador

Disclaimer:

The document reflects only the authors' view and the European Commission is not responsible for any use that may be made of the information it contains.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 863353

Versioning and Contributions History

Version	*Date*	*Authors*	*Notes*
0.1	9.11.2021	Renato Furter	Initial Draft
0.2	13.3.2022	Ron Trompert	Some modifications and additions
1.0	18.3.2022	Renato Furter	Formatting and polishing
1.1	05.07.2022	Pedro Ferreira	Review
1.2	01.08.2022	Hugo Gonzalez	Security verification
1.3	16.08.2022	Jakub Mościcki	Review

Index

Index of Figures

1 Introduction

1.1 Preliminaries

This deliverable describes the work performed in Task 2.5 “Security in Federation” which is part of Work Package 2. This task is still in progress at the time of writing of this document.

Security in the Science Mesh Federation is addressed at two levels: by introducing and publishing[1] security policies and procedures for Science Mesh nodes and central operations (Chapter 2); and by implementing practical security review processes such as code review of common Science Mesh software components and technical assessment and pentesting of the fully assembled system[2] (Chapters 3 and 4). These elements are currently under development and will be concluded for the final deliverable report.

1.2 The ScienceMesh

The ScienceMesh is designed to be a highly distributed platform with a very lightweight and almost fully decentralised infrastructure. It consists of several independent sites running their own Enterprise File Sync and Share (EFSS) systems. Each of the sites is expected to be sustainable by itself financially and each of them has their own policies and procedures related to user management, data handling, operations, and security. Finally, each of the Sites has their own agreements with their clients and/or the users for which they run the service. These sites, instead of operating as a disjoint collection of service islands, become nodes in a mesh of interconnected storage, applications, and users where researchers can share data as well as applications.

Interoperability between EFSS services is guaranteed by the Open Cloud Mesh standard (OCM[3]). To this “technical” coupling of nodes through the OCM standard, ScienceMesh will add agreed-upon policies and procedures with respect to operations and security, together with a governance structure. The goal is to create a coherent Infrastructure that can guarantee service level having an adequate quality. Security policies that are going to contribute to this are described in this document and the documents it references.

ScienceMesh’s small technical footprint will be matched by an equally lean administrative structure. It is our aim to rely as much as possible on policies, procedures and agreements that are already locally available, and augment them with what is necessary for the ScienceMesh to operate. This will also help with the platform’s future sustainability and funding of activities, by keeping overhead costs as low as possible.

That said, each site joining the ScienceMesh is a potential risk from a security perspective. Each site has their own different hardware and software, as well as their own sets of local policies and practices. This makes the security in such a distributed collaborative environment more complex and diverse than in a single system, even though the same principles of security still do apply. But taking all these factors into consideration, the actual security layer of the Mesh itself is a very thin and lightweight one as the main responsibility lies within the joining sites, that they comply with the

[1] Security policies and procedures are in Zenodo open repository https://zenodo.org

[2]Pen testing is short for penetration testing where a simulated cyber attack is performed on a computer system in order to find exploitable vulnerabilities.

[3] https://github.com/cs3org/OCM-API

security standards that are defined in the policies.

A short overview of the Architecture of the ScienceMesh can be found in chapter two "Architecture of the ScienceMesh" of Deliverable 2.2 "All Operational Procedures Defined"[4]. Figure 1 below shows a simplified view of the ScienceMesh.

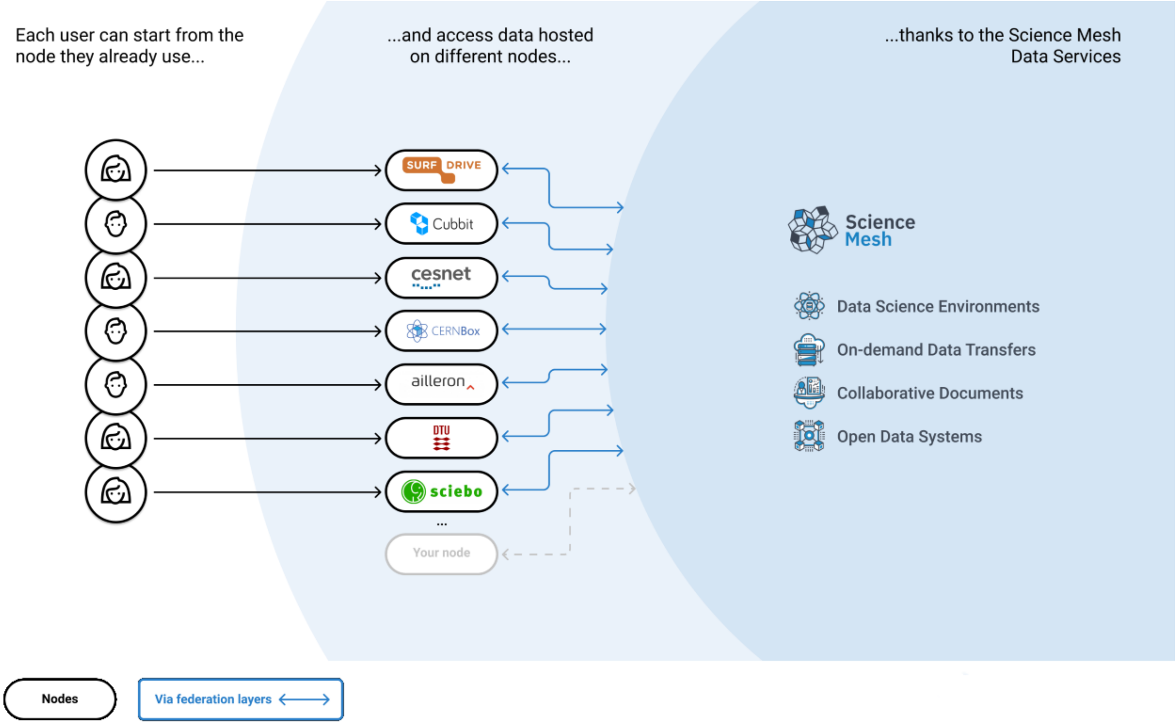

Each user can start from the node they already use...
...and access data hosted on different nodes...
...thanks to the Science Mesh Data Services
SURF DRIVE
Cubbit
cesnet
CERNBox
ailleron
DTU
sciebo
...
Your node
Science Mesh
Data Science Environments
On-demand Data Transfers
Collaborative Documents
Open Data Systems
Nodes
Via federation layers

Figure 1: Schematic overview of the ScienceMesh architecture, showing its information flows. Users can login into their own EFSS node and access data and applications not only located on their own node but on other nodes that are part of the ScienceMesh as well.

Task 2.5 concentrates mainly on the Policies and Procedures and on the code quality of the IOP software, developed by the CS3MESH4EOSC project.

In this document several acronyms are used. These are explained in the ScienceMesh Glossary[5].

1.3 Scope

This document describes security policies and procedures each participating site (service node) must follow to be part of the ScienceMesh. It also gives an outlook on future work that will be done until the end of the CS3MESH4EOSC project.

The distributed architecture of the ScienceMesh led us to re-use some of the elements created within the AARC[6] project. The AARC project was created to create turn-key solutions to bring research collaborators closer together – especially in federated environments. As the ScienceMesh is

[4] https://doi.org/10.5281/zenodo.5602984
[5] https://doi.org/10.5281/zenodo.5038662
[6] https://aarc-project.eu/

exactly this – a federated environment - it was a perfect fit. More about the AARC project and which parts of it were used in CS3MESH4EOSC can be found in chapter 2.1. The policies described here are part of the ScienceMesh Policy Framework[7] and they are specifically based on the AARC Policy Development Kit (PDK)[8].

The PDK provides templates for policies to regulate and facilitate trust within a federated infrastructure. In this task, we have concentrated on operational security, privacy statement and incident response.

1.4 Boundaries

This work deals with security aspects directly related to the ScienceMesh. For individual sites, we assume that a certain level of security is implicitly in place as it is in the interest of the site operator that their services are running with the latest security patches of the operating system and installed software. The Sites are required to follow best practices to operate in a secure manner by the ScienceMesh policies, but the policies do not go into specifics. The Sites already have policies and procedures in place concerning their own local security.

The Sites are autonomous and can therefore operate independently from each other. However, federating Sites into an e-infrastructure requires operations and security-related policies that are site-overarching. Therefore, to join the ScienceMesh, they must meet minimal requirements. These requirements are the policies and procedures which we established and are part of the ScienceMesh Policy Framework. The latter specifies how the Sites should behave, more than providing exact instructions on how to implement such a behaviour. What was still missing from this policy framework were the security-related components, which this deliverable aims to provide.

[7] https://doi.org/10.5281/zenodo.5040151

[8] https://aarc-community.org/policies/policy-development-kit/

2 Security Policies & Procedures

In this chapter, the Service Operation Security Policy, Incidence Response Procedure, and Privacy Policy are described. The sections below also provide references to these documents. These three policies are a part of the ScienceMesh Policy Framework[3] and deal with site-overarching security issues. They must be accepted and complied with in order to join the network. Sites are required to have local counterparts of them. Since our aim is to keep the costs of the central part of the Science Mesh as low as possible, Sites will not be audited, and their security policies will not be reviewed. However, they do need to comply with the Science Mesh Service Operation Security Policy, Privacy Policy and Incident Response Procedure. In case of a violation of those policies, the Site Suspension Procedure will be executed on the violating site. The procedure will be initiated by the central service when a violation is detected.

2.1 The AARC Policy Development Kit

The AARC Project has created a Policy Development Kit that is of use to projects like the CS3MESH4EOSC. The PDK is designed for research services which are operated in a federated environment. The aim of the AARC Policy Development is to provide guidelines as to what policies need to be established in a federated environment and it provides templates that can be used to describe those policies. Its main purpose is to prevent federated infrastructures having to reinvent the wheel every time.

Since it focuses on research infrastructure within a federated system, this toolkit is a good starting point for the CS3MESH4EOSC project. It provides basic templates that can be used and/or adapted to the purpose of the ScienceMesh. The templates listed below are provided by default for the corresponding policies:

- Top Level Infrastructure Policy
- **Incident Response Procedure**
- Membership Management Policy
- Acceptable Authentication Assurance
- Risk Assessment
- Policy on the Processing of Personal Data
- **Privacy Policy**
- **Service Operations Security Policy**
- Acceptable Use Policy

For the CS3MESH4EOSC project in particular, we identified the following policies and procedures to be of importance and thus deemed to be reused: **Incident Response Procedure, Service Operation Security Policy and Privacy Policy.** Other policies that are part of the AARC PDK could be relevant as well for the ScienceMesh, but to a large extent they are already covered by the existing ScienceMesh policies described in the ScienceMesh Policy Framework. For this reason, we limit ourselves to the three aforementioned policies in this deliverable.

2.2 Service Operation Security Policy

The Service Operation Security Policy[9] defines the requirements and conditions of a Site to be able to join the ScienceMesh from a security point of view. These requirements and conditions are the following:

Security contact provision

To have a working Incident Response Procedure, a valid security contact needs to be provided.

Responsibility of the Service owner

The Service owner of a Site joining the ScienceMesh is responsible for the safe and secure operation of the service. All Sites are required to have, locally, a security operation policy in place and to act according to it. All members of the ScienceMesh must be sure that the new Site meets minimal security standards imposed by the community. On the other hand, it is a decision of a particular Site whether they implicitly trust all the other Sites in the infrastructure (with the possibility to put some of them on a deny-list if the need arises), or whether prefer to stick to an allow-list and thus block all communication to any other sites.

Security best practices

Site administrators should keep their systems up to date and respond to requests sent to them by the ScienceMesh bodies in timely manner.

Privacy

Each joining site needs to have a privacy statement which will be displayed to the users of that given service.

2.3 Privacy Policy

The Privacy Policy[10] of the ScienceMesh describes how the processing of the personal data that is collected is handled in general, but also in detail. Both the handling of personal data for end-users as well as for site representatives are discussed in view of GDPR compliance. It describes the type of data and the purpose for which it is collected. Furthermore, it describes who can access the data and how and when data is deleted. Each joining site must have its own privacy policy describing their use and processing of data for their service.

[9] https://doi.org/10.5281/zenodo.6279398

[10] https://doi.org/10.5281/zenodo.6089064

2.4 Incident Response Procedure

The Incident Response Procedure[11] is based on the template provided by the AARC Policy Development kit[4]. As mentioned above, sites are required to have their own incident response procedure in place. Under normal circumstances, local security incidents are supposed to be handled by the Site in question. However, when a Site's EFSS system is involved and other ScienceMesh sites could be impacted, this ScienceMesh Incident Response Procedure will come into play.

Each participating service must provide a security contact who can be reached in case of a security issue. It is the site's responsibility to keep this contact up-to-date and that requests to this contact will be answered in a timely manner. How this information is provided, and which role is given to whom in the case of an incident is defined in the Incident Response Procedure document. That document also provides a step-by-step breakdown of actions to take following a security incident.

A critical aspect of a successful, distributed incident response capability is a clearly identified individual or team that is responsible for incident coordination. In the current model of the ScienceMesh there is no established cross-site body. A lightweight, centralised coordination capability must be established to ensure the effective resolution of security incidents across the infrastructure, through a helpdesk which participating Sites will contribute to, in a rotating manner.

In the event of an incident, the CERT team of the member which is responsible for the helpdesk would also be responsible for the administrative handling of the case. This doesn't mean that this member needs to single-handedly solve the security incident, but rather that it would be responsible for making sure that the lifetime of that incident has been followed up on as described and up until it can be considered closed.

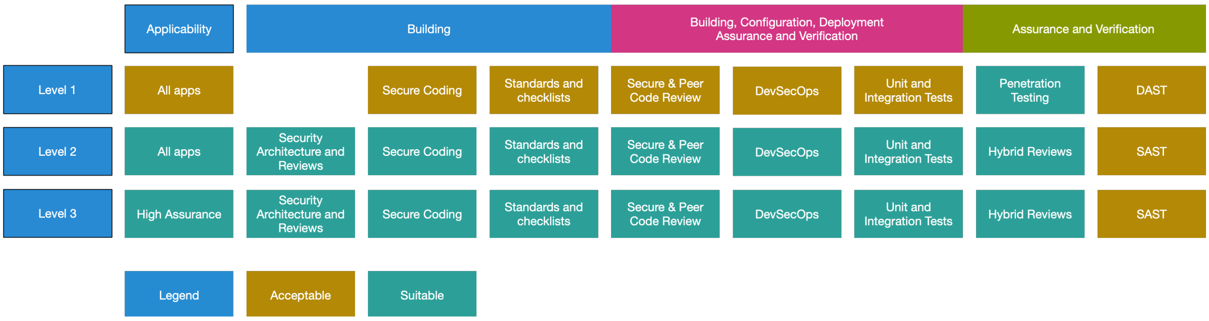
[11] https://doi.org/10.5281/zenodo.6276063

3 Security review of the core middleware component

The Interoperability Platform (IOP) is the middleware at the core of the Science Mesh, allowing applications and storage to interact in a transparent manner. A security review of the Reva software — core component of the IOP (https://github.com/sciencemesh/sciencemesh) — has been performed as part of the Task 2.5. The review team was composed of the software developer (Javier Ferrer, CERN), WP3 leader (Hugo Gonzalez, CERN) and the CERN security team (Dagmar Wikarska[12], DTU and Liviu Valsan[13], CERN).

The aim of the Reva security review is to provide an assessment and overview of the core software security aspects, development guidelines for further enhancement of the foundation technology stack and recommendations for service operators on secure deployment practices.

The security survey has been conducted using the OWASP Application Security Verification Standard.



	Applicability	Building			Building, Configuration, Deployment Assurance and Verification			Assurance and Verification	
Level 1	All apps		Secure Coding	Standards and checklists	Secure & Peer Code Review	DevSecOps	Unit and Integration Tests	Penetration Testing	DAST
Level 2	All apps	Security Architecture and Reviews	Secure Coding	Standards and checklists	Secure & Peer Code Review	DevSecOps	Unit and Integration Tests	Hybrid Reviews	SAST
Level 3	High Assurance	Security Architecture and Reviews	Secure Coding	Standards and checklists	Secure & Peer Code Review	DevSecOps	Unit and Integration Tests	Hybrid Reviews	SAST
	Legend	Acceptable	Suitable						

Figure 2: ASVS security verification blocks

The OWASP Application Security Verification Standard (ASVS) Project provides a basis for testing web application technical security controls and also provides developers with a list of requirements for secure development.

The primary aim of the OWASP Application Security Verification Standard (ASVS) Project is to normalize the range in the coverage and level of rigor available in the market when it comes to performing Web application security verification using a commercially-workable open standard. This standard provides a basis for testing application technical security controls, as well as any technical security controls in the environment, that are relied on to protect against vulnerabilities such as Cross-Site Scripting (XSS) and SQL injection. This standard can be used to establish a level of confidence in the security of Web applications.

The main objectives are:

- Help the development and operational team of ScienceMesh adopt or adapt a high-quality secure coding standard
- Help the ScienceMesh architects and developers build secure software by designing and

[12] Dagmar Wikarska is designing security requirements at CERN in the Computer Security team, working for her MSc thesis: "Filtering as a Method Towards Agile Security Requirements Engineering". She is also a co-founder of DEKK Institute, investigating social cohesion through data-driven approach in Slovakia. In the past, she has been part of UNDP as an ICT Engineer, she worked at EATON as an Embedded Systems Engineer, and as a research assistant at Brno University of Technology. After obtaining her Information Security bachelor's degree at BUT, she continued her studies at Technical University of Denmark. She is a former president of student organization BEST Copenhagen, and a main organizer of TEDxTechnicalUniversityOfDenmark.

[13] Liviu is a passionate Computer Systems Engineer with over 18 years of combined experience in a multitude of roles. He currently works as a Cyber Security Engineer at CERN

building security in, and verifying that they are in place and effective by the use of unit and integration tests that implement ASVS tests

- Help deploy secure software via the use of repeatable, secured builds
- Help security reviewers use a comprehensive, consistent, high-quality standard for hybrid code reviews, secure code reviews, peer code reviews, retrospectives, and work with developers to build security unit and integration tests. This work may serve as a plan-to-action for a penetration test.
- Assist partners to benchmark the application deployment by the percentage of coverage of the ASVS for dynamic, interactive, and static analysis tools
- Minimize overlapping and competing requirements from other standards used by respective partners, by either aligning strongly with them (NIST 800-63) or being strict super sets (OWASP Top 10 2017, PCI DSS 3.2.1), which will help reduce compliance costs, effort, and time wasted in accepting unnecessary differences as risks.

The security verification, rather than being done in an artificial environment has been conducted in a production service — CERNBox — as the verification target. CERNBox is used by more than 37K users and currently holds more than 15 PB of data and more than 2 billion files.

Appendix I contains all the results results of the survey and security recommendations, however we provide here a brief summary of the findings. From all the security points in the Appendix, 51.4% of them are satisfied with the current software implementation, 29.4% are partially satisfied, 1.8% are not done but are possible and 17.4% of the points are not applicable in the context of the IOP.

For the points that are satisfied we have found that the current implementation is strong on the sanitisation of user input and has built-in security controls for authenticated access. The main recommendations are to avoid loading scripts from external CDN providers and use locally loaded modules under the same domain.

The results of this ASVS security verification have been included in Dagmar's joint DTU-CERN MSc thesis titled "Filtering as a Method Towards Agile Security Requirements Engineering" (to be published).

4 Future plans: technical assessment of the fully assembled Science Mesh service

The goal of this technical assessment is to review the functioning and end-to-end interactions of the Science Mesh service consisting of the main IOP middleware component interconnected with the EFSS platform plugins and EFSS end-user interfaces. This assessment is necessary because the potential attack surface of fully assembled service is larger than the attack surface of individual service components.

This assessment requires the Science Mesh service to be fully assembled and needs to be timed with the availability of all software components, including Owncloud OC10, Owncloud OCIS and Nextcloud connectors. At the time of writing this report these components are in the final stages of beta testing.

4.1 Penetration Test of Science Mesh service

Task 2.5 foresees a penetration test, which will happen, as mentioned above, in the third Quarter of 2022. This will allow possible issues to be assessed and fixed over a stable version of the code base, rather than an evolving one. The penetration test will be carried out by CESNET and planning for that started in the first Quarter of 2022.

The aim of the penetration tests is to establish whether

- unauthorised access to services/data/systems can be obtained
- data can be illegally modified/destroyed
- system/service availability can be inhibited
- authentication data can be obtained
- the infrastructure can be misused to attack third-party networks and services
- vulnerabilities exist that could cause any of the above-mentioned instances

The results of the penetration tests will be the following:

- Concrete suggestions for improvement to increase the level of protection of the IOP
- Assessment of the threat potential of the ScienceMesh infrastructure from the perspective of an attacker who could successfully compromise a service in the DMZ (Demilitarized Zone) and then escalate his privileges on the system to root privileges
- Identification and countermeasure specifications of potential vulnerabilities in the IOP service from the perspective of a compromised site
- Detailed recommendations for improving security.

The result of the penetration test will be a report with the findings and will be available before the end of the project.

5 Concluding Remarks

The Polices and Documents referred to in this document are in pre-production stage. They will be assessed and reviewed based on experience gained from turning the infrastructure into production, also using input from the various ScienceMesh Sites. During this key period of the Project, the policies in the ScienceMesh Policy Framework will be verified and updated according to the latest developments.

At the time of writing, the documents are available in Zenodo. Similar policies of other e-infrastructures have been studied to serve as an example and inspiration for the current versions.

As discussed in Chapter 3, there is still work to do, especially the technical assessment and the penetration test, which will give valuable insights on how to make the ScienceMesh a rock solid, trustable platform that users and site administrators can use with no hesitation. A review of the OCM invitation work-flow across federation nodes will also be beneficial as it will help to identify protocol-level security enhancements.