CMD & Service Management Tools

Task 5.2 Training Material

January 2025

T5.3 Objectives

- This task is focused on providing a solution to protect the Encryption and Decryption API from unauthorised access, whether by clients without any kind of permission, or without the required permissions.

- The solution should verify the identity of the client, and permit or deny a request based on some security policies, which specify the necessary credentials in order to access the given API endpoint (e.g. a valid identifying token, possessing a certain role within the identify manager like being an admin, …)

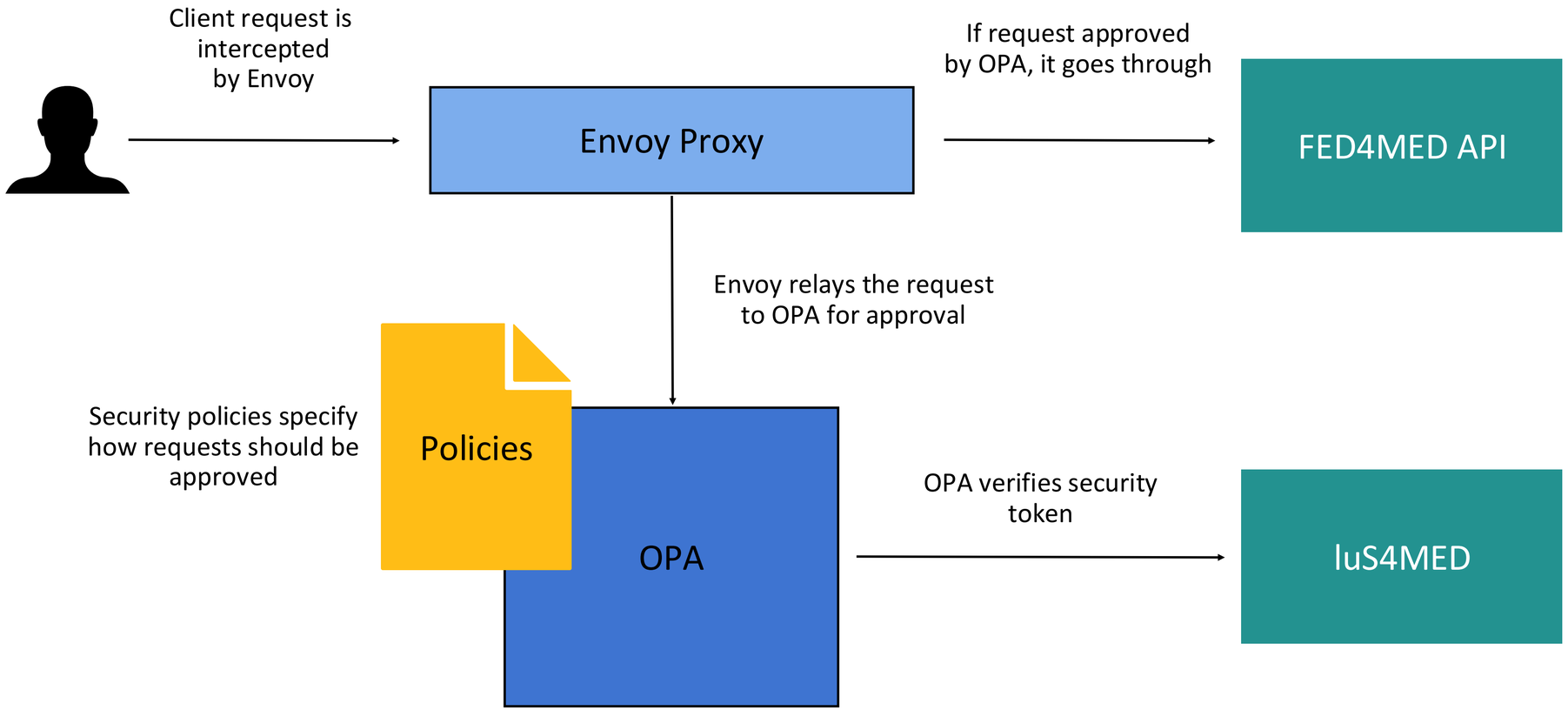
T5.3 Solutions

- Leveraging the Open Policy Agent (OPA) to process API requests based on security policies.

- Leveraging Envoy as a proxy to transparently sit between the client and the API to be protected (the FED4MED Encryption and Decryption service).

- Verifying security tokens provided through luS4MED (Ledger uSelf for Medical Data), an SSI solution meant for users' authentication, allowing only those who have been authenticated to have access to CMD data, preserving privacy, confidentiality, avoiding data breaches, and avoiding compromising patients' records. This solution also mitigates the risk of cyberattacks implementing access controls, and monitoring suspicious activities through AI log monitoring tools.

T5.2 Solution



CYLCOMED

THANK YOU FOR YOUR ATTENTION

cylcomed.eu

Co-funded by
the European Union

CYLCOMED project has received funding from the Horizon Europe research and innovation programme under grant agreement N° 101095542