MEDINA

Security framework to achieve a continuous audit-based certification in compliance with the EU-wide cloud security certification scheme

Authors
Cristina Regueiro, Aitor Gómez, Santiago de Diego, Borja Urquizu (TECNALIA)

Trustworthy Blockchain based-tools for auditors in a certification process

Introduction

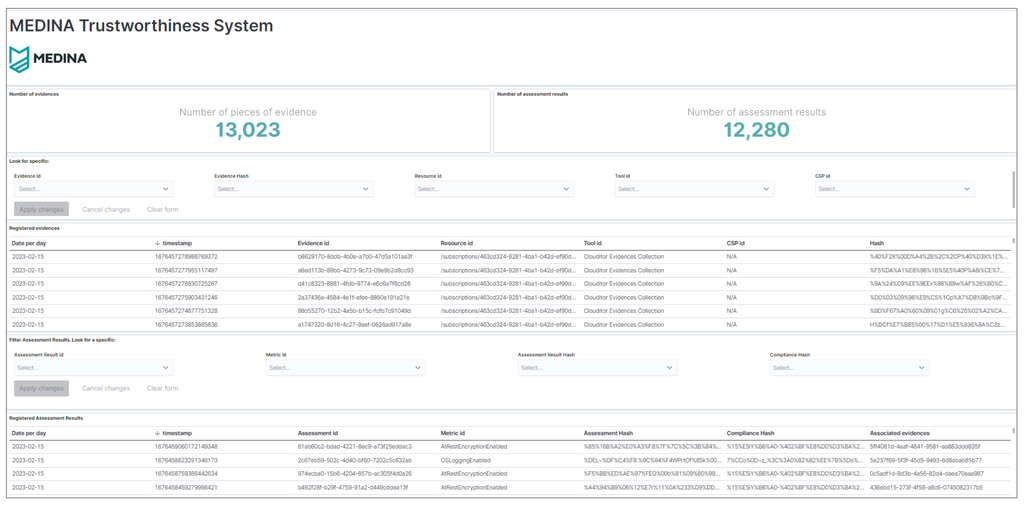
MEDINA project aims to develop an automatic **framework for continuous evidence-based auditing to achieve EUCS certification compliance in an easy way.** However, automatic tools also need to be trustworthy to **enhance objectivity, accuracy, efficiency, and consistency while reducing risks**. They help auditors and organizations maintain the credibility of the certification process and support ongoing improvement efforts.

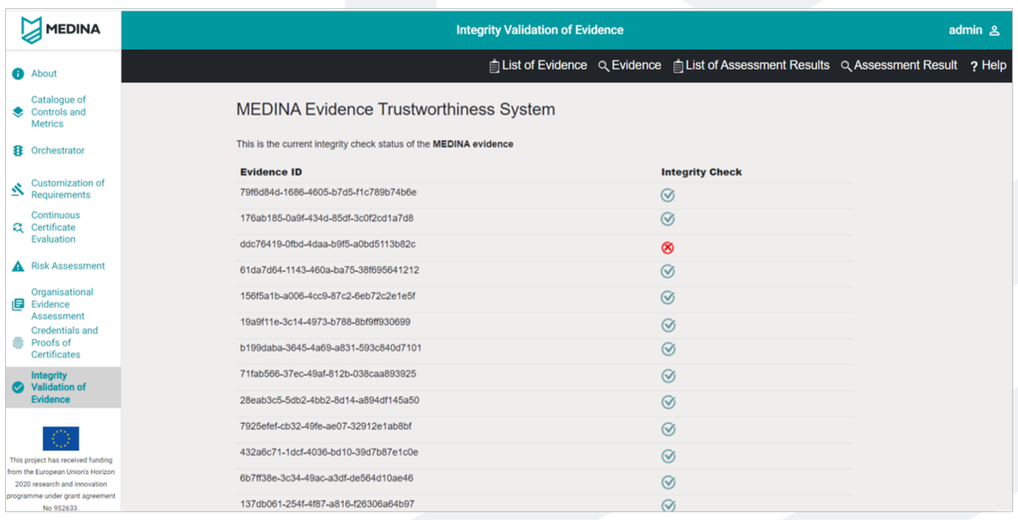
MEDINA considers the use of the **Blockchain** technology as a secure backbone as it is valuable in trusted systems because of its ability to provide data **immutability, transparency, security, decentralisation and resistance to tampering**, which contributes to the reliability and integrity of the MEDINA framework. There are two components in MEDINA which provide enhance trustworthy information for auditors.

MEDINA Evidence and Assessment Results Trustworthiness System

The **MEDINA Evidence Trustworthiness Management System**, provides a secure mechanism to maintain an audit trail of evidence and assessment results. It is implemented in **Smart Contracts** backboned by a **Blockchain network**, providing the following functionalities:

- It includes the logic to **provide the required information to be audited** (about evidence and assessment results).
- It provides **long-term information recording**, creating a secure record of information on a verifiable (**verification**), permanent (**traceability**) and resistant to modification (**integrity**) way.
- It includes the logic for external users to **access audited information** (about evidence and assessment results) **in a graphical and user-friendly way**.
- It provides a **trustworthy records for auditors** to be able to perform **manual or automated inspections** when needed while guaranteeing the integrity of information.

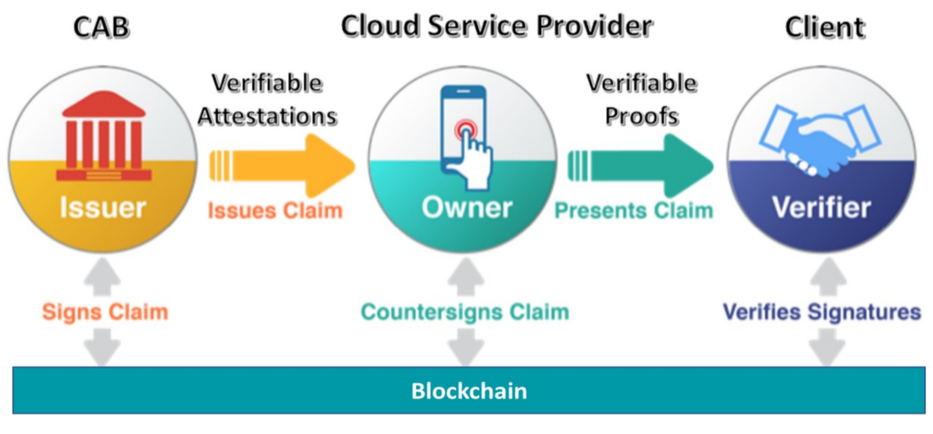


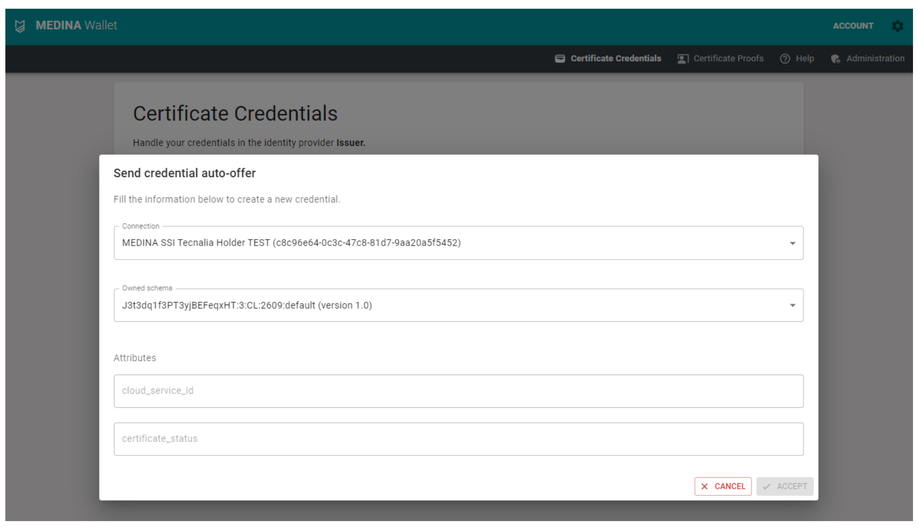


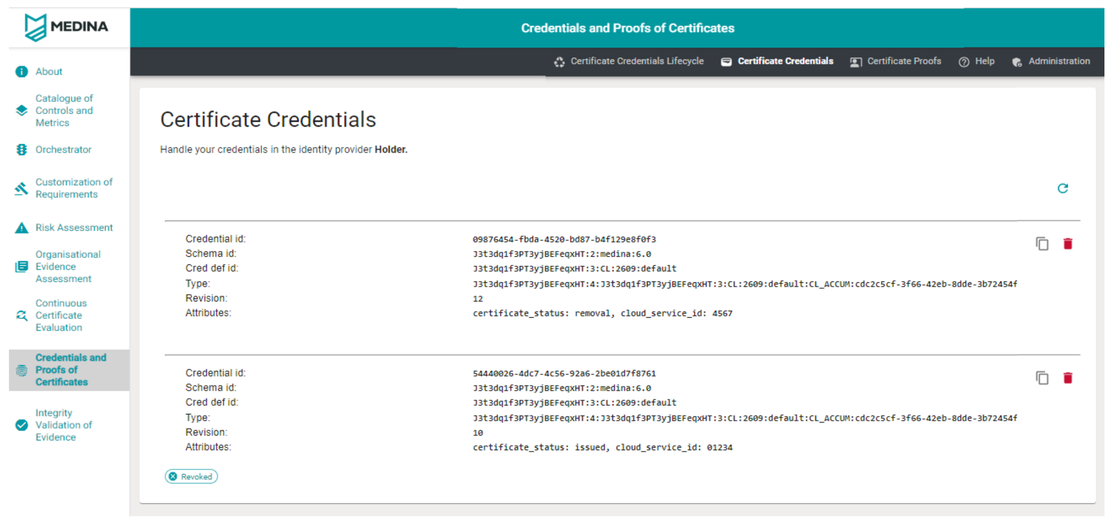
MEDINA Self Sovereign Identity Framework

The **MEDINA Self Sovereign Identity (SSI) Framework** provides a secure mechanism for Cloud Service Providers (CSPs) to **prove the certification status** of their cloud services according to the Certification Authority Board (CAB) issuance. It is composed of four main components:

- **Issuer:** It creates, signs and issues verifiable credentials with the cloud service certification status. The CAB will be the trusted authority acting as issuer of the conformity assessment result reports.
- **Owner:** It refers to the CSP; it locally owns, stores and controls the credentials about his cloud services. It also generates verifiable proofs of the certification status based on the own verifiable credentials.
- **Verifier**: It refers to an external user or auditor who needs to identify cloud service certification status based on verifiable credentials issued by trusted issuers.
- **Blockchain:** It is the secure global repository for public key identifiers in SSI, needed for the signatures' validation. It provides trust, integrity and availability.







tecnalia
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 952633

Contact
Cristina Regueiro (TECNALIA)
Tel: +34 946 43 08 50
Email: cristina.regueiro@tecnalia.com

https://medina-project.eu/

https://twitter.com/MedinaprojectEU
https://www.youtube.com/@MedinaprojectEU
https://www.linkedin.com/groups/12486585/
https://www.slideshare.net/MEDINAContinuousclou