MEDINA

Initial Experiences with OSCAL and Continuous Monitoring in the EUCS

Dr. Jesus Luna Garcia
Robert Bosch GmbH, Germany

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

Agenda

MEDINA

- Background
- Experimenting with EUCS-Continuous & OSCAL
- Summary

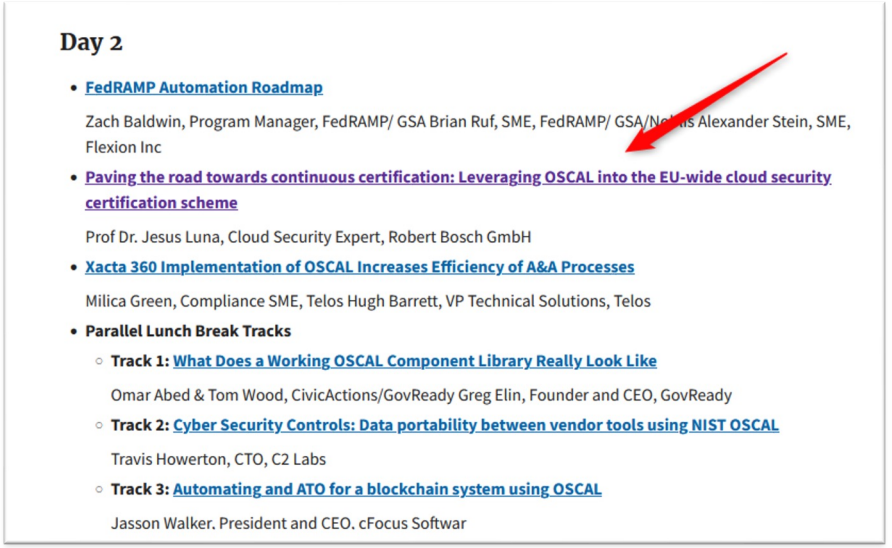
Background

EU Cybersecurity Act (EUCSA)

EU Cybersecurity Certification Scheme for Cloud Services (EUCS)

Back at the 2nd OSCAL Workshop…

- The EU Cybersecurity Act (EUCSA, April-2019), proposes the creation EU-wide cybersecurity certification schemes in order to:
  - provide an EU-wide cybersecurity baseline (requirements, audit methods)
  - enable customers to make risk-based decisions about cybersecurity
  - ***enable continuous cybersecurity compliance***
- Two EUCSA-derived certification schemes are under preparation by ENISA:
  - EUCC – Cybersecurity Certification Scheme for Common Criteria
  - ***EUCS - Cybersecurity Certification Scheme for Cloud Services***



Day 2

- **FedRAMP Automation Roadmap**

  Zach Baldwin, Program Manager, FedRAMP/ GSA Brian Ruf, SME, FedRAMP/ GSA/Novalis Alexander Stein, SME, Flexion Inc
- **Paving the road towards continuous certification: Leveraging OSCAL into the EU-wide cloud security certification scheme**

  Prof Dr. Jesus Luna, Cloud Security Expert, Robert Bosch GmbH
- **Xacta 360 Implementation of OSCAL Increases Efficiency of A&A Processes**

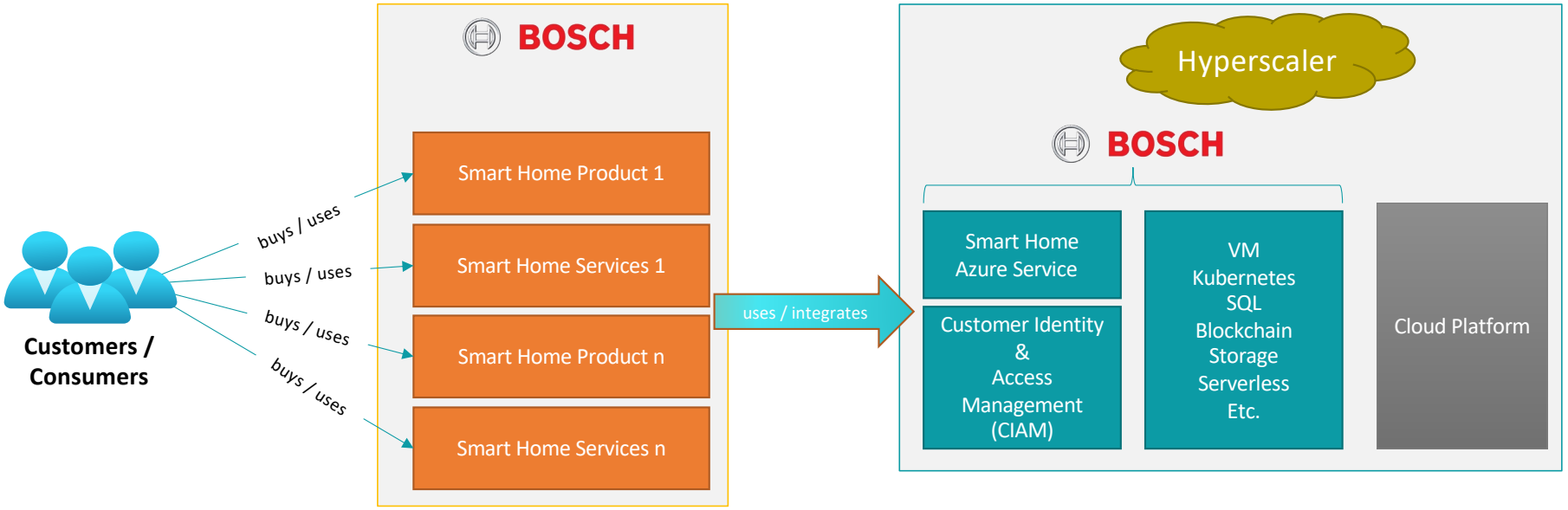
  Milica Green, Compliance SME, Telos Hugh Barrett, VP Technical Solutions, Telos
- **Parallel Lunch Break Tracks**
  - **Track 1: What Does a Working OSCAL Component Library Really Look Like**

    Omar Abed & Tom Wood, CivicActions/GovReady Greg Elin, Founder and CEO, GovReady
  - **Track 2: Cyber Security Controls: Data portability between vendor tools using NIST OSCAL**

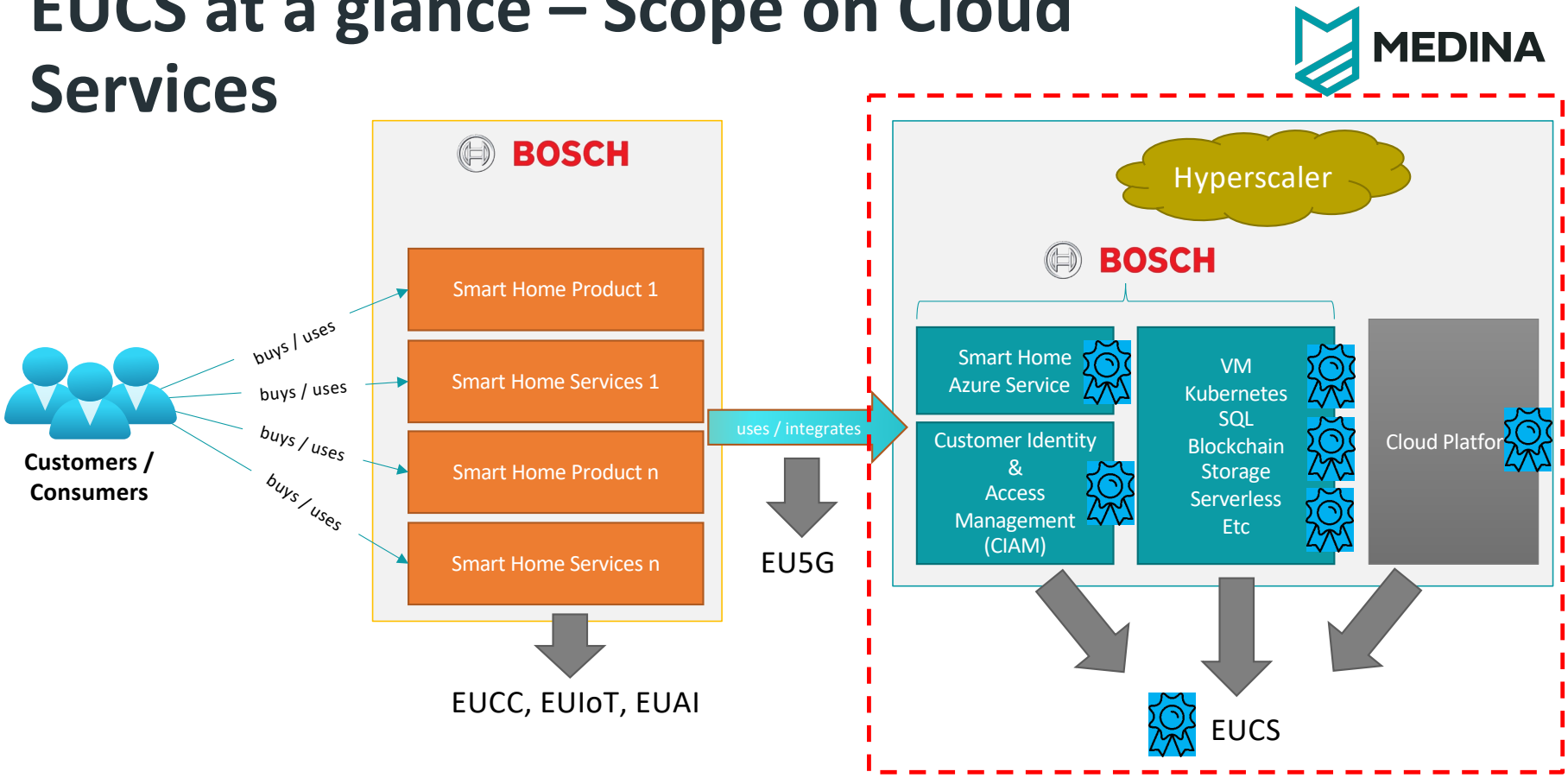
    Travis Howerton, CTO, C2 Labs
  - **Track 3: Automating and ATO for a blockchain system using OSCAL**

    Jasson Walker. President and CEO. cFocus Softwar

EUCS at a glance – Scope on Cloud Services



EUCS at a glance – Scope on Cloud Services



Defining Continuous Monitoring in EUCS

Just "*gather, compare, & report*"

enisa

EUCS – CLOUD SERVICES SCHEME
December 2020

Continuous monitoring

The requirements related to continuous monitoring typically mention "automated monitoring" or "automatically monitor" in their text. The intended meaning of "monitor automatically" is:

1. Gather data to analyse some aspects of the activity being monitored at discrete intervals at a sufficient frequency;
2. Compare the gathered data to a reference or otherwise determine conformity to specified requirements in the EUCS scheme;
3. Report deviations to subject matter experts who can analyse the deviations in a timely manner;
4. If the deviation indicates a nonconformity, then initiate a process for fixing the nonconformity; and
5. If the nonconformity is major, notify the CAB of the issue, analysis, and planned resolution.

These requirements stop short on requiring any notion of continuous auditing, because technologies have not reached an adequate level of maturity. Nevertheless, the introduction of continuous auditing, at least for level High, remains a mid- or long-term objective, and the introduction of automated monitoring requirement in at least some areas is a first step in that direction, which can be met with the technology available today.

Further guidance will be provided about acceptable mechanisms and processes.

Source: https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme

Defining Continuous Monitoring in EUCS

Just "*gather, compare, & report*"

Source: https://starecat.com/what-could-possibly-go-wrong-cutting-fail/

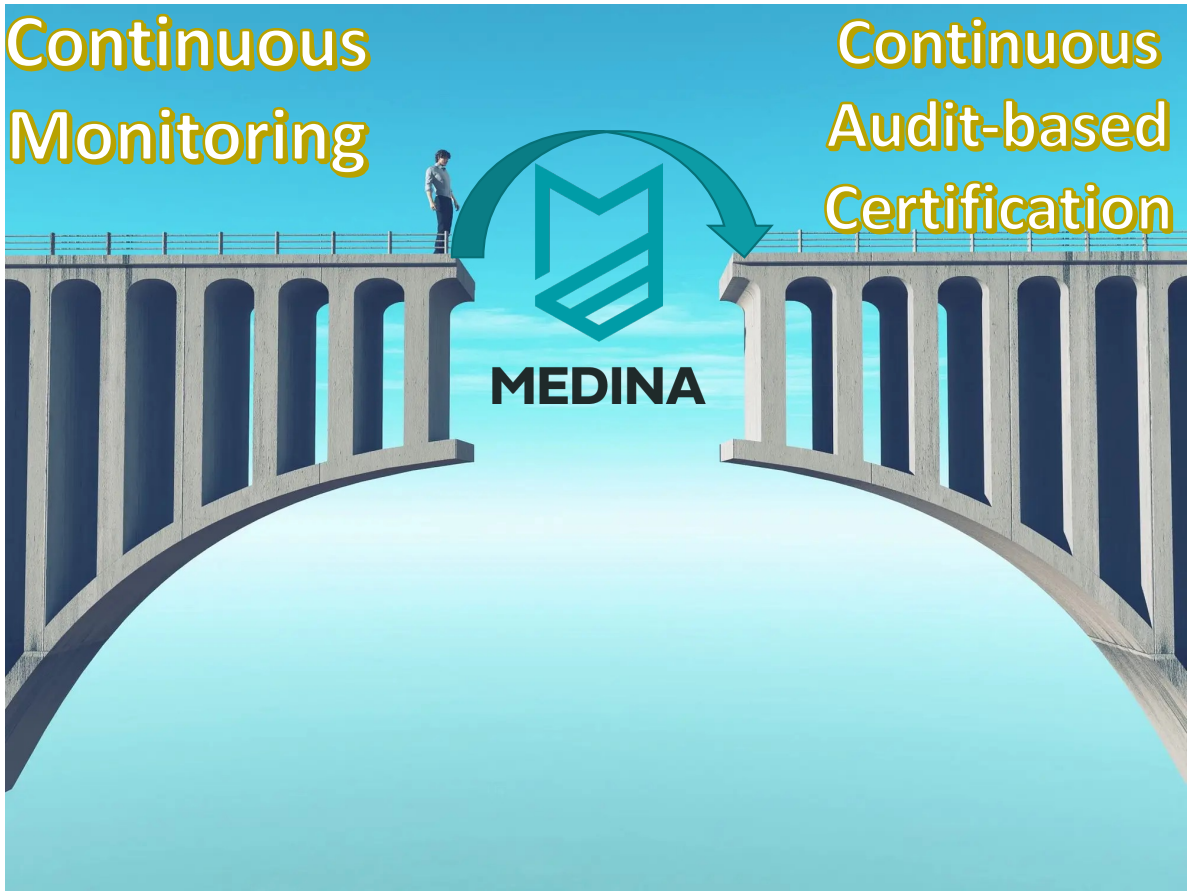
Experimenting with EUCS-Continuous and OSCAL

H2020 MEDINA Project

3/24/22

Why the EU-funded MEDINA Project?

MEDINA



TODAY

Let's understand the real-world implications from an EUCS perspective…

TOMORROW

…and one day we will fully realize automation in EUCS processes!

MEDINA At a Glance

- 1st November 2020 – 30th October 2023
- EU Budget 4,480,308.75€

Consiglio Nazionale delle Ricerche

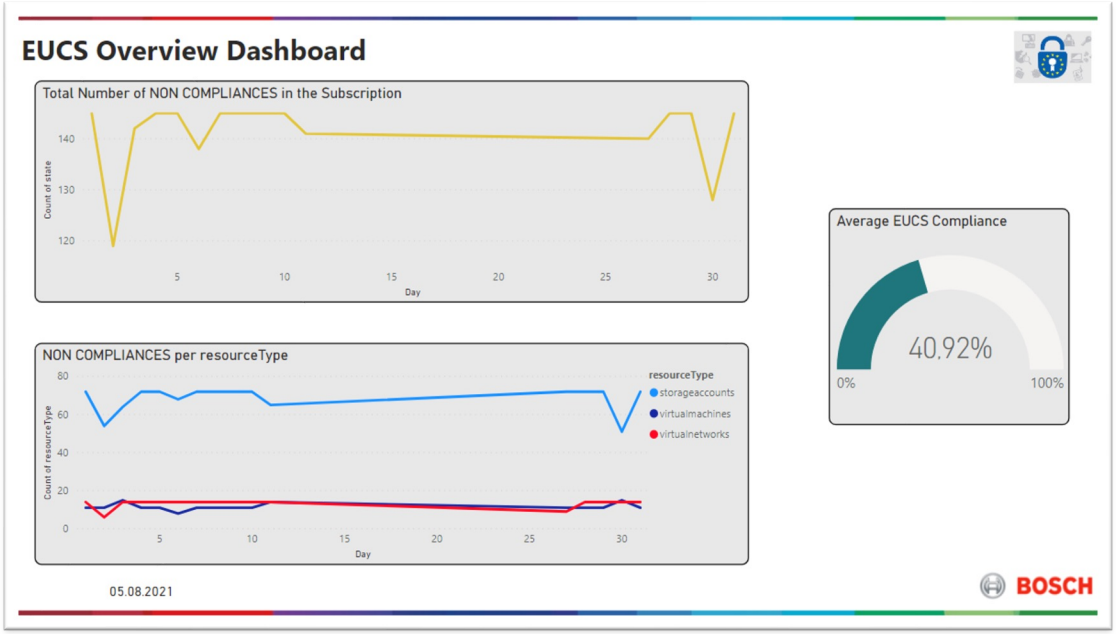
Paving to Road for EUCS-Continuous

MEDINA

Existing Certifications	Approach in MEDINA
Assurance based on point-in-time assessments	Continuous audit-based certification Tamper-proof evidence stored in DLT
Mostly manual/time consuming assessment processes	NLP to ease assessment of organizational measures OSCAL automation for CSP-agnostic assessments
Lack of transparency in cloud security posture	Role-based visualizations provide different levels of granularity and assurance for EUCS certificates
High customization effort in commercial CSPM tools (Cloud Security Posture Management)	Automated generation of compliance assessment rules based derived from EUCS catalogue

Experimenting with EUCS

- In March 2021, ENISA released a “call for experimentation” related to different aspects of the candidate EUCS.
- MEDINA contributed with the experimentation of *automated monitoring requirements, including an OSCAL – EUCS PoC.*
  - *Running period: 30 days*
  - *Testbed: well-know hyperscaler*
  - *Tools: hyperscaler’s CSPM, MEDINA’s homebrew metrics & dashboards*



Obtained Results

- OSCAL format for EUCS:
  - Machine-readability benefits EUCS automation
  - NIST OSCAL as a promising alternative for representing EUCS catalogue and assessments

OSCAL	EUCS	Examples
Groups/ID	Domain	A7
Groups/title	Category	A7 Operational Security
Groups/parts/prose(objective)	Objective	Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures
Groups/Controls/properties/value(label)	Control ID	OPS-02
Groups/Controls/title	Control	CAPACITY MANAGEMENT - MONITORING
Groups/Controls/parts/prose/(control-objective)	Control Objective	The capacities of critical resources such as personnel and IT resources are monitored.
Groups/Controls/parts/parts/properties/value(label)	Requirement ID	OPS-02.3
Groups/Controls/parts/parts/prose(item)	Requirement	The provisioning and de-provisioning of cloud services shall be automatically monitored to guarantee fulfilment of OPS-02.1

Let’s not Forget About the Auditors’ Perspective!

MEDINA

- The experiment shown that (very) different levels of automation can be achieved for implemented EUCS requirements.
- Auditor’s involvement is still required to ensure that the automated monitoring provides trustworthy evidence
- Standardization of audit processes, good practices (including EUCS Metrics) is still needed to leverage the full potential of automation
- About the auditor’s toolset:
  - Egg-chicken problem – who certifies the tools for certification?

Summary

What comes next?

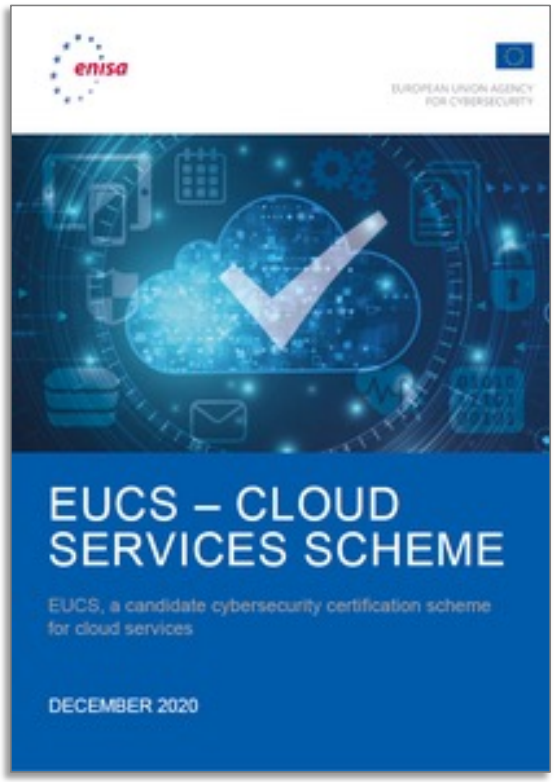
How-To EUCS-Continuous?

MEDINA

1. Provide a clear **implementation guidance** about EUCS requirements where some degree of automated monitoring is needed.
2. Provide clear **audit/assessment guidance** related to EUCS requirements needing some degree of automated monitoring.
3. Consider integrating a **catalogue of metrics** as part of the implementation guidance for EUCS.
4. Consider **focusing the EUCS requirements** needing some sort of automated monitoring only on capabilities offered by cloud platforms, and not by external systems.
5. **Guidance on selecting tools/technologies** for automated (continuous) monitoring.
6. Actively monitor the development of **NIST OSCAL**.

Summary

- MEDINA aims to facilitate adoption of EUCS, specifically for automated monitoring, while paving the road for continuous certification.
- Is EUCS' automation the silver bullet in cloud cybersecurity certification?
- Can MEDINA and OSCAL be game changers in the cybersecurity audit/certification practice?



Thank you!

www.medina-project.eu // jesus.lunagarcia@de.bosch.com