FedRAMP

Developer Data Bites

April 13, 2023

GSA

info@fedramp.gov
fedramp.gov

Introduction

Purpose: To create space for dialogue between developers who use OSCAL and the FedRAMP® automation team.

Outcomes:

- Shared understanding of the GSA public portal prototype
- Feedback on the GSA public portal prototype
- Productive discussion around formation of early adopters workgroup

Agenda:

- Welcome
- Pre-Submitted Q&A
- Demo – GSA Public Portal Prototype
- Open Forum
- Next Steps & Closing

Data Bites Guiding Principles

Keep the discussion respectful

Be curious, seek understanding

Speak from your own experience

Challenge through questions

Focus on ideas

Keep it technical

Pre-Submitted Questions

Pre-Submitted Questions

Question: OSCAL alignment with RAR?

For JAB authorization, when applying for the initial JAB P-ATO, the RAR must first be completed, and is valid for 1 year. The OSCAL models provided by FedRAMP do not include reference to which controls are required for RAR, and which are for SAP and SAR. Is there going to be a model for the RAR, so CSPs can submit the RAR through OSCAL and attain the P-ATO?

None of existing FR OSCAL documentation addresses RAR use case. It is currently not supported at the moment but could be an interesting use case and perhaps something for the future if GSA would like to pursue. Escalating to PMO review team SMEs for consideration.

FedRAMP Automation GitHub Updates

Update on FedRAMP automation repository

10x Flexion Transition

- 10x/Flexion team has transitioned the majority of Schematron validations support but is still available for consultation to FedRAMP team for limited period of time.
- A new dedicated resource has been added to the FedRAMP validations team: Dimitri Zhurkin

Issues/Ticket Tags

- **Newly opened issues this cycle**
  - #395 - SSP element Href attribute error
  - #397 - Issues with NodeJS upgrade.
  - #398, 399, 401-404 All related to response points misalignment and errors in Rev 4 profiles
  - #405 - RAR submission for OSCAL
- **Closed issues this cycle related to Schematron Validations**
  - #400, 403 - New response points (compared to security test case procedures)

Demo – GSA Public Portal Prototype

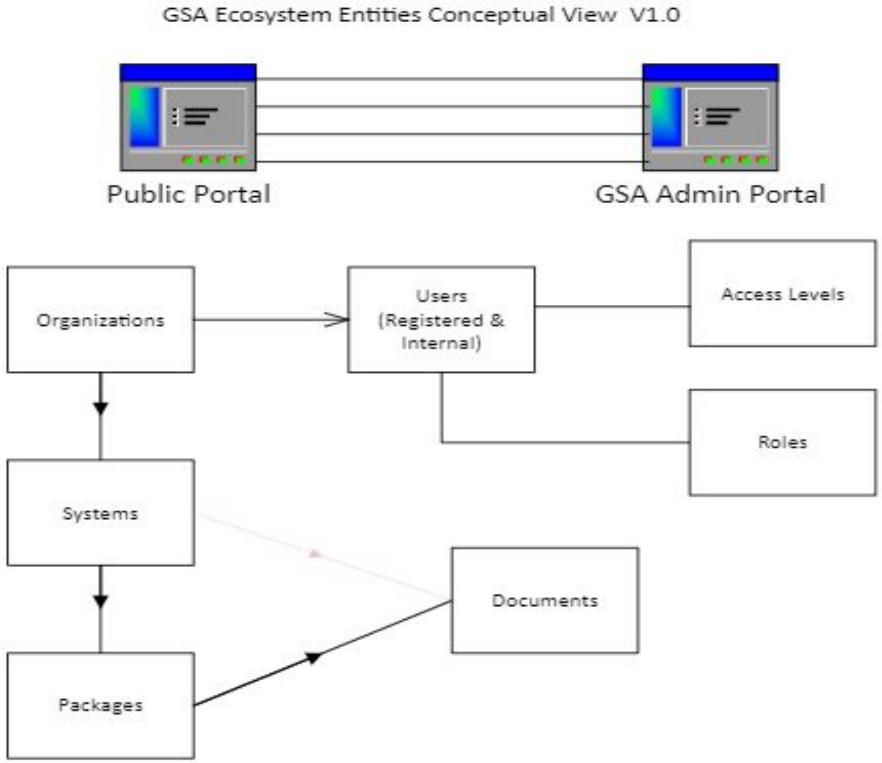
GSA Public Portal Prototype

Current Status

- Built on initial pre-release version of Automation Ecosystem REST APIs.
- No ATO at this time, so **NO sensitive data**. Test Data Only. Currently dev, test and integration environments are stood up.
- Limited functionality.
  - Register and sign up for portal and REST API access.
  - Validate OSCAL SSP, SAP, SAR, and POAM files (XML and JSON).
  - Upload OSCAL and associated package artifacts with versioning.
  - Generate word versions of OSCAL documents (SSP only currently, others-future).
  - Artifacts are structured in ATO packages associated with systems and organizations.
- Allows Automation Team to collaborate with early adopters and find potential issues with automation ecosystem and resolve them.

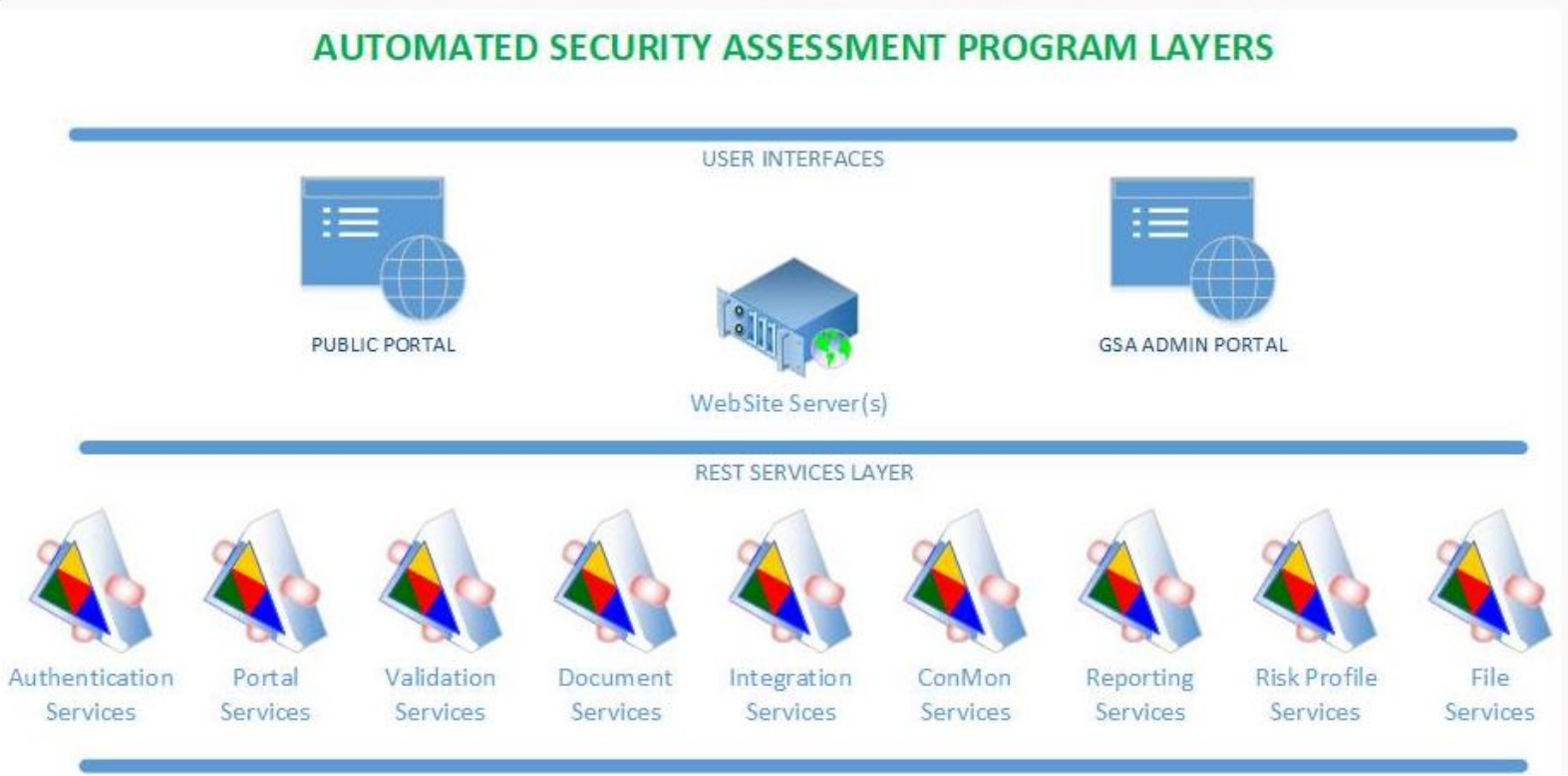
GSA Public Portal Prototype

Entity/Architecture Overviews



GSA Public Portal Prototype

Entity/Architecture Overviews



GSA Public Portal Prototype

Next Steps

- Participation is voluntary; consider your willingness to share outcomes.
- Onboarding will be done one-on-one to establish access roles and credentials.
- New GitHub repos will be established for portal and REST API collaboration
  - Currently in the process of standing up portals and REST APIs on Cloud.gov at a MODERATE level.
- Once hosting has been established, there will be migration to Cloud.gov.
- We are targeting 3rd Quarter 2023 to be able to accept sensitive data.
- **Send email to oscal@fedramp.gov with your interest to participate.**

Open Forum

What topics do you want to see in the future?

Quick Poll

What do you want to see?

1. Demo of NIST Deepdiff tool
2. Something else, I will submit my ideas in the chat.

Thank you

Our next Developer Data Bites virtual meeting will be on **Thursday, May 11, 2023 at 12p ET**.

Submit questions and future discussion topics to OSCAL@fedramp.gov

Learn more at fedramp.gov

@FEDRAMP

How to Submit Issues with FedRAMP

Ensuring your outstanding issues or questions are received:

Issues can be submitted in several ways:

Preferred	Alternate
Open an issue on fedramp-automation github so that it will benefit the NIST/FedRAMP community. https://github.com/GSA/fedramp-automation/issues	Email us at oscal@fedramp.gov

OSCAL Resources

NIST:

https://pages.nist.gov/OSCAL/

Learning Resources: https://pages.nist.gov/OSCAL/learn/

Current release: https://github.com/usnistgov/OSCAL/releases

Development version: https://github.com/usnistgov/OSCAL/tree/develop

Content repo: https://github.com/usnistgov/oscal-content

FedRAMP:

Current repo: https://github.com/GSA/fedramp-automation

Current issues: https://github.com/GSA/fedramp-automation/issues

Validations work: https://github.com/18F/fedramp-automation/tree/master/src/validations

Web based validation tool:

https://federalist-2372d2fd-fc94-42fe-bcc7-a8af4f664a51.app.cloud.gov/site/18f/fedramp-automation/#/documents/system-security-plan

Useful Links

3rd Party Tools

- https://www.oxygenxml.com/xml_editor/download_oxygenxml_editor.html (Oxygen XML Editor)
- https://github.com/usnistgov/OSCAL/tree/main/xml/schema (NIST xsd schemas)
- https://github.com/usnistgov/oscal-content/tree/main/nist.gov/SP800-53/rev4/xml (NIST profiles)
- https://github.com/GSA/fedramp-automation/tree/master/dist/content/rev4/baselines/xml (FedRAMP profiles)
- https://code.visualstudio.com/download (Visual Studio Code)
- https://marketplace.visualstudio.com/items?itemName=qub.qub-xml-vscode
- https://marketplace.visualstudio.com/items?itemName=redhat.vscode-xml

Rev 5 Update

Rev 5 Timeline

Estimated Release Date of XXXXXXX

- Phase 1 Release: XXXXXXX
  - Rev 5 Baselines
  - CSP Transition Plan
- Phase 2 Release: XXXXXXX
  - Templates
  - OSCAL Docs
- Phrase 3 Release: XXXXXXX
  - Everything else (+45 documents)