Federal Identity, Credential, and Access Management Sub Committee

Delivering Automation for Continuous Compliance with OSCAL

Version 1.0

June 14, 2024

Revision History

Document Version	Document Date	Revision Details
1.0	06/14/2024	Initial Report

Table of Contents

Executive Summary

Overview of Proof of Concept

The FPKI PA support team has developed a Proof of Concept demonstrating the use of OSCAL for Continuous Compliance Automation. The Proof of Concept leveraged the OSCAL standard to achieve a continuous compliance capability for an 800-63 Credential Service Provider.

As part of the proof of concept, we undertook the following work

1. Generating requirements artifacts using the OSCAL standard, and uploading them to a public git repository
2. Establishing a test environment running the login.gov application.
3. Developing tooling to support automation of compliance verification against the to demonstrate the concept and capability for automation.

Outcomes of Proof of Concept

The output of this activity includes three elements:

1. Demonstration that OSCAL supports continuous compliance automation.
2. A toolkit for continuous assessment of applications that integrates with a popular, standard unit testing framework and produces OSCAL outputs.
3. A demonstrated framework for implementing continuous compliance for Credential Service Providers.

Recommendations

The following next steps are recommended to leverage the framework demonstrated in the POC, and to reduce the cost of compliance management for GSA and PKI partner agencies.

For community members to leverage this framework and adopt continuous compliance, officially sanctioned OSCAL versions of the policy documents must be provided for the community to leverage.

RECOMMENDATION 1: *Publish key policy documents in the OSCAL format, including Federal PKI Policies, and the 800-63 set of specifications, as discussed in this section.*

The largest participants in the ICAM and FPKI ecosystem will benefit the most from compliance automation and adoption of the OSCAL standard. By engaging these members closely, a virtuous cycle of process improvement can be started.

RECOMMENDATION 2: Engage SSP partners Treasury, Entrust and US Access, to share the POC results and information about the POC framework.

Investment in automation requires confidence that the ability to achieve compliance will not be compromised through adoption of improved processes. ICAM should demonstrate leadership by publicly assuring members of the community that investments in automation will not compromise their ability to maintain compliance.

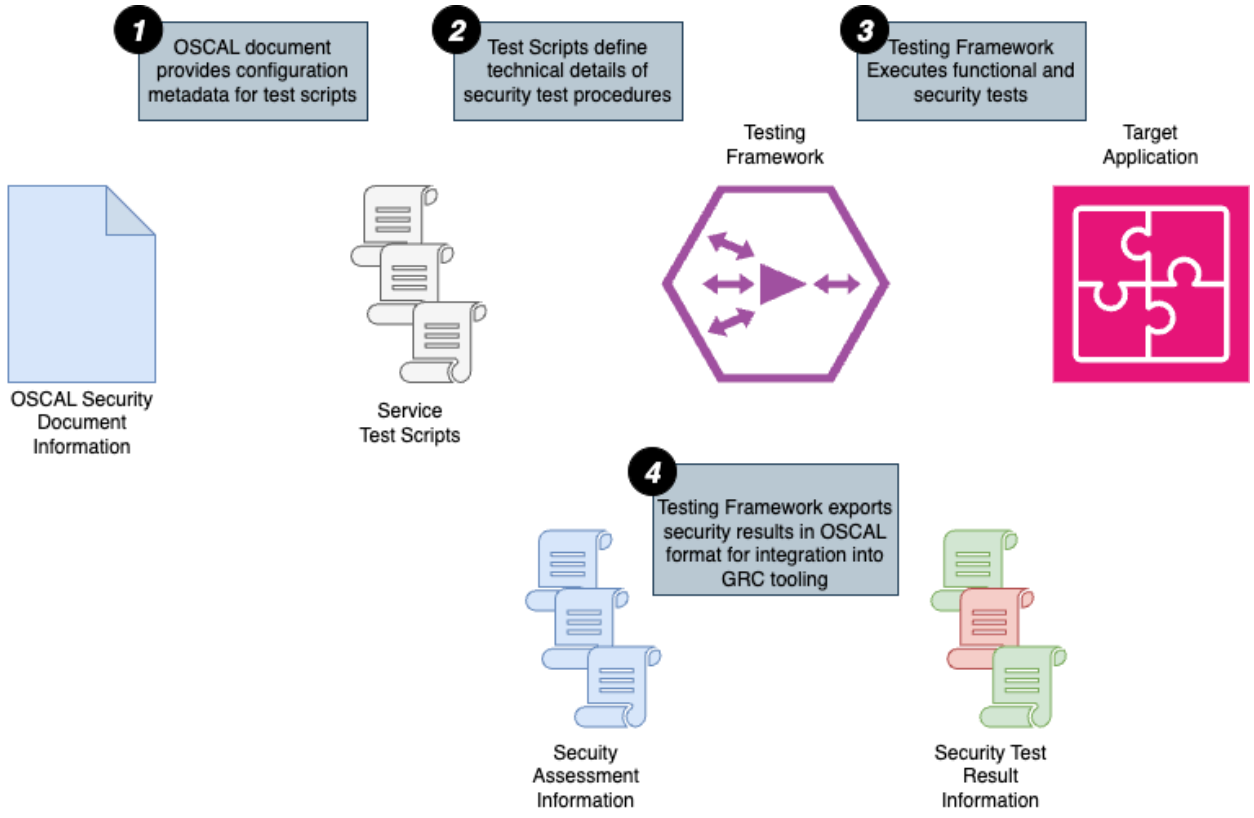
RECOMMENDATION 3: Develop guidelines for submission of Audit Artifacts in OSCAL formats, and adopt or implement tooling to support integration of OSCAL artifacts into the Annual Review Process.

Introduction

The FPKI PA support team has developed a Proof of Concept demonstrating the use of OSCAL for Continuous Compliance Automation. The Proof of Concept demonstrated a continuous compliance capability for 800-63 Credential Service Providers leveraging the OSCAL standard.

For this proof of concept, we developed an integration library for a widely used software testing framework that enabled the existing functional tests to export information about related security controls in the OSCAL format.

The following image illustrates the proof of concept implementation:



Compliance

Compliance is a critical component of information security. It is a key component of the NIST Cyber Security Framework, and one of the five security management pillars identified in the Jargon Free Security Model.

The Jargon Free Security Model identifies compliance as "Essential Busywork" because maintenance of compliance artifacts is essential for trustworthiness across organization boundaries, but maintenance of the artifacts themselves does not improve an organization's security posture. For this reason, reduction of the cost of managing compliance is the most important goal for a security program.

Compliance Automation

One of the best ways to reduce the cost of managing compliance is to automate the generation of the required compliance artifacts. If deployed properly, automation allows security personnel to focus on implementing the required security controls, and leaving the creation of documents to the automated system.

Continuous Compliance

Beyond the cost reduction, compliance automation can deliver other benefits. Chief among them is the ability to continuously monitor compliance and alert relevant personnel to changes to a systems configuration that violate a compliance requirement.

Continuous compliance reduces risk by ensuring that vulnerabilities in the environment are quickly discovered and reported so that they can be addressed.

Compliance Roles and Landscape

To understand compliance automation with OSCAL, it is essential to have a clear picture of the compliance landscape, and identify the critical roles involved in the compliance process.

Compliance is always measured against a specific, published version of a set of requirements, sometimes called **Controls**. Controls are collected in a single document, called a **Catalog**.

Requirements are always published by some recognized **Governance Authority**. In Federal Government systems, the requirements are usually published by NIST under the authorization of the White House, Congress, or an executive branch agency such as OMB, or GSA.

A general requirements document such as a *Catalog* is intended to cover a broad range of systems, deployed into a wide variety of environments, and targeting many potential use cases. For this reason it is common for a *Catalog* to be tailored for a specific environment and use case. A tailored set of requirements from a *Catalog* is known as a **Profile**. Well known examples of *Profiles* include the Low, Moderate, and High baselines from the 800-53r5 specification.

This tailoring allows the *Controls* in a *Catalog* to be adapted to the needs of a particular application, referred to as an **Information System**. An information system is composed of a set of **Components**, each of which is responsible for enforcing some subset of *Controls*. A document which describes how a *Component* can implement security controls is called a **Component Definition**.

The person or organization deploying the *Information System* is known as the **System Owner**. The system owner documents how their *Information System* implements the required *Controls* in a **System Security Plan**. The *System Security Plan* identifies all *Components* of the system, and every *Control* which the system implements. It describes how the *Control* is implemented by the *Information System*.

To ensure that the *Information System* implements all required *Controls* and conforms to the *System Security Plan*, an **Information System Security Officer** must be appointed for the system. The primary responsibility of the *Information System Security Officer* is to perform security assessments of the system, including audits and vulnerability assessments. The *Information System Security Officer* can create an **Assessment Plan** describing how they will perform the assessments, describing the frequency and methodology of the tests.

After completing the assessment, the *Information System Security Officer* will produce a document describing the **Assessment Results**, including descriptions of the results of the assessment, which may incorporate observations, risks, and findings. An observation is anything noted by the assessor, including evidence of compliance as well as evidence of non-compliance. A risk is a description of a potential negative system outcome, which may be based on a specific observation. A finding defines the state of a *Control* in the system - satisfied or not satisfied - based on the observations made in the context of the risks.

For any findings in the *Assessment Results* where a control is not satisfied, the *Information System Owner* and *Information System Security Officer* must determine how the *Information System* will be updated to address the finding. This is documented in a **Plan of Action and Milestones** which describes how the *System Owner* will correct the negative findings in the *Assessment Results.*

Proof of Concept

This section describes the scope and objectives of the Proof of Concept, and introduces the technologies used for the proof of concept.

Project Scope and Objectives

Relevant Standards

800-63B-3

800-63-3 provides technical requirements for federal agencies implementing digital identity services. The guidelines cover identity proofing and authentication of users (such as employees, contractors, or private individuals) interacting with government IT systems over open networks. They define technical requirements in each of the areas of identity proofing, registration, authenticators, management processes, authentication protocols, federation, and related assertions.

800-63B-3 was chosen because it focuses on user authentication, and provides a number of technical requirements which are good candidates for automating compliance verification.

Underlying Technologies

Login.gov

Login.gov is a web site offering "the public's one account for the government." Because login.gov is the largest Credential Service Provider in the federal space, it is a good candidate for demonstrating continuous compliance in the context of 800-63.

The source code for login.gov has been published online in a github repository.

18F/identity-idp: Login.gov Core App: Identity Provider (IdP) (github.com)

Ruby/Rails

The IDP for login.gov is implemented using a web application framework called Ruby on Rails. Ruby is an object oriented programming language that is popular in government projects. The Ruby language is popular with 18F, a GSA sponsored initiative that develops technology solutions for the federal government.

Ruby Programming Language (ruby-lang.org)

Ruby on Rails — https://rubyonrails.org/

RSpec

The login.gov idp uses an automated testing framework for Ruby called RSpec. The RSpec system enables software developers to define test cases in a custom language, and provide the output in a variety of formats.

RSpec: https://rspec.info/

OSCAL

The Open Security Controls Assessment Language (OSCAL) is a set of formats expressed in XML, JSON, and YAML. These formats provide machine-readable representations of control catalogs, control baselines, system security plans, and assessment plans and results. OSCAL is developed by NIST, in collaboration with industry.

OSCAL is discussed at more length in a later section of this document.

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

JSON

JSON (JavaScript Object Notation) is a lightweight data-interchange format. It is easy for humans to read and write, and easy for machines to parse and generate. JSON is a text format that is language independent but uses conventions that are familiar to programmers of the C-family of languages.

JSON - https://www.json.org/json-en.html

GRC Tools

Governance, Risk and Compliance (GRC) tools are software tools that support tracking of information related to Governance Controls.

OSCAL

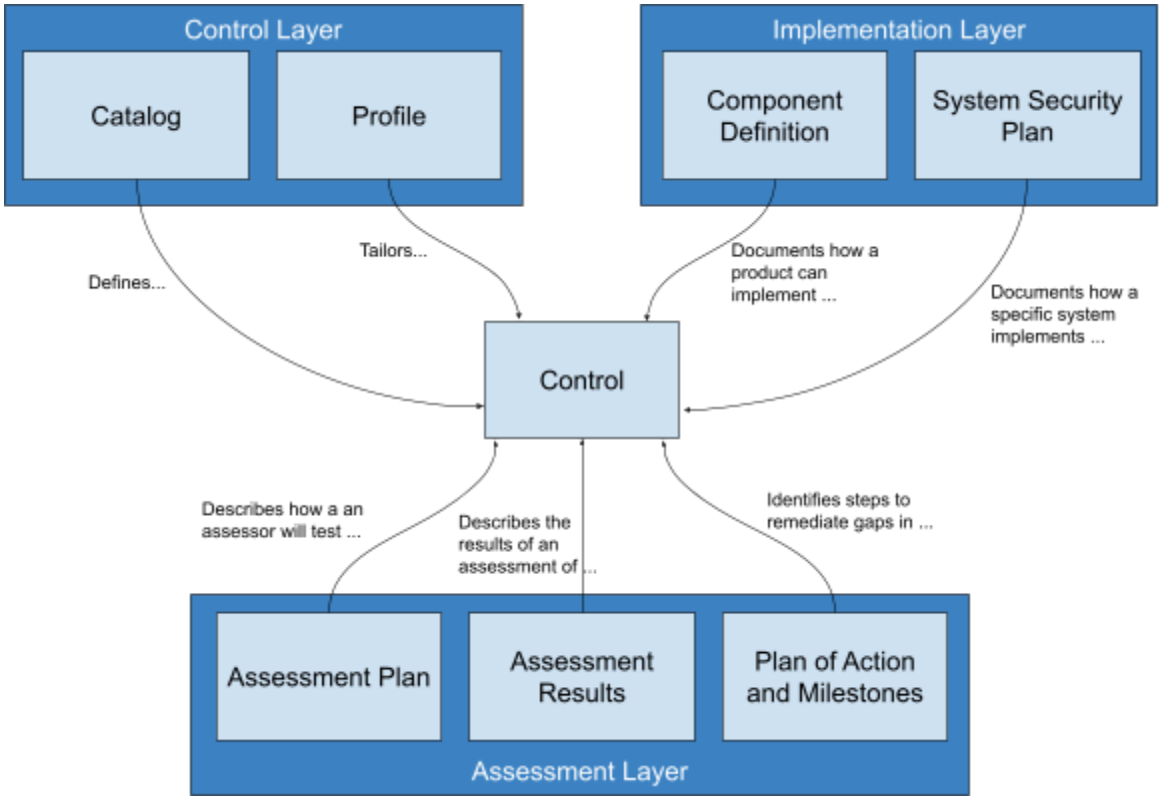
What is OSCAL

The Open Security Controls Assessment Language (OSCAL) is a specification published by NIST that provides a standardized framework for defining compliance artifacts.

It defines the following formats:

- Control Layer: Document or Tailor controls
    - Catalog: A format for documenting Security Controls and associated information
    - Profile: A format for tailoring controls defined in a catalog. Profiles allow system implementers to identify a subset of applicable controls that are relevant to a specific system, and add additional information about controls in the context of s system.
- Implementation Layer: Describes how a system implements controls
    - Component Definition: Describes how a software component can support a set of controls.
    - System Security Plan: Describes how a specific system supports the relevant controls.
- Assessment Layer: Describes how to assess compliance to a control, or the results of a compliance assessment.
    - Assessment Plan: Describes how a control will be assessed
    - Assessment Results: Describes the results of a control assessment
    - Plan of Actions and Milestones: Describes how gaps identified in an assessment will be addressed.

The central element of OSCAL documents is the Control. A control is a security requirement that can potentially be levied on a system. Each of the document formats relates to controls differently, as illustrated below:

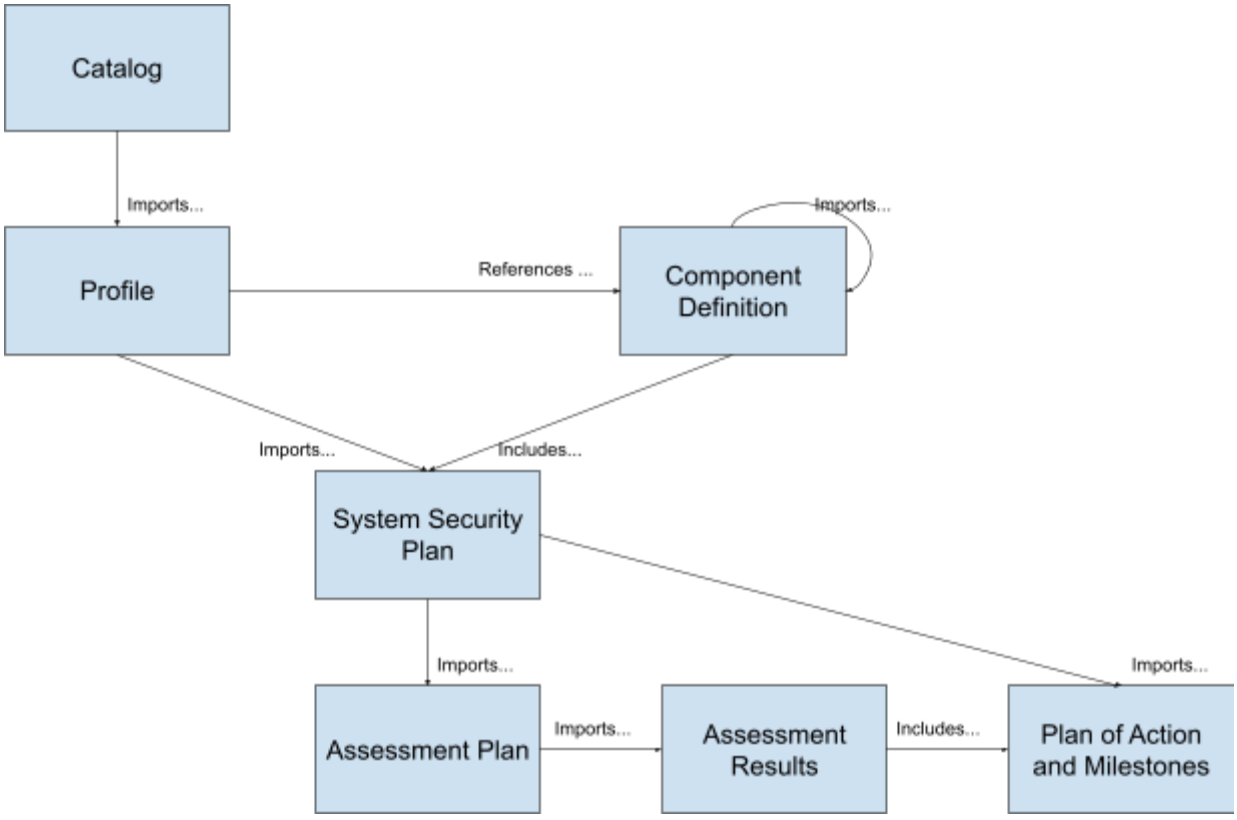


Controls are defined in a catalog, and may be tailored and customized in a profile.

A component definition describes how a piece of software could meet a set of selected controls, whereas a System Security Plan defines how a specific system actually meets the required controls.

Assessment Plans define how a control implementation will be assessed, and an assessment result describes the outcome of a plan. For any controls where the implementation does not meet the requirements, a Plan of action and Milestones will document how the gap will be closed.

The OSCAL specifications are designed to work together through cross referencing and inclusion, as illustrated below:



This cross referencing enables OSCAL artifacts to build on each other, and allows different participants in the overall process to focus on producing the information for which they are most authoritative.

Governing bodies and other policy authorities publish catalogs. They may also publish Profiles, if appropriate, to support multiple baselines or other subsets of controls.

Profiles may also be published by system owners to document tailoring of the controls or baselines within their own environments.

Software developers provide Component Definitions describing the features of their software that can be used to satisfy controls that might apply to their software.

System Owners produce System Security Plans by importing and including the contents of a profile and set of Component Definitions to identify the requirements their system must meet and describes how their own specific system implements the requirements.

Auditors will generate an Assessment Plan, which describes the steps required to verify that the system implements the controls as described in the System Security Plan, and will generate an Assessment Result after completing their assessment in order to document positive and negative results of an assessment, including issues risks and findings.

Finally, the Auditor and System Owner will collaborate to produce a Plan of Action and Milestones documenting how audit findings will be addressed by the System Owner.

	Catalog	Profile	Component Definition	System Security Plan	Assessment Plan	Assessment Results	Plan of Action and Milestones
Governance Authority	Publish	Publish	N/A	N/A	N/A	N/A	N/A
System Owner	N/A	Publish	N/A	Publish	N/A	N/A	Publish
Software Vendor/ Developer	N/A	N/A	Publish	N/A	N/A	N/A	N/A
Auditor	N/A	N/A	N/A	N/A	Publish	Publish	Publish

POC Approach:

Identification of Scope

In order to demonstrate end to end compliance automation within the timeframe permitted for the proof of concept, the scope of the demonstration was reduced to a handful of compliance requirements. Since the target of our POC demonstration was the code that operates login.gov, we selected requirements from the 800-63 volume on Authentication and Lifecycle Management (800-63B-3):

Requirement ID	Requirement Language
ms-01	Memorized secrets SHALL be at least 8 characters in length if chosen by the subscriber.
ms-02	The verifier SHALL use approved encryption and an authenticated protected channel when requesting memorized secrets in order to provide resistance to eavesdropping and MitM attacks.
ms-03	When processing requests to establish and change memorized secrets, verifiers SHALL compare the prospective secrets against a list that contains values known to be commonly-used, expected, or compromised.
ms-04	Verifiers SHOULD offer guidance to the subscriber, such as a password-strength meter [Meters], to assist the user in choosing a strong memorized secret.

Requirement ID	Requirement Language
ms-05	Verifiers SHALL store memorized secrets in a form that is resistant to offline attacks.
ms-06	Verifiers SHALL implement a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber's account as described in Section 5.2.2.

Preparing Control and System Documentation

There is not an official catalog representing 800-63-3 that the project could leverage. Therefore we created a minimal conformant catalog incorporating only the controls that are relevant to the test. This catalog can be viewed here. A profile was created incorporating the controls in the catalog.

Next, OSCAL component definitions were generated for all components that implemented the controls that were in scope for the proof of concept. Component definitions were generated for the following subcomponents of the login.gov system:

- "devise": a library providing enhanced authentication, session management and credential protections for ruby on rails applications
- "Puma": a replacement web server for rails applications that provides enhanced performance.

The component definitions identify the controls which can be implemented by the component, and describe how they could be implemented.

A System Security Plan was assembled based on the catalog and control definitions. It incorporates the component definitions and describes how the entire system complies with all required security controls.

Automating Compliance Verification

Automation of Compliance Verification relied on enhancement of the existing unit testing framework used for login.gov.

The RSpec framework is able to inspect the configuration of the system and its environment, and therefore can identify gaps in implementation or configuration that would result in non-compliance to the required security controls. This tool is an integrated part of the login.gov software application, and is used for functional testing. Leveraging the same tooling for compliance verification minimizes the additional effort required from developers and system administrators.

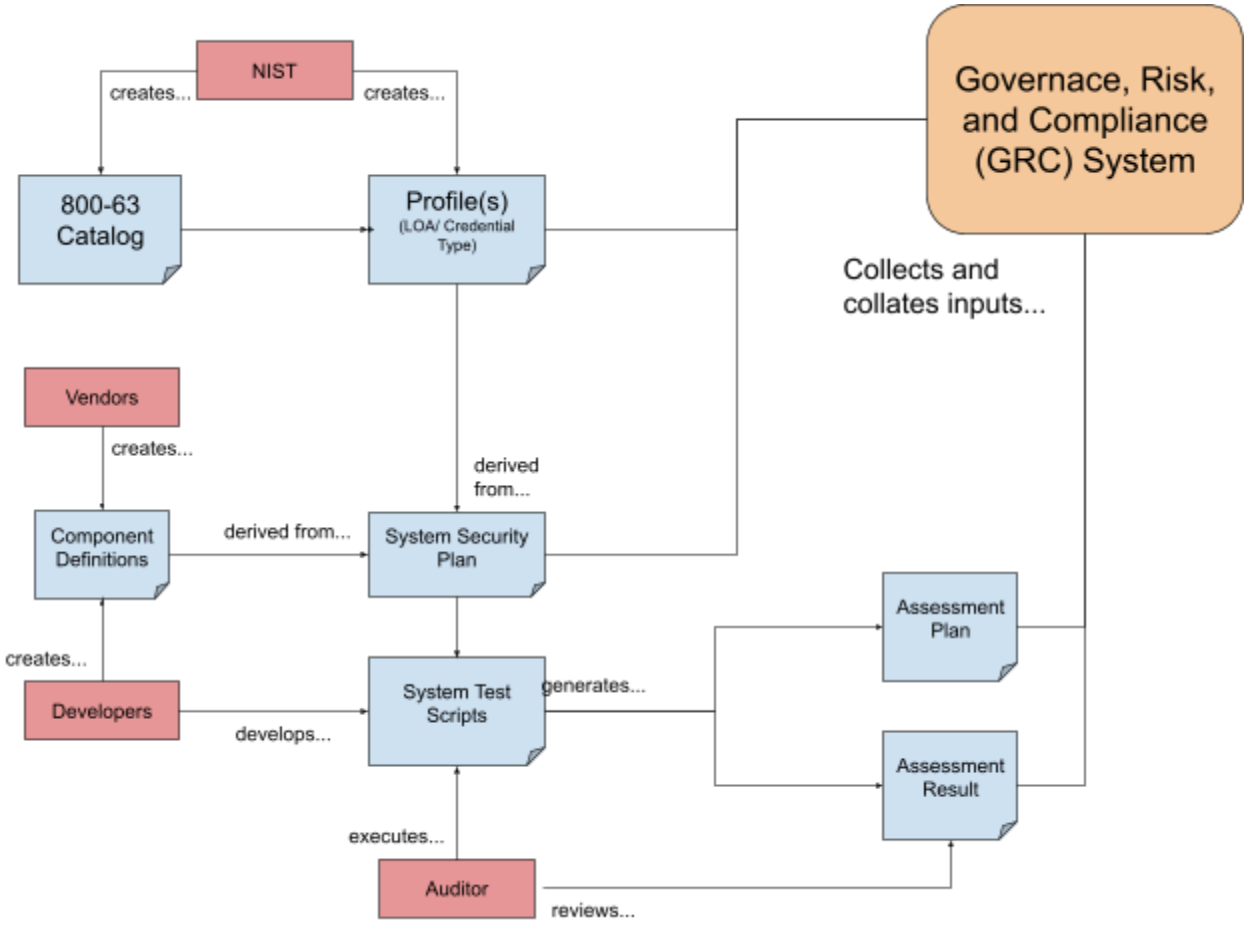
As part of the POC, the development team created an extension for the RSpec framework that generates OSCAL output representing Assessment Plans and Assessment Results. This enables security specific tests to be written in order to verify compliance, but also allows existing tests to be reused for compliance verification with the addition of some extra information in the test.

A Notional Production Workflow

While the scope of the POC was reduced, and was not intended as a production capability, the basic building blocks of the POC could be used in the context of a production capability.

The most important element of a production capability that was not present in the POC is a Governance Risk and Compliance (GRC) tool. OSCAL is a specification for describing audit related data in a structured way. The GRC tool ingests OSCAL artifacts and correlates the data contents into a unified view to produce an actionable compliance snapshot. As an open standard with backing from NIST and FedRAMP, OSCAL is a significant enabler for interoperability between and across GRC tools.

The diagram below shows how the system demonstrated in the POC is envisioned to work in a production environment:



Note that the actual security testing may be executed by the auditor, with a tool of their choice. The auditor may review the results of the assessment by importing them into any GRC tool that can receive and process OSCAL inputs.

The illustrated process reduces the effort and cost of compliance in the following ways:

1. Artifacts can build upon each other, and can be automatically constructed or derived from elements produced externally, saving considerable time and effort when creating necessary audit artifacts.
2. The technical testing tools currently used to perform functional testing can be adapted to perform security testing and produce outputs that feed directly into a GRC system to monitor compliance to requirements and standards.

Results

Despite its limited scope, the Proof of Concept demonstrated the feasibility of continuous compliance automation for a Credential Service Provider, leveraging the OSCAL standard against a real-life, critical U.S. Government application.

The software produced for the POC is suitable for integration into real applications leveraging the RSpec testing framework, and several individuals from the login.gov team have expressed interest in leveraging it for compliance automation against 800-53.

In addition, the POC has demonstrated the utility of OSCAL for 800-63 compliance automation. Beyond its roots in FedRAMP and ATO, OSCAL is a general purpose language that can be applied to a wide variety of compliance regimes and use cases.

Conclusion

Community Benefits

The benefits of OSCAL, conclusively demonstrated by the proof of concept, are as follows:

- It can be applied in a generic way to multiply compliance Regimes.
- The separation of the standard into distinct sub-specifications enables different participants in the process to manage only those sub-elements that are relevant to them.
- The integration of the sub-specifications through cross-referencing creates a consistent view of data that can dynamically integrate updates from different process stakeholders into a holistic, actionable view.
- The open and unencumbered nature of the specification encourages its integration into a wide variety of open-source and proprietary solutions.

The POC offers the following specific benefit to the broader community:

- Examples of OSCAL artifacts representing an end-to-end use case for continuous compliance automation with OSCAL
- An implementation of the security testing pattern used for the POC. The implementation can be used directly, or the code can be used as a template and reference implementation for that pattern in other languages and frameworks.

Next Steps

As discussed in this paper, automation with OSCAL relies on the ability to leverage existing OSCAL data and add the elements necessary to support the capability or pattern that is required.

Ultimately, the anchor for any OSCAL compliance activity is the Catalog. A catalog contains the authoritative record of the Controls that all other OSCAL artifacts rely upon. A catalog should be published by an authoritative source so that other entities can rely upon it with confidence.

Publish sanctioned versions of ICAM and FPKI policies in OSCAL formats

Official OSCAL catalogs should be released by ICAM, reflecting the critical policies over which they have governance. Catalogs should be released covering the following documents:

- Federal Bridge and Common Certificate Policies

In addition, ICAM should collaborate with NIST to publish or adopt the following critical documents as OSCAL catalogs:

- Special Publication 800-63
- FIPS 201
- Special Publication 800-79
- Special Publication 800-157

Catalogs should be prepared in coordination with the OSCAL community, which includes federal and private sector entities supporting automation for continuous compliance and reporting using the OSCAL specification. Coordination with the community will ensure that the catalogs developed can be leveraged as effectively as possible by existing tooling and systems.

Outreach and education for critical community stakeholders

The largest participants in the ICAM and FPKI ecosystem will benefit the most from compliance automation and adoption of the OSCAL standard. By engaging these members closely, a virtuous cycle of process improvement can be started.

Support continuous compliance by sanctioning the OSCAL standard for Annual Reviews

Investment in automation requires confidence that the ability to achieve compliance will not be compromised through adoption of improved processes. ICAM should demonstrate leadership by publicly assuring members of the community that investments in automation will not compromise their ability to maintain compliance.

Appendix A: OSCAL Artifacts

Catalog


```
{
  "$schema":
"https://github.com/usnistgov/OSCAL/releases/download/v1.1.2/oscal_catalog_schema.json",
  "catalog": {
    "uuid": "79765999-6d98-4011-aab9-1790a98243fa",
    "metadata": {
      "title": "POC Catalog for NIST SP 800-63-3",
      "last-modified": "2024-05-07T00:00:00.00Z",
      "version": "0.1-demo",
      "oscal-version": "1.1.2"
    },
    "groups": [
      {
        "id": "ms",
        "title": "Memorized Secrets",
        "controls": [
          {
            "id": "ms-01",
            "title": "Password length",
            "parts": [
              {
                "id": "ms-01-smt",
                "name": "statement",
```

```
                "prose": "Memorized secrets SHALL be at least 8 characters in length if chosen by the subscriber."
            }
        ]
    },
    {
        "id": "ms-02",
        "title": "Verifier shall use protected channel",
        "parts": [
            {
                "id": "ms-02-smt",
                "name": "statement",
                "prose": "The verifier SHALL use approved encryption and an authenticated protected channel when requesting memorized secrets in order to provide resistance to eavesdropping and MitM attacks."
            }
        ]
    },
    {
        "id": "ms-03",
        "title": "Compare passwords against known compromised list",
        "parts": [
            {
                "id": "ms-03-smt",
                "name": "statement",
                "prose": "When processing requests to establish and change memorized secrets, verifiers SHALL compare the prospective secrets against a list that contains values known to be commonly-used, expected, or compromised."
```

```
            }
          ]
        },
        {
          "id": "ms-04",
          "title": "Verifier should offer guidance",
          "parts": [
            {
              "id": "ms-04-smt",
              "name": "statement",
              "prose": "Verifiers SHOULD offer guidance to the subscriber, such as a password-strength meter [Meters], to assist the user in choosing a strong memorized secret."
            }
          ]
        },
        {
          "id": "ms-05",
          "title": "Secure storage of memorized secrets",
          "parts": [
            {
              "id": "ms-05-smt",
              "name": "statement",
              "prose": "Verifiers SHALL store memorized secrets in a form that is resistant to offline attacks."
            }
          ]
        },
```

```
            {
              "id": "ms-06",
              "title": "Implement rate limiting",
              "parts": [
                {
                  "id": "ms-06-smt",
                  "name": "statement",
                  "prose": "Verifiers SHALL implement a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber’s account as described in Section 5.2.2."
                }
              ]
            }
          ]
        }
      ]
    }
}
```


Profile


```
{
  "$schema": "https://github.com/usnistgov/OSCAL/releases/download/v1.1.2/oscal_profile_schema.json",
  "profile": {
    "uuid": "70167545-32d3-4ace-9e14-c90d095765c3",
    "metadata": {
      "title": "800-63 Profile for Proof of Concept",
      "last-modified": "2024-06-06T00:00:00Z",
```

```
        "version": "0.1",
        "oscal-version": "1.1.4"
      },
      "imports": [
        {
          "href": "../catalogs/800-63-poc-catalog.json",
          "include-controls": [
            {
              "with-ids": [
                "ms-01",
                "ms-02",
                "ms-03",
                "ms-04",
                "ms-05",
                "ms-06"
              ]
            }
          ]
        }
      ]
    }
}
```


System Security Plan

UPDATE WITH NEW REQUIREMENTS AND INSERT

Component Definitions

Rails-Devise


```
{
   "component-definition": {
      "uuid": "c040baf0-844c-473e-9048-5ec032c18d7f",
      "metadata": {
         "title": "Rails/Devise Component Definition",
         "last-modified": "2024-05-07T00:00:00.00Z",
         "version": "0.1-demo",
         "oscal-version": "1.1.2"
      },
      "components": [
         {
            "uuid": "4459bba1-a93e-46f2-97ed-03b198a1071f",
            "type": "software",
            "title": "devise",
            "description": "Devise is a flexible authentication solution for Rails based on Warden.",
            "props": [
               {
                  "ns": "http://csrc.nist.gov/ns/oscal",
                  "name": "asset-type",
                  "value": "web-server"
               },
               {
                  "ns": "http://csrc.nist.gov/ns/oscal",
                  "name": "public",
```

```
            "value": "no"
        },
        {
            "ns": "http://csrc.nist.gov/ns/oscal",
            "name": "virtual",
            "value": "yes"
        },
        {
            "ns": "http://csrc.nist.gov/ns/oscal",
            "name": "implementation-point",
            "value": "internal"
        }
    ],
    "control-implementations": [
        {
            "uuid": "2236c549-e6c3-4a85-b06e-2415e4f0b6c9",
            "source": "https://pages.nist.gov/REPLACE-WITH-OSCAL-IO-REFERENCE",
            "description": "Implementation of 800-63B requirements with the Rails Application Server.",
            "implemented-requirements": [
                {
                    "uuid": "852825aa-877e-4812-a015-eef2303f794d",
                    "control-id": "MS-01",
                    "description": "Login.gov implements requirement MS-01 as documented in the statements below",
                    "statements": [
                        {
```

```
                    "uuid": "90af122b-89a8-47ce-9adf-e64ed060ea18",
                    "statement-id": "ms-01_smt",
                    "description": "Password length is configured in the initializer file located at config/initializers/devise.rb. It is controlled by the variable config.password_length."
                }
            ]
        }
    ]
  }
}
```


Rails-Puma


```
{
   "component-definition": {
      "uuid": "655A6431-8C60-4686-B33B-2C7B35ABAD79",
      "metadata": {
         "title": "Rails Component Definition",
         "last-modified": "2024-05-07T00:00:00.00Z",
         "version": "0.1-demo",
         "oscal-version": "1.1.2"
      },
      "components": [
         {
```

```
"uuid": "76ECE90B-E3CD-40C7-9448-80BDD001CA2E",
"type": "software",
"title": "puma",
"description": "Web Server providing access to the IDP",
"purpose": "enable access to the server via web browser",
"props": [
  {
    "ns": "http://csrc.nist.gov/ns/oscal",
    "name": "asset-type",
    "value": "web-server"
  },
  {
    "ns": "http://csrc.nist.gov/ns/oscal",
    "name": "public",
    "value": "yes"
  },
  {
    "ns": "http://csrc.nist.gov/ns/oscal",
    "name": "virtual",
    "value": "yes"
  },
  {
    "ns": "http://csrc.nist.gov/ns/oscal",
    "name": "implementation-point",
    "value": "internal"
  }
```

```
        ],
        "protocols": [
          {
            "name": "http",
            "port-ranges": [
              {
                "start": 80,
                "end": 80
              }
            ]
          },
          {
            "name": "https",
            "port-ranges": [
              {
                "start": 443,
                "end": 443
              }
            ]
          }
        ],
        "control-implementations": [
          {
            "uuid": "5CA7C326-0E1E-4EAA-893D-D86F931F36E0",
            "source": "https://pages.nist.gov/REPLACE-WITH-OSCAL-IO-REFERENCE",
            "description": "Implementation of 800-63B requirements by the Rails Web
Server.",
```

```
                "implemented-requirements": [
                    {
                        "uuid": "148695C5-9935-4C7A-AFD7-469CE28402B8",
                        "control-id": "ms-13",
                        "description": "Login.gov implements requirement ms-13 as documented in the statements below",
                        "statements": [
                            {
                                "uuid": "98289486-DD7D-40B4-A0AD-D0E81F32E656",
                                "statement-id": "ms-13_smt",
                                "description": "The server may be started with HTTPS=on in order to provide TLS"
                            }
                        ]
                    }
                ]
            }
        ]
    }
}
```


Rails-Puma-Devise (Capability)


```
{
    "$schema": "https://github.com/usnistgov/OSCAL/releases/download/v1.1.2/oscal_component_schema.json",
```

```
  "component-definition": {
    "uuid": "02f07ee6-656c-46a0-bc81-7a34dda3f043",
    "metadata": {
      "title": "Rails Component Definition",
      "last-modified": "2024-05-07T00:00:00.00Z",
      "version": "0.1-demo",
      "oscal-version": "1.1.2"
    },
    "import-component-definitions": [
      {
        "href": "rails-devise-module-component-def.json"
      },
      {
        "href": "rails-puma-component-def.json"
      }
    ],
    "capabilities": [
      {
        "uuid": "132C0573-2439-4ED8-BD73-D870DCC89779",
        "name": "Vanilla Rails Implementation",
        "description": "An implementation of Ruby on Rails that does not include any third party compoenents",
        "incorporates-components": [
          {
            "component-uuid": "76ECE90B-E3CD-40C7-9448-80BDD001CA2E",
            "description": "Ruby on Rails puma web server component."
          },
```

```
            {
                "component-uuid": "c040baf0-844c-473e-9048-5ec032c18d7f",
                "description": "Devise: Ruby on Rails authentication module"
            }
          ]
        }
      ]
    }
}
```


Assessment Plans

MS-01


```
{
   "assessment-plan": {
      "uuid": "da1ce957-e50e-42a0-936e-1a44f9d8a96c",
      "metadata": {
         "title": "Automated Testing Plan for login.gov. It confirms passwords are set to the appropriate minimum length",
         "last-modified": "2024-06-14T10:25:10+00:00",
         "version": "2024-06-14T10:25:10+00:00",
         "oscal-version": "1.1.2"
      },
      "import-ssp": {
         "href": "../system-security-plans/CSP_POC_ssp.json"
      },
      "reviewed-controls": {
```

```
        "control-selections": [
          {
            "include-controls": [
              {
                "control-id": "ms-01",
                "statement-ids": [
                  "ms-01_smt"
                ]
              }
            ]
          }
        ]
      }
    }
}
```


MS-02


```
{
   "assessment-plan": {
      "uuid": "04465aa4-eebc-4527-894f-649e900081b8",
      "metadata": {
         "title": "Automated Testing Plan for login.gov. It confirms that TLS is configured on the server",
         "last-modified": "2024-06-14T10:25:10+00:00",
         "version": "2024-06-14T10:25:10+00:00",
         "oscal-version": "1.1.2"
      },
```

```
        "import-ssp": {
            "href": "../system-security-plans/CSP_POC_ssp.json"
        },
        "reviewed-controls": {
            "control-selections": [
                {
                    "include-controls": [
                        {
                            "control-id": "ms-02",
                            "statement-ids": [
                                "ms-13_smt"
                            ]
                        }
                    ]
                }
            ]
        }
    }
}
```


MS-03


```
{
    "uuid": "d01d4771-4c62-49df-9b96-26c8f821b40f",
    "metadata": {
        "title": "Automated Testing Plan for login.gov. It verifies that passwords are compared against a list that contains values known to be commonly-used, expected, or compromised.",
        "last-modified": "2024-06-14T10:25:10+00:00",
```

```
        "version": "2024-06-14T10:25:10+00:00",
        "oscal-version": "1.1.2"
    },
    "import-ssp": {
        "href": "../system-security-plans/CSP_POC_ssp.json"
    },
    "reviewed-controls": {
        "control-selections": [
            {
                "include-controls": [
                    {
                        "control-id": "ms-03",
                        "statement-ids": [
                            "ms-03-smt"
                        ]
                    }
                ]
            }
        ]
    }
}
```


MS-04


```
{
    "uuid": "7a75d646-a3dd-4e33-92c1-53450950a645",
    "metadata": {
```

```
        "title": "Automated Testing Plan for login.gov. It verifies that the system offers guidance to the subscriber, such as a password-strength meter",
        "last-modified": "2024-06-14T10:25:10+00:00",
        "version": "2024-06-14T10:25:10+00:00",
        "oscal-version": "1.1.2"
    },
    "import-ssp": {
        "href": "../system-security-plans/CSP_POC_ssp.json"
    },
    "reviewed-controls": {
        "control-selections": [
            {
                "include-controls": [
                    {
                        "control-id": "ms-04",
                        "statement-ids": [
                            "ms-04-smt"
                        ]
                    }
                ]
            }
        ]
    }
}
```


MS-05


```
{
```

```
    "uuid": "b4704d49-8018-4bdd-a4e9-eb76172cf372",
    "metadata": {
        "title": "Automated Testing Plan for login.gov. It verifies that the system stores memorized secrets in a form that is resistant to offline attacks.",
        "last-modified": "2024-06-14T10:25:10+00:00",
        "version": "2024-06-14T10:25:10+00:00",
        "oscal-version": "1.1.2"
    },
    "import-ssp": {
        "href": "../system-security-plans/CSP_POC_ssp.json"
    },
    "reviewed-controls": {
        "control-selections": [
            {
                "include-controls": [
                    {
                        "control-id": "ms-05",
                        "statement-ids": [
                            "ms-05-smt"
                        ]
                    }
                ]
            }
        ]
    }
}
```

MS-06


```
{
   "uuid": "90c897a2-bf0c-4943-b592-59815c8118f8",
   "metadata": {
      "title": "Automated Testing Plan for login.gov. It verifies that the system has implemented a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber’s account",
      "last-modified": "2024-06-14T10:25:10+00:00",
      "version": "2024-06-14T10:25:10+00:00",
      "oscal-version": "1.1.2"
   },
   "import-ssp": {
      "href": "../system-security-plans/CSP_POC_ssp.json"
   },
   "reviewed-controls": {
      "control-selections": [
         {
            "include-controls": [
               {
                  "control-id": "ms-06",
                  "statement-ids": [
                     "ms-06-smt"
                  ]
               }
            ]
         }
      ]
```

```
  }
}
```


Assessment Results

MS-01


```
{
  "assessment-results": {
    "uuid": "4aa4f301-1189-40a6-8011-3bbd956d3c08",
    "metadata": {
      "title": "Test Result for login.gov.",
      "last-modified": "2024-06-14T10:25:10+00:00",
      "version": "2024-06-14T10:25:10+00:00",
      "oscal-version": "1.1.2"
    },
    "import-ap": {
      "href": "../assessment-plans/ms-01-assessment-plan.json"
    },
    "results": [
      {
        "uuid": "d89f1b4d-b437-4e95-bba8-072457c858ee",
        "title": "confirms passwords are set to the appropriate minimum length",
        "description": "confirms passwords are set to the appropriate minimum length",
        "start": "2024-06-14T10:25:10+00:00",
        "reviewed-controls": {
          "control-selections": [
            {
```

```
            "include-controls": [
                {
                    "control-id": "ms-01"
                }
            ]
        }
    ]
},
"observations": [
    {
        "uuid": "b537dd0f-1214-4f0f-ad3e-33e6f490858e",
        "title": "confirms passwords are set to the appropriate minimum length",
        "description": "confirms passwords are set to the appropriate minimum length",
        "methods": [
            "TEST"
        ],
        "collected": "2024-06-14T10:25:10+00:00"
    }
],
"findings": [
    {
        "uuid": "a2775ec2-618d-4267-8b7c-85cf814305d5",
        "title": "Automated Test Outcome",
        "description": "confirms passwords are set to the appropriate minimum length",
        "target": {
            "type": "statement-id",
```

```
                    "target-id": "ms-01_smt",
                    "status": {
                        "state": "satisfied",
                        "reason": "pass"
                    }
                }
            }
        ]
    }
  ]
}
}
```


MS-02


```
{
   "assessment-results": {
      "uuid": "316b0362-0ebf-420c-8727-34fcd47dc607",
      "metadata": {
         "title": "Test Result for login.gov.",
         "last-modified": "2024-06-14T10:25:10+00:00",
         "version": "2024-06-14T10:25:10+00:00",
         "oscal-version": "1.1.2"
      },
      "import-ap": {
         "href": "../assessment-plans/ms-02-assessment-plan.json"
      },
      "results": [
```

```
{
    "uuid": "d6e32d62-3c64-458d-939e-43826137a26f",
    "title": "confirms that TLS is configured on the server",
    "description": "confirms that TLS is configured on the server",
    "start": "2024-06-14T10:25:10+00:00",
    "reviewed-controls": {
        "control-selections": [
            {
                "include-controls": [
                    {
                        "control-id": "ms-02"
                    }
                ]
            }
        ]
    },
    "observations": [
        {
            "uuid": "c1c364ae-4feb-4106-b88c-ba2d11d8fcba",
            "title": "confirms that TLS is configured on the server",
            "description": "confirms that TLS is configured on the server",
            "methods": [
                "TEST"
            ],
            "collected": "2024-06-14T10:25:10+00:00"
        }
```

```
            ],
            "findings": [
               {
                  "uuid": "1f0be873-0c31-4004-9188-d7dadfba9600",
                  "title": "Automated Test Outcome",
                  "description": "confirms that TLS is configured on the server",
                  "target": {
                     "type": "statement-id",
                     "target-id": "ms-13_smt",
                     "status": {
                        "state": "not-satisfied",
                        "reason": "fail"
                     }
                  }
               }
            ]
         }
      ]
   }
}
```


MS-03


```
{
   "assessment-results": {
      "uuid": "00f706d8-dc08-43d9-ab04-9fe893df4977",
      "metadata": {
```

```
        "title": "Test Result for login.gov.",
        "last-modified": "2024-06-14T10:25:10+00:00",
        "version": "2024-06-14T10:25:10+00:00",
        "oscal-version": "1.1.2"
    },
    "import-ap": {
        "href": "../assessment-plans/ms-03-assessment-plan.json"
    },
    "results": [
        {
            "uuid": "d4f5992a-b4dc-42f4-a852-377e30c5e075",
            "title": "verifies that passwords are compared against a list that contains values known to be commonly-used, expected, or compromised.",
            "description": "verifies that passwords are compared against a list that contains values known to be commonly-used, expected, or compromised.",
            "start": "2024-06-14T10:25:10+00:00",
            "reviewed-controls": {
                "control-selections": [
                    {
                        "include-controls": [
                            {
                                "control-id": "ms-03"
                            }
                        ]
                    }
                ]
            },
```

```
"observations": [
  {
    "uuid": "8839494d-f87e-4f8d-9add-1a9f0f60ceba",
    "title": "verifies that passwords are compared against a list that contains values known to be commonly-used, expected, or compromised.",
    "description": "verifies that passwords are compared against a list that contains values known to be commonly-used, expected, or compromised.",
    "methods": [
      "TEST"
    ],
    "collected": "2024-06-14T10:25:10+00:00"
  }
],
"findings": [
  {
    "uuid": "3e2e1dda-a73a-4b2d-9db7-6c6a20904233",
    "title": "Automated Test Outcome",
    "description": "verifies that passwords are compared against a list that contains values known to be commonly-used, expected, or compromised.",
    "target": {
      "type": "statement-id",
      "target-id": "ms-03_smt",
      "status": {
        "state": "satisfied",
        "reason": "pass"
      }
    }
  }
```

```
            ]
          }
        ]
    }
}
```


MS-04


```
{
    "assessment-results": {
        "uuid": "3947bc1f-7b6b-4d7b-91f1-1d2c6ee83be9",
        "metadata": {
            "title": "Test Result for login.gov.",
            "last-modified": "2024-06-14T10:25:10+00:00",
            "version": "2024-06-14T10:25:10+00:00",
            "oscal-version": "1.1.2"
        },
        "import-ap": {
            "href": "../assessment-plans/ms-04-assessment-plan.json"
        },
        "results": [
            {
                "uuid": "c37e7081-df0c-4877-8b24-1581765824f4",
                "title": "verifies that the system offers guidance to the subscriber, such as a password-strength meter",
                "description": "verifies that the system offers guidance to the subscriber, such as a password-strength meter",
                "start": "2024-06-14T10:25:10+00:00",
```

```
"reviewed-controls": {
    "control-selections": [
        {
            "include-controls": [
                {
                    "control-id": "ms-04"
                }
            ]
        }
    ]
},
"observations": [
    {
        "uuid": "caa20b47-3c3d-4e2a-b481-91c87408c6b9",
        "title": "verifies that the system offers guidance to the subscriber, such as a password-strength meter",
        "description": "verifies that the system offers guidance to the subscriber, such as a password-strength meter",
        "methods": [
            "TEST"
        ],
        "collected": "2024-06-14T10:25:10+00:00"
    }
],
"findings": [
    {
        "uuid": "19cde0b2-b73e-45fe-b167-3bcd8c348dfa",
```

```
                "title": "Automated Test Outcome",
                "description": "verifies that the system offers guidance to the subscriber, such as a password-strength meter",
                "target": {
                    "type": "statement-id",
                    "target-id": "ms-04_smt",
                    "status": {
                        "state": "satisfied",
                        "reason": "pass"
                    }
                }
            }
        ]
    }
  ]
 }
}
```


MS-05


```
{
  "assessment-results": {
    "uuid": "cac08b88-fa2b-42c2-883b-fca150a93c05",
    "metadata": {
      "title": "Test Result for login.gov.",
      "last-modified": "2024-06-14T10:25:10+00:00",
      "version": "2024-06-14T10:25:10+00:00",
      "oscal-version": "1.1.2"
```

```
},
"import-ap": {
    "href": "../assessment-plans/ms-05-assessment-plan.json"
},
"results": [
  {
    "uuid": "4d7d2e21-9439-409c-95ba-a6b6995c925f",
    "title": "verifies that the system stores memorized secrets in a form that is resistant to offline attacks.",
    "description": "verifies that the system stores memorized secrets in a form that is resistant to offline attacks.",
    "start": "2024-06-14T10:25:10+00:00",
    "reviewed-controls": {
      "control-selections": [
        {
          "include-controls": [
            {
              "control-id": "ms-05"
            }
          ]
        }
      ]
    },
    "observations": [
      {
        "uuid": "d317b4e9-a9e1-494b-ad94-3ca8b9b87fe9",
        "title": "verifies that the system stores memorized secrets in a form that is resistant to offline attacks.",
```

```
            "description": "verifies that the system stores memorized secrets in a form that is resistant to offline attacks.",
            "methods": [
              "TEST"
            ],
            "collected": "2024-06-14T10:25:10+00:00"
          }
        ],
        "findings": [
          {
            "uuid": "8396115b-292a-4554-ab49-d497aec930a2",
            "title": "Automated Test Outcome",
            "description": "verifies that the system stores memorized secrets in a form that is resistant to offline attacks.",
            "target": {
              "type": "statement-id",
              "target-id": "ms-05_smt",
              "status": {
                "state": "not-satisfied",
                "reason": "fail"
              }
            }
          }
        ]
      }
    ]
  }
```

}

MS-06

{

"assessment-results": {

"uuid": "b06f37fc-7a21-4b66-a5e6-3f6bca596d72",

"metadata": {

"title": "Test Result for login.gov.",

"last-modified": "2024-06-14T10:25:10+00:00",

"version": "2024-06-14T10:25:10+00:00",

"oscal-version": "1.1.2"

},

"import-ap": {

"href": "../assessment-plans/ms-06-assessment-plan.json"

},

"results": [

{

"uuid": "4a28b9f1-3b04-4ffd-a76e-96226dbb2212",

"title": "verifies that the system has implemented a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber’s account",

"description": "verifies that the system has implemented a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber’s account",

"start": "2024-06-14T10:25:10+00:00",

"reviewed-controls": {

"control-selections": [

{

```
            "include-controls": [
              {
                "control-id": "ms-06"
              }
            ]
          }
        ]
      },
      "observations": [
        {
          "uuid": "dad9c2be-5c03-456a-946e-fec66e835acb",
          "title": "verifies that the system has implemented a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber’s account",
          "description": "verifies that the system has implemented a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber’s account",
          "methods": [
            "TEST"
          ],
          "collected": "2024-06-14T10:25:10+00:00"
        }
      ],
      "findings": [
        {
          "uuid": "235d2195-cfbf-42ae-bc78-bfca0d2029ba",
          "title": "Automated Test Outcome",
```

```
                "description": "verifies that the system has implemented a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber’s account",
                "target": {
                    "type": "statement-id",
                    "target-id": "ms-06_smt",
                    "status": {
                        "state": "satisfied",
                        "reason": "pass"
                    }
                }
            }
        ]
    }
}
```