****

**SSOi Integration Agreement**

**Please validate and provide required\* information.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Application Overview** | | | | |
| IAM SR Number: | | | 1461 | |
| VASI Id: | | | 2103 | |
| Application Name: | | | Content Management System (CMS) for va.gov | |
| **[ACSVC-7289]** User-Friendly Application Name:  *Application name displayed to the user on SSOi screens.* | | | VA.gov CMS | |
| Application Business Owner:  *This person will be copied on all communication regarding SSOi integration milestones.* | | | Erika Washburn | |
| Application Business Owner Email: | | | Erika.Washburn@va.gov | |
| Application POC:  *This is the person IAM will reach out to for the integration.* | | | Eric Oliver | |
| Application POC Email: | | | eric.oliver3@va.gov | |
| Application Technical POC:  *This person will lead your application team in making the changes to integrate with SSOi.* | | | Eric Oliver  Edmund Dunn  Nathan Douglas | |
| Application Technical POC Email: | | | [eric.oliver3@va.gov](mailto:eric.oliver3@va.gov)  [edmund.dunn@va.gov](mailto:edmund.dunn@va.gov)  [nathan.douglas@va.gov](mailto:nathan.douglas@va.gov) | |
| Application Email Group:  *Will receive SSOi notifications (e.g., environment downtime messages). Must contain VA addresses only.* | | | [cms-admin@va.gov](mailto:cms-admin@va.gov) | |
| **Background** | | | | |
| Application Overview: | | | The va.gov Content Management System (CMS) will support the new va.gov (launched Nov 7, 2018); it will manage the content displayed on va.gov and several of its subdomains, and internal stakeholders will be given privileges to edit content.  CMS is requesting integration with IAM SSOi to address the mandate that all internal, user-facing VA applications become two-factor authentication (2FA)-compliant. | |
| Do all of your application users have a VA PIV Card?  If no, explain: | | | Yes | |
| User Population Overview: | | | 1,500 VA employees authorized to edit content displayed on the website | |
| **User Population > Initial Implementation (if applicable)** | | | | |
|  | Time Period: | | January 2019 | |
| Total User Population: | | 50 | |
| Estimated Logins per day: | | 100 | |
| Peak Usage Periods: | | 9 a.m. – 5 p.m. (EST), Monday – Friday | |
| Estimated Logins per hour: | | 10 | |
| **User Population > Full Implementation** | | | | |
|  | Time Period: | | End of February 2019 | |
| Total User Population: | | 1,500 | |
| Estimated Logins per day: | | 200 | |
| Peak Usage Periods: | | 9 a.m. – 5 p.m. (EST), Monday – Friday | |
| Estimated Logins per hour: | | 30 | |
| Continued Expected Growth Rate: | | | 10% / year | |
| **Application Profile [*To be completed by Technical POC*]** | | | | |
| Is the application hosted internally or externally to the VA network? | | | Internally | |
| Unprotected Production URL | | | cms.va.gov | |
| **IAM Environment** | | **Application Environment** | | **Application URL** |
| **[ACSVC-7290]** Production | | Production | | <https://prod.cms.va.gov> |
| **[ACSVC-7291]** Pre-Production | | Pre-Production | | <https://test.staging.cms.va.gov/> (new request)  <https://staging.cms.va.gov> (currently configured) |
| **[ACSVC-7292]** Software Quality Assurance | | Software Quality Assurance | | <https://staging.cms.va.gov> |
| **[ACSVC-7293]** Integrated Development | | Development | | [https://staging.cms.va.gov](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fstaging.cms.va.gov%2F&data=05%7C01%7C%7C9b49a46dbf0441ac23fe08dbae605a9b%7Ce95f1b23abaf45ee821db7ab251ab3bf%7C0%7C0%7C638295501082950000%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=TWXpW%2F4jC%2B3BXDjtpDG1lg7iALf1M6oerKiWyG9tOk0%3D&reserved=0) |

**The following section documents the design and data to be exchanged for this integration.**

|  |  |  |  |
| --- | --- | --- | --- |
| **SSOi Integration Pattern(s)** | | | |
| **[ACSVC-7294]** IdP to SP Federation |  | An SSOi SAML partnership where the SSOi service is the IdP, and the application (typically external to VA) is in the SP role. SSOi uses a previously authenticated session user as the subject for this IdP and generates a **signed and encrypted** new SAML token for the partner application to process. Support for government approved algorithms must be provided **(e.g., signature: rsa-sha256 and encryption: AES256).**  Refer to the [SSOi IdP to SP Federation (SAML) Playbook Page](https://vaww.oed.portal.va.gov/sites/vrm/IAM/playbooks/Pages/SSOi/IdP%20to%20SP%20Federation%20(SAML).aspx) for detailed technical specifications.  For specific traits available to SAML Partners. see the Attribute Statement in the example [SAML Token](https://vaww.oed.portal.va.gov/sites/vrm/IAM/playbooks/Documents/SSOi/Patterns/SSOi%20IDP%20to%20SP%20Sample%20SAML.xml). | |
| **[ACSVC-7326]** **Login Model** | | | |
| ***These are the standard authentication methods IAM SSOi supports.*** See [Appendix B](#B) for the SSOi Central Login Page. | | | |
| PIV authentication [LOA3] | | | |
| VA Active Directory (username/password) [LOA2] | | | |
| Integrated Windows Authentication [LOA2] | | | |
|  | **Yes** | **No** | **Comments** |
| Do your users require a VistA account for application access? |  |  |  |
| **[ACSVC-7295]** **Authentication Traits [*To be confirmed by Technical POC*]** | | | |
| VA default |  | For specific traits available to WebAgent Partners, see [SSOi Authentication Trait Sets](https://vaww.oed.portal.va.gov/sites/vrm/IAM/playbooks/Pages/SSOi/SSOi%20Authentication%20Trait%20Sets.aspx).  For specific traits available to SAML Partners, see the Attribute Statement in the example [SAML Token](https://vaww.oed.portal.va.gov/sites/vrm/IAM/playbooks/Documents/SSOi/Patterns/SSOi%20IDP%20to%20SP%20Sample%20SAML.xml). | |
| VHA (includes ICN, VistAId) |  |
| VBA (includes Corporate Participant ID) |  |
| SAML |  |
| **[ACSVC-7296]** **Timeout** | | | |
| Timeout at SAML partner site must not initiate a login request back to SSOi unless the user is offered both options to either log back in or exit the application. Only available for the IdP to SP Federation integration pattern. | | | |
| **[ACSVC-7297]** **Logout Model** | | | |
| No external logout: Application logout only. No redirect back to SSOi. Only available for the IdP to SP Federation integration pattern. | | | |

**Approval:**

***The application representatives agree to the SSOi integration as defined above and to comply with the requirements detailed in Appendix A. Additional technical specifications are detailed in the*** [***SSOi Playbook***](https://vaww.oed.portal.va.gov/sites/vrm/IAM/playbooks/Pages/SSOi/SSOi.aspx)***.***

**Note:** Once the Integration Agreement is reviewed and finalized, the Integration Agreement will be sent to the Application POC in an email requesting approval.

The application representatives include the following:

 6/8/2023

Erika Washburn, CMS POC Date

**Appendix A: SSOi**

**Background and Reference**

The Identity and Access Management (IAM) Single Sign-On – Internal (SSOi) service is an authentication service specifically designed for controlling access for Department of Veterans Affairs (VA) internal users (employees and contractors) accessing VA applications. This service enhances the user experience by reducing the time associated with multiple log-on and log-off activities that require application-specific identifiers and passwords. The service also enables enriched password management and reduction in help desk support.

**Integration Requirements for IdP to SP Federation**

**Note:** CMS is the consuming application/system referenced in the integration requirements below.

**Functional Requirements for Integrated Application**

1. The consuming application/system shall accept requests through the consuming application/system SSOi uniform resource locator (URL).
2. The consuming application/system shall process the IAM **signed and encrypted** SSOi Security Assertion Markup Language (SAML) Token.
3. The consuming application/system shall authorize the user based on the following SSOi user session attributes in the SAML default Authentication Trait Set.

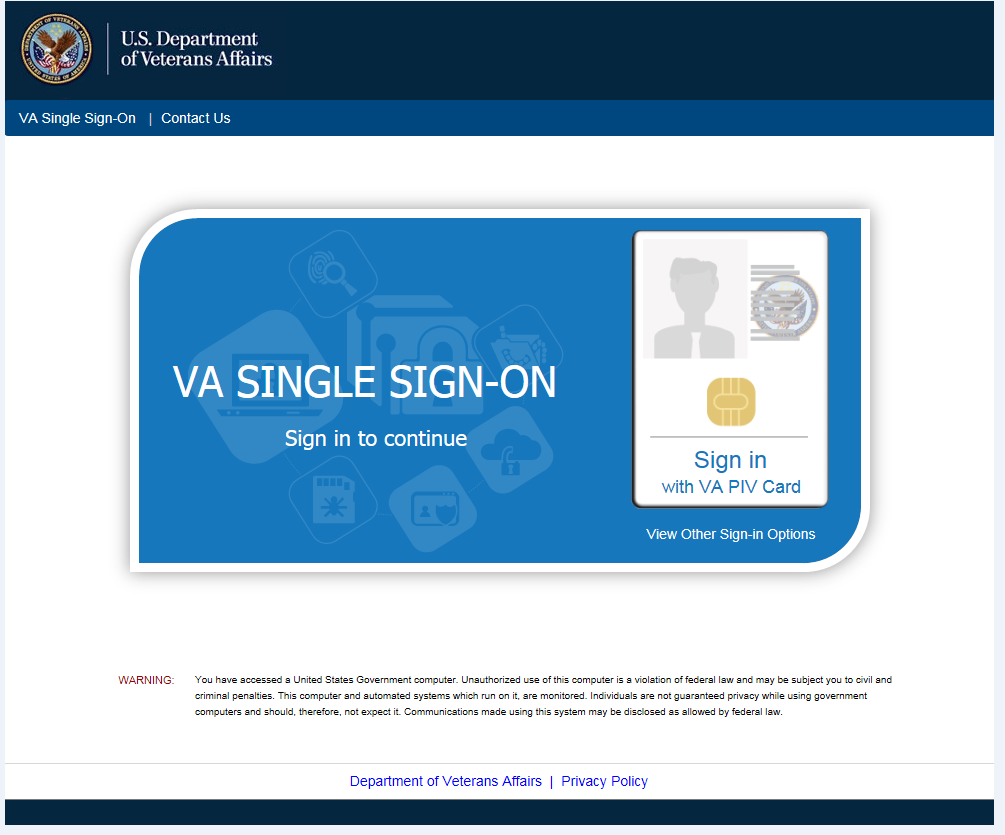
For specific traits available to SAML Partners, see the Attribute Statement in the example [SAML Token](https://vaww.oed.portal.va.gov/sites/vrm/IAM/playbooks/Documents/SSOi/Patterns/SSOi%20IDP%20to%20SP%20Sample%20SAML.xml).

1. When the user initiates the logout, the consuming application/system shall use one of the following options:

* Redirect to an application logout page
* Redirect to the SSOi Logout Page

1. When the user attempts access after the application session has expired, the consuming application/system shall redirect to an application timeout page (this page may include an option to login again via SSOi).

**Appendix B: SSOi Central Login Page**



**Revision History**

The revision history cycle begins once changes or enhancements are requested after the Integration Agreement has been baselined.

| **Date** | **Version** | **Description** | **Author** |
| --- | --- | --- | --- |
| 9/20/2023 | 2.1 | Removed the <https://dev.cms.va.gov> URL and replaced it with <https://staging.cms.va.gov>. | Linda Lotier |
| 6/08/2023 | 2.0 | Added new environment configured against IAM Pre-Prod (ACSVC-6767) | Linda Lotier |
| 6/06/2019 | 1.1 | Added Application Email Group and updated Application Production Environment URL. | Linda Lotier |
| 1/22/2019 | 1.0 | Baselined Integration Agreement | Linda Lotier |

*Place latest revisions at top of table.*