|  |  |  |
| --- | --- | --- |
| watermarkEE FIM  V1.000 Objective Offer RELYING PARTY (RP) E-Enterprise authentication through IOT-approved IDENTITY PROVIDERS (IdPs) using approved configuration management & specifications for availability, performance, lifespan, and security and standard operating procedures Capabilities Trusted Single Factor Authentication to approved Identity Providers with limited attributes. BRIDGE SUPPORT Weekdays 99%  Fri 9PM – Mon 8AM 97%  99.5% < 5 sec | 99.0% < 2 sec  Recovery: 48hrs – Same Location  Disaster Recovery: No | |  | | --- | | E-Enterprise Federated Identity Management[API SPECIFICATIONS](https://e-enterprise.gov/api-specs.docx) | [GETTING STARTED](https://e-enterprise.gov/about) |  VERSION Management[EE-FIM V1.000](https://GITHUB/LOCATION) • Release 01/01/2018 • Renew 01/01/2021 Single Factor OpenId Connect/OAuth2 without Assurance Level or Attribution Support [EE-FIM Vn.000](https://GITHUB/LOCATION) • Release 01/01/2018 • Renew 01/01/2021 Single Factor OpenId Connect/OAuth2 with … Service AssistanceHours • M-F 8am – 6PM EST Except Fed HolidaysCONTACT • 800-890-1995 [helpdesk@epacdx.net](mailto:helpdesk@epacdx.net)EMERGENCY: TBDTechnology REQUIREMENTS Identity Providers – OpenID Connect / OAuth 2.0 Support\*  Relying Parties – OpenID Connect / OAuth 2.0 Support\* Change Management Releases: Fri 9PM-Mon 8AM EST or Holidays as scheduled  Emergency Changes as approved by CM Chairperson or as escalated through Incident Management & Contingency Plans |

### Release Management

#### [EE-FIM V1.001](https://GITHUB/LOCATION) • Release 01/01/2018 • Renew 01/01/2021

Single Factor OpenId Connect/OAuth2 without Assurance Level or Attribution Support

### Supporting Documentation

#### [RULES OF BEHAVIOR](#_RULES_OF_BEHAVIOR) • Release 01/01/2018 • Renew 01/01/2021

Security, Privacy, Non-disclosure requirements for duties tied to systems and contracts

#### [Configuration Management PLAN • Release 01/01/2018 • Renew 01/01/2021](#_Configuration_ManagemenT_PLAN)

Change Management procedures for scheduling, changing, version control, auditing, documentation & publishing in a secure manner.

#### [IdentitY PROVIDER POLICY GUIDE](https://GITHUB/LOCATION) • Release 01/01/2018 • Renew 01/01/2021

Federated Security/Privacy requirements for use of Personally Identifiable Information including white listing content and revisions – Availability?

#### [RELYING PARTY POLICY GUIDE](https://GITHUB/LOCATION) • Release 01/01/2018 • Renew 01/01/2021

Federated Security/Privacy requirements for use of Personally Identifiable Information including white listing content and revisions

#### [SCOPE / CLAIM CRITERIA V1.00\*](https://GITHUB/LOCATION) • Release 01/01/2018 • Renew 01/01/2021

Federated Security/Privacy requirements for use of Personally Identifiable Information including white listing content and revisions

#### [Cost/CONTRACT REQUIREMENTS](https://GITHUB/LOCATION) • N/A • N/A

V1.000 for Federated Identity Management incurs no costs or contract requirements for procurement

#### [Release MANAGEMENT V1.000](https://GITHUB/LOCATION) • Release 01/01/2018 • Renew 01/01/2021

Single Factor OpenId Connect/OAuth2 without Assurance Level or Attribution Support

Do you have specific configuration management requirements for the EE-FIM Federated Bridge?

* Notification/Timing/testing requirements for routine text/configuration changes?
* Notification/Timing/testing requirements for normal changes beyond text/config changes?
* Notification/Timing/testing requirements for significant changes that change content, function, or interface compatibility?
* Security scanning/corrective measures requirements?
* Other?

What level of impact may EE-FIM changes have on availability?

Business Days: %Emergency and low impact text/configuration changes Only?)

Weekends/Holidays % (9PM FRI – MON 8AM – or specify)

On Premises Contingency? Contingency Plan Recovery within nn days/nn:nn hrs

Disaster Recovery N/A or within days/hrs

Do major changes require capacity planning/performance testing?

* Nnnnn user authentications per minute (tested?/estimated?)
* nn% < 5 seconds (tested?/estimated?)
* nn% < 2 seconds (tested?/estimated?)
* % Other – Specify \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

#### [**RULES OF BEHAVIOR**](https://GITHUB/LOCATION) • Release 01/01/2018 • Renew 01/01/2021

Do you have a specific “Rules of Behavior” including:

* “Non-Disclosure Agreements”?
* “Permissible Uses for Sharing Personally Identifiable Information”?
* Security Incident Reporting Procedures?
* Minimum System Security Controls for Identity Providers or Relying Parties?

#### **[Configuration ManagemenT PLAN](https://GITHUB/LOCATION)** • Release 01/01/2018 • Renew 01/01/2021

Change Management procedures for scheduling, changing, version control, auditing, documentation & publishing in a secure manner.

Do you have specific configuration management requirements?

* Notification/Timing/testing requirements for routine text/configuration changes?
* Notification/Timing/testing requirements for normal changes beyond text/config changes?
* Notification/Timing/testing requirements for significant changes that change content, function, or interface compatibility?
* Security scanning/corrective measures requirements?
* Other?

#### [IdentitY PROVIDER POLICY GUIDE](https://GITHUB/LOCATION) • Release 01/01/2018 • Renew 01/01/2021

Do you wish to interoperate as an Identity Provider on the E-Enterprise Bridge?

Does your IdP offer a Privacy Policy? Specify Link? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

What Personally Identifying Information (PII) do you collect?

What are the permissible uses of your shared PII?

What PII would you allow/offer for permissible uses to external applications/relying parties?

What PII do you disallow sharing with external applications/relying parties?

Would you allow “White Listing” – allow your IdP users to selectively authorize shared access to PII (referred to as Scopes/Claims) with other E-Enterprise Relying Parties/Identity Providers with the option to return and revoke white list access?

What level of availability does your Identity Provider solution offer?\*

Business Days: %

Weekends/Holidays % (9PM FRI – MON 8AM – or specify)

On Premises Recovery within days/hrs

Disaster Recovery within days/hrs

What level of service does your service support?\*

* Nnnnn user authentications per minute (tested?/estimated?)
* nn% < 5 seconds (tested?/estimated?)
* nn% < 2 seconds (tested?/estimated?)
* % Other – Specify \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\*Note: Relying Parties must consider adding all performance and availability impacts for local, EE-FIM Bridge and IdP Performance together

SCOPES

|  |  |  |  |
| --- | --- | --- | --- |
| openid | Standard | y | requests access to a claim that uniquely identifies the user; informs the Authorization Server that the Client is making an OpenID Connect request |
| profile | Standard | n | requests access to default profile claims |
| email | Standard | n | requests access to email and email\_verified claims |
| address | Standard | n | requests access to address claim |
| phone | Standard | n | requests access to phone\_number and phone\_number\_verified claims |
| offline\_  access | Standard | n | requests that an OAuth 2.0 Refresh Token be issued that can be used to obtain an Access Token that grants access to the End-User's UserInfo Endpoint even when the End-User is not present (not logged in) |
| params | Proposed | n | requests access to additional information not captured in the standardized scopes above |
| assurance | Proposed | n | requests access to the values assurance level (IAL, AAL, and FAL) claims |
| idp\_meta- data | Proposed | n | requests access to additional metadata provided by IdP |

CLAIMS

|  |  |  |
| --- | --- | --- |
| **OpenID Claim** | **source** | **notes** |
| sub | idp | See description of these fields at the following URL: |

OpenID Claims

<https://openid.net/specs/openid-connect-core-1_0.html#StandardClaims>

Profile Claims

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **profile\_claim** | | **source** | | | **notes** |
| name | | idp | | | See description of these fields at the following URL: <https://openid.net/specs/openid-connect-core-1_0.html#StandardClaims> |
| family\_name | | idp | | |
| given\_name | | idp | | |
| middle\_name | | idp | | |
| nickname | | idp | | |
| preferred\_username | | idp | |  | |
| profile | | idp | |
| picture | | idp | |
| website | | idp | |
| gender | | idp | |
| birthdate | | idp | |
| zoneinfo | | idp | |
| locale | | idp | |
| updated\_at | | idp | |