

# Fast Fed

A new standard to simplify SSO adoption

# The Problem

Low adoption of federation in enterprise settings

## Why?

It's hard to configure.

## Amazon Web Services cloud application

You must be signed in as a [super administrator](#) for this task.

Using Security Assertion Markup Language (SAML), your users can use their Google Cloud credentials to sign in to enterprise-cloud applications.

### Set up SSO via SAML for Amazon Web Services

Here's how to set up single sign-on (SSO) via SAML for the Amazon Web Services® application.

#### Step 1: Set up Amazon Web Services as a SAML 2.0 service provider (SP)

1. [Sign in](#) to your [Google Admin console](#).  
Sign in using an *administrator account*, not your current account `darinmcadams@gmail.com`
2. From the Admin console Home page, go to **Apps** > **SAML Apps**.  
To see Apps on the Home page, you might have to click **More controls** at the bottom.
3. Click the **Download** button to download the Google IdP metadata and the X.509 Certificate.
4. In a new browser tab, log in to the AWS Management Console and open the IAM console at <https://console.aws.amazon.com/iam/>.
5. In the navigation pane, select **identity providers** and then click **Create SAML Provider**.
6. Select **SAML** as the **Provider Type**, and give it a name such as **GoogleApps**.
7. Upload the IDP metadata you saved earlier from the Google Admin console SAML settings.
8. Click **Next Step** and on the following page, click **Create**.
9. Click the **Roles** tab on the left sidebar and click **Create a New Role** to create a role which will define the permissions.
10. Select **Set role name**. This name will be displayed next to the login name on the AWS console.
11. Select **Role for Identity Provider Access**.
12. Select **Grant Web Single Sign-On (WebSSO) access to SAML providers**. Click **Next Step**.
13. Leave the **Establish trust** settings as they are. Click **Next Step**.
14. Use the **Attach policy** settings to define the policies your Federated Users will have. Click **Next Step**.
15. On the following page, review your settings, then click **Create the Role**.
16. Select your Google service from the identity providers list and note the Provider ARN. This contains your **AWS Account ID** and the name of the provider (example: `arn:aws:iam::ACCOUNT_NUMBER:saml-provider/GoogleApps`).
17. Click **Save** to save the Federated Web single sign-on configuration details.

#### Step 2: Set up Google as a SAML identity provider (IdP)

1. In a new browser tab, [Sign in](#) to your [Google Admin console](#).  
Sign in using an *administrator account*, not your current account `darinmcadams@gmail.com`
2. From the Admin console Home page, go to **Apps** > **SAML Apps**.  
To see Apps on the Home page, you might have to click **More controls** at the bottom.
3. Click **Google IDP**.
4. Select **Info**.
5. The

44 STEPS

You can copy the **Entity ID** and the **Single Sign-On URL** field values and download the **X.509 Certificate**, paste them into the appropriate service provider Setup fields, and then click **Next** or  
You can download the IDP metadata, upload it into the appropriate service provider Setup fields, and then come back to the Admin console and click **Next**.

6. In the **Basic application information** window, the **Application name** and **Description** values automatically populate.
7. Click **Next**.

#### Step 3: Enter the Amazon Web Services specific service provider details in Google Admin console


1. In the **Service Provider Details** section, enter the following into the **Entity ID**, **ACS URL**, and **Start URL** fields:  
ACS URL: `https://signin.aws.amazon.com/saml`  
Entity ID: `https://signin.aws.amazon.com/saml`  
Start URL: `<Empty>`
2. Leave **Signed Response** unchecked.  
When the **Signed Response** checkbox is unchecked, only the assertion is signed. When the **Signed Response** checkbox is checked, the entire response is signed.
3. The default **Name ID** is the primary email. Multi-value input is not supported. You can change the Name ID mapping as per your requirement. Custom attributes of the user schema can also be used after creating them via [Google Admin SDK APIs](#). The custom attributes for the user schema need to be created prior to setting up the Amazon Web Services SAML application.
4. Click **Next**.
5. Click **Add new mapping** and map the attribute value `"https://aws.amazon.com/SAML/Attributes/RoleSessionName"` to **Basic Information** > **Primary Email** and the attribute value `"https://aws.amazon.com/SAML/Attributes/Role"` to a **custom attribute** corresponding to the Amazon Web Services account.
6. In the drop-down list, first select the **Category** and then choose a **User attribute** to map the attribute from the Google profile.
7. Click **Finish**.

#### Step 4: Enable the Amazon Web Services app

1. [Sign in](#) to your [Google Admin console](#).  
Sign in using an *administrator account*, not your current account `darinmcadams@gmail.com`
2. From the Admin console Home page, go to **Security**.  
To see **Security**, you might have to click **More controls** at the bottom.
3. Select **Amazon Web Services**.
4. At the top right of the gray box, click **Edit Service**.
5. To apply settings to all organizations, click **On for everyone**, then click **Save**.
6. To apply settings to individual organizational units, click **On for selected units**.
  - At the left, select the organizational unit that contains the users you want to change.
  - To change the setting, select **On** or **Off**.
  - To keep the setting the same, even if the parent setting is **Overridden**, select **Inherit—Reverts to the same setting as its parent**.
  - Click **Save**—Saves your new setting (even if the parent setting is **Overridden**).
- Learn more about the [organizational structure](#).
7. Ensure that your Amazon Web Services user account is signed in to your Google domain.

#### Step 5: Verify that SSO is working between G Suite and Amazon Web Services (only)

**Note:** Make sure you're still signed in to the account where you set up Amazon Web Services.

1. Open a G Suite core service, such as Google Calendar.
2. At the top right, click the App Launcher .
3. Scroll to the apps section and click **Amazon Web Services**.
4. If you are signed in to more than one account, select the account where Amazon Web Services is configured.
5. If you configured more than one role, select a role from the list.
6. Click **Sign In**.

You are signed in to Amazon Web Services.

# Lots of Pain

## **System Administrator**

Budget 1-2 weeks to configure SSO to each application

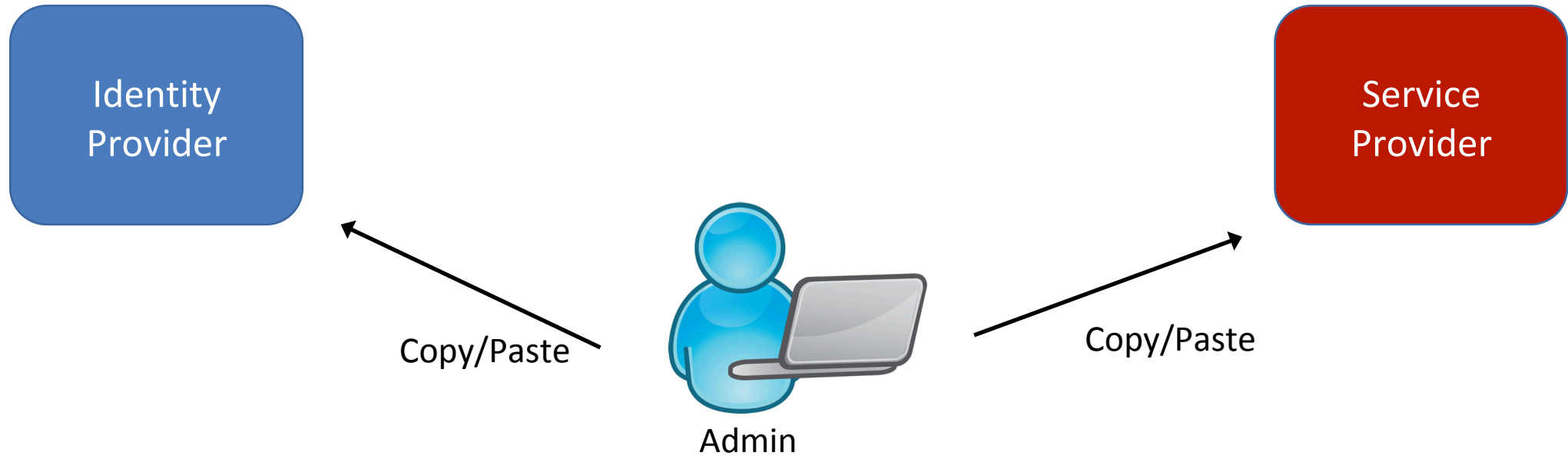
## **Identity Providers**

Each app is different. Custom integration & documentation.

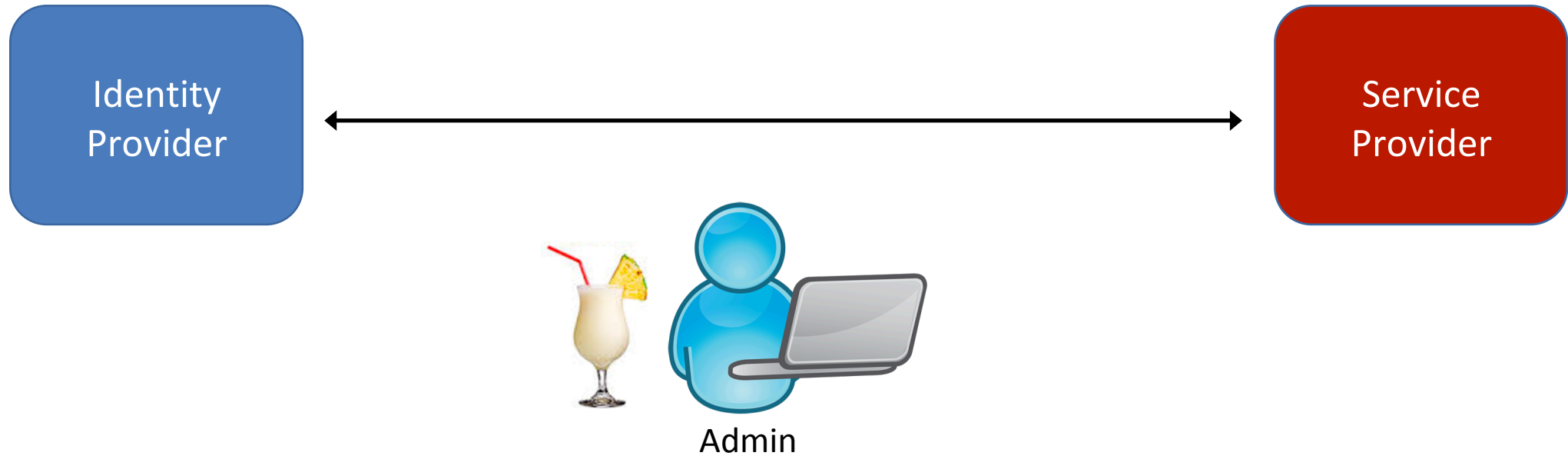
## **Service Providers**

Getting into Identity Provider catalogs. Not self-service.  
What should I be doing!?

# Today's Registration Experience



# Desired Registration Experience



# Learn More

<https://www.youtube.com/watch?v=ucQl5p6sa4A>

The image shows a YouTube video player interface. At the top, there is a navigation bar with the YouTube logo and a search bar. The video content area displays a presentation slide with the title "FASTFED - A NEW STANDARD TO SIMPLIFY SSO ADOPTION" and the names "DARIN MCADAMS, ERIK GUSTAVSON" and the date "JUNE 25, 2019". The slide also features the Identiverse logo and a "CELEBRATING 10 YEARS ANNIVERSARY" badge. Below the video player, the video title "FastFed - A new standard to make SSO easy - June 25 | Identiverse 2019" is displayed, along with the view count "668 views • Aug 16, 2019" and interaction buttons for likes, comments, shares, and saves.

YouTube

Search

FASTFED - A NEW STANDARD TO SIMPLIFY SSO ADOPTION  
DARIN MCADAMS, ERIK GUSTAVSON  
JUNE 25, 2019

identiverse

FAST FED  
A NEW STANDARD TO SIMPLIFY SSO ADOPTION

Erik Gustavson, Engineering Manager, Google  
Darin McAdams, Principal Engineer, AWS

identiverse  
WASHINGTON D.C. 2019

0:01 / 22:09

FastFed - A new standard to make SSO easy - June 25 | Identiverse 2019

668 views • Aug 16, 2019

8 0 SHARE SAVE ...

# Learn More

<https://bitbucket.org/openid/fastfed/src/master/>

The screenshot shows the Bitbucket web interface for the 'fastfed' repository. On the left is a dark blue sidebar with navigation icons and labels. The main content area on the right shows the repository's file structure and a table of recent commits.

**fastfed**

OpenID Foundation / Untitled project

**fastfed** Clone

master

/

Name	Size	Last commit	Message
discussion_artifacts		2019-02-11	Incorporates latest round of feedba...
html_spec		2020-10-07	Update document revision date
license		2019-08-28	Add txt version of license
scenarios		2020-03-08	New SCIM interop profile. Desired_...
text_spec		2020-10-07	Update document revision date
xml_spec		2020-10-07	Update document revision date
README.md	631 B	2017-10-17	README.md created online with Bit...



## 2 Common FAQs

## 2 Common FAQs

**Question:** Does this replace SAML, OIDC, or SCIM?

## 2 Common FAQs

**Question:** Does this replace SAML, OIDC, or SCIM?

*No. It tackles the “44 steps” to setup these technologies.*

## 2 Common FAQs

**Question:** Does this replace SAML, OIDC, or SCIM?

*No. It tackles the “44 steps” to setup these technologies.  
Also, subsets of each to implement.*

## 2 Common FAQs

**Question:** Does this replace SAML, OIDC, or SCIM?

*No. It tackles the “44 steps” to setup these technologies.  
Also, subsets of each to implement.*

**Question:** What's the difference between FastFed and OpenID Federation?

## 2 Common FAQs

**Question:** Does this replace SAML, OIDC, or SCIM?

*No. It tackles the “44 steps” to setup these technologies.  
Also, subsets of each to implement.*

**Question:** What’s the difference between FastFed and OpenID Federation?

*Solving different problems, but complementary.*

# Current Status

# Current Status

We're building!

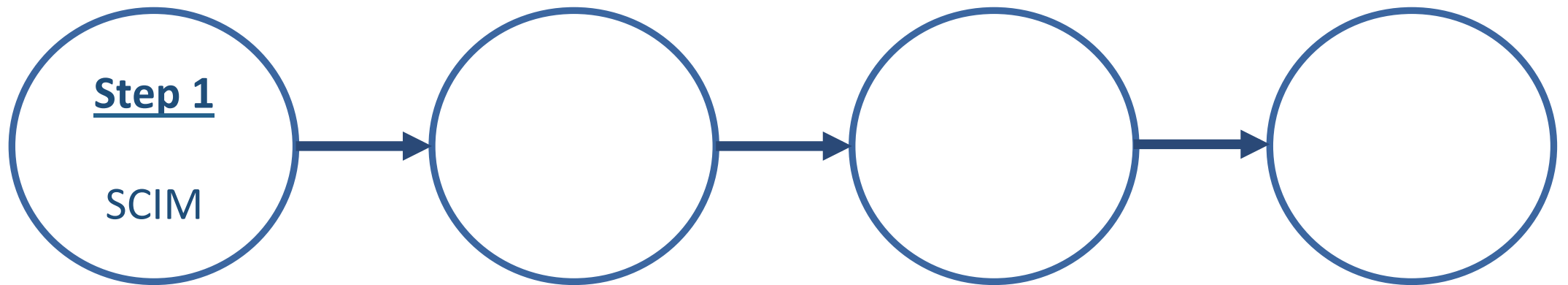
Iteratively, not big bang.



# Current Status

We're building!

Iteratively, not big bang.



# FastFed Enterprise SCIM Profile 1.0 - draft 03

fastfed-scim-1\_0

## Abstract

This specification defines the requirements to implement the FastFed Profile for SCIM 2.0 Enterprise provisioning. This profile supports continual provisioning, update, and deprovisioning of end-users between the Identity Provider and Application Provider.

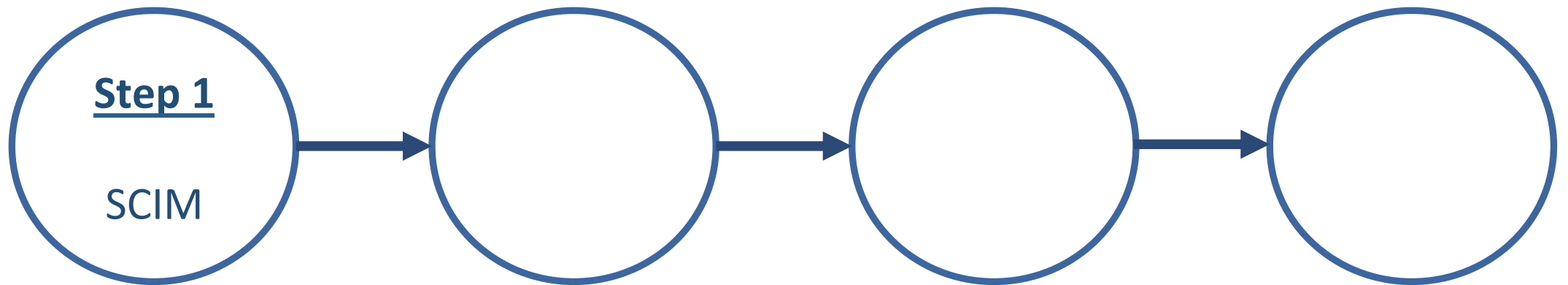
## Table of Contents

- 1. **Introduction**
  - 1.1. **Requirements Notation and Conventions**
  - 1.2. **Terminology**
- 2. **Overview**
  - 2.1. **Roles and Responsibilities**
  - 2.2. **Client Authentication**
- 3. **Protocol Extensions**
  - 3.1. **FastFed Metadata**
    - 3.1.1. **Provisioning Profile URN**
    - 3.1.2. **Application Metadata**
  - 3.2. **FastFed Handshake**
    - 3.2.1. **FastFed Registration Request**
      - 3.2.1.1. **Usage of the OAuth-2.0 JWT Profile**
    - 3.2.2. **FastFed Registration Response**
      - 3.2.2.1. **Usage of the OAuth-2.0 JWT Profile**
- 4. **Interoperability Requirements**
  - 4.1. **General Requirements**
  - 4.2. **User Provisioning**
    - 4.2.1. **Create User**
    - 4.2.2. **Update User**
    - 4.2.3. **Deactivate or Reactivate User**
    - 4.2.4. **Delete User**
    - 4.2.5. **Get User By Id**
    - 4.2.6. **List Users By Alternate Identifier**
  - 4.3. **Group Provisioning**
    - 4.3.1. **Create Group**
    - 4.3.2. **Update Group Metadata**
    - 4.3.3. **Deactivate Group**
    - 4.3.4. **Delete Group**

# Current Status

We're building!

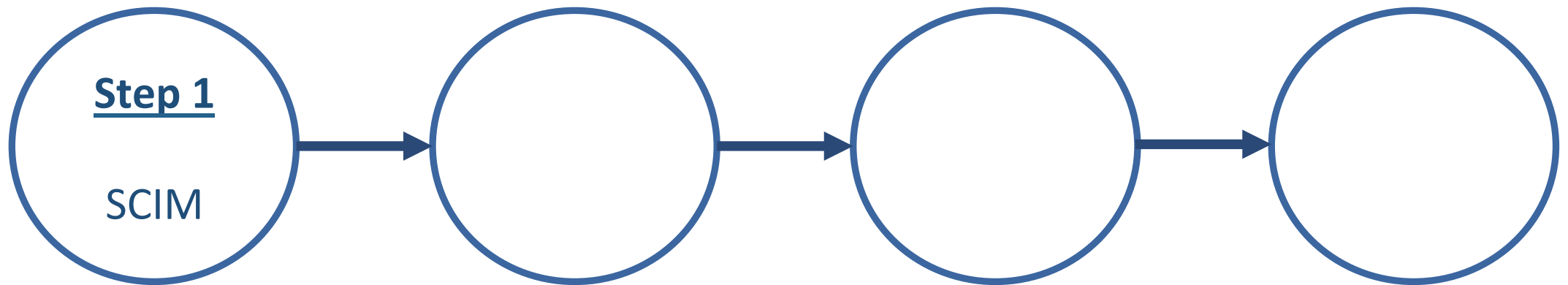
Iteratively, not big bang.



# Current Status

We're building!

Iteratively, not big bang.

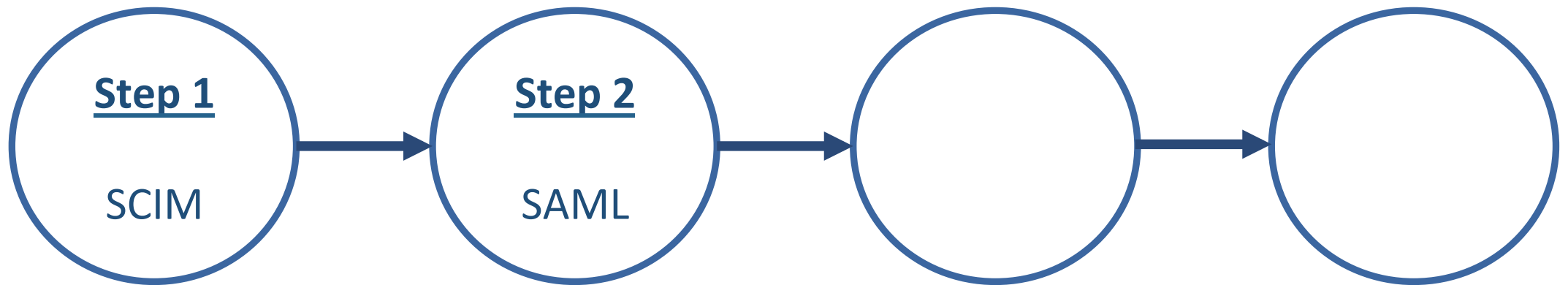


AWS  
Azure  
Okta  
OneLogin  
PingOne

# Current Status

We're building!

Iteratively, not big bang.

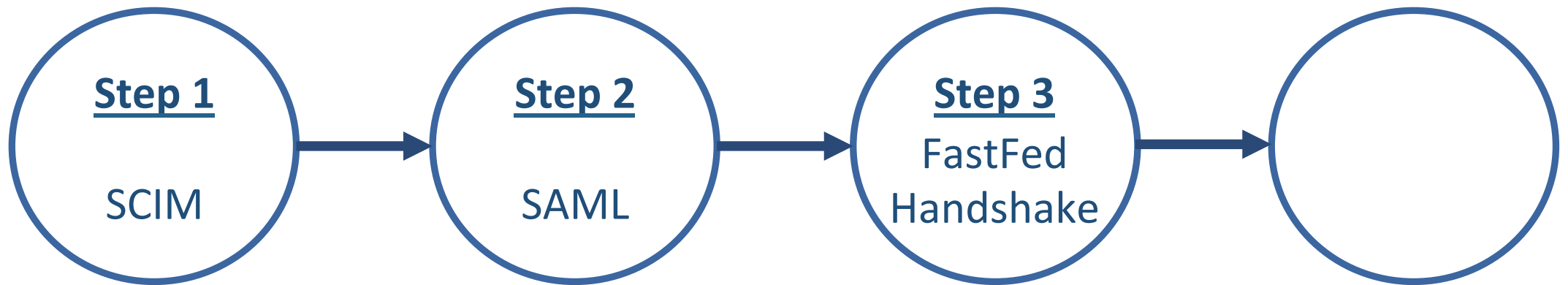


AWS  
Azure  
Okta  
OneLogin  
PingOne

# Current Status

We're building!

Iteratively, not big bang.

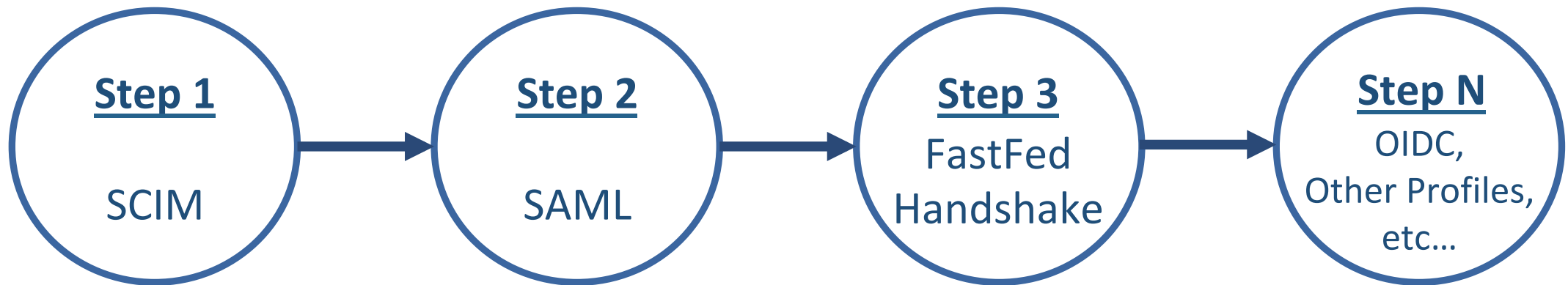


AWS  
Azure  
Okta  
OneLogin  
PingOne

# Current Status

We're building!

Iteratively, not big bang.




AWS  
Azure  
Okta  
OneLogin  
PingOne

# Open Source



fastfed4j

# Open Source



Why GitHub? ▾TeamEnterpriseExplore ▾MarketplacePricing ▾

Search

/



Sign in

Sign up

fastfed4j / fastfed4j

Watch 1Star 0Fork 1

<> CodeIssuesPull requests 1ActionsProjectsSecurityInsights



### Join GitHub today

GitHub is home to over 50 million developers working together to host and review code, manage projects, and build software together.


Sign up

Dismiss

master ▾2 branches0 tags

Go to file

Code ▾

**Darin McAdams** Added test suite for ContractChange, plus ... 350b59f 25 days ago 7 commits

src	Added test suite for ContractChange, plus associated b...	25 days ago
.gitignore	Initial commit	3 months ago
LICENSE	Initial commit	3 months ago
README.md	Initial commit	3 months ago
pom.xml	Adds toJson() methods, plus general code cleanup	2 months ago

### About

Implementation of OpenID FastFed specification in Java

Readme

Apache-2.0 License

### Releases

No releases published

# Open Source

## fastfed4j

~80% Complete  
12K lines of code (so far)

The screenshot shows the GitHub repository page for `fastfed4j`. The repository is owned by `fastfed4j` and has 1 watch, 0 stars, and 1 fork. The repository is currently on the `master` branch, with 2 branches and 0 tags. The repository description is "Implementation of OpenID FastFed specification in Java". The repository is licensed under the Apache-2.0 License. The repository has 7 commits, with the most recent commit by Darin McAdams adding a test suite for `ContractChange`, plus associated files, 25 days ago. The repository contains the following files:

File	Commit Message	Commit Date
<code>src</code>	Added test suite for <code>ContractChange</code> , plus associated b...	25 days ago
<code>.gitignore</code>	Initial commit	3 months ago
<code>LICENSE</code>	Initial commit	3 months ago
<code>README.md</code>	Initial commit	3 months ago
<code>pom.xml</code>	Adds <code>toJson()</code> methods, plus general code cleanup	2 months ago

The repository page also features a "Join GitHub today" banner, a "Sign up" button, and a "Dismiss" button. The repository is also featured in the "About" section, which includes a "Readme" link and a link to the "Apache-2.0 License". The "Releases" section shows that no releases have been published.

# Spec Status

Implementors Draft?

# Spec Status

~~Implementors Draft?~~

Draft

# Spec Status

Called for Implementors Draft earlier this year

# Spec Status

Called for Implementors Draft earlier this year

8 objections

# Spec Structure

## FastFed Core 1.0 - draft 02

fastfed-core-1\_0

### Abstract

FastFed simplifies the administrative effort to configure identity federation between an identity provider and a hosted application. The specification defines metadata documents, APIs, and flows to enable an administrator to quickly connect two providers that support common standards such as OpenID Connect, SAML, and SCIM, and allows configuration changes to be communicated directly between the identity provider and hosted application on a recurring basis.

### Table of Contents

- 1. **Introduction**
  - 1.1. **Requirements Notation and Conventions**
  - 1.2. **Terminology**
- 2. **Overview**
  - 2.1. **Metadata**
  - 2.2. **Endpoints**
  - 2.3. **Endpoint Discovery**
  - 2.4. **FastFed Handshake**
  - 2.5. **User Schemas and Provisioning**
    - 2.5.1. **Schema Selection**
    - 2.5.2. **Attribute Filtering**
- 3. **Metadata**
  - 3.1. **Metadata Serialization**
  - 3.2. **Metadata Languages and Scripts**
  - 3.3. **Provider Metadata**
    - 3.3.1. **Capabilities**

# Spec Structure

## FastFed Core 1.0 - draft 02

fastfed-core-1\_0

### Abstract

FastFed simplifies the administrative effort of an identity provider and a hosted application. The specification enables an administrator to quickly connect an application to OpenID Connect, SAML, and SCIM, and allows for interoperability between the identity provider and hosted application.

### Table of Contents

- 1. Introduction
  - 1.1. Requirements Notation and Conventions
  - 1.2. Terminology
- 2. Overview
  - 2.1. Metadata
  - 2.2. Endpoints
  - 2.3. Endpoint Discovery
  - 2.4. FastFed Handshake
  - 2.5. User Schemas and Provisioning
    - 2.5.1. Schema Selection
    - 2.5.2. Attribute Filtering
- 3. Metadata
  - 3.1. Metadata Serialization
  - 3.2. Metadata Languages and Scripts
  - 3.3. Provider Metadata
    - 3.3.1. Capabilities

## FastFed Basic SCIM Profile 1.0 - draft 02

fastfed-scim-1\_0

### Abstract

This specification defines the requirements to implement the FastFed Profile for SCIM 2.0 Basic provisioning. This profile supports continual provisioning, update, and deprovisioning of end-users between the Identity Provider and Application Provider.

### Table of Contents

- 1. Introduction
  - 1.1. Requirements Notation and Conventions
  - 1.2. Terminology
- 2. Overview
  - 2.1. Roles and Responsibilities
  - 2.2. Client Authentication
- 3. Protocol Extensions
  - 3.1. FastFed Metadata
    - 3.1.1. Provisioning Profile URN
    - 3.1.2. Application Metadata
  - 3.2. FastFed Handshake
    - 3.2.1. FastFed Registration Request
      - 3.2.1.1. Usage of the OAuth-2.0 JWT Profile
    - 3.2.2. FastFed Registration Response
      - 3.2.2.1. Usage of the OAuth-2.0 JWT Profile
- 4. Interoperability Requirements
  - 4.1. General Requirements



# Spec Structure

## FastFed Core 1.0 - draft 02

fastfed-core-1\_0

### Abstract

FastFed simplifies the administrative effort of an identity provider and a hosted application. The specification enables an administrator to quickly connect an application to OpenID Connect, SAML, and SCIM, and allows for interoperability between the identity provider and hosted application.

### Table of Contents

- 1. Introduction
  - 1.1. Requirements Notation and Conventions
  - 1.2. Terminology
- 2. Overview
  - 2.1. Metadata
  - 2.2. Endpoints
  - 2.3. Endpoint Discovery
  - 2.4. FastFed Handshake
  - 2.5. User Schemas and Provisioning
    - 2.5.1. Schema Selection
    - 2.5.2. Attribute Filtering
- 3. Metadata
  - 3.1. Metadata Serialization
  - 3.2. Metadata Languages and Scripts
  - 3.3. Provider Metadata
    - 3.3.1. Capabilities

## FastFed Basic SCIM Profile 1.0 - draft 02

fastfed-scim-1\_0

### Abstract

This specification defines the requirements to implement the FastFed Basic SCIM Profile. This profile supports continual provisioning, up to the Identity Provider and Application Provider.

### Table of Contents

- 1. Introduction
  - 1.1. Requirements Notation and Conventions
  - 1.2. Terminology
- 2. Overview
  - 2.1. Roles and Responsibilities
  - 2.2. Client Authentication
- 3. Protocol Extensions
  - 3.1. FastFed Metadata
    - 3.1.1. Provisioning Profile URN
    - 3.1.2. Application Metadata
  - 3.2. FastFed Handshake
    - 3.2.1. FastFed Registration Request
      - 3.2.1.1. Usage of the OAuth-2.0 JWT Profile
    - 3.2.2. FastFed Registration Response
      - 3.2.2.1. Usage of the OAuth-2.0 JWT Profile
- 4. Interoperability Requirements
  - 4.1. General Requirements

## FastFed Basic SAML Profile 1.0 - draft 02

fastfed-saml-1\_0

### Abstract

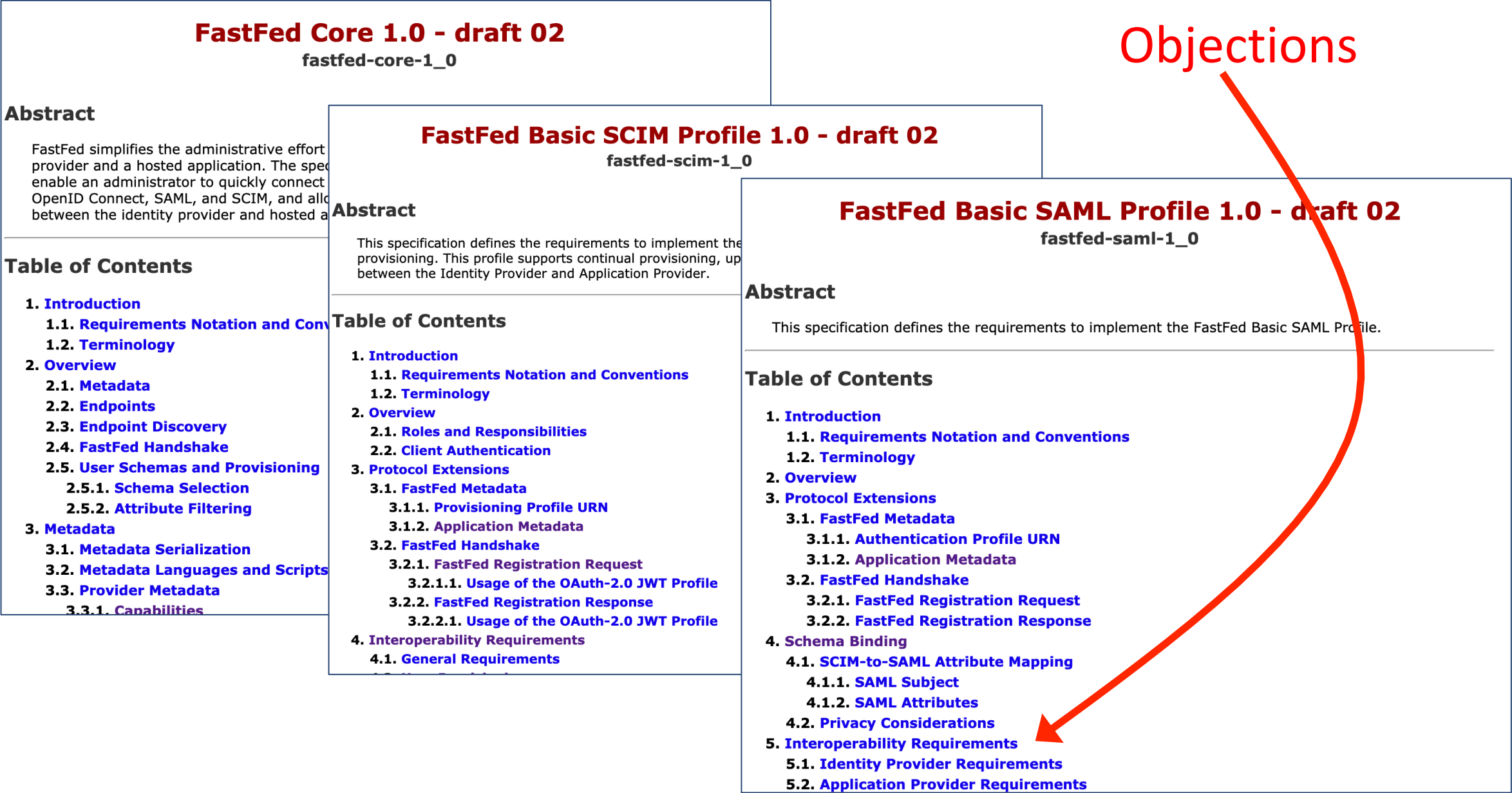
This specification defines the requirements to implement the FastFed Basic SAML Profile.

### Table of Contents

- 1. Introduction
  - 1.1. Requirements Notation and Conventions
  - 1.2. Terminology
- 2. Overview
- 3. Protocol Extensions
  - 3.1. FastFed Metadata
    - 3.1.1. Authentication Profile URN
    - 3.1.2. Application Metadata
  - 3.2. FastFed Handshake
    - 3.2.1. FastFed Registration Request
    - 3.2.2. FastFed Registration Response
- 4. Schema Binding
  - 4.1. SCIM-to-SAML Attribute Mapping
    - 4.1.1. SAML Subject
    - 4.1.2. SAML Attributes
  - 4.2. Privacy Considerations
- 5. Interoperability Requirements
  - 5.1. Identity Provider Requirements
  - 5.2. Application Provider Requirements

# Spec Structure

Objections



# Naming Confusion

## **FastFed Basic SAML Profile 1.0 - draft 02**

**fastfed-saml-1\_0**

### **Abstract**

This specification defines the requirements to implement the FastFed Basic SAML Profile.

### **Table of Contents**

- 1. Introduction**
  - 1.1. Requirements Notation and Conventions**
  - 1.2. Terminology**
- 2. Overview**
- 3. Protocol Extensions**
  - 3.1. FastFed Metadata**
    - 3.1.1. Authentication Profile URN**
    - 3.1.2. Application Metadata**
  - 3.2. FastFed Handshake**
    - 3.2.1. FastFed Registration Request**
    - 3.2.2. FastFed Registration Response**
- 4. Schema Binding**
  - 4.1. SCIM-to-SAML Attribute Mapping**
    - 4.1.1. SAML Subject**
    - 4.1.2. SAML Attributes**
  - 4.2. Privacy Considerations**
- 5. Interoperability Requirements**
  - 5.1. Identity Provider Requirements**
  - 5.2. Application Provider Requirements**

Confusing

# Naming Confusion

## FastFed Basic SAML Profile 1.0 - draft 02

fastfed-saml-1\_0

### Abstract

This specification defines the requirements to implement the FastFed Basic SAML Profile.

### Table of Contents

- 1. Introduction
  - 1.1. Requirements Notation and Conventions
  - 1.2. Terminology
- 2. Overview
- 3. Protocol Extensions
  - 3.1. FastFed Metadata
    - 3.1.1. Authentication Profile URN
    - 3.1.2. Application Metadata
  - 3.2. FastFed Handshake
    - 3.2.1. FastFed Registration Request
    - 3.2.2. FastFed Registration Response
- 4. Schema Binding
  - 4.1. SCIM-to-SAML Attribute Mapping
    - 4.1.1. SAML Subject
    - 4.1.2. SAML Attributes
  - 4.2. Privacy Considerations
- 5. Interoperability Requirements
  - 5.1. Identity Provider Requirements
  - 5.2. Application Provider Requirements

Confusing

# Naming Confusion

## FastFed Basic SAML Profile 1.0 - draft 02

fastfed-saml-1\_0

### Abstract

This specification defines the requirements to implement the FastFed Basic SAML Profile.

### Table of Contents

- 1. Introduction
  - 1.1. Requirements Notation and Conventions
  - 1.2. Terminology
- 2. Overview
- 3. Protocol Extensions
  - 3.1. FastFed Metadata
    - 3.1.1. Authentication Profile URN
    - 3.1.2. Application Metadata
  - 3.2. FastFed Handshake
    - 3.2.1. FastFed Registration Request
    - 3.2.2. FastFed Registration Response
- 4. Schema Binding
  - 4.1. SCIM-to-SAML Attribute Mapping
    - 4.1.1. SAML Subject
    - 4.1.2. SAML Attributes
  - 4.2. Privacy Considerations
- 5. Interoperability Requirements
  - 5.1. Identity Provider Requirements
  - 5.2. Application Provider Requirements

## FastFed Enterprise SAML Profile 1.0 - draft 03

fastfed-saml-1\_0

### Abstract

This specification defines the requirements to implement the FastFed Enterprise SAML Profile.

### Table of Contents

- 1. Introduction
  - 1.1. Requirements Notation and Conventions
  - 1.2. Terminology
- 2. Overview
- 3. Protocol Extensions
  - 3.1. FastFed Metadata
    - 3.1.1. Authentication Profile URN
    - 3.1.2. Application Metadata
  - 3.2. FastFed Handshake
    - 3.2.1. FastFed Registration Request
    - 3.2.2. FastFed Registration Response
- 4. Schema Binding
  - 4.1. SCIM-to-SAML Attribute Mapping
    - 4.1.1. SAML Subject
    - 4.1.2. SAML Attributes
  - 4.2. Privacy Considerations
- 5. Interoperability Requirements
  - 5.1. Identity Provider Requirements
  - 5.2. Application Provider Requirements

# SAML Subject

# SAML Subject

## **BEFORE**

“MUST be the username”

# SAML Subject

## BEFORE

“MUST be the username”

## NOW

Configurable



App chooses 1 of N options

Guidance on choosing

SCIM Attribute	SAML NameID Format
externalId	urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
userName	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
emails[primary eq true].value	urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress

As a reference to implementors, the following considerations can be taken into account when choosing a SAML subject:

- The format of `externalId` is defined in section 3.1 of the SCIM Core specification [\[RFC7643\]](#). It is a persistent identifier, often a GUID, which is intended to reliably identify a user within the Identity Provider. However, it will vary between Identity Providers. Therefore, if an Application anticipates that Administrators may occasionally switch Identity Providers (as can happen in commercial settings, for example), additional matching rules may be necessary to reconcile provisioning events arriving from different sources.

Note that while the SCIM Core specification defines the `externalId` as optional, this profile requires Identity Providers to support it, and hence Applications can depend upon it being available.

- The format of `userName` is defined in section 4.1.1 of the SCIM Core specification [\[RFC7643\]](#). It is a displayable, user-friendly identifier for a user. In practice, the `userName` can often be an email, but other formats occur. No assumptions should be made about the format of the `userName` other than it being a string that the end-user typically enters as a login when authenticating.

If the Administrator switches Identity Providers, it is usually the case that the `userName` remains consistent across providers, making it easier to correlate authentication and provisioning events to a single user when events are arriving from different sources.

Note that `userName` is mutable, meaning an end-user can change their `userName`. In addition `userName` can be recycled and reassigned to other end-users. Therefore, Applications should consider how such situations will be handled. The ability to be notified when `userName` is changed or recycled, such as via the SCIM profile [\[FastFedProfile.EnterpriseSCIM\]](#), can help keep an Application Provider up-to-date with changes.

- The attribute "`emails[primary eq true].value`" represents the primary email address of the user, where `emails` is defined in section 4.1.2 of the SCIM Core specification [\[RFC7643\]](#).

If an end-user does not have a value for email defined within the Identity Provider, the end-user will be unable to authenticate to the Application. As a result, choosing email as a SAML Subject is appropriate only when an Application requires an email address and is willing to reject end-users who lack it.

In addition, emails can be changed or recycled in the same manner as the `userName`. Therefore, similar mechanisms are necessary to handle such events.

- In some circumstances, it may be necessary to use multiple attributes to best match a SAML Authentication response against a specific end-user in the Application. If this occurs, it is acceptable to use both the SAML Subject and the SAML Attributes in combination to perform the matching. In this scenario, the choice of SAML Subject becomes somewhat flexible, and one may choose whichever option is most likely to be available and useful.

# Up Next

Another call for vote on Implementors Draft