

# SAML Authentication

Binod Paneru

Software Engineer at Gurzu Inc

<https://www.linkedin.com/in/binod-paneru-74a93a9b/> (Linkedin)

<https://github.com/binpaneru1> (Github)

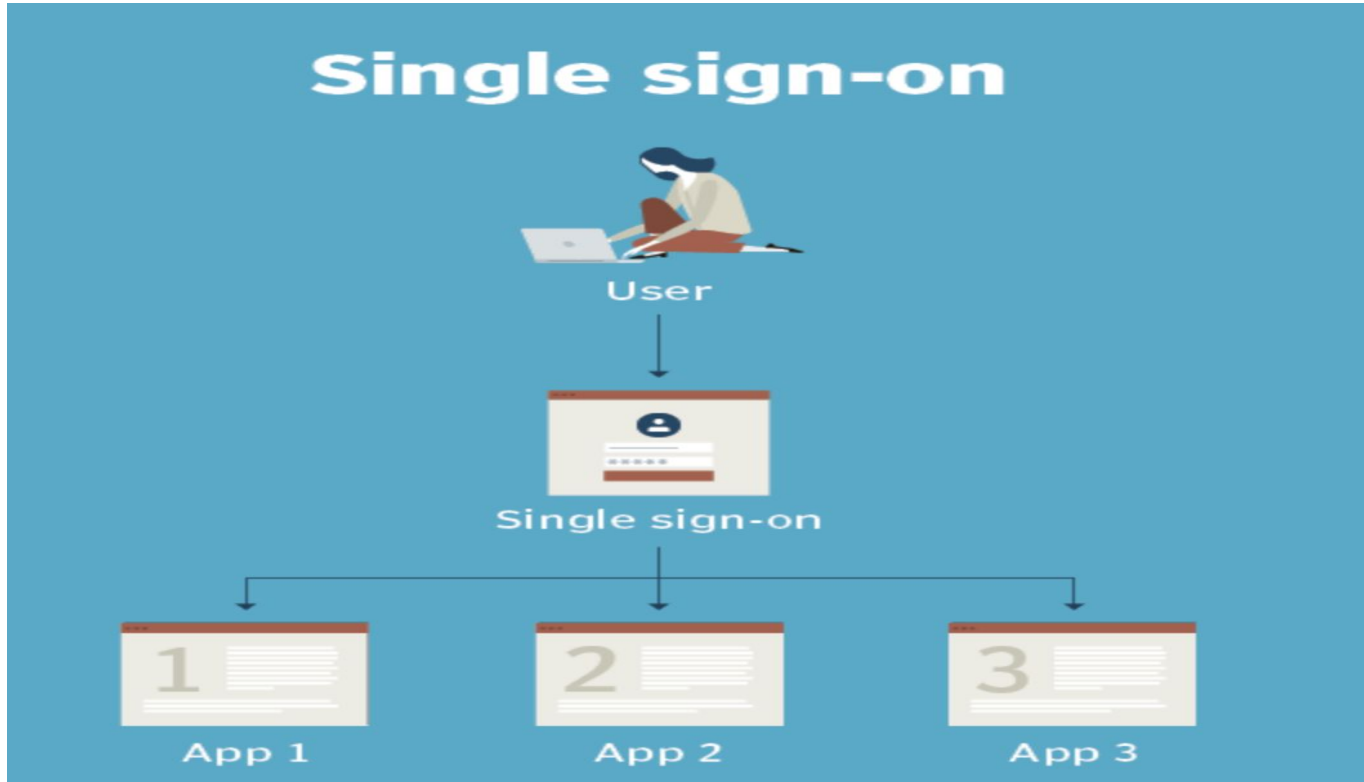
# SAML

- SAML stands for Security Assertion Markup Language.
- It is an XML-based open-standard for transferring identity data between two parties: an identity provider (IdP) and a service provider (SP).
- Identity Provider
- Service Provider

# BENEFITS OF SAML AUTHENTICATION

- Improved User Experience
- Increased Security

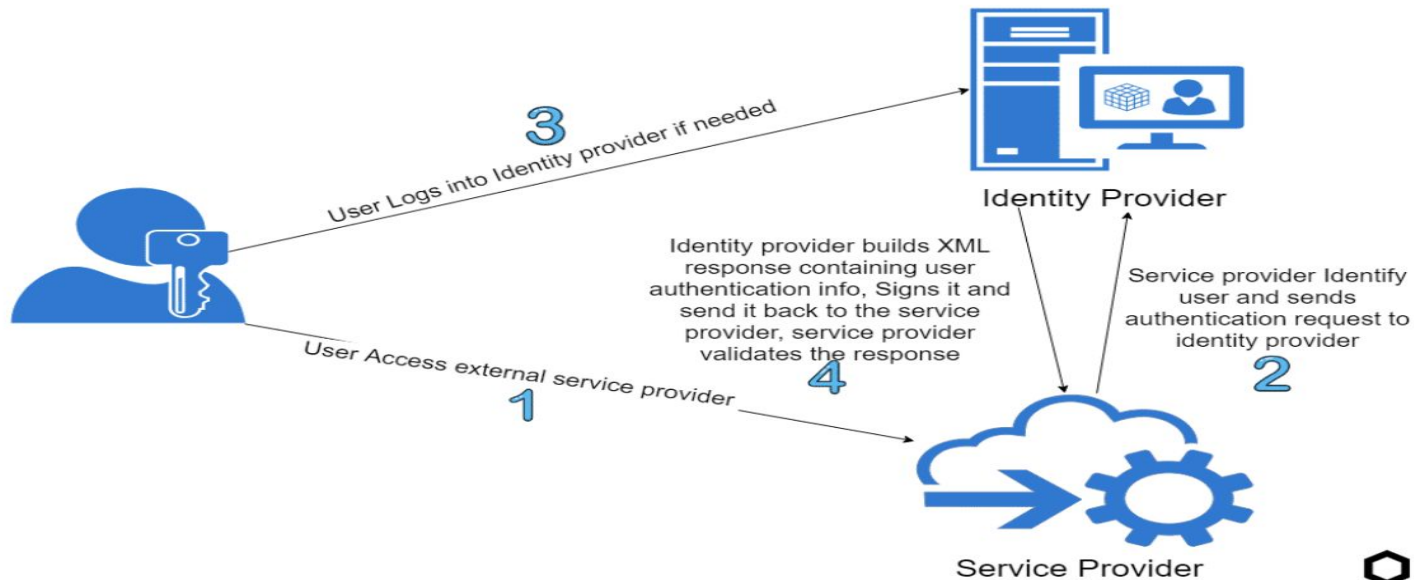
# WHAT IS SSO?



# How Does SAML Authentication Works?

# SSO PROCESS

## Single Sign On Process



# SAML Response

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2p:Response xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">https://cg-se.isr.co.jp/sso/sample2/</saml2:Issuer>
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo>
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#WithComments" />
      <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
      <ds:Reference URI="#cg-5c324402-5cd4-4628-a74c-0be2db022147">
        <ds:Transforms>
          <ds:Transform Algorithm="Follow link (cmd + click) 000/09/xmldsig#enveloped-signature" />
          <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
            <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="xsd" />
          </ds:Transform>
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmenc#sha256" />
        <ds:DigestValue>m3Phdc59nyUxblkkiRLZV93pY8Lnu5p6yltcBFGK0s</ds:DigestValue>
      </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue>HujRsAhubTse7FCBE/Gyw4crE/f4XxkfJ7FbxL85P96gp37Rl6gQqyAY970D1gB1C7foxb2foFBmtHdUrYSCE63EQin
```



# RUBY-SAML


- The Ruby SAML library is for implementing the client side of a SAML authorization, i.e. it provides a means for managing authorization initialization and confirmation requests from identity providers.

Configuration in okta

# CREATE AN APP INTEGRATION

**APPLICATIONS**

**Create a new app integration** ×

**Sign-in method**  
[Learn More](#) 

☐

**OIDC - OpenID Connect**  
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.

☒

**SAML 2.0**  
XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.

☐

**SWA - Secure Web Authentication**  
Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.

☐

**API Services**  
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

Cancel

Next

# GENERAL SETTING

## Create SAML Integration

1 General Settings

2 Configure SAML

3 Feedback

### 1 General Settings

App name

App logo (optional)





App visibility

☐ Do not display application icon to users

[Cancel](#)

[Next](#)

# CONFIGURE SAML

## A SAML Settings

### General

Single sign on URL ?

☒ Use this for Recipient URL and Destination URL

☐ Allow this app to request other SSO URLs

Audience URI (SP Entity ID) ?

Default RelayState ?

If no value is set, a blank RelayState is sent

Name ID format ?

Unspecified ▼

Application username ?

Okta username ▼

Update application username on

Create and update ▼

### What does this f

This form genera  
for the app's SAN

### Where do I find t needs?

The app you're tr  
should have its o  
using SAML. You  
doc, and it shoul  
information you r  
form.

## A SAML Settings

### General

Single sign on URL ?

https://cd5117cc3dee.ngrok.io/okta/callback

☒ Use this for Recipient URL and Destination URL

☐ Allow this app to request other SSO URLs

Audience URI (SP Entity ID) ?

http://www.okta.com/exk6cuz11y6qjGTR35d7

Default RelayState ?

gurzu.com

If no value is set, a blank RelayState is sent

Name ID format ?

EmailAddress ▼

Application username ?

Okta username ▼

Update application username on

Create and update ▼

# The following is needed to configure sso-test-setup

## 1 Identity Provider Single Sign-On URL:

```
https://dev-47544890.okta.com/app/dev-47544890_sso-test-setup_1/exk6cuz11y6qjGTR35d7/sso/saml
```

## 2 Identity Provider Single Logout URL:

```
https://dev-47544890.okta.com/app/dev-47544890_sso-test-setup_1/exk6cuz11y6qjGTR35d7/slo/saml
```

## 3 Identity Provider Issuer:

```
http://www.okta.com/exk6cuz11y6qjGTR35d7
```

## 4 X.509 Certificate:

```
-----BEGIN CERTIFICATE-----
MIIDQCCApCgAwIBAgIGAYL3YpTOMA0GCSqGSIb3DQEBCwUAMIGUMQswCQYDVQQGEwJVUzETMBEG
A1UEAwKQ2FsaWZvcn5pYTEwMBQGA1UEBwwNU2FuIEZyYW55aXNjbzENMAsGA1UECgwET2t0YTEU
MBIGA1UECwwLU1NPUHJvdmlkZXIxFTATBgNVBAMMDGR1di00NzU0NDg5MDEcMBoGCSqGSIb3DQEJ
ARYNaW5mb0Bva3RhLmNvbTAeFw0yMjA5MDEwNDQ5MD1aFw0zMjA5MDEwNDUwMD1aMIGUMQswCQYD
VQQGEwJVUzETMBEGA1UEAwKQ2FsaWZvcn5pYTEwMBQGA1UEBwwNU2FuIEZyYW55aXNjbzENMAsG
A1UECgwET2t0YTEUMBIGA1UECwwLU1NPUHJvdmlkZXIxFTATBgNVBAMMDGR1di00NzU0NDg5MDEc
MBoGCSqGSIb3DQEJARYNaW5mb0Bva3RhLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQEA
ggEBAKKXoJEBQC127rC7Wq101ImgpUg46zWKAnGE0tCdRKFDCN/cgG8XM1fAtLtAzx6YSpy+MkrF
S58Zw0w5+wB+m043eb14hw7g999vT9AKnY9suWbhd6U3t1eZrbDqcs03KgmhgQFzRrIt+01/BO
BcX07MYIjNmPsOBH24XC3xw7e+69VRcN4t1QJZnZhNgD1c1w2dd1axPRVXumtb001ELjdmZW9NG
0ia78RfNifRz1V20Gq0BApA1nXLQVFsAJGuR+h12ogRoHEmpUAvQr+vYAFHzM5mtmXZSrCPXI m2C
7u9DXbGfJ4DmoF4sAUpZwMW+xEkQv9AWGP3a0SyywUCAwEAATANBgkqhkiG9w0BAQsFAAOCAQEA
Urr3JATX6oj09JeEkZ7aj9T1pfpB3s9iVT3KRgHWP/g65GZ2nfrGk1IaW+ayNECEy9gaxJsYPxUri
EGcraoTNme5Y1wLtwGwByd13w/C2MjxnFK7yNIdksUDZ2nHMWJYsCICGvPopZX+robpNdRxcRhb
1Hnp3tTJX60hMjRbGU0IpywQESwISJLSzX072oTeQILuz4GBdajuGHZQAZFBqhYTFRZ2urgh9Y4
oUbdmcSVVnozeKt1vD+a1tU9GnUey3oY48Fmx6xZPRpTd0IowxvW/F+MyPZJN86U7meQe81Vo/g
BZ4Ku61rW0rB5LH9Jrt4rFcK+nDw71n2oHuNw==
-----END CERTIFICATE-----
```

[Download certificate](#)

# SAML IN RUBY (GEM: RUBY-SAML)

## ruby-saml 1.14.0

SAML toolkit for Ruby on Rails

### VERSIONS:

**1.14.0** - February 01, 2022 (72 KB)  
**1.13.0** - September 06, 2021 (71.5 KB)  
**1.12.2** - April 12, 2021 (68.5 KB)  
**1.12.1** - April 05, 2021 (68.5 KB)  
**1.12.0** - February 19, 2021 (68.5 KB)

[Show all versions \(83 total\) →](#)

### RUNTIME DEPENDENCIES (2):

**nokogiri** >= 1.10.5  
**rexml** >= 0

### DEVELOPMENT DEPENDENCIES (9):

**coveralls** >= 0  
**minitest** ~> 5.5  
**mocha** ~> 0.14  
**pry-byebug** >= 0  
**rake** ~> 10  
**shoulda** ~> 2.11  
**simplecov** >= 0  
**systemu** ~> 2  
**timecop** ~> 0.9

[Show all transitive dependencies →](#)



811

TOTAL DOWNLOADS

**53,302,474**

FOR THIS VERSION

**1,136,279**

### GEMFILE:

```
gem 'ruby-saml', '~> 1.14.0'
```



### INSTALL:

```
gem install ruby-saml
```



### LICENSE:

**MIT**



# INTEGRATION IN RAILS

```
gem 'ruby-saml', '~> 1.11.0'
```

```
gem 'nokogiri', '~> 1.5.10'
```

```
def show
```

```
  company_email_domain = params[:company_email]
```

```
  settings = SettingSaml.find_by(company_email_domain: company_email_domain)&.fetch_settings
```

```
  request = OneLogin::RubySaml::Authrequest.new
```

```
  redirect_to request.create(settings), allow_other_host: true
```

```
end
```

[https://dev-47544890.okta.com/app/dev-47544890\\_ssotestsetup\\_1/exk6cuz11y6qjGTR35d7/sso/saml?SAMLRequest=fZHLbsIwEEV%2FJTuvEj%2FygFgECRWpQqIboF10g4yZlDSJHTI00H59k1YVIFVdjuaemfHxBFVdNXLUwYNZwbEDdN4MEVpXWPNgDXY1tGtoT4WG59UyIwfnGpSUJnrHE52HYwE8MG%2BtLYPCUls6RbWqqp3SJfHm%2FbjCqGHWldzDyY9GcRSNUxYMQKBtTVXT3HW2iNb10ILrmi2ncCkT3X1y%2FpEc3x83qzDej2ifocMDiLeYZ2QbMoBcRMrnSSz8KGW5PxYafLHv63wX80SkfRSxg4VBp4zLiGBC%2BCz1mdhwJkUoBXsl3gu0%2BH20CBjxLnVlUA6LMtK1RlqFBUqjakDptFzPnpayD0r1K%2B4Waf5nmtY6q21FppMhLb%2Bva6eDrN7V%2BXy%2BKvpLwYTeUj%2FV%2FXd0vwA%3D](https://dev-47544890.okta.com/app/dev-47544890_ssotestsetup_1/exk6cuz11y6qjGTR35d7/sso/saml?SAMLRequest=fZHLbsIwEEV%2FJTuvEj%2FygFgECRWpQqIboF10g4yZlDSJHTI00H59k1YVIFVdjuaemfHxBFVdNXLUwYNZwbEDdN4MEVpXWPNgDXY1tGtoT4WG59UyIwfnGpSUJnrHE52HYwE8MG%2BtLYPCUls6RbWqqp3SJfHm%2FbjCqGHWldzDyY9GcRSNUxYMQKBtTVXT3HW2iNb10ILrmi2ncCkT3X1y%2FpEc3x83qzDej2ifocMDiLeYZ2QbMoBcRMrnSSz8KGW5PxYafLHv63wX80SkfRSxg4VBp4zLiGBC%2BCz1mdhwJkUoBXsl3gu0%2BH20CBjxLnVlUA6LMtK1RlqFBUqjakDptFzPnpayD0r1K%2B4Waf5nmtY6q21FppMhLb%2Bva6eDrN7V%2BXy%2BKvpLwYTeUj%2FV%2FXd0vwA%3D)

# WHAT HAPPENS IN CALLBACK?

```
def redirect_callback
  set_setting_saml_from_relay_state(params[:RelayState])
  saml_response = OneLogin::RubySaml::Response.new(params[:SAMLResponse], :settings => @setting_saml.fetch_settings)
  if saml_response.is_valid?
    user = User.find_or_create_by(email: saml_response.nameid) do |user|
      user.password = Devise.friendly_token.first(6)
    end
    sign_in(user)
    redirect_to root_url
  else
    raise response.errors.inspect
  end
end
```

# SLO IN RAILS

```
def destroy
  logout_request = OneLogin::RubySaml::Logoutrequest.new
  logout_request_id = logout_request.uuid
  relay_state = current_user.email
  slo_url = logout_request.create(settings, :RelayState => relay_state)
  puts slo_url
  redirect_to slo_url, allow_other_host: true
end
```

# REFERENCES

<https://auth0.com/blog/how-saml-authentication-works/>

[https://www.onelogin.com/learn/saml#:~:text=What%20SAML%20is%20and%20How,the%20service%20provider%20\(SP\).](https://www.onelogin.com/learn/saml#:~:text=What%20SAML%20is%20and%20How,the%20service%20provider%20(SP).)

<https://github.com/onelogin/ruby-saml>

Any Questions?