Reference Learning Service Provider Integration

Project.PLNPusdiklat.KKJ

Table of Contents

SAML Integration

Read references here:
- https://www.varonis.com/blog/what-is-saml/
- https://everything1know.wordpress.com/2019/02/19/saml-2-0-artifact-binding/
- https://auth0.com/blog/how-saml-authentication-works/

Identity Provider

- IdP Entity ID :
  `https://idp.pln-pusdiklat.co.id`
- IdP Base URL :
  `https://elearning.pln-pusdiklat.co.id/sso`
- IdP Metadata :
  `https://elearning.pln-pusdiklat.co.id/sso/saml2/idp/metadata.php`
- IdP Certificate :

```
-----BEGIN CERTIFICATE-----
MIIE6zCCA1OgAwIBAgIUZV1/i6e+Mqk4817TZD9IHIU7fBgwDQYJKoZIhvcNAQEL
BQAwgYQxCzAJBgNVBAYTAklEMRQwEgYDVQQIDAtES0kgSmFrYXJ0YTEYMBYGA1UE
BwwPSmFrYXJ0YSBTZWxhdGFuMRYwFAYDVQQKDA1QTE4gUHVzZGlrbGF0MQswCQYD
VQQLDAJJVDEgMB4GA1UEAwwXaWRwLnBsbi1wdXNkaWtsYXQuY28uaWQwHhcNMjAx
MDEyMTQwNzM1WhcNMzAxMDEyMTQwNzM1WjCBhDELMAkGA1UEBhMCSUQxFDASBgNV
BAgMC0RLSSBKYWthcnRhMRgwFgYDVQQHDA9KYWthcnRhIFNlbGF0YW4xFjAUBgNV
BAoMDVBMTiBQdXNkaWtsYXQxCzAJBgNVBAsMAklUMSAwHgYDVQQDDBdpZHAucGxu
LXB1c2Rpa2xhdC5jby5pZDCCAaIwDQYJKoZIhvcNAQEBBQADggGPADCCAYoCggGB
AMhPqONg18xZ/rmwq860zFkwzny/qYzr4V0oLWSwgMIFadRyR9bFfhXSx7nLa6Ug
PcLRahlAUhgWPju3Xu7x71xkMD7RCnyb1uu/kaHGP3PqWWVhyPjOxoUOFH4qrOKm
3sK6UU5bKodrPy5HCXV6hNvn1RkDndeVE6L4NqMTmo81ROgEAFwRhD3G88MaADbT
YsHr5T8gOlB1tr2Hza9cX1LxAXsRFGek36nSvPKOUCb+MIpiX0A5Rcw0ZBfA7ZaT
Q1jggzhMSkX2v8wTuQHcZB5/ki0h4Dz5BWXH7gZXMDaSEVll6wsGSFb7+axTUmpJ
c3QNtvhj7KuUXXFCPmUdGA0fJUt9SWI/H8LrEs29iE66dW/1gYbjOdZyxsprCF+U
VCxuQUf2fO/FhI2Jb/2gbatRsQfMmSrBTaoqxQrWEZg8jtexHBSZzODqbiWsBaqE
MIpAwSmQ1i1ZZ3JSv0L4Ki6jrzAbeHy8YgAwU2Nmequ86tEsx+h0tK7e4HaZBq7P
KQIDAQABo1MwUTAdBgNVHQ4EFgQUu8wggv566xgb/7vxCNZpbOLg5L8wHwYDVR0j
BBgwFoAUu8wggv566xgb/7vxCNZpbOLg5L8wDwYDVR0TAQH/BAUwAwEB/zANBgkq
hkiG9w0BAQsFAAOCAYEAtG5am9NvU+hgCtORPhR/vUeGjSYnQqYT2HKHzh0Utavr
LzLxNhTfddH8btfklAow+elGiMLSdzq/5RhD2d00iXZ0qZiob1ZnE15PIY/NrkRr
IMjj4P1lho/kLDuSlXsGV4l0QwDQYDZh9DSE6AaUPl6LjSEk54e5Wbk9jTkAIMsh
r6+enaEa/Plg3bowMo7ZSr7IjBVPEsGTt6dTqz03oC6rF/mrzTIgMA5igQ6XxHOQ
CqJyvemoeRFJkqCoOsTCsGURp+6xhUJ96EaA2PtKMaCIPHkWiR+uyXT+ASIbpe3Y
8UpktwwLXryp4lm4UwYCCmzkl1bb6a21Z9fSyKe9ErzoVxY9r5MzYcr65bOLmveb
GxgqgmF7g74bUnF3LAgWyC1/sq+C/rKZR7SWZzu6bivWNmtA93qIpvNS5EyqPcrS
KErbXsKLZ7O/JAOe5OplxpL67ga69vzorkR7z3EbKfT4MvVUwZj5fqJfXmw88UqA
Axg+5DL5ZaXXcoY5hr3q
-----END CERTIFICATE-----
```

Reference Learning as Service Provider (SP)

- SP Entity ID: `referencelearning.pln.co.id`

IdP Requirements

Provide information required for registering Service Provider to IdP

- **Domain or IP Address** pointed to hosted application as Service Provider. URI must be accessible from internet (e.g. https://mylearning.pln.co.id)
- **SAML SP Metadata** contains
    - SAML `SingleLogoutService` Endpoints
    - SAML `AssertionConsumerService` Endpoints
    - SAML SP Certificate

SP Metadata

Real World Metadata Example:

https://corputube.pln.co.id/sp/module.php/saml/sp/metadata.php/pln-sso-auth

Expected Generated Metadata:

```xml
<?xml version="1.0"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
entityID="referencelearning.pln-pusdiklat.co.id">
  <md:SPSSODescriptor
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol
urn:oasis:names:tc:SAML:1.1:protocol">
    <md:KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>

<ds:X509Certificate>SP_CERTIFICATE_OR_PUBLIC_KEY</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
    <md:KeyDescriptor use="encryption">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>

<ds:X509Certificate>SP_CERTIFICATE_OR_PUBLIC_KEY</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
```

```xml
    <md:SingleLogoutService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://referencelearning.pln.co.id/SAML2_LOGOUT_ENDPOINT_HTTP"/>
    <md:SingleLogoutService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
Location="https://referencelearning.pln.co.id/SAML2_LOGOUT_ENDPOINT_SOAP"/>
    <md:AssertionConsumerService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://referencelearning.pln.co.id/SAML2_ACS_ENDPOINT"
index="0"/>
    <md:AssertionConsumerService
Binding="urn:oasis:names:tc:SAML:1.0:profiles:browser-post"
Location="https://referencelearning.pln.co.id/SAML1_ACS_ENDPOINT"
index="1"/>
    <md:AssertionConsumerService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact"
Location="https://referencelearning.pln.co.id/SAML2_ACS_ENDPOINT_ARTIFACT"
index="2"/>
    <md:AssertionConsumerService
Binding="urn:oasis:names:tc:SAML:1.0:profiles:artifact-01"
Location="https://referencelearning.pln.co.id/SAML1_ACS_ENDPOINT_ARTIFCAT"
index="3"/>
  </md:SPSSODescriptor>
  <md:ContactPerson contactType="technical">
    <md:GivenName>developer</md:GivenName>
    <md:EmailAddress>mailto:dev@pln-pusdiklat.co.id</md:EmailAddress>
  </md:ContactPerson>
</md:EntityDescriptor>
```

SAML Response

Example of received attributes after authentication success

```
{
    "Attributes": {
        "username": [
            "9216XXXXX"
        ],
        "employee_no": [
            "9216XXXXX"
        ],
        "full_name": [
            "JOHN DOE"
        ]
    },
    "Authority": "pln-sso-auth",
    "AuthnInstant": 1614031966,
    "Expire": 1614060766
}
```

Laravel Integration

Follow the Instruction README.md on this project
https://drive.google.com/file/d/1jeAWqlln7Gi6GZxYMS06ANMIHi4QTFeV/view?usp=sharing