

SpringOne Platform by Pivotal

Demystifying SAML

By Sree Tummididi & Filip Hanik

House Keeping

1. We're hiring!

Spring Security Engineer

<https://pivotal.io/careers/openings/spring-engineer-spring-security/1320220>

2. Rate the session

3. Talk: 30 minutes, 10 min break, 30 minutes

4. Contribute to open source at any capacity

Sree Tummidi

Product Manager

Started out as Software Engineer

Identity and Security @ Pivotal

@sreetummidi

Sree Tummidi

Product Manager

Started out as Software Engineer

Identity and Security @ Pivotal

@sreetummidi

Pivotal®



CLOUDFOUNDRY



Filip Hanik

Software Engineer

Spring Security SAML

@fhanik @pivotal

About to embark on a journey

Into the abyss of SAML

Demistify Concept

Demistify Concept

It's important to filter out what you need to know

Demistify Concept

It's important to filter out what you need to know

Avoid drowning in what you don't need to know...

Demistify Concept

It's important to filter out what you need to know

Avoid drowning in what you don't need to know...

Understand the bits that are flowing back and forth at the lowest level, to be able to utilize it at the highest

Demistify Concept

It's important to filter out what you need to know

Avoid drowning in what you don't need to know...

Understand the bits that are flowing back and forth at the lowest level, to be able to utilize it at the highest

Being able to research further with a familiarity of the topic

Demistify Concept

Have Fun

History

History

SAML v1.0

History

SAML v1.0

SAML v1.1

History

SAML v1.0

SAML v1.1

SAML v2.0★

What is
going
on???

What is
going
on???

What is
going
on???

Demystify Oauth/OIDC: <https://www.youtube.com/watch?v=u4BHKcZ2rxk>

FEDERATION ENTITY ID
Relying
XML SIGNATURE
PARTY
BINDING
Party
ATTRIBUTES
ASSERTIONS
PROFILE
Artifact
XML ENCRYPTION
METADATA
CLAIM
Identity Provider

What is SAML?

Story Time - Meet the actors

Story Time - Meet the actors

User



Identity
Provider



Service
Provider



Meet the actors

User Agent

User



Asserting Party

Identity Provider



Relying Party

Service Provider



Some More Terminology

SAML 2.0

The Specifications

The Specifications

Metadata

Binding

Conformance

Core/Protocol

Profile

We focus on

We focus on

Today's Reality

Demo - IDP Initiated Login

github.com/fhanik/springone2018

assertion

[*uh*-**sur**-shuhn]

noun

1. a positive statement or declaration, often without support or reason:
a mere assertion; an unwarranted assertion.
2. an act of **asserting**.

assertion

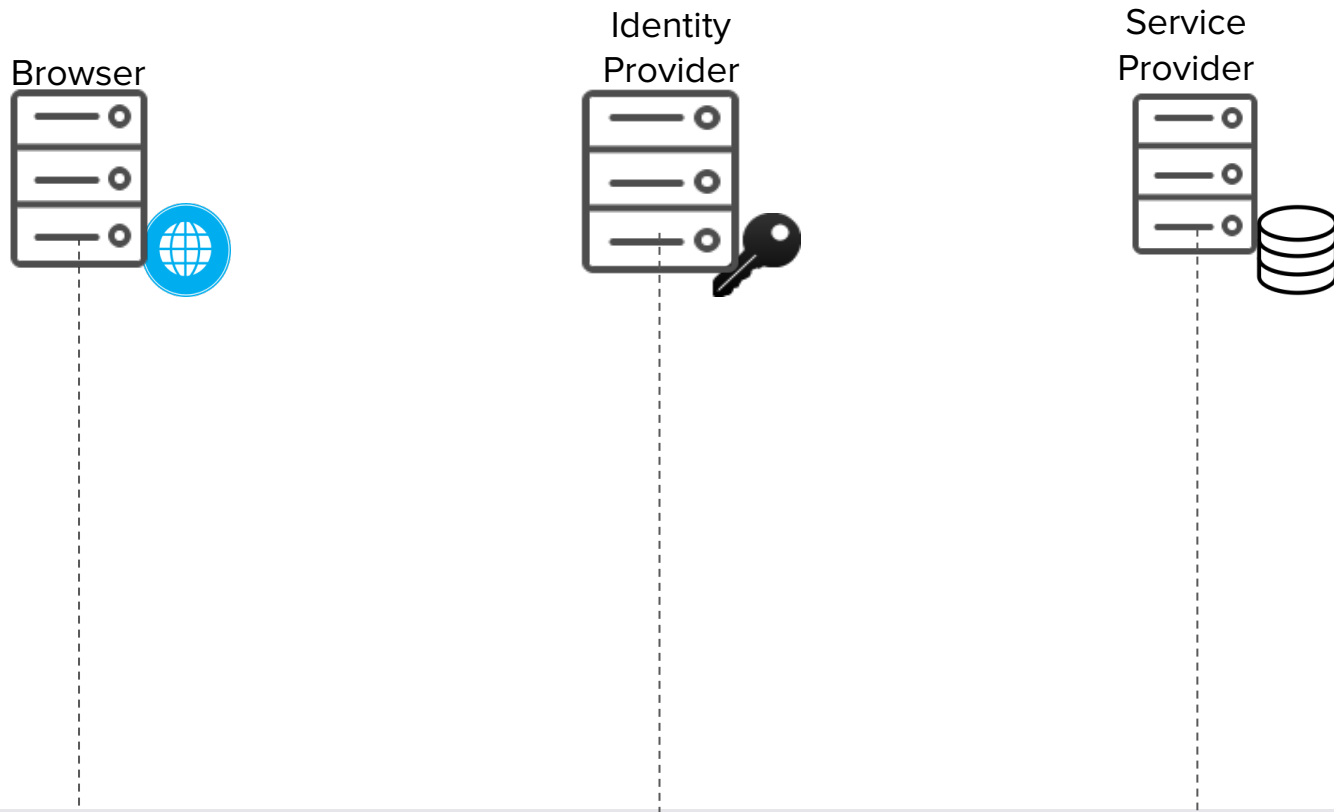
[*uh-sur-shuhn*]

noun

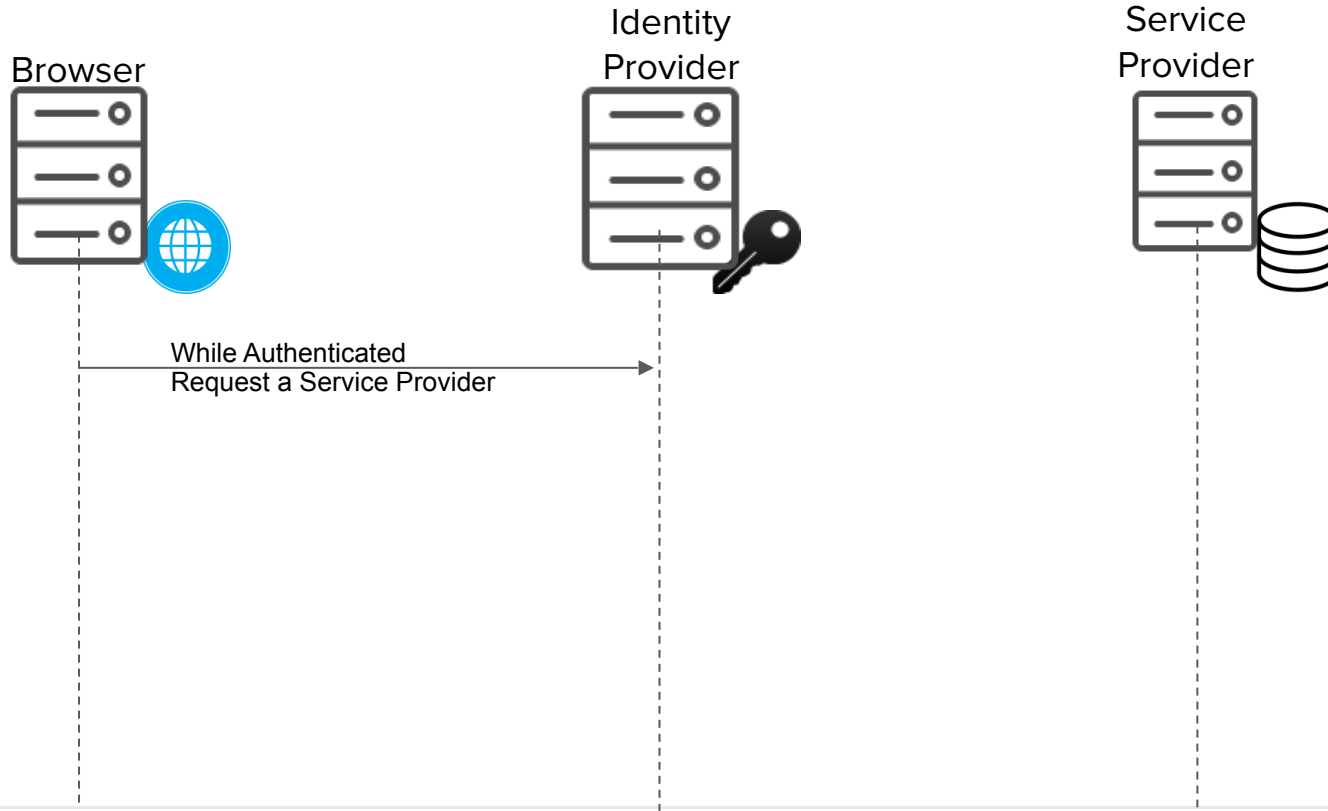
1. a positive statement or declaration, **often without support or reason:**
a mere assertion; an unwarranted assertion.
2. an act of **asserting**.

IDP Initiated Login

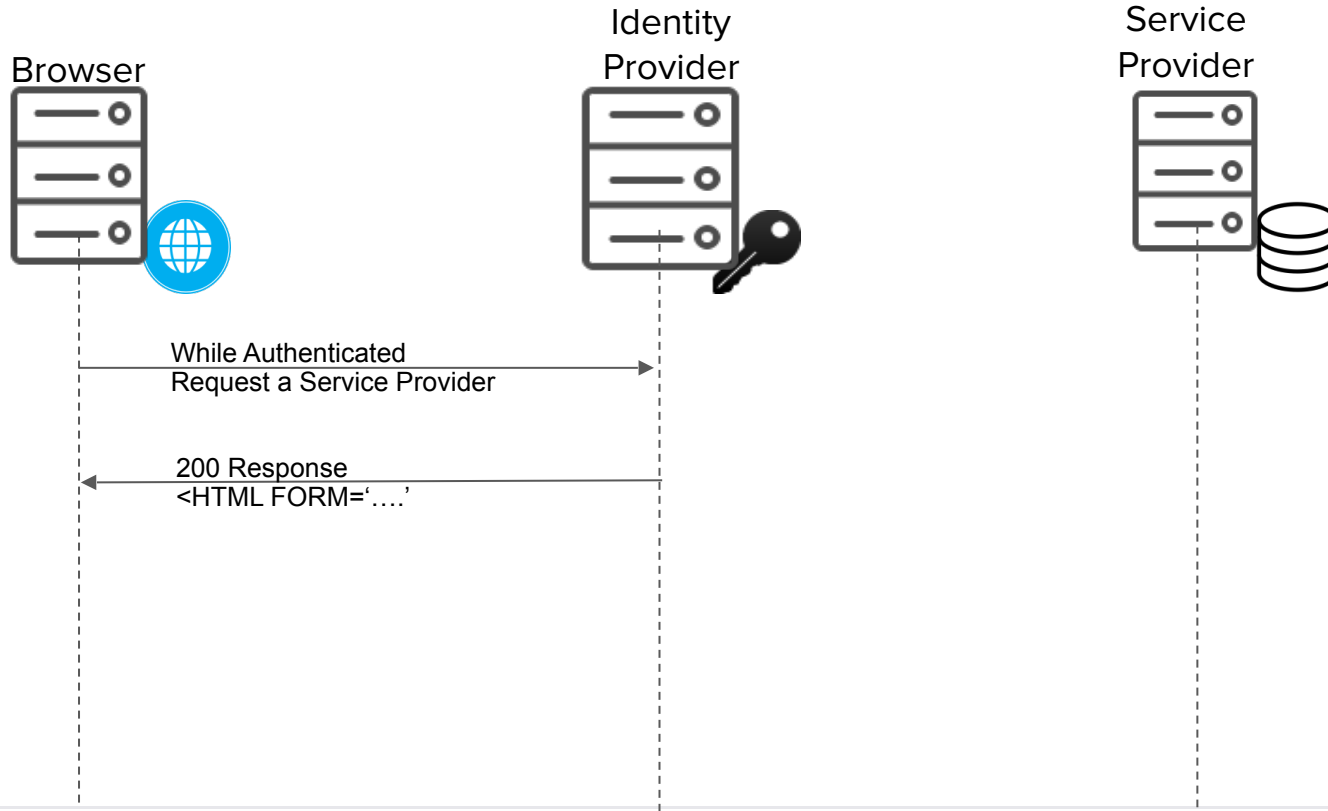
IDP Initiated Login



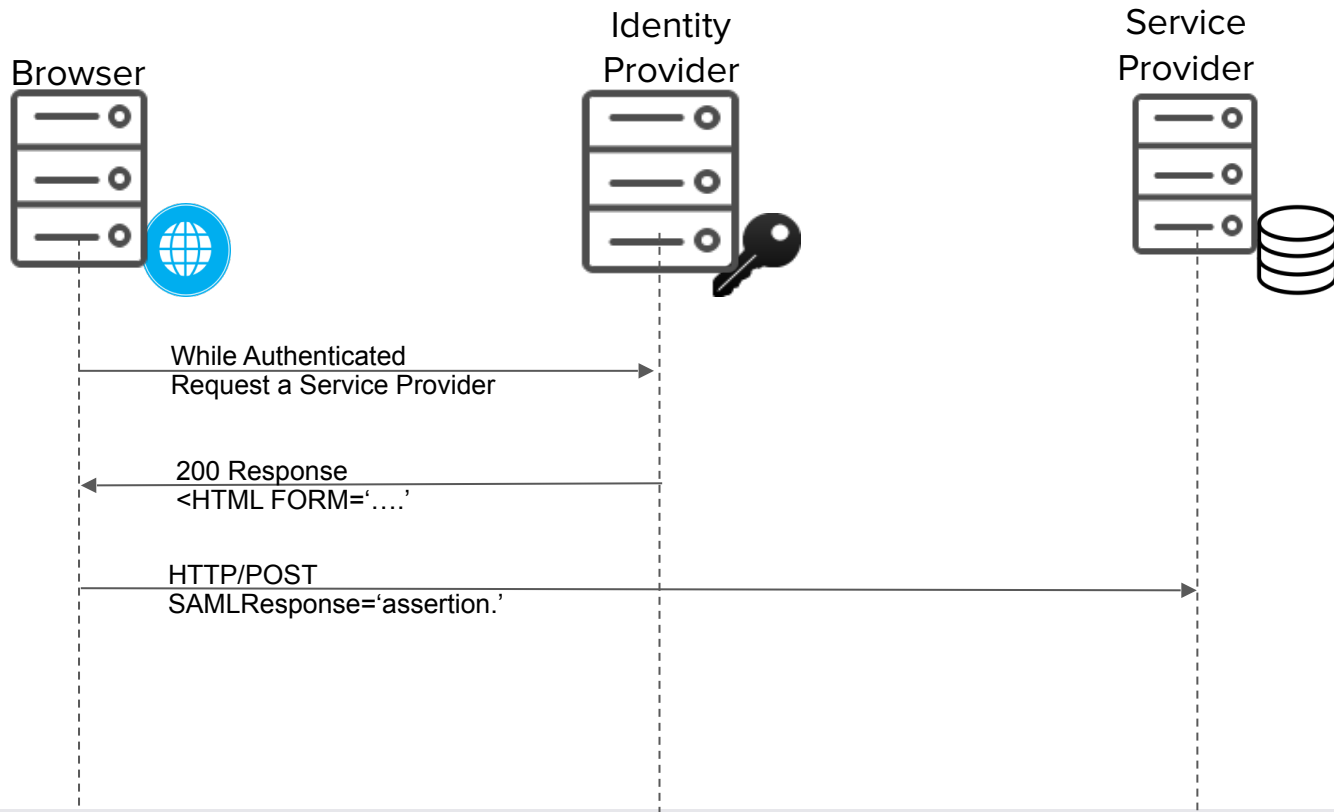
IDP Initiated Login



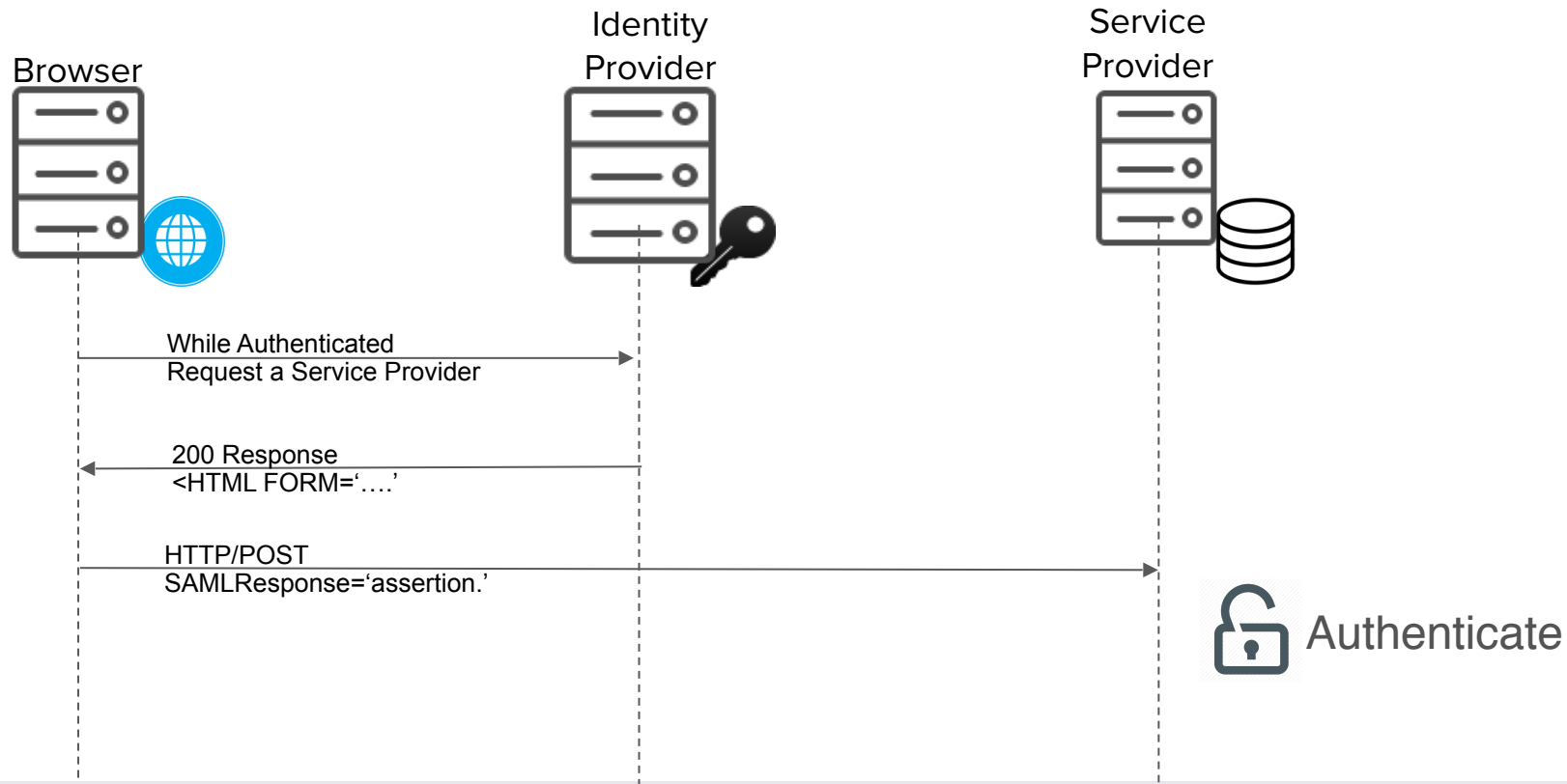
IDP Initiated Login



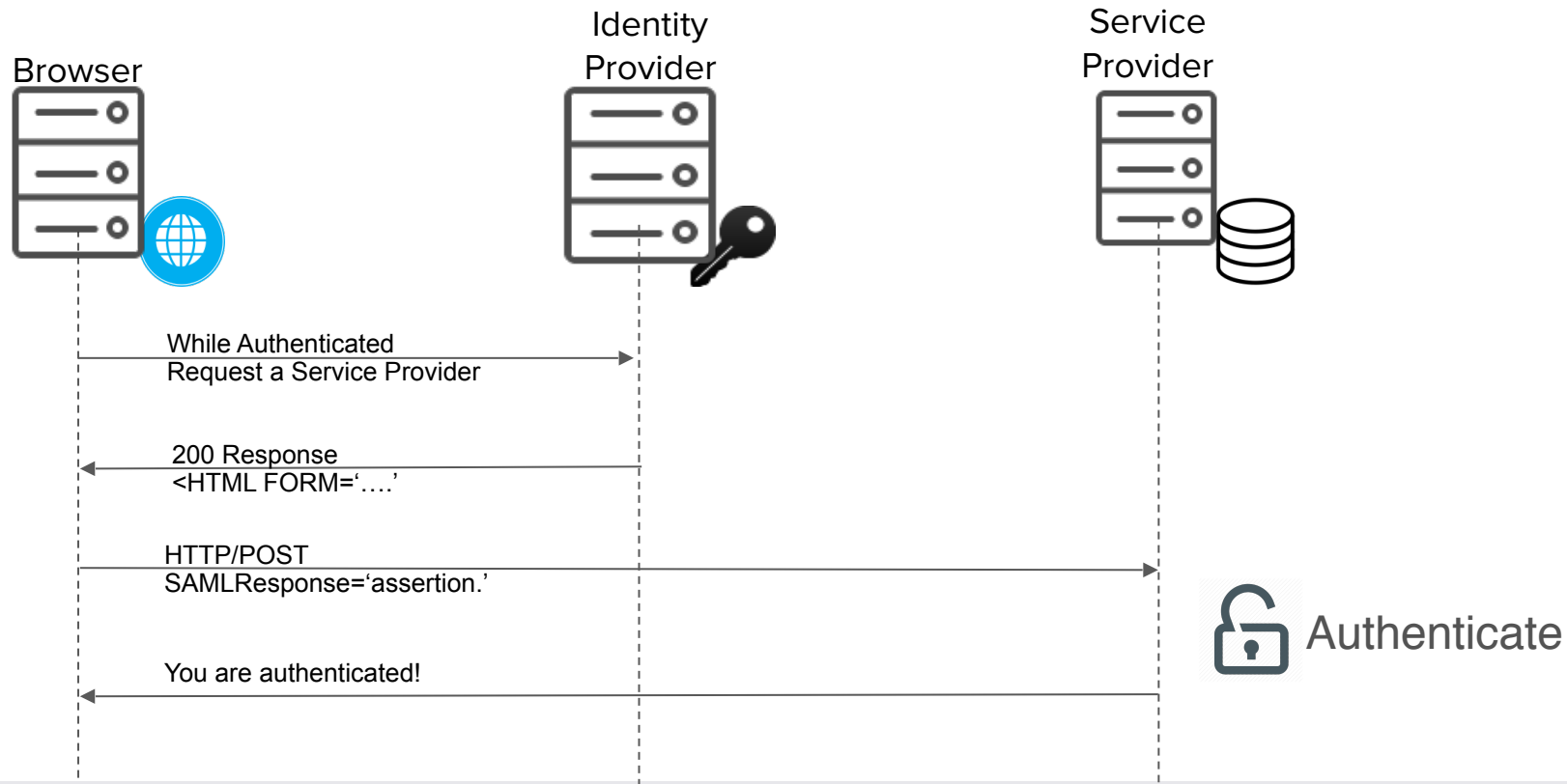
IDP Initiated Login



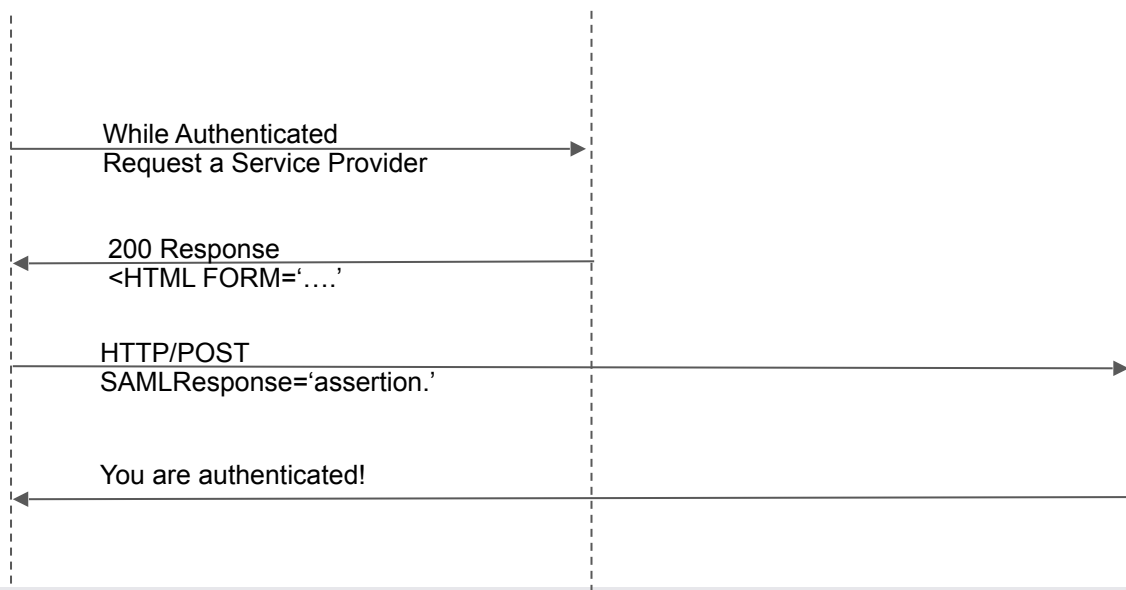
IDP Initiated Login



IDP Initiated Login



IDP Initiated Login

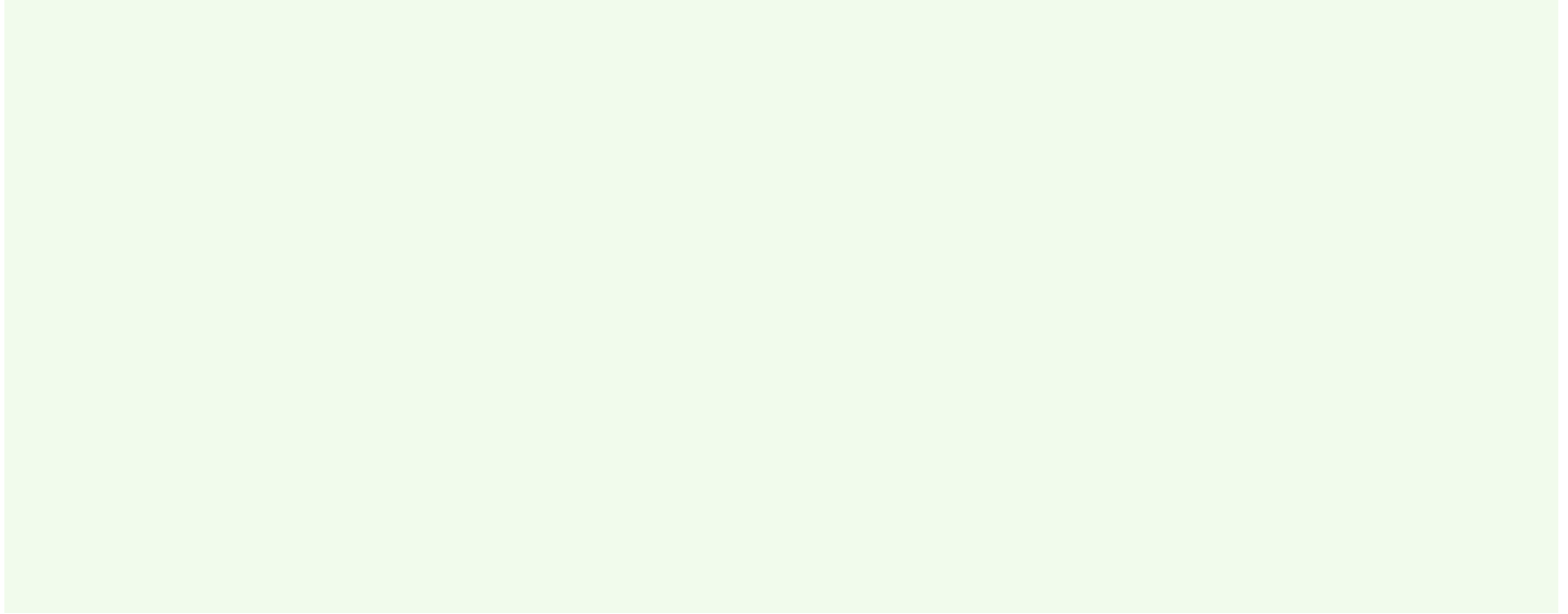


Demo - IDP Initiated Login

Introspect

github.com/fhanik/springone2018

IDP Initiated Login



IDP Initiated Login

```
POST /demo-sp/saml/sp/SSO HTTP/1.1  
Host: localhost:9091  
Content-Type: application/x-www-form-urlencoded  
  
SAMLResponse=encoded-saml-response
```

IDP Initiated Login

POST /demo-sp/saml/sp/SSO HTTP/1.1

Host: localhost:9091

Content-Type: application/x-www-form-urlencoded

SAMLResponse=encoded-saml-response

IDP Initiated Login

POST /demo-sp/saml/sp/SSO HTTP/1.1

Host: localhost:9091

Content-Type: application/x-www-form-urlencoded

SAMLResponse=encoded-saml-response

IDP Initiated Login

```
POST /demo-sp/saml/sp/SSO HTTP/1.1  
Host: localhost:9091  
Content-Type: application/x-www-form-urlencoded
```

SAMLResponse=encoded-saml-response

SAMLResponse HTTP parameter

```
<Response
  Destination="http://localhost:9091/demo-sp/saml/sp/SSO/alias/demo-sp">
  <Issuer>http://localhost:9092/demo-idp</saml2:Issuer>
  <ds:Signature>...</ds:Signature>
  <Status><StatusCode Value="...Success"/></Status>
  <Assertion>
    <Subject>
      <NameID>user</NameID>
    </Subject>
    <Assertion>
  </Response>
```

SAMLResponse

<Response

Destination="http://localhost:9091/demo-sp/saml/sp/SSO/alias/demo-sp">

<Issuer>http://localhost:9092/demo-idp</saml2:Issuer>

<ds:Signature>...</ds:Signature>

<Status><StatusCode Value="...Success"/></Status>

<Assertion>

<Subject>

<NameID>user</NameID>

</Subject>

<Assertion>

</Response>

SAMLResponse

```
<Response
  Destination="http://localhost:9091/demo-sp/saml/sp/SSO/alias/demo-sp">
  <Issuer> http://localhost:9092/demo-idp </saml2:Issuer>
  <ds:Signature>...</ds:Signature>
  <Status><StatusCode Value="...Success"/></Status>
  <Assertion>
    <Subject>
      <NameID>user</NameID>
    </Subject>
    <Assertion>
  </Response>
```

SAMLResponse

```
<Response
  Destination="http://localhost:9091/demo-sp/saml/sp/SSO/alias/demo-sp">
  <Issuer>http://localhost:9092/demo-idp</saml2:Issuer>
  <ds:Signature>...</ds:Signature>
  <Status><StatusCode Value="...Success"/></Status>
  <Assertion>
    <Subject>
      <NameID>peter_parker</NameID>
    </Subject>
    <Assertion>
  </Response>
```

SAMLResponse

```
<Response
  Destination="http://localhost:9091/demo-sp/saml/sp/SSO/alias/demo-sp">
  <Issuer>http://localhost:9092/demo-idp</saml2:Issuer>
  <ds:Signature>...</ds:Signature>
  <Status><StatusCode Value="...Success"/></Status>
  <EncryptedAssertion>
    <Subject>
      <NameID>peter_parker</NameID>
    </Subject>
    <EncryptedAssertion>
  </Response>
```

SAMLResponse

```
<Response
  Destination="http://localhost:9091/demo-sp/saml/sp/SSO/alias/demo-sp">
  <Issuer>http://localhost:9092/demo-idp</saml2:Issuer>
  <ds:Signature>...</ds:Signature>
  <Status><StatusCode Value="...Success"/></Status>
  <Assertion>
    <Subject>
      <EncryptedNameID>234a43ccd</EncryptedNameID>
    </Subject>
  </Assertion>
</Response>
```


Service Provider vs Identity Provider

Metadata

Service Provider vs Identity Provider

Service Provider vs Identity Provider

SAML Providers...

...require mutual trust

Metadata

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 ▼

[Show Advanced Settings](#)

Metadata

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 ?

Application username ?

[Show Advanced Settings](#)

Metadata is available as XML

```
curl http://localhost:9091/demo-sp/saml/sp/metadata
```

```
curl http://localhost:9092/demo-idp/saml/idp/metadata
```

Metadata

```
<md:EntityDescriptor entityID="http://localhost:9092/demo-idp">
  <md:IDPSSODescriptor WantAuthnRequestsSigned="true">
    <md:KeyDescriptor use="signing"> <!--or encryption-->
      <ds:X509Certificate>MIICmT...YBGT</ds:X509Certificate>
    </md:KeyDescriptor>
    <md:SingleLogoutService
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
      Location="http://localhost:9092/demo-idp/saml/idp/logout/alias/demo-idp"/>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress/>
    <md:SingleSignOnService
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
      Location="http://localhost:9092/demo-idp/saml/idp/SSO/alias/demo-idp"/>
    </md:IDPSSODescriptor>
```

Metadata

```
<md:EntityDescriptor entityID="http://localhost:9092/demo-idp">
  <md:IDPSSODescriptor WantAuthnRequestsSigned="true">
    <md:KeyDescriptor use="signing"> <!--or encryption-->
      <ds:X509Certificate>MIICmT...YBGT</ds:X509Certificate>
    </md:KeyDescriptor>
    <md:SingleLogoutService
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
      Location="http://localhost:9092/demo-idp/saml/idp/logout/alias/demo-idp"/>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress/>
    <md:SingleSignOnService
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
      Location="http://localhost:9092/demo-idp/saml/idp/SSO/alias/demo-idp"/>
    </md:IDPSSODescriptor>
  </md:EntityDescriptor>
```

Metadata - Identity Provider

```
<md:EntityDescriptor entityID="http://localhost:9092/demo-idp">
  <md:IDPSSODescriptor WantAuthnRequestsSigned="true">
    <md:KeyDescriptor use="signing"> <!--or encryption-->
      <ds:X509Certificate>MIICmT...YBGT</ds:X509Certificate>
    </md:KeyDescriptor>
    <md:SingleLogoutService
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
      Location="http://localhost:9092/demo-idp/saml/idp/logout/alias/demo-idp"/>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress/>
    <md:SingleSignOnService
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
      Location="http://localhost:9092/demo-idp/saml/idp/SSO/alias/demo-idp"/>
  </md:IDPSSODescriptor>
```


Metadata

```
<md:EntityDescriptor entityID="http://localhost:9092/demo-idp">
  <md:IDPSSODescriptor WantAuthnRequestsSigned="true">
    <md:KeyDescriptor use="signing"> <!--or encryption-->
      <ds:X509Certificate>MIICmT...YBGT</ds:X509Certificate>
    </md:KeyDescriptor>
    <md:SingleLogoutService
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
      Location="http://localhost:9092/demo-idp/saml/idp/logout/alias/demo-idp"/>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress/>
    <md:SingleSignOnService
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
      Location="http://localhost:9092/demo-idp/saml/idp/SSO/alias/demo-idp"/>
    </md:IDPSSODescriptor>
```

Metadata

```
<md:EntityDescriptor entityID="http://localhost:9092/demo-idp">
  <md:IDPSSODescriptor WantAuthnRequestsSigned="true">
    <md:KeyDescriptor use="signing"> <!--or encryption-->
      <ds:X509Certificate>MIICmT...YBGT</ds:X509Certificate>
    </md:KeyDescriptor>
    <md:SingleLogoutService
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
      Location="http://localhost:9092/demo-idp/saml/idp/logout/alias/demo-idp"/>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress/>
    <md:SingleSignOnService
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
      Location="http://localhost:9092/demo-idp/saml/idp/SSO/alias/demo-idp"/>
    </md:IDPSSODescriptor>
```

Metadata

```
<md:EntityDescriptor entityID="http://localhost:9092/demo-idp">
  <md:IDPSSODescriptor WantAuthnRequestsSigned="true">
    <md:KeyDescriptor use="signing"> <!--or encryption-->
      <ds:X509Certificate>MIICmT...YBGT</ds:X509Certificate>
    </md:KeyDescriptor>
    <md:SingleLogoutService
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
      Location="http://localhost:9092/demo-idp/saml/idp/logout/alias/demo-idp"/>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress/>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent/>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified/>
    <md:SingleSignOnService
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
      Location="http://localhost:9092/demo-idp/saml/idp/SSO/alias/demo-idp"/>
  </md:IDPSSODescriptor>
```

Metadata - Identity Provider

```
<md:EntityDescriptor entityID="http://localhost:9092/demo-idp">
  <md:IDPSSODescriptor WantAuthnRequestsSigned="true">
    <md:KeyDescriptor use="signing"> <!--or encryption-->
      <ds:X509Certificate>MIICmT...YBGT</ds:X509Certificate>
    </md:KeyDescriptor>
    <md:SingleLogoutService
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
      Location="http://localhost:9092/demo-idp/saml/idp/logout/alias/demo-idp"/>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress/>
    <md:SingleSignOnService
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
      Location="http://localhost:9092/demo-idp/saml/idp/SSO/alias/demo-idp"/>
    </md:IDPSSODescriptor>
```

Metadata - Service Provider

```
<md:EntityDescriptor entityID="http://localhost:9092/demo-idp">
  <md:SPSSODescriptor
    AuthnRequestsSigned="true"
    WantAssertionsSigned="true">
    <md:KeyDescriptor use="signing"> <!--or encryption-->
      <ds:X509Certificate>MIICmT...YBGT</ds:X509Certificate>
    </md:KeyDescriptor>
    <md:SingleLogoutService
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
      Location="http://localhost:9092/demo-idp/saml/idp/logout/alias/demo-idp"/>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress/>
    <md:SingleSignOnService
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
      Location="http://localhost:9092/demo-idp/saml/idp/SSO/alias/demo-idp"/>
  </md:SPSSODescriptor>
```

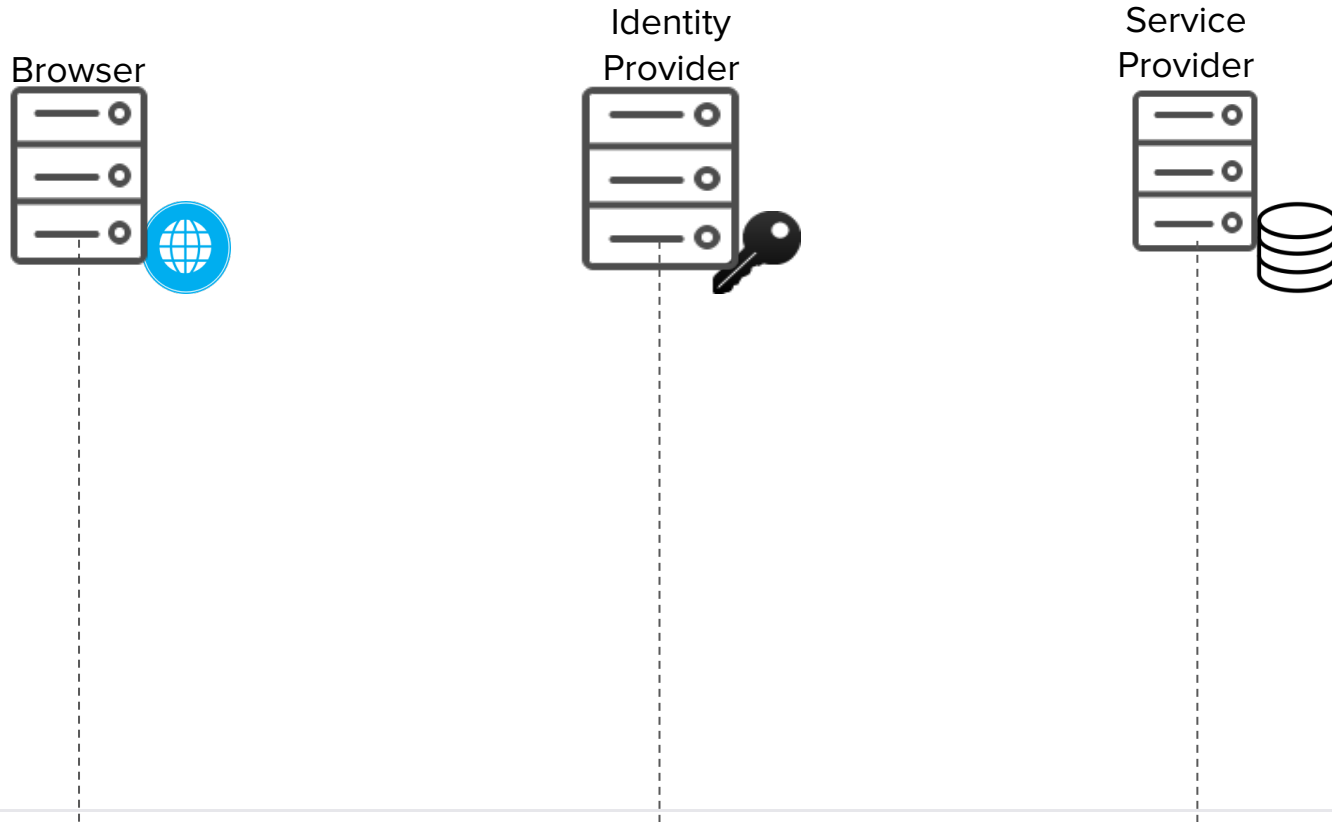
Metadata - Service Provider

```
<md:EntityDescriptor entityID="http://localhost:9092/demo-idp">
  <md:IDPSSODescriptor WantAuthnRequestsSigned="true">
    <md:KeyDescriptor use="signing"> <!--or encryption-->
      <ds:X509Certificate>MIICmT...YBGT</ds:X509Certificate>
    </md:KeyDescriptor>
    <md:AssertionConsumerService
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
      Location="http://localhost:9092/demo-idp/saml/idp/SSO/alias/demo-idp"/>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress/>
    <md:SingleSignOnService
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
      Location="http://localhost:9092/demo-idp/saml/idp/SSO/alias/demo-idp"/>
    </md:SPSSODescriptor>
```

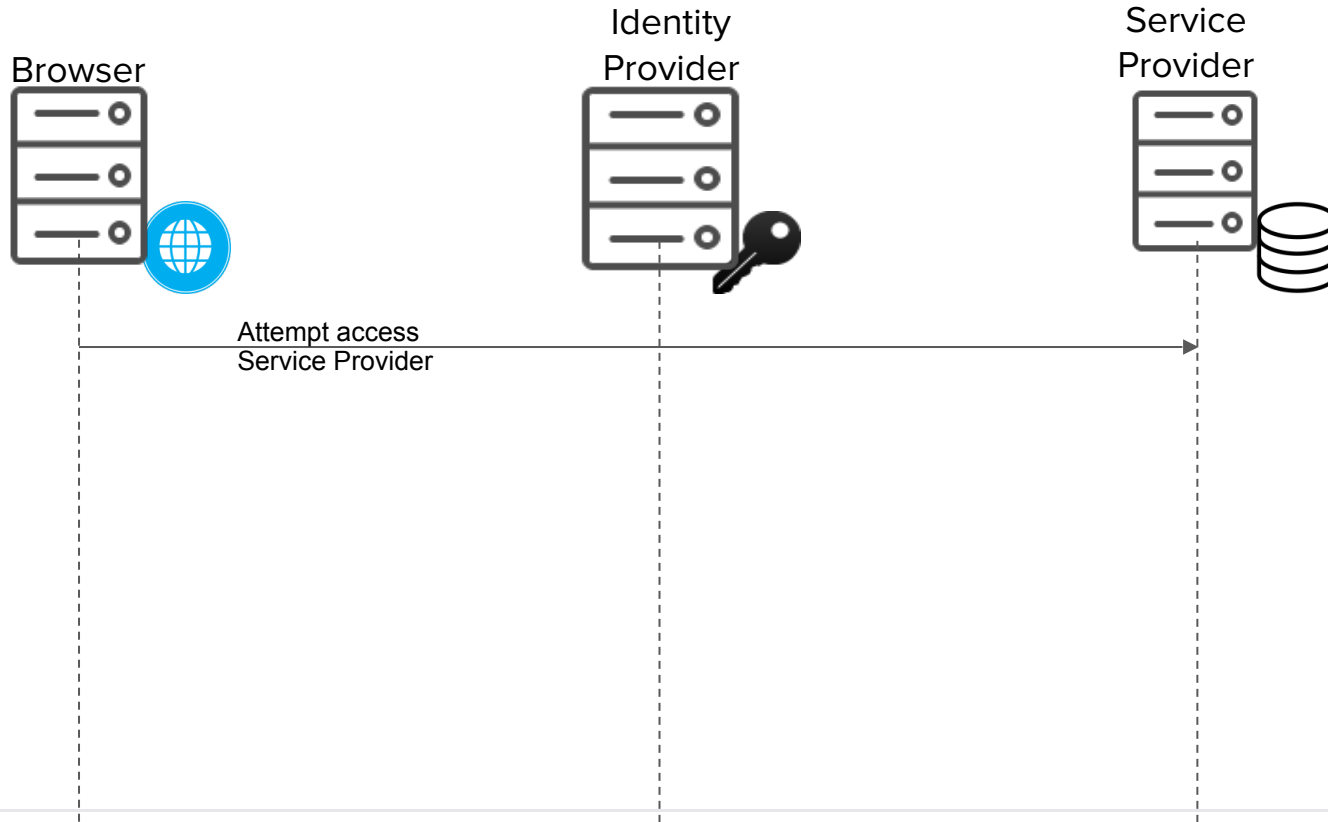
SP Initiated Login

SP Initiated Login

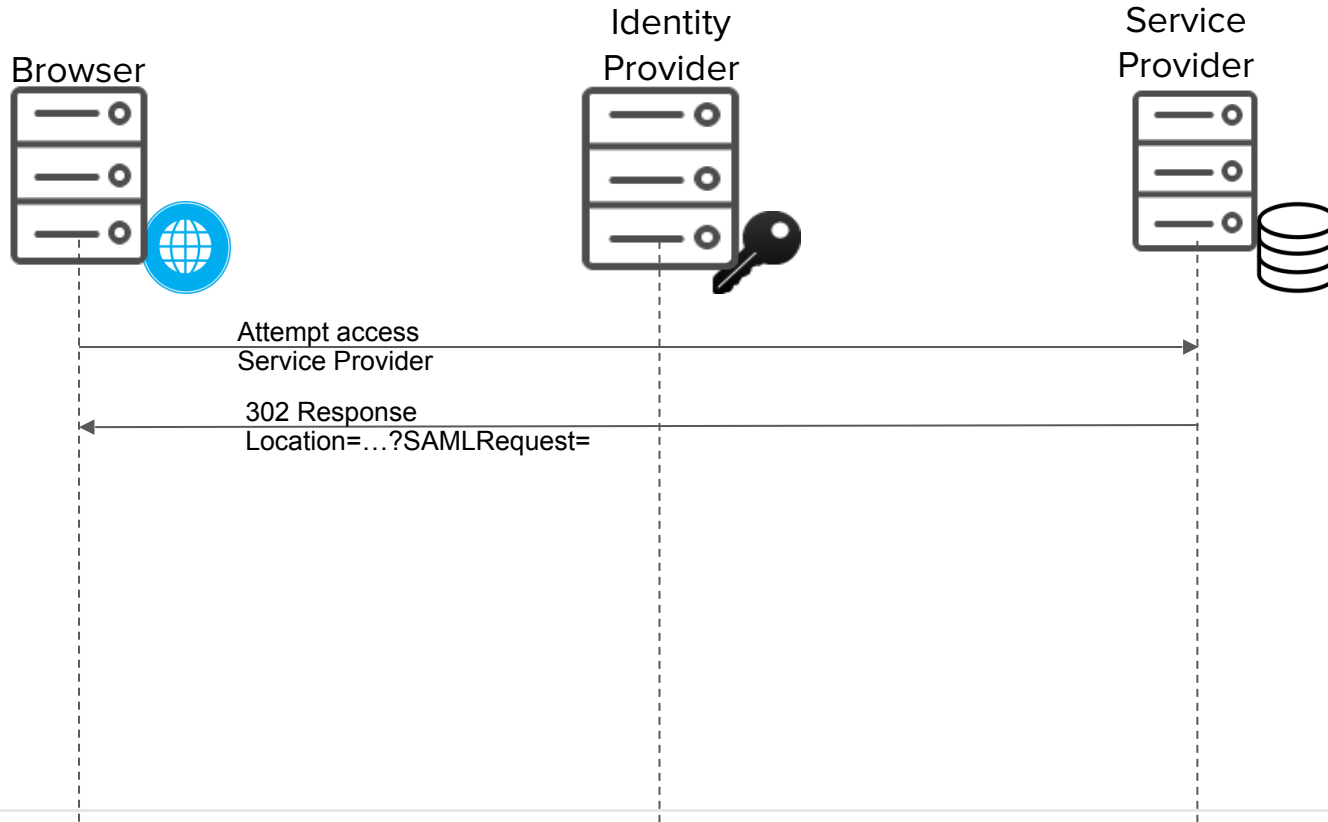
SP Initiated Login



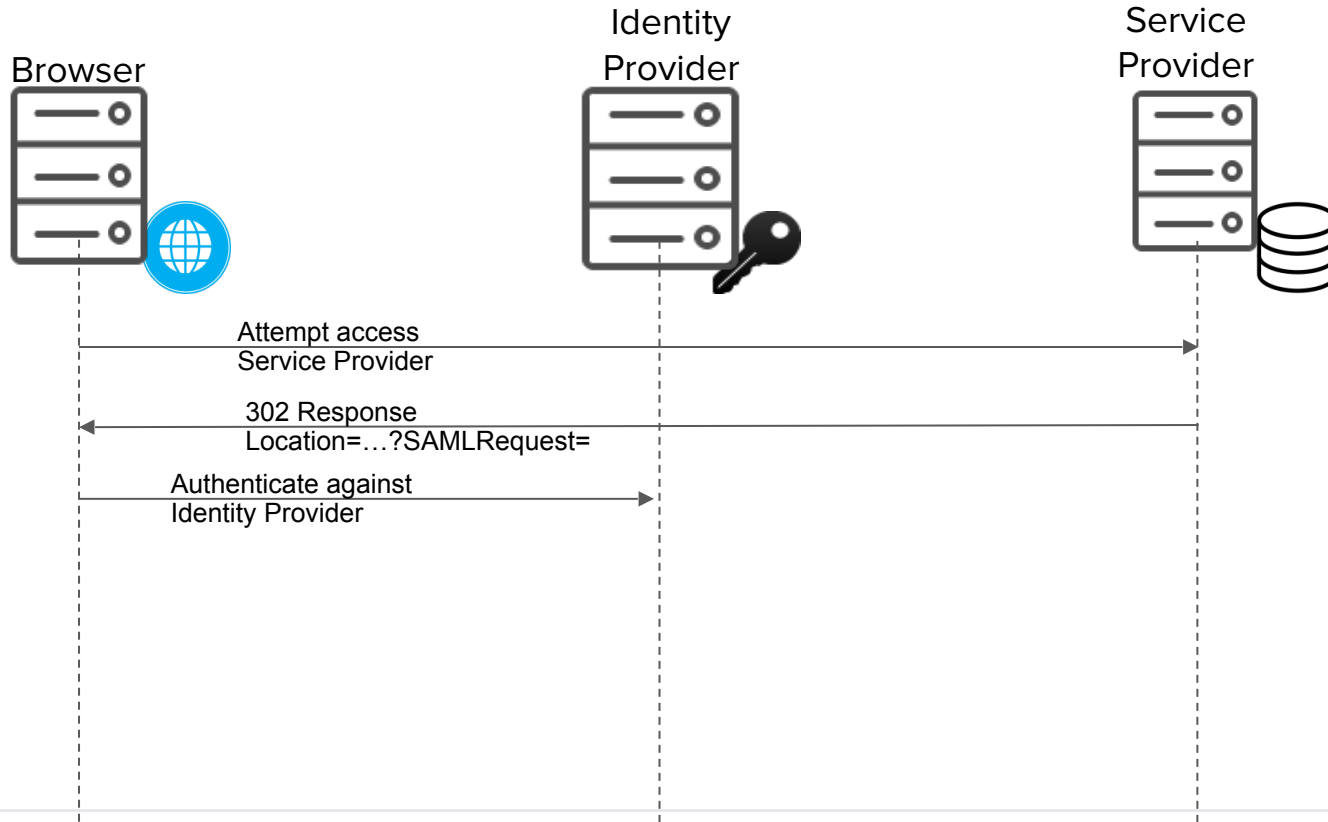
SP Initiated Login



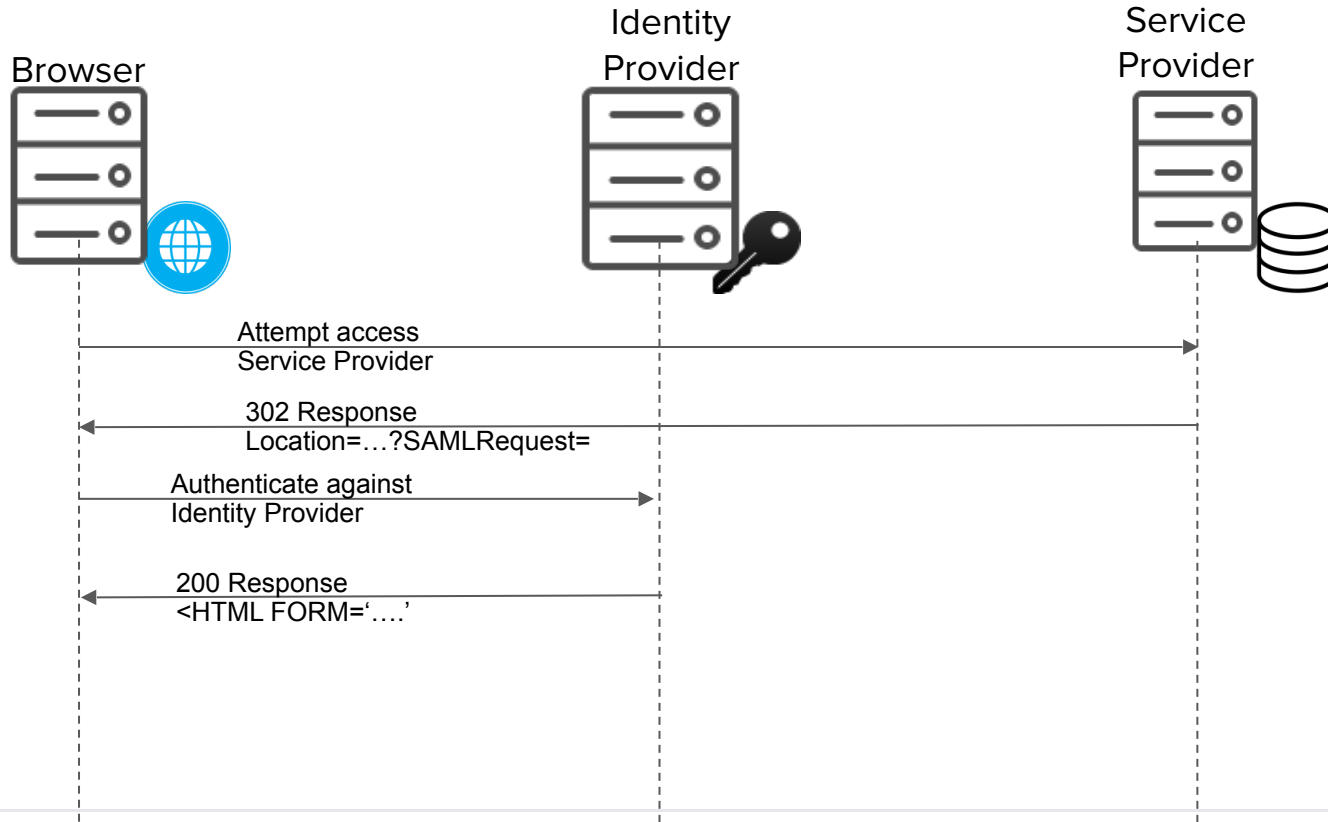
SP Initiated Login



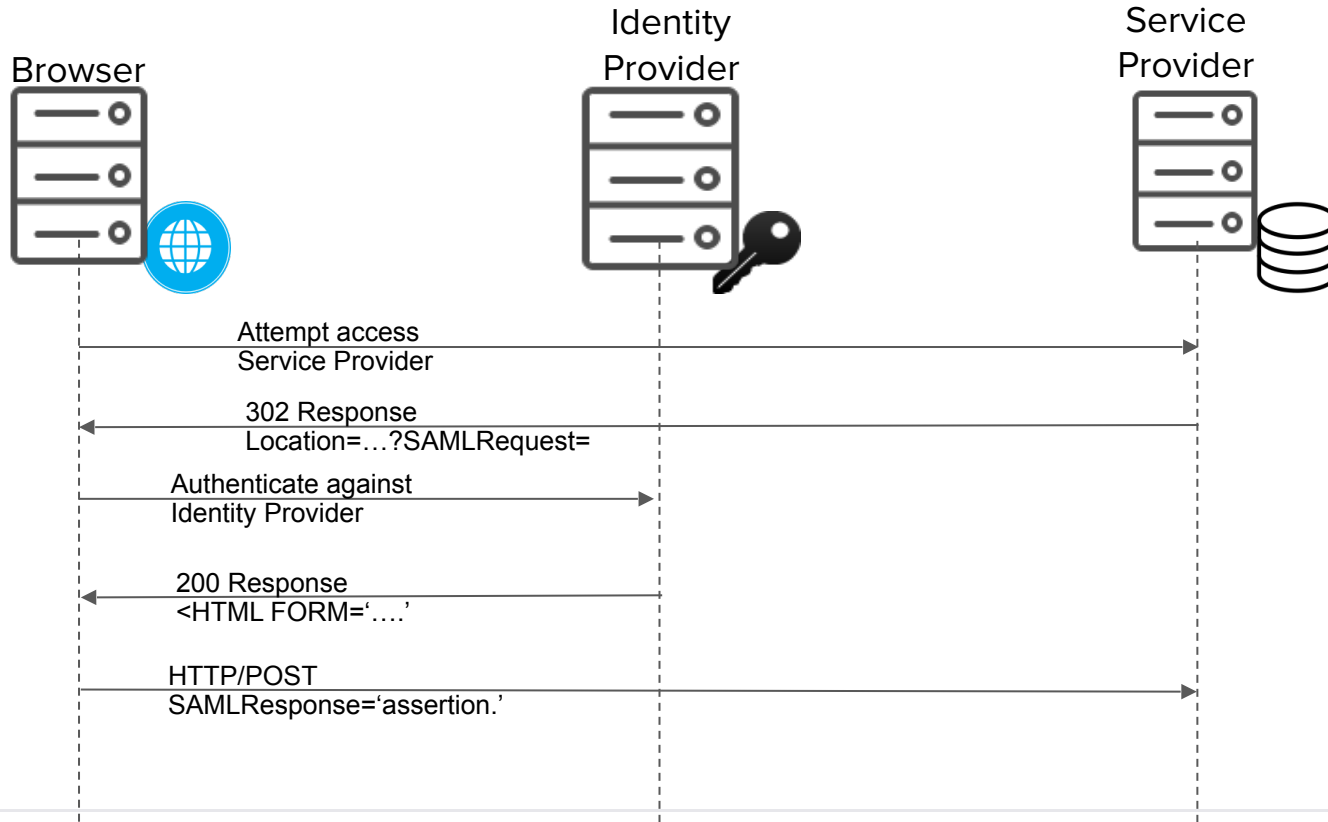
SP Initiated Login



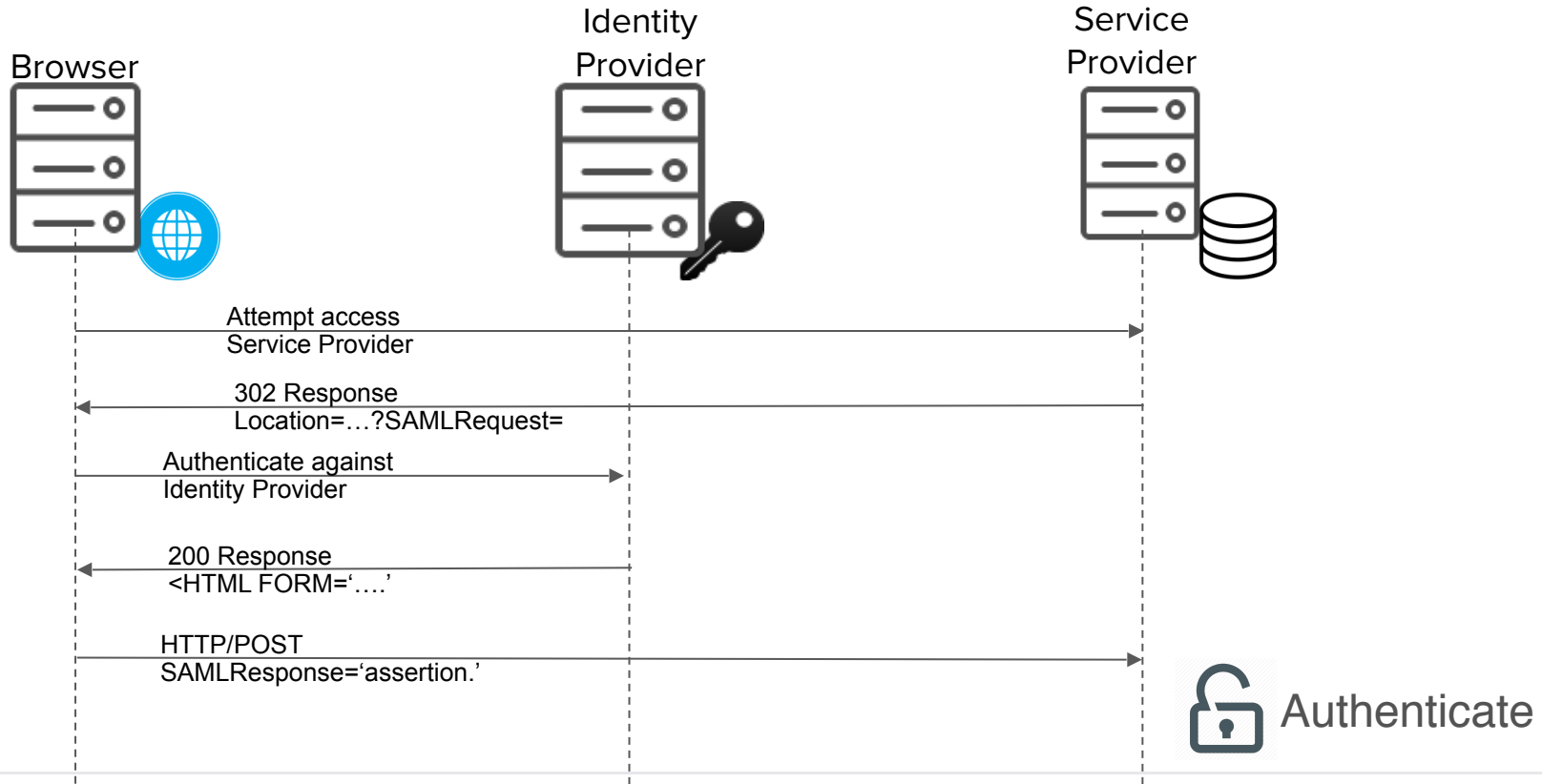
SP Initiated Login



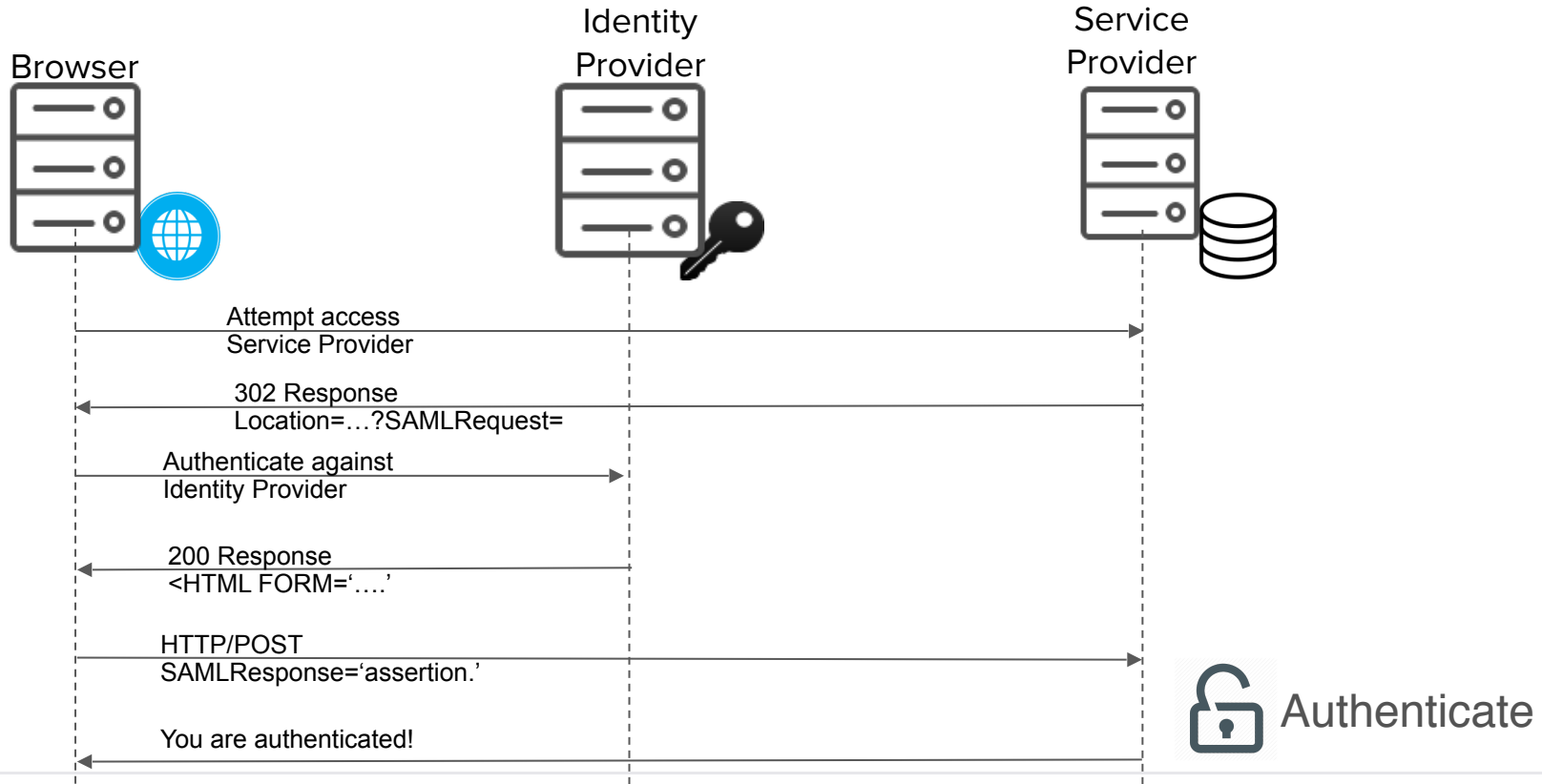
SP Initiated Login



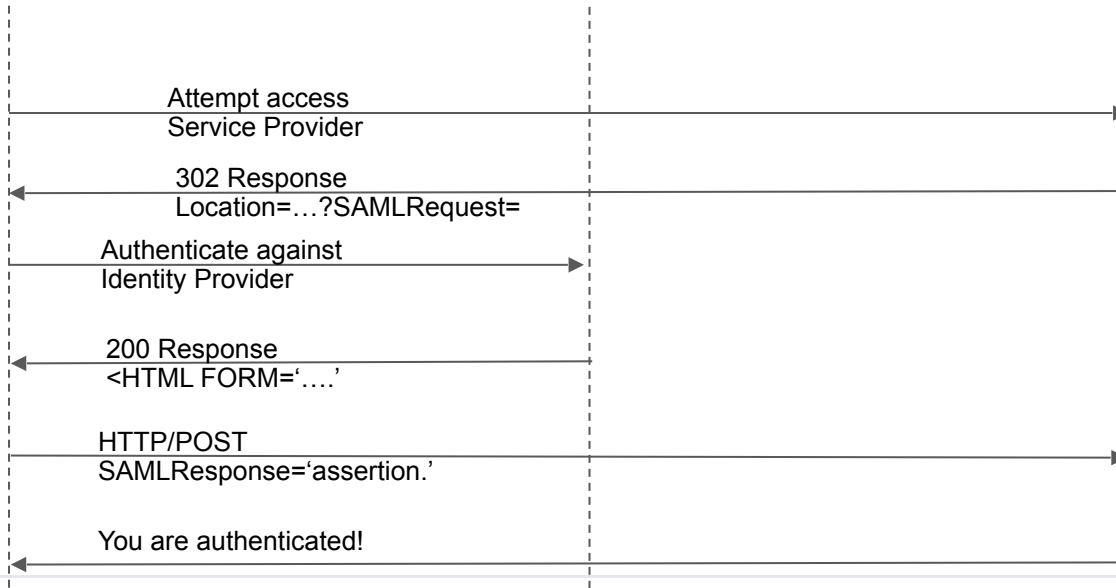
SP Initiated Login



SP Initiated Login



SP Initiated Login



Distributed Sign Off

Single Logout - SP Initiated

User



Service
Provider



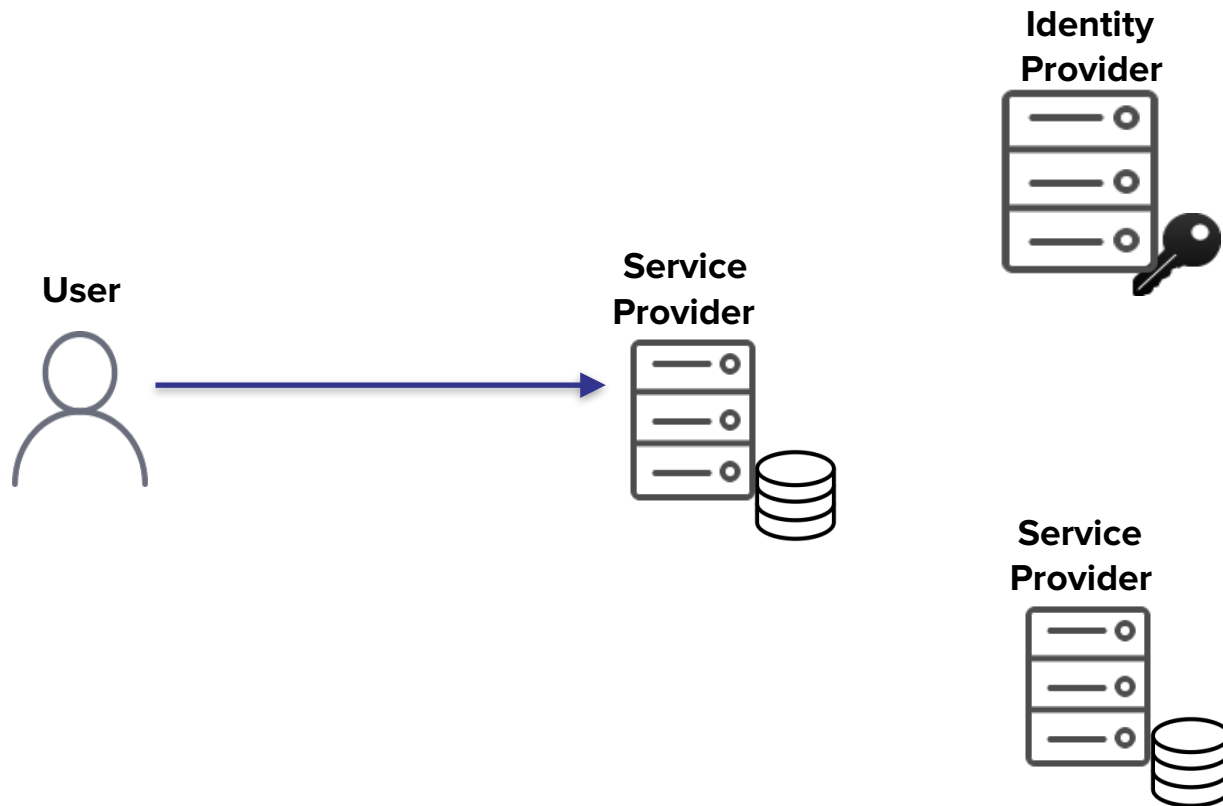
Identity
Provider



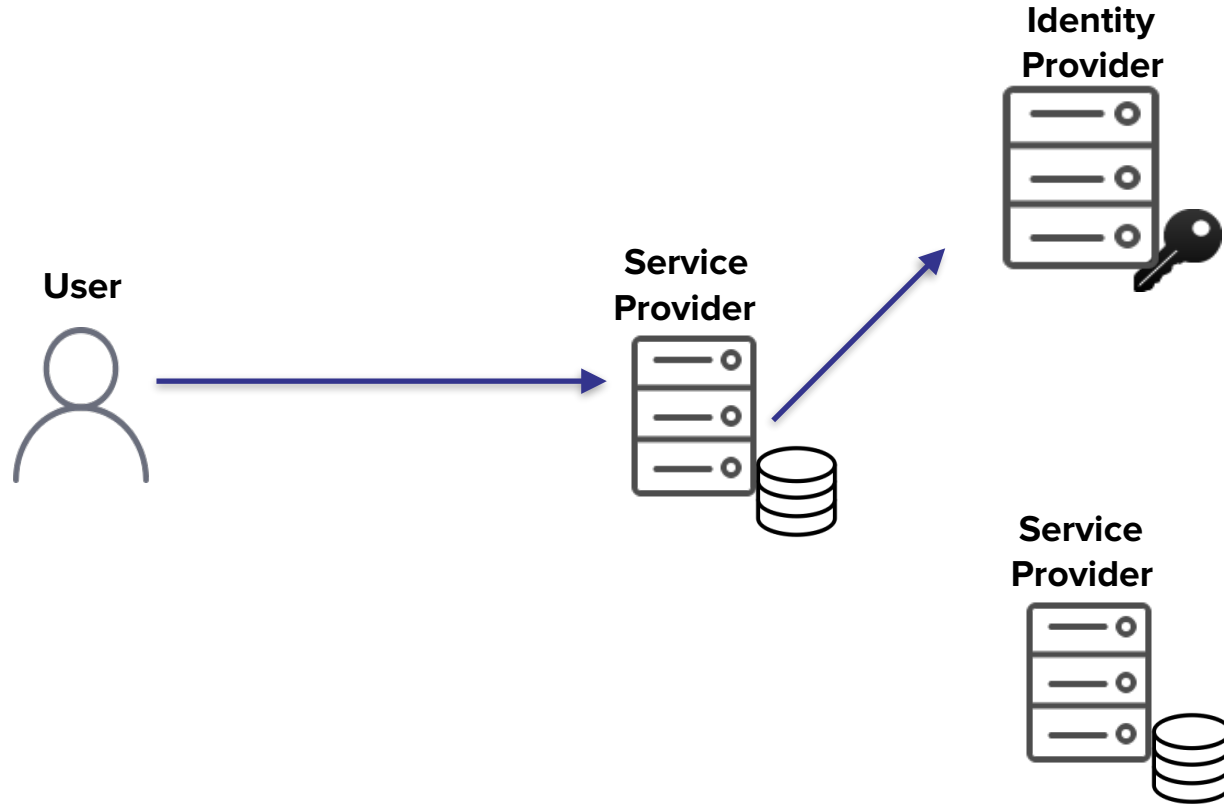
Service
Provider



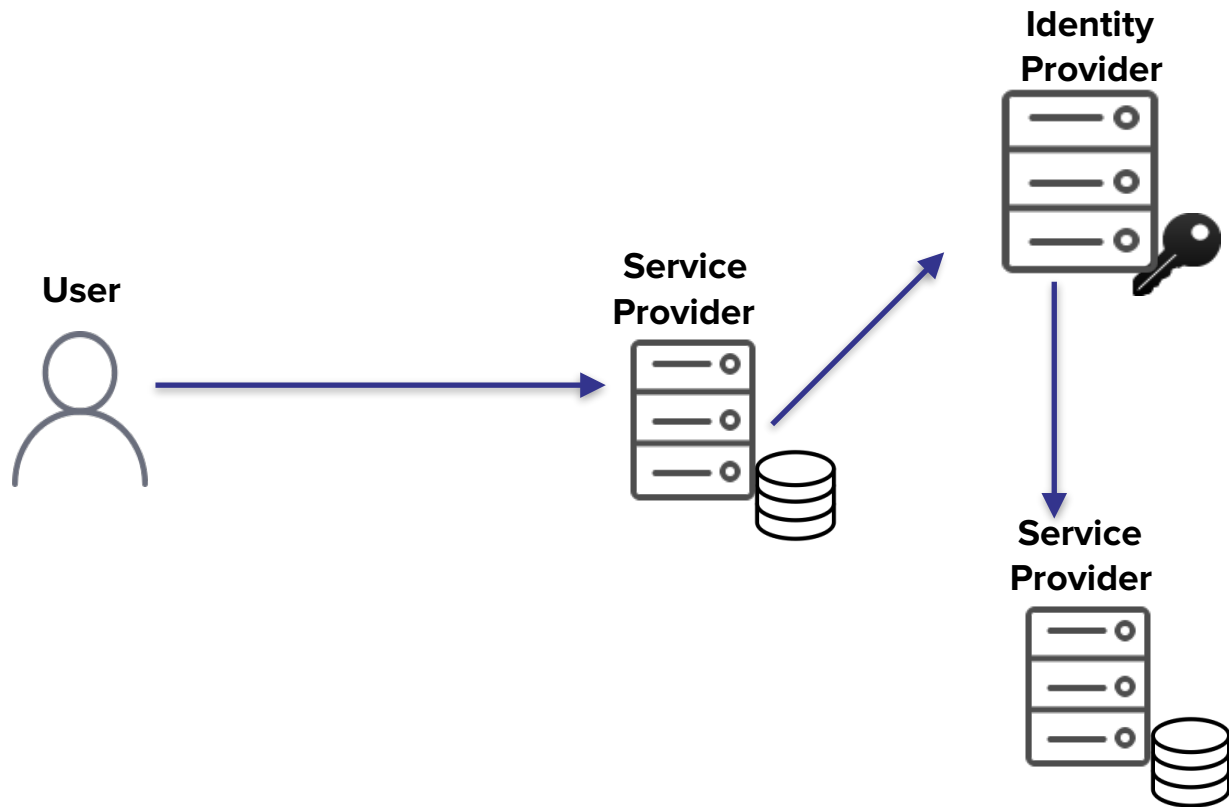
Single Logout - SP Initiated



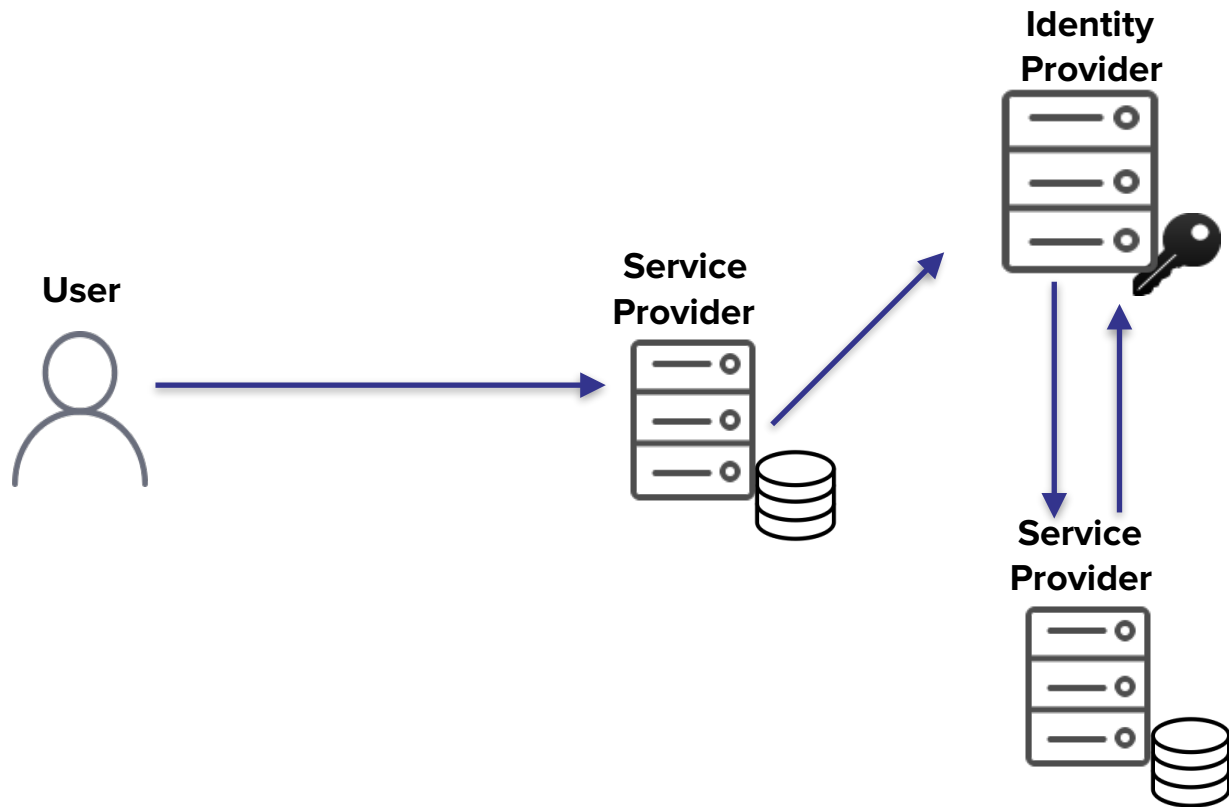
Single Logout - SP Initiated



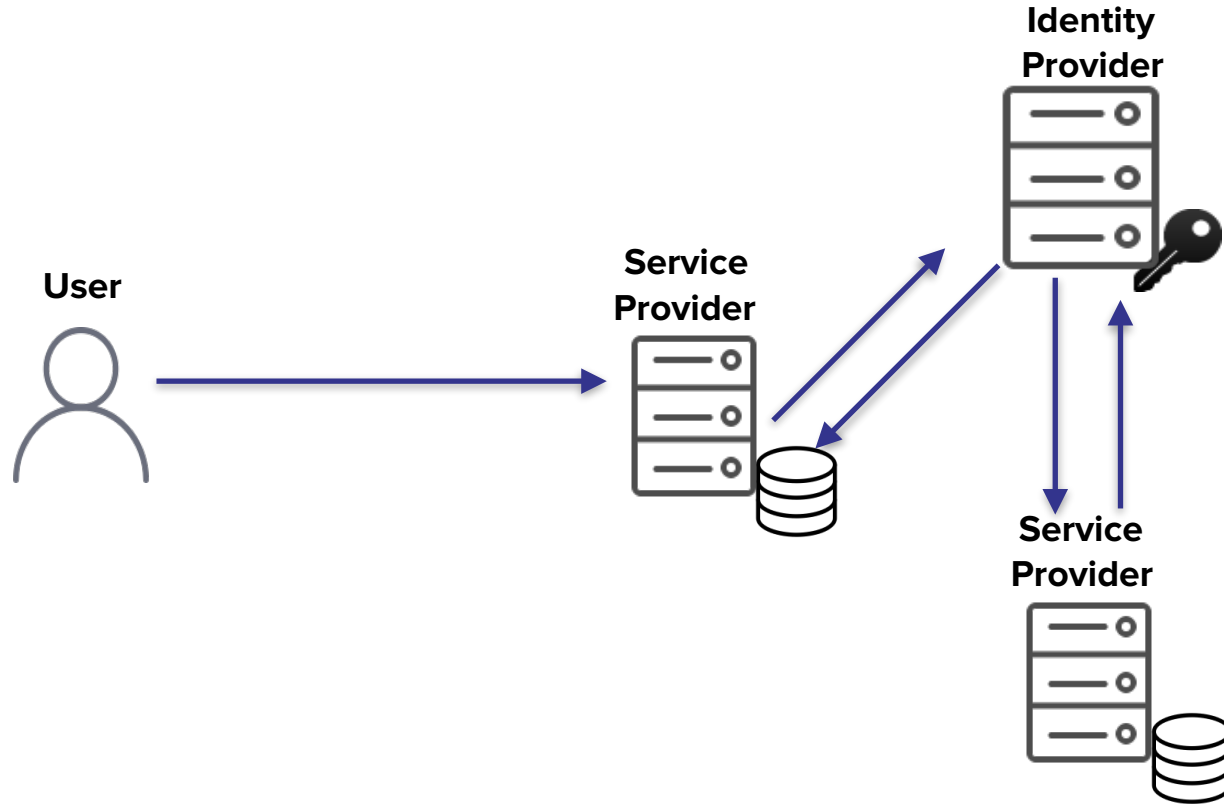
Single Logout - SP Initiated



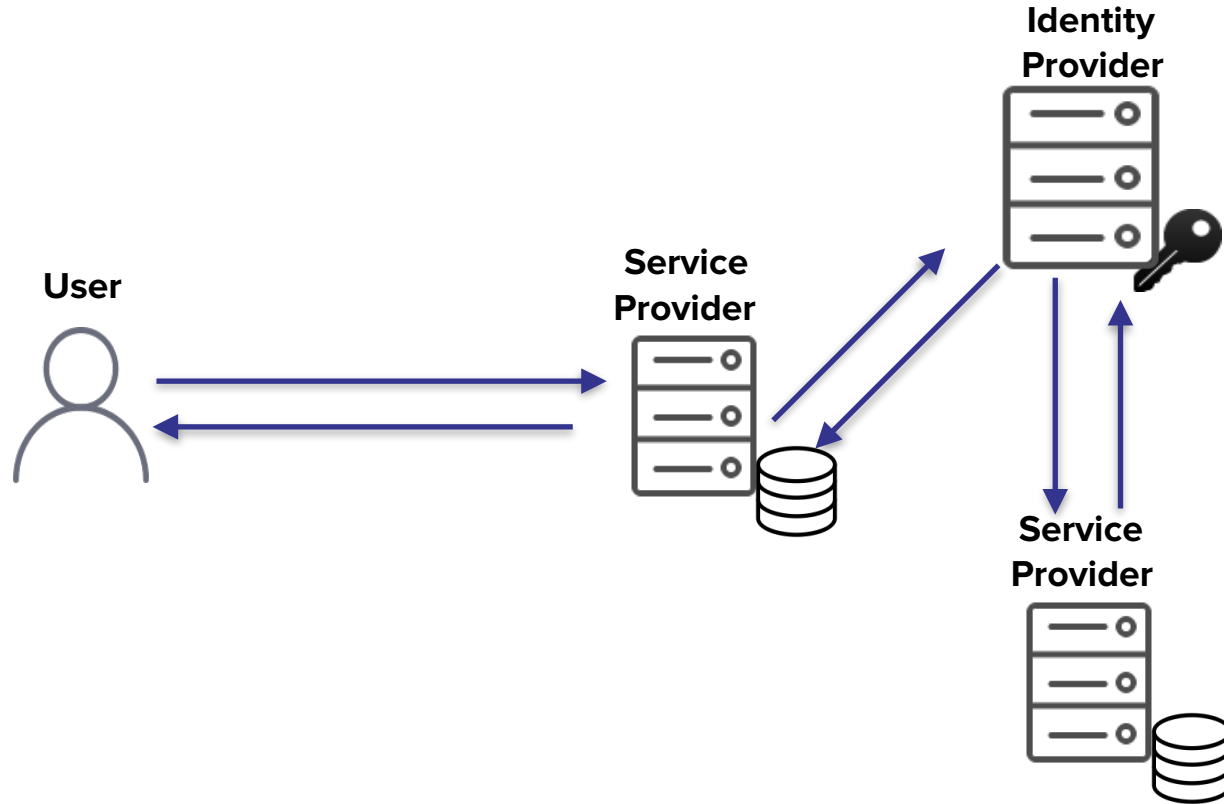
Single Logout - SP Initiated



Single Logout - SP Initiated



Single Logout - SP Initiated



Single Logout - No back channel

Browser



Service
Provider



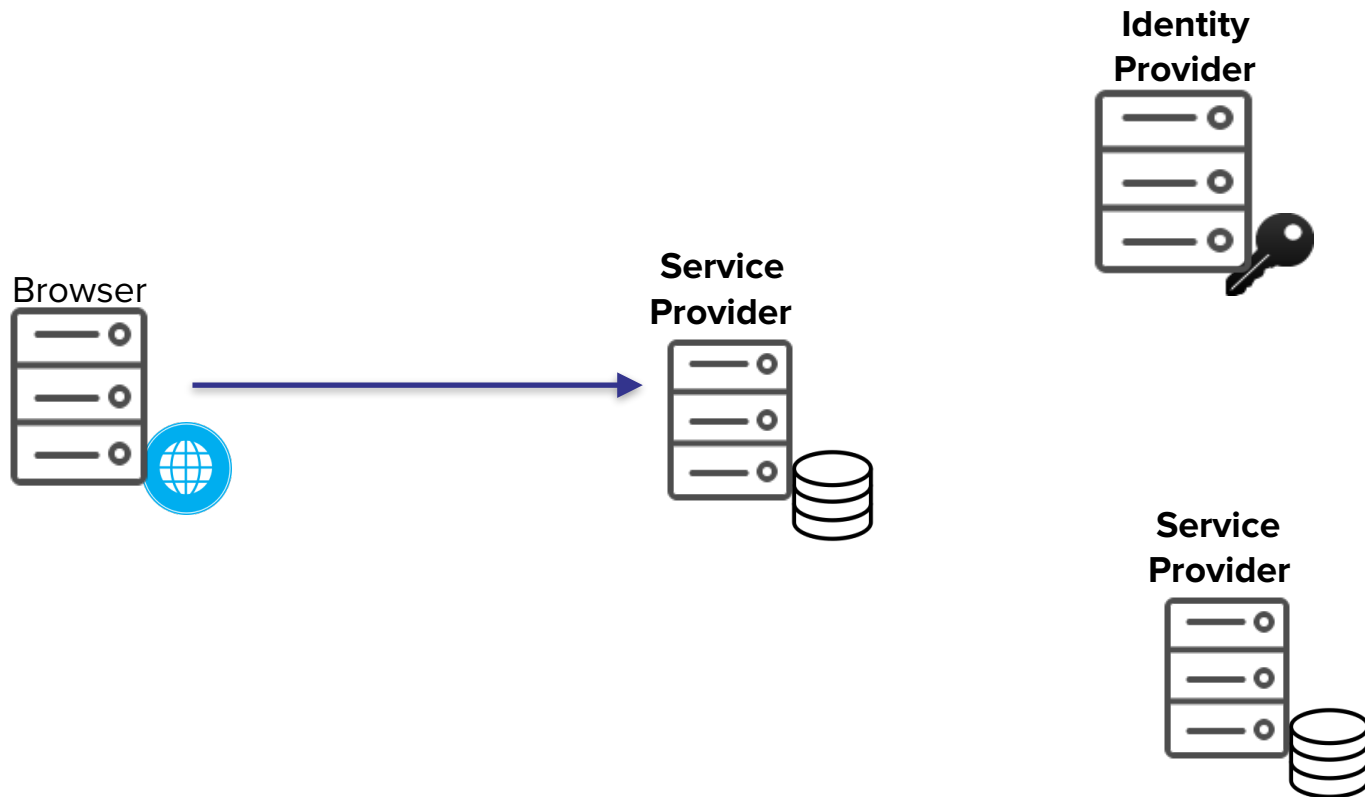
Identity
Provider



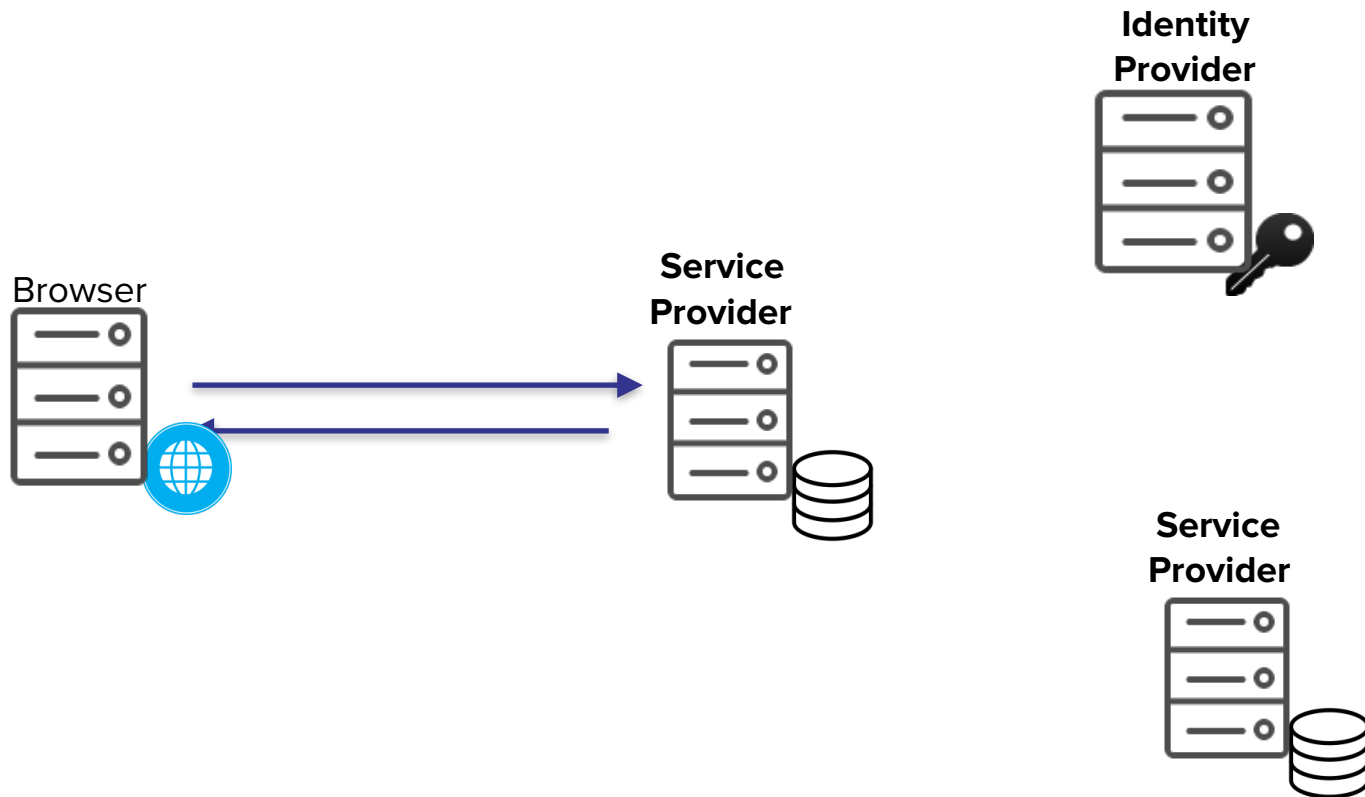
Service
Provider



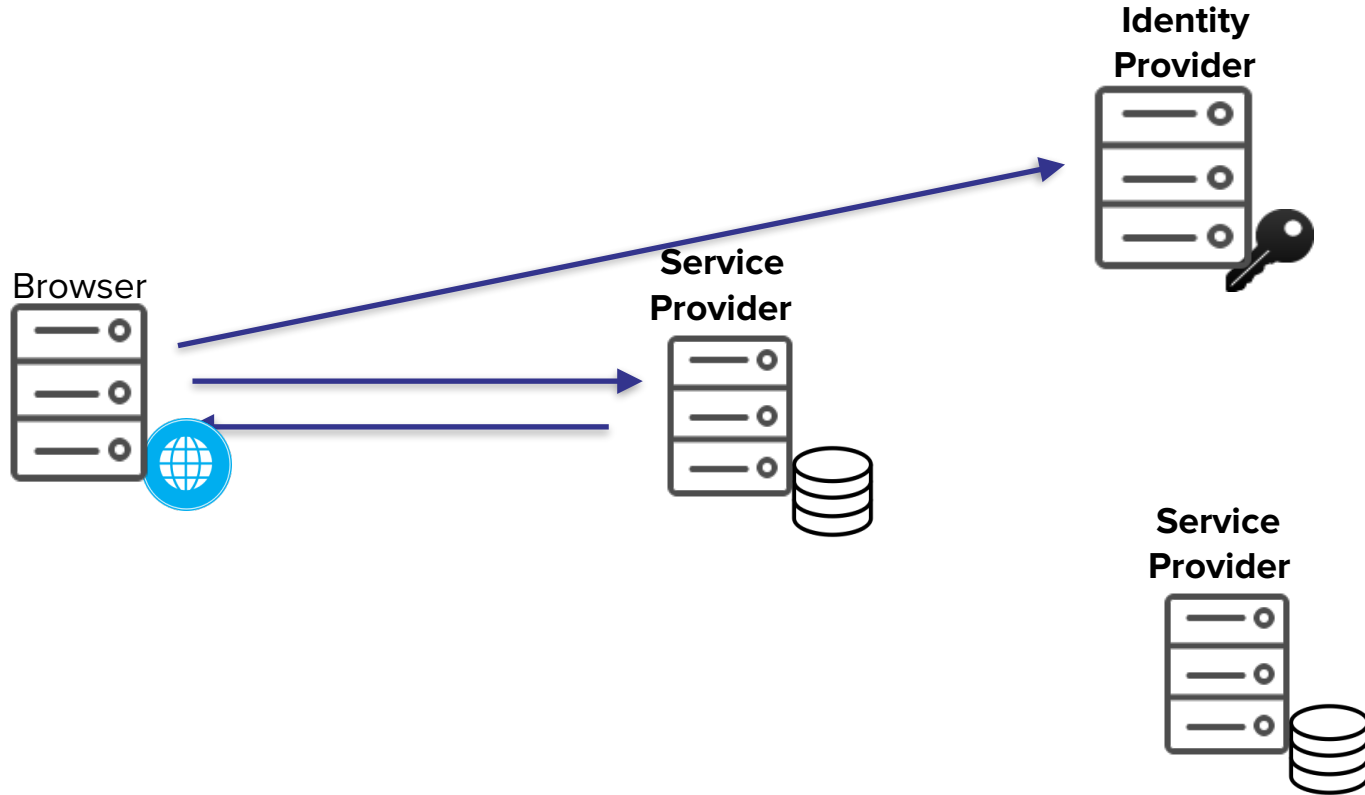
Single Logout - No back channel



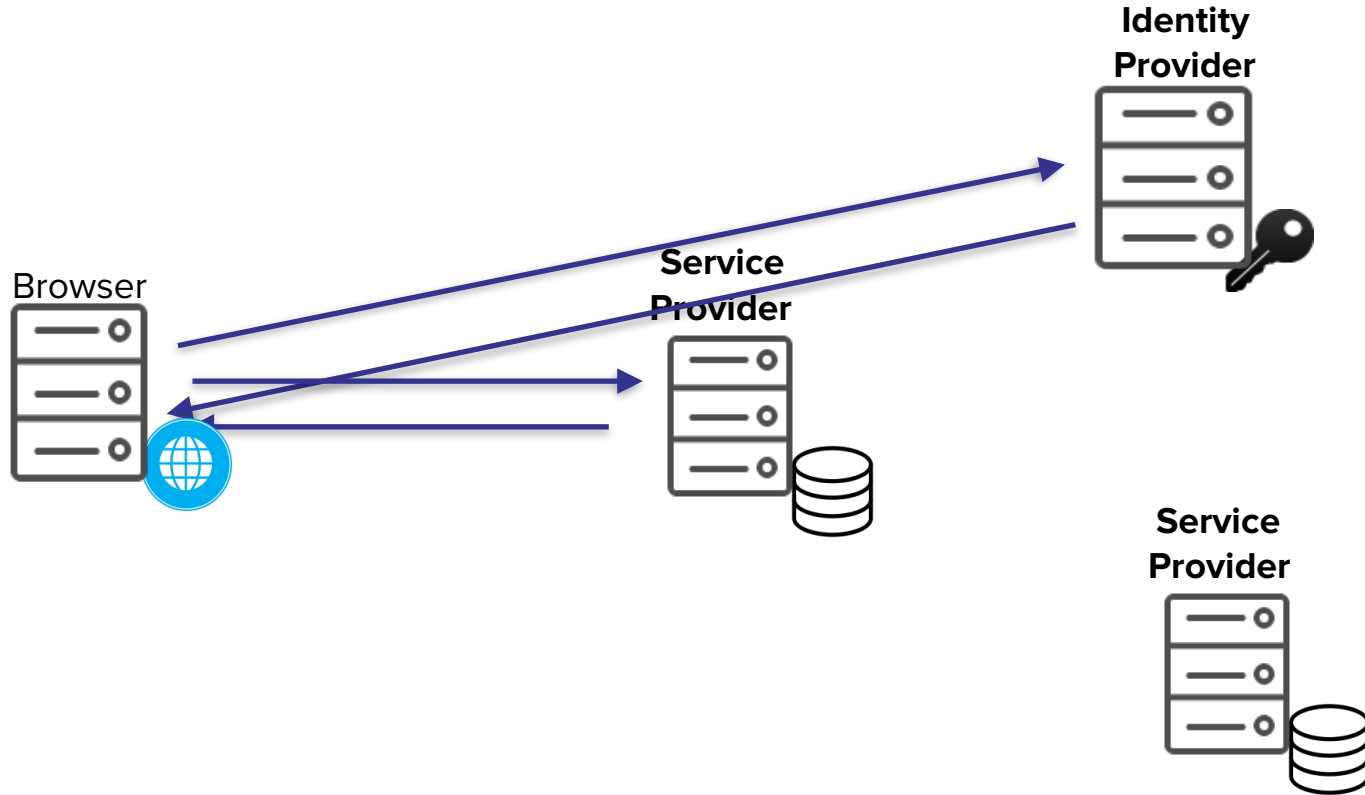
Single Logout - No back channel



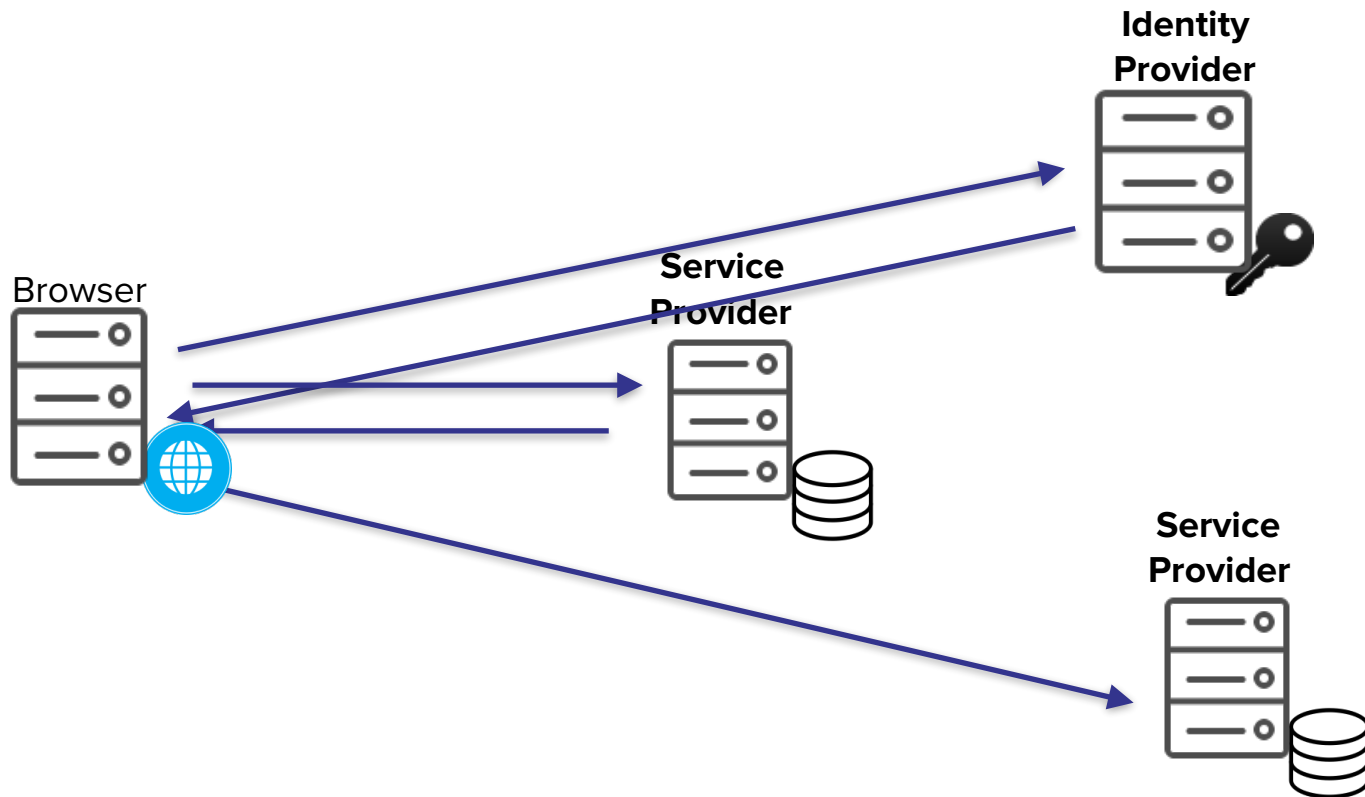
Single Logout - No back channel



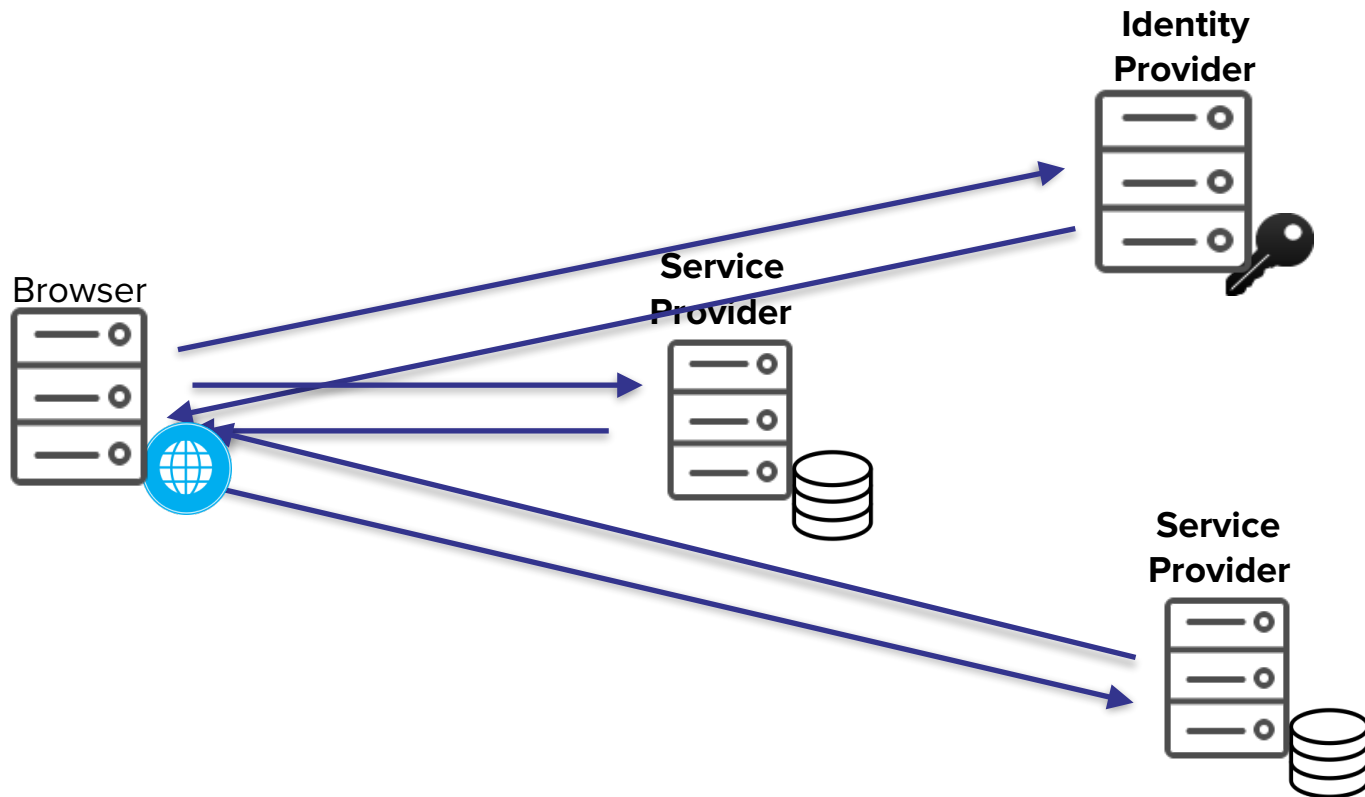
Single Logout - No back channel



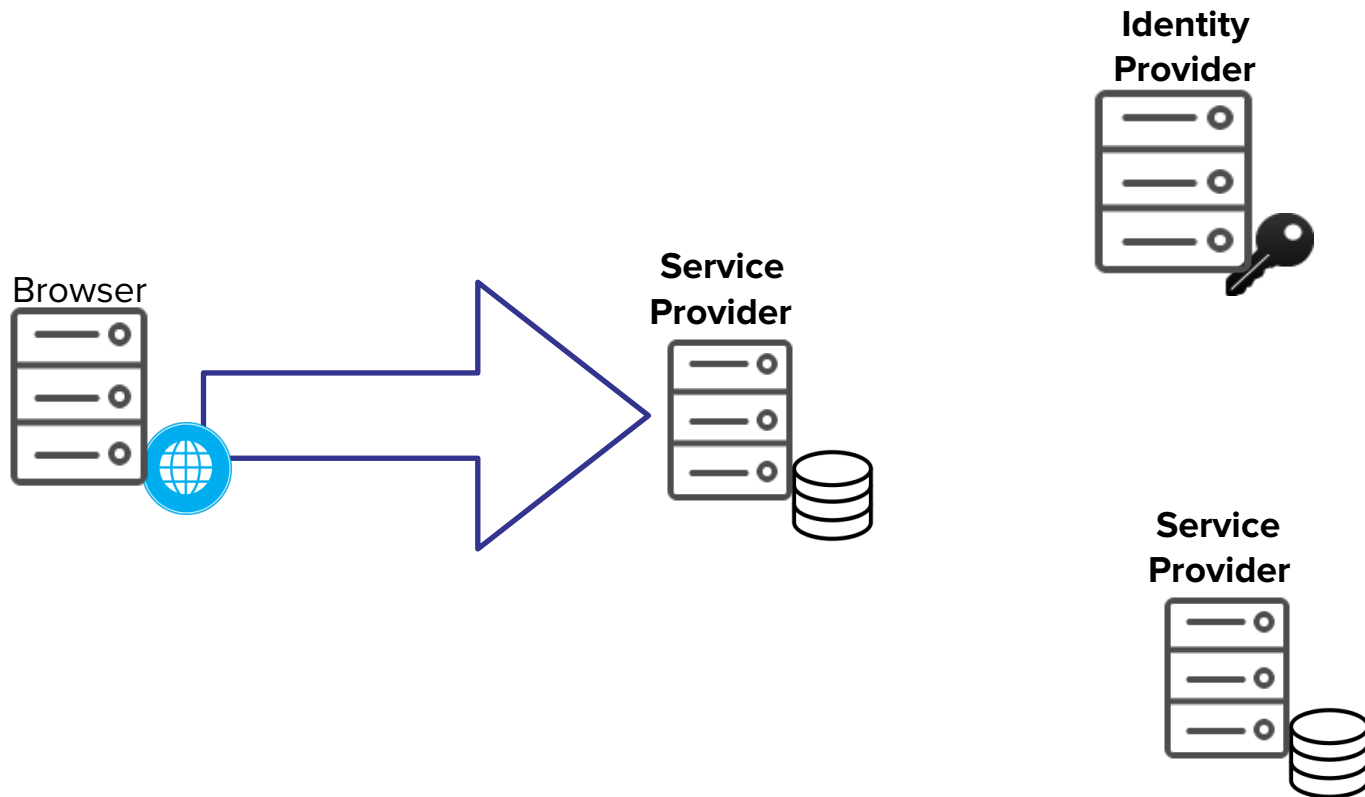
Single Logout - No back channel



Single Logout - No back channel



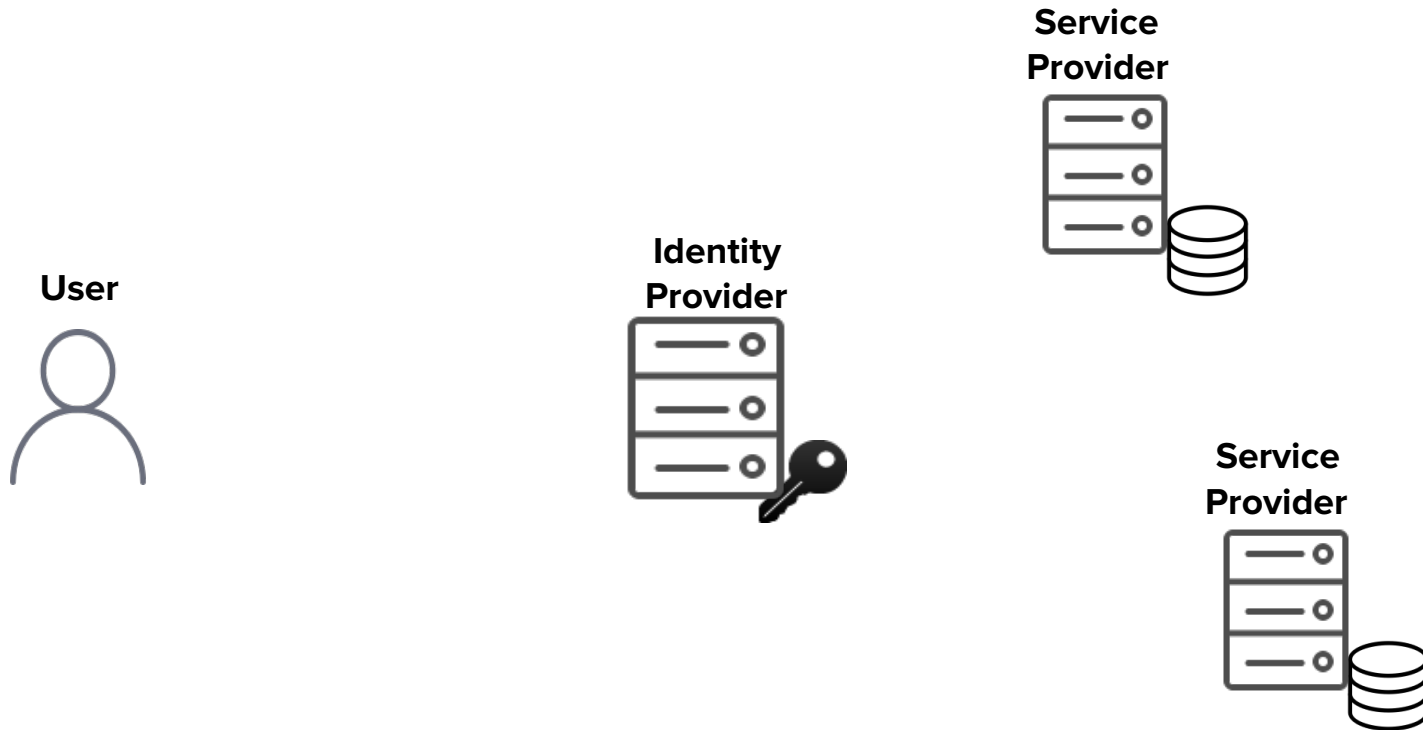
Single Logout - No back channel



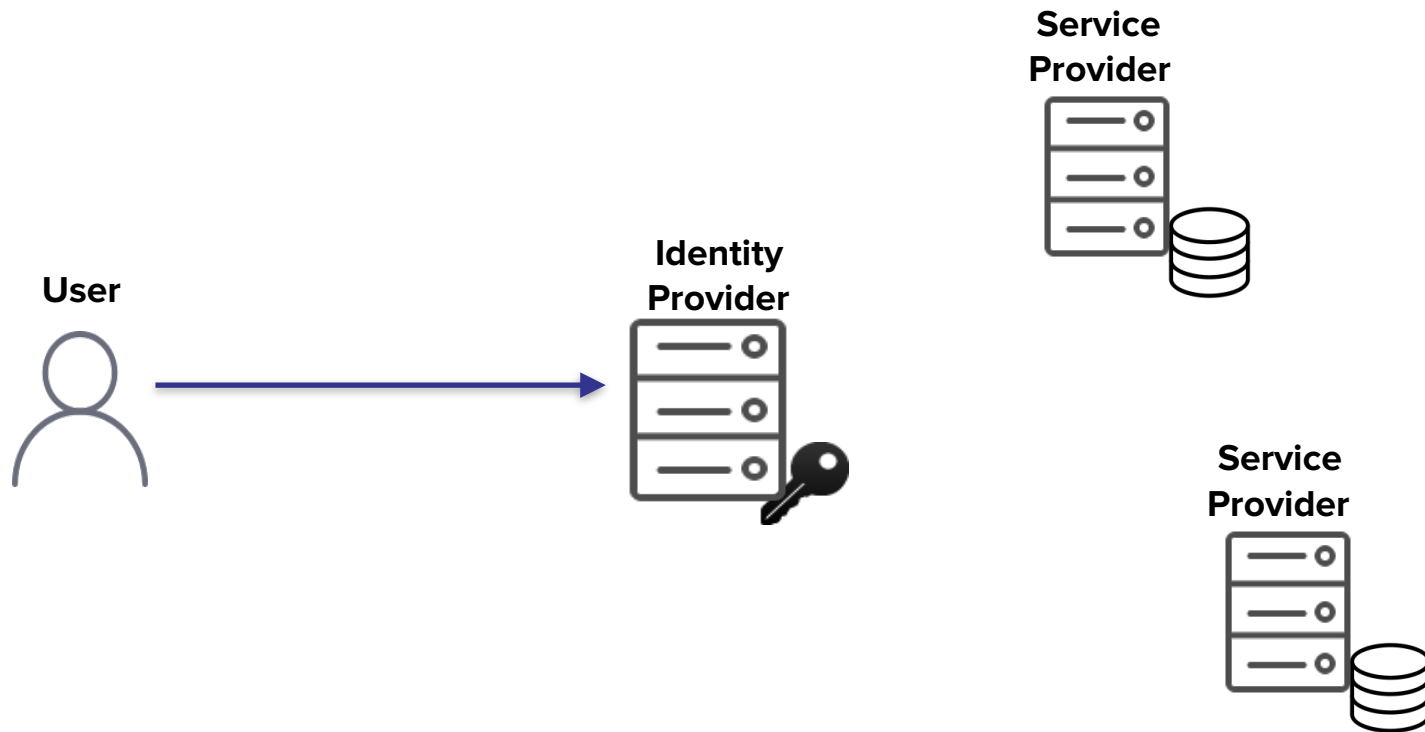
Demo - Distributed Sign Off

github.com/fhanik/springone2018

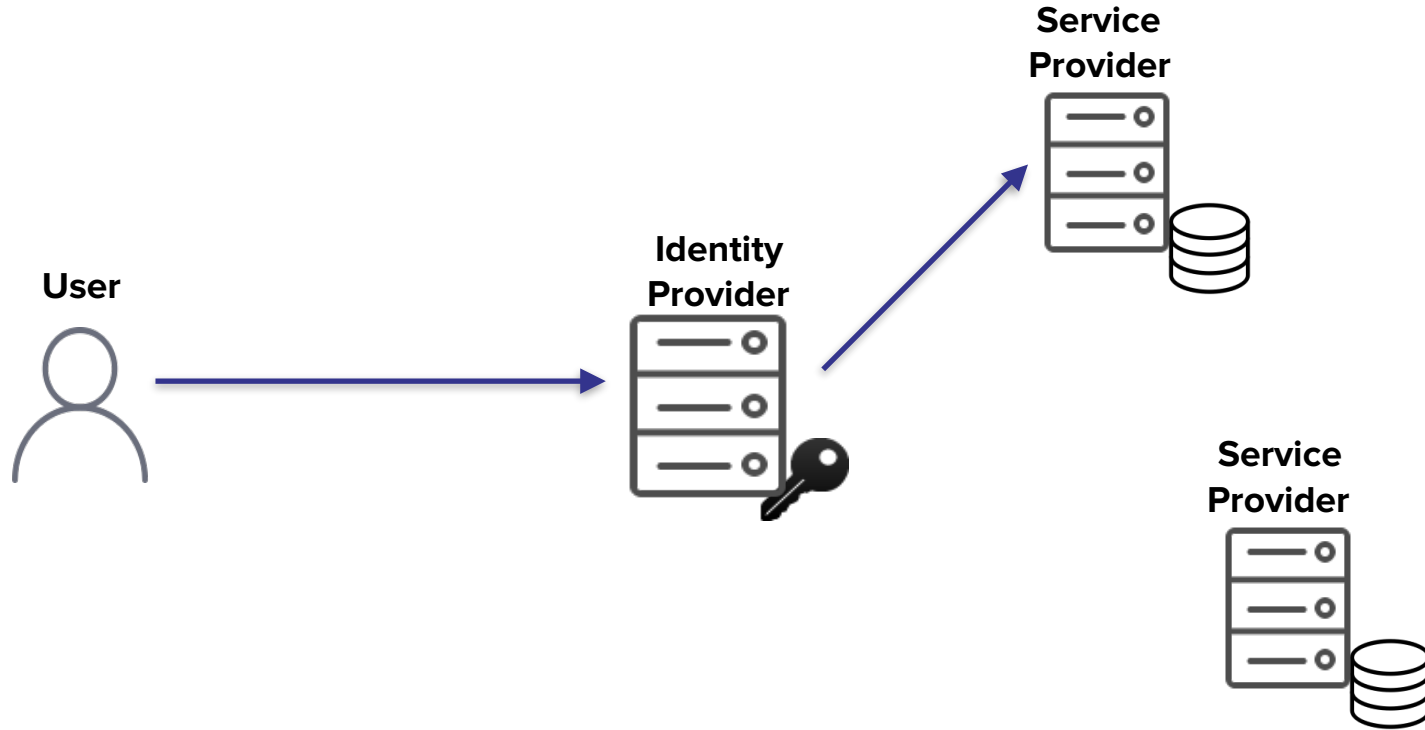
Single Logout - Initiate from the IDP



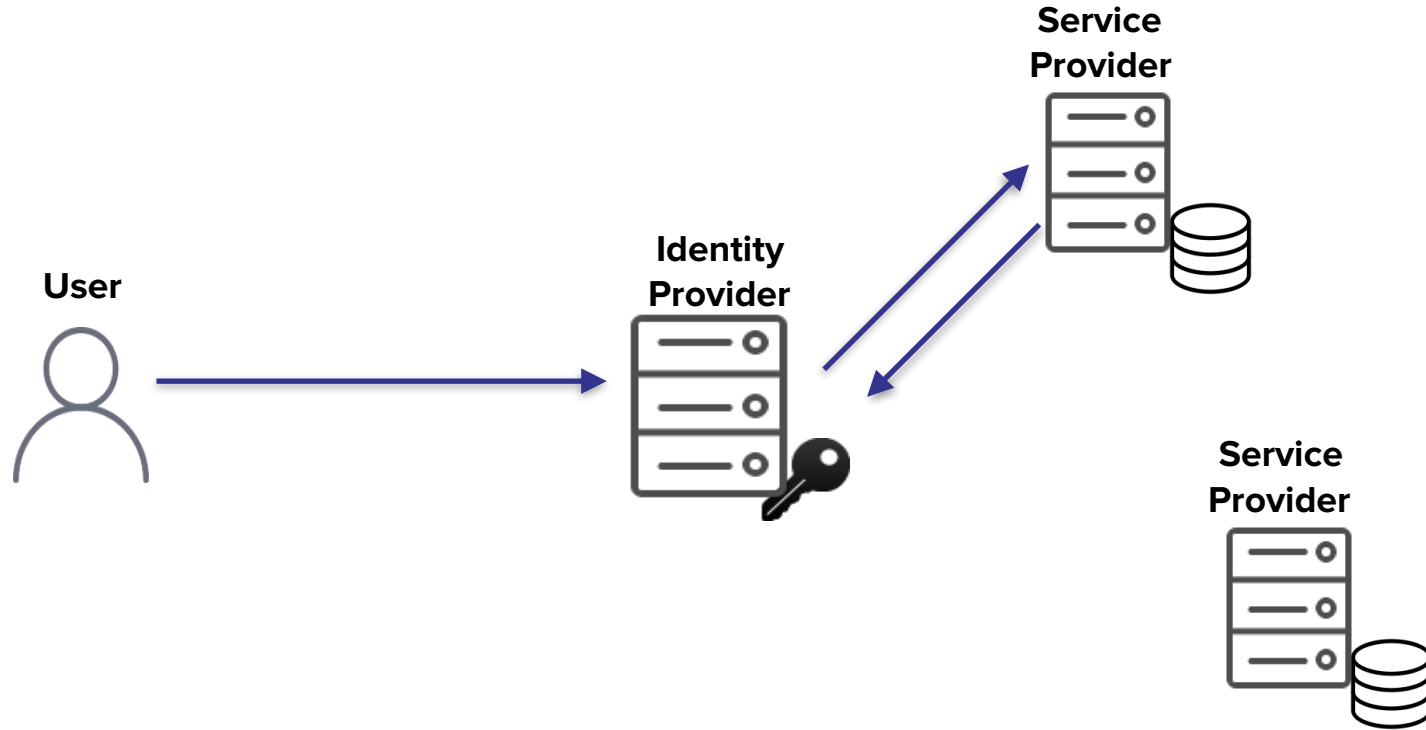
Single Logout - Initiate from the IDP



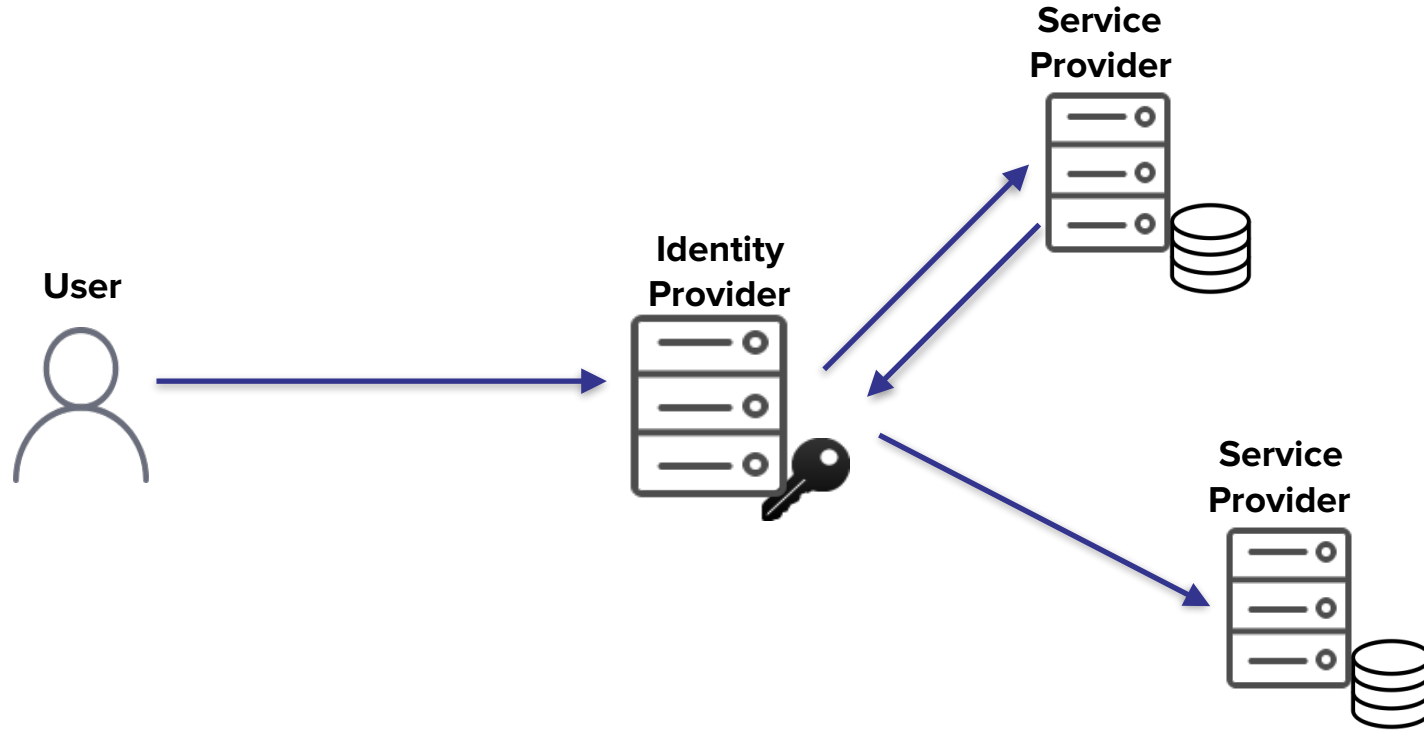
Single Logout - Initiate from the IDP



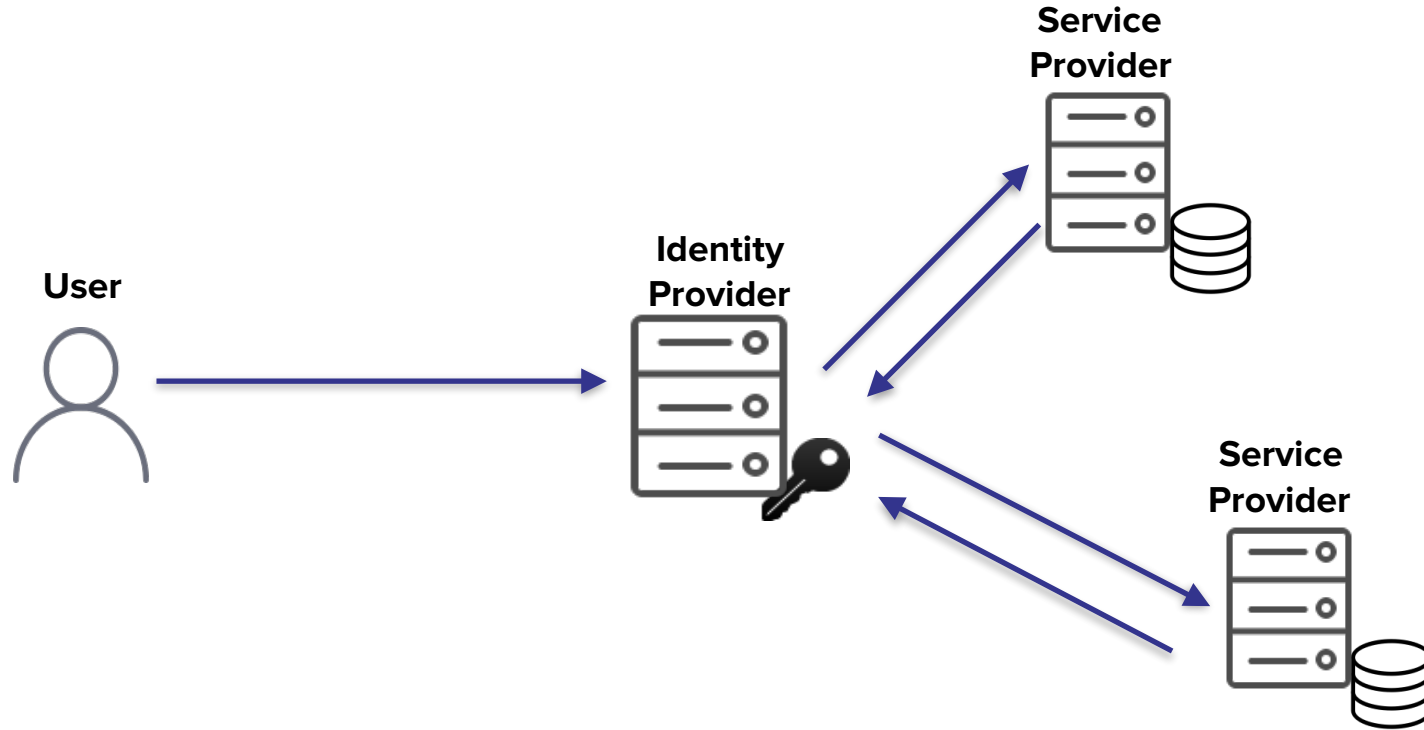
Single Logout - Initiate from the IDP



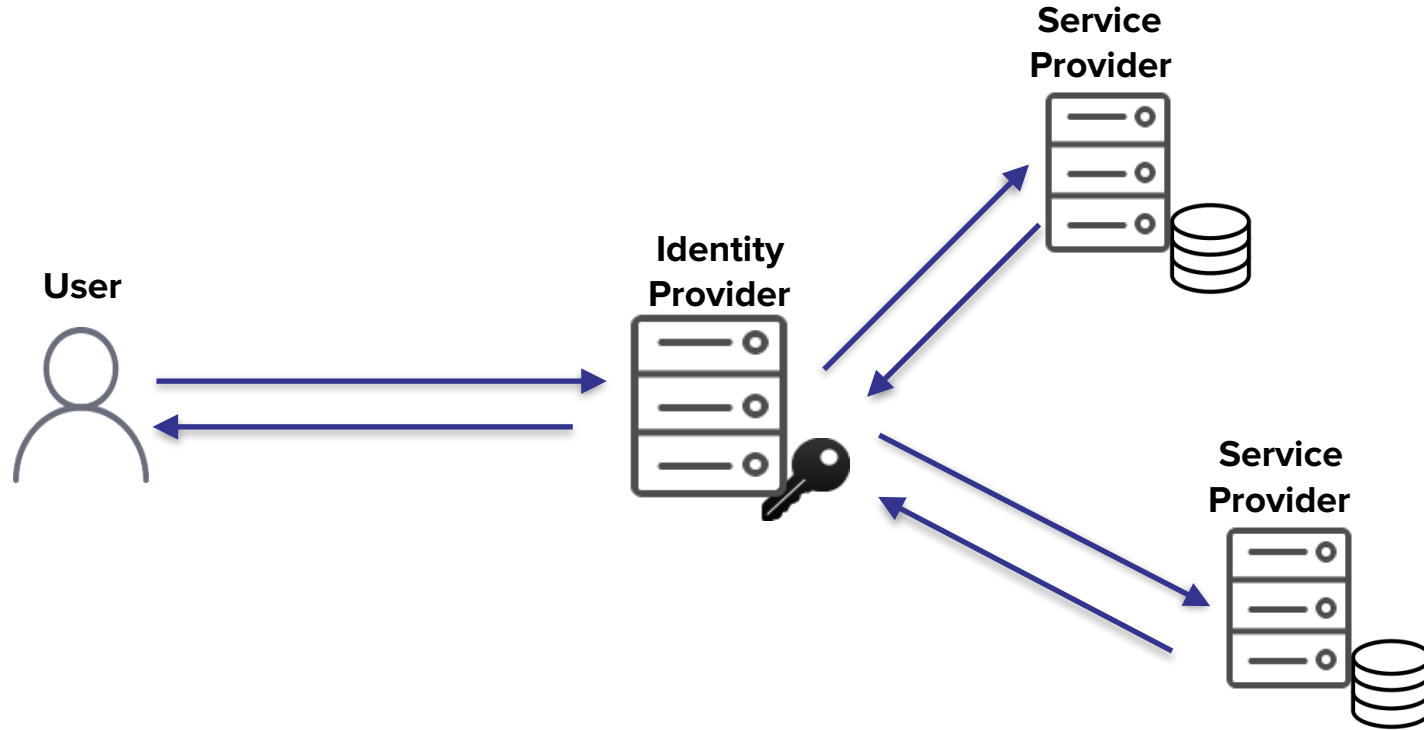
Single Logout - Initiate from the IDP



Single Logout - Initiate from the IDP



Single Logout - Initiate from the IDP



Other features of SAML

Assertion Queries

Attribute Queries

Artifact Resolution
(pass by reference)

Name Identifier
(management)

Name Identifier
(mapping)

SOAP / URI
(bindings)

RelayState

ECP Profile
(browserless)

Other features of SAML

Assertion Queries

Attribute Queries

**Artifact Resolution
(pass by reference)**

Name Identifier
(management)

Name Identifier
(mapping)

SOAP / URI
(bindings)

RelayState

ECP Profile
(browserless)

Other features of SAML

Assertion Queries

Attribute Queries

Artifact Resolution
(pass by reference)

**Name Identifier
(management)**

**Name Identifier
(mapping)**

SOAP / URI
(bindings)

RelayState

ECP Profile
(browserless)

Other features of SAML

Assertion Queries

Attribute Queries

Artifact Resolution
(pass by reference)

Name Identifier
(management)

Name Identifier
(mapping)

**SOAP / URI
(bindings)**

RelayState

**ECP Profile
(browserless)**

SAML vs. OpenID Connect

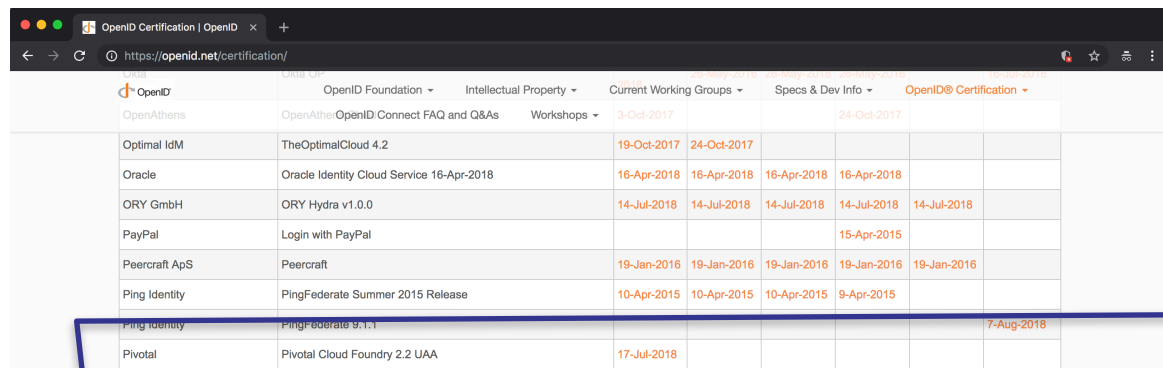
	SAML	OpenID Connect
Timeline	2002-2012	2010-2017
Protocol & Formats	HTTP with XML	REST with JSON
Relevance	Prevalent standard in enterprises	Born in the social age. Being adopted by Cloud Providers - Microsoft/Salesforce/Google
User Claims	SAML Assertion	ID Token
Backchannel	Attribute Query	/userinfo endpoint
Browserless/Native	ECP Profile	OAuth Resource Owner Password Grant
Inter-Op	Token exchanges to convert SAML-OpenID Connect and vice-versa	

UAA & Pivotal SSO are OpenID Connect Certified Providers !!

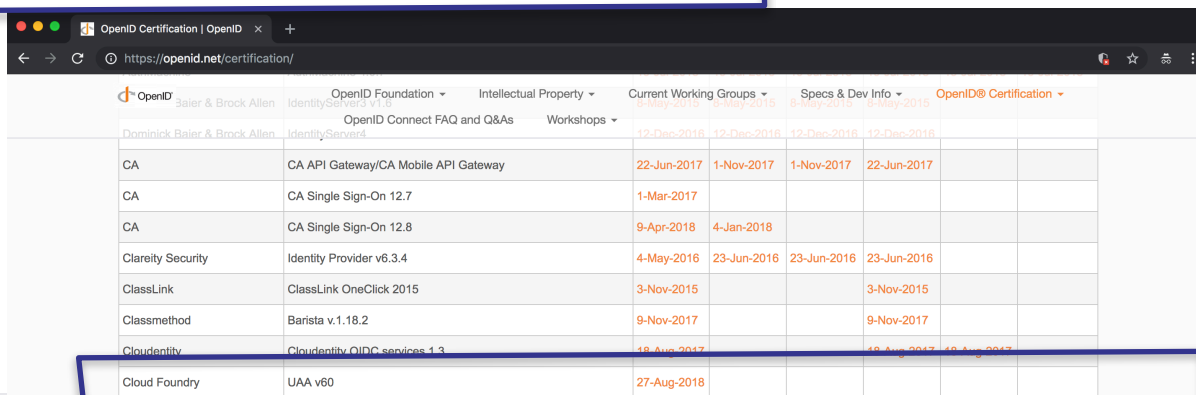
	OpenID	OpenID Foundation	Intellectual Property	Current Working Groups	Specs & Dev Info	OpenID Certification
	OpenAthens	OpenID Connect FAQ and Q&As	Workshops	3-Oct-2017	24-Oct-2017	
	Optimal IdM	TheOptimalCloud 4.2		19-Oct-2017	24-Oct-2017	
	Oracle	Oracle Identity Cloud Service 16-Apr-2018		16-Apr-2018	16-Apr-2018	16-Apr-2018
	ORY GmbH	ORY Hydra v1.0.0		14-Jul-2018	14-Jul-2018	14-Jul-2018
	PayPal	Login with PayPal				15-Apr-2015
	Peercraft ApS	Peercraft		19-Jan-2016	19-Jan-2016	19-Jan-2016
	Ping Identity	PingFederate Summer 2015 Release		10-Apr-2015	10-Apr-2015	9-Apr-2015
	Ping Identity	PingFederate 9.1.1				7-Aug-2018
	Pivotal	Pivotal Cloud Foundry 2.2 UAA		17-Jul-2018		

OpenID		OpenID Foundation	Intellectual Property	Current Working Groups	Specs & Dev Info	OpenID® Certification
Baier & Brock Allen		IdentityServer v1.6	OpenID Connect FAQ and Q&As	8-May-2015	8-May-2015	8-May-2015
Dominic Baier & Brock Allen		IdentityServer	Workshops	12-Dec-2016	12-Dec-2016	12-Dec-2016
CA	CA API Gateway/CA Mobile API Gateway	22-Jun-2017	1-Nov-2017	1-Nov-2017	22-Jun-2017	
CA	CA Single Sign-On 12.7	1-Mar-2017				
CA	CA Single Sign-On 12.8	9-Apr-2018	4-Jan-2018			
Clareity Security	Identity Provider v6.3.4	4-May-2016	23-Jun-2016	23-Jun-2016	23-Jun-2016	
ClassLink	ClassLink OneClick 2015	3-Nov-2015			3-Nov-2015	
Classmethod	Barista v.1.18.2	9-Nov-2017			9-Nov-2017	
Cloudentity	Cloudentity OIDC services 1.3	18-Aug-2017			18-Aug-2017	18-Aug-2017
Cloud Foundry	UAA v60	27-Aug-2018				

UAA & Pivotal SSO are OpenID Connect Certified Providers !!



	OpenID Foundation	Intellectual Property	Current Working Groups	Specs & Dev Info	OpenID® Certification
OpenID	OpenID Foundation	OpenID Connect FAQ and Q&As	Workshops	3-Oct-2017	24-Oct-2017
Optimal IdM	TheOptimalCloud 4.2		19-Oct-2017	24-Oct-2017	
Oracle	Oracle Identity Cloud Service 16-Apr-2018		16-Apr-2018	16-Apr-2018	16-Apr-2018
ORY GmbH	ORY Hydra v1.0.0		14-Jul-2018	14-Jul-2018	14-Jul-2018
PayPal	Login with PayPal			15-Apr-2015	
Peercraft ApS	Peercraft		19-Jan-2016	19-Jan-2016	19-Jan-2016
Ping Identity	PingFederate Summer 2015 Release		10-Apr-2015	10-Apr-2015	9-Apr-2015
Ping Identity	PingFederate 9.1.1				7-Aug-2018
Pivotal	Pivotal Cloud Foundry 2.2 UAA		17-Jul-2018		



	OpenID Foundation	Intellectual Property	Current Working Groups	Specs & Dev Info	OpenID® Certification
CA	CA API Gateway/CA Mobile API Gateway		22-Jun-2017	1-Nov-2017	1-Nov-2017
CA	CA Single Sign-On 12.7		1-Mar-2017		
CA	CA Single Sign-On 12.8		9-Apr-2018	4-Jan-2018	
Clareity Security	Identity Provider v6.3.4		4-May-2016	23-Jun-2016	23-Jun-2016
ClassLink	ClassLink OneClick 2015		3-Nov-2015		3-Nov-2015
Classmethod	Barista v.1.18.2		9-Nov-2017		9-Nov-2017
Cloudidentity	Cloudidentity OIDC versions 1.3		18-Aug-2017		18-Aug-2017
Cloud Foundry	UAA v60		27-Aug-2018		

Recap

- Identity Provider aka Asserting Party
- Service Provider aka Relying Party is the Application
- Single Sign On / Single Sign Off most common Profiles

Recap

- Today HTTP Redirect/Post are preferred bindings
- Back channel (IDP / SP) is not that common
- Similarities between OIDC and SAML

SpringOne Platform by Pivotal

Thank You

Your Super Heroes: Sree Tummidu & Filip Hanik