Identity Provider & Service Provider

Presentation by

Nabeel Ahmad

and

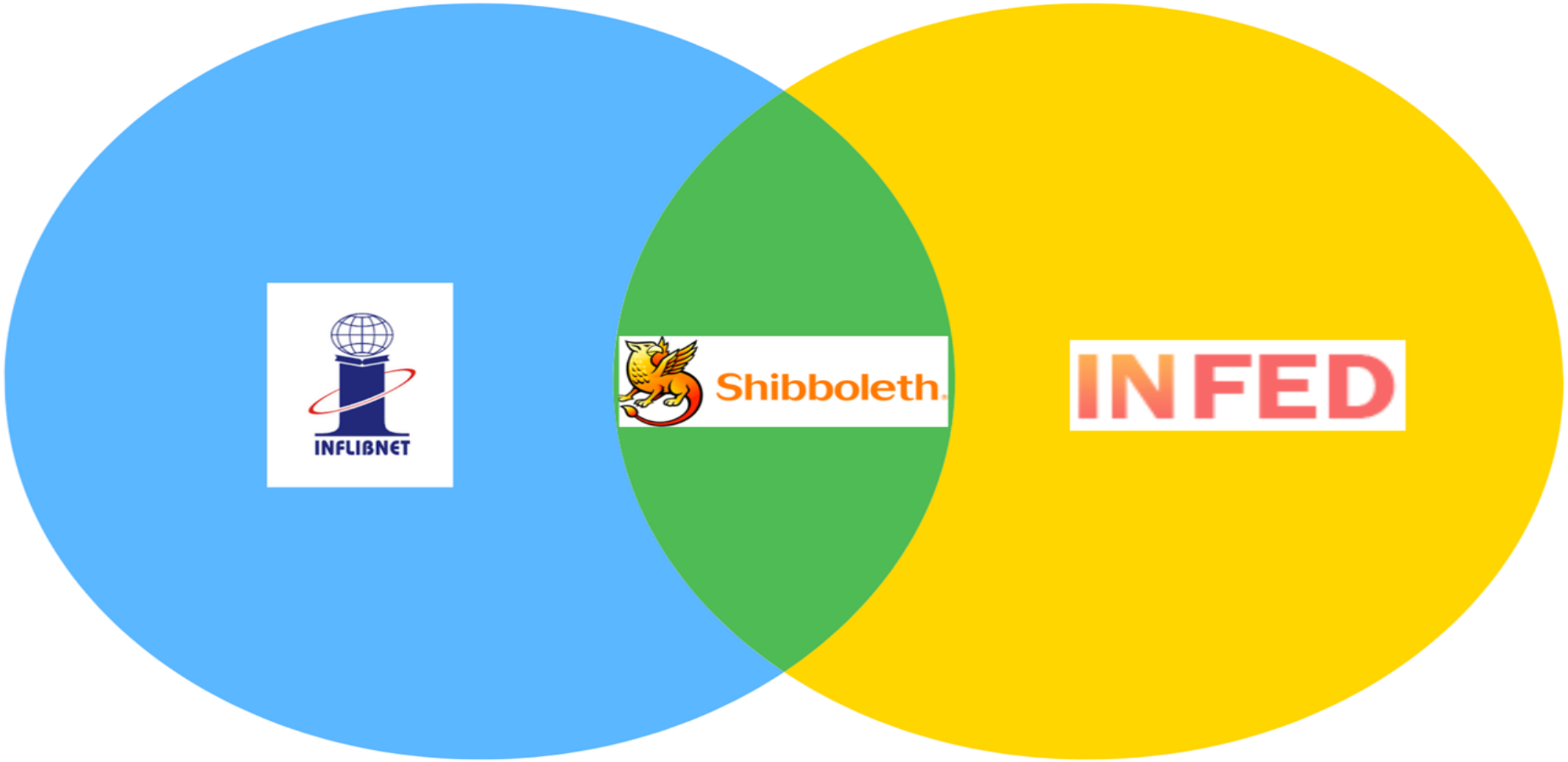
Aravind Nair

- Information and Library Network (INFLIBNET) Centre, Gandhinagar is an autonomous Inter-University Centre of UGC (Ministry of Education, Govt. of India).
- Initiated by the UGC in March 1991 as a project under the IUCAA, it became an autonomous Inter-University Centre in June 1996.
- INFLIBNET modernises university libraries in India to maximise information use. INFLIBNET aims to promote intellectual communication in India.

INFED

- INDIAN Access Management Federation (INFED) was established by INFLIBNET to coordinate with in the process of implementing a user authentication and access control mechanism.
- The INDIAN Access Management Federation (INFED) oversees the management of trust between all parties, including publishers and member institutions.
- In order to authenticate authorised users from institutions, the INDIAN Access Management Federation (INFED) has embraced Shibboleth, an open source programme based on standards.

- Shibboleth is a standards-based, open-source SSO solution that allows various institutions to access network services in a federation and it uses (SAML).
- Shibboleth is a open-source software package that authenticates authorised users using an organization's internal identity and access management system.
- it establishes protocols for the safe exchange of identity information between institutions and service providers.
- Shibboleth builds rust relationship, providing federated, single sign-on access for end-users.


INFLIBNET
Shibboleth
INFED

Single Sign-On (SSO) System

Single sign-on is an authentication scheme that allows a user to log in with a single ID to any of several related, yet independent, software systems.
True single sign-on allows the user to log in once and access services without re-entering authentication factors.
Reference (How its works): https://www.onelogin.com/learn/how-single-sign-on-works

LDAP (Lightweight Directory Access Protocol)

LDAP, the Lightweight Directory Access Protocol, is a mature, flexible, and well supported standards-based mechanism for interacting with directory servers.

It's often used for authentication and storing information about users, groups, and applications, but an LDAP directory server is a fairly general-purpose data store and can be used in a wide variety of applications.

Reference: https://www.techtarget.com/searchmobilecomputing/definition/LDAP
https://www.varonis.com/blog/the-difference-between-active-directory-and-ldap

SAML (Security Assertion Markup Language)

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 — Performs authentication and passes the user's identity and authorization level to the service provider.

Service Provider — Trusts the identity provider and authorizes the given user to access the requested resource.

Reference: https://auth0.com/blog/how-saml-authentication-works/
: https://www.onelogin.com/learn/saml

The sv-saml-client3.xml file looks like this

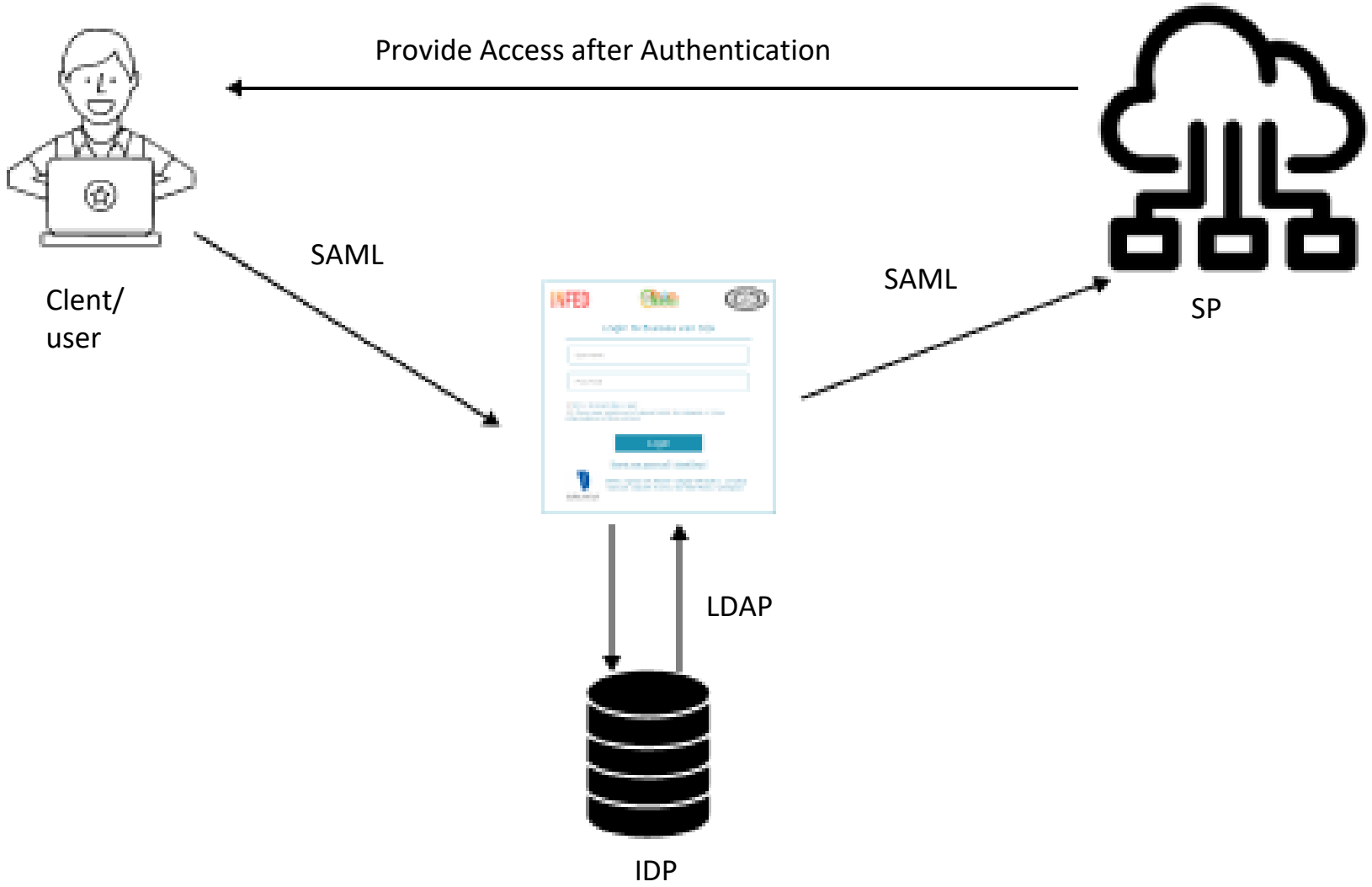
```
<xwss:JAXRPCSecurity xmlns:xwss="http://java.sun.com/xml/ns/
xwss/config">
   <xwss:Service>
      <xwss:SecurityConfiguration dumpMessages="true">
        <xwss:SAMLAssertion type="SV" strId="SV-123"/>
         <xwss:Sign includeTimestamp="false">
            <xwss:X509Token certificateAlias="xws-security-
client"/>
            <xwss:Target type="qname">
                {http://schemas.xmlsoap.org/soap/
envelope/}Body
            </xwss:Target>
            <xwss:SignatureTarget type="uri" value="SV-123">
               <xwss:Transform algorithm="http://docs.oasis-
open.org/wss/2004/01/
                    oasis-200401-wss-soap-message-
security-1.0#STR-Transform">
                  <xwss:AlgorithmParameter
name="CanonicalizationMethod"
                     value="http://www.w3.org/2001/10/
xml-exc-c14n#"/>
               </xwss:Transform>
            </xwss:SignatureTarget>
         </xwss:Sign>
         <xwss:Timestamp />
      </xwss:SecurityConfiguration>
   </xwss:Service>
    <xwss:SecurityEnvironmentHandler>
      sample.SecurityEnvironmentHandler
    </xwss:SecurityEnvironmentHandler>
</xwss:JAXRPCSecurity>
```

Refrence: https://docs.oracle.com/cd/E17802_01/webservices/webservices/docs/1.6/tutorial/doc/XWS-SecuritySamples7.html

Login Page


INFED
eShodh Sindhu
Login to Elsevier
Username
Password
Don't Remember Login
Clear prior granting of permission for release of your information to this service.
Login
Forgot your password? | Need Help?
Access Elsevier products using your institutional credentials
ELSEVIER

Shibboleth


Provide Access after Authentication
SAML
SAML
Clent/
user
SP
LDAP
IDP

Identity Provider & Service Provider (Components of Shibboleth)

Shibboleth consists of the following two primary components:

- **Identity Provider**: Identity Provider software is run by the institutions having a database of users entitled, to access subscription-based e-resources or services. Shibboleth leverages the organization's identity and access management system so that the individual's relationship with the institution can be used to determine access rights to subscription-based e-resources or services. In other words, different categories of users in an institution may have access to different sets of resources based on attributes assigned to them.
- **Service Provider:** Service Provider software is run by the publisher of a subscription-based e-resource or service. The Service Provider receives a set of pre-defined attributes from the Identity Provider and provides access to subscribed e-resources or services to the user depending upon the attributes received.

List of All Federations on Shibboleth

- https://technical.edugain.org/status

Software Used

- The software used for implementation of Shibboleth is all open source software developed by other projects incluading-shibboleth IDP (IDP.war), Shibboleth SP, Open LDAP, SHARPE PostgreSQL, In house-developed user creation interface, Web Server (Apache), Application Server (Tomcat), AuthN: SSOHandler used for authentication, AuthZ: Attribute Authority allowing AuthZ, HTTP, form-based or existing session/assertion (Cookie), etc.

OpenSAML

OpenSAML is a set of open source C++ & Java libraries meant to support developers working with the Security Assertion Markup Language (SAML). OpenSAML 2, the current version, supports SAML 1.0, 1.1, and 2.0.
Reference: https://shibboleth.atlassian.net/wiki/spaces/OpenSAML/overview

OpenAthens

It is an authentication system that allows you to access a range of quality information online.
OpenAthens is an identity and access management service, supplied by Jisc, a British not-for-profit information technology services company. Identity provider organisations can keep usernames in the cloud, locally or both. Integration with ADFS, LDAP or SAML is supported.
Reference: https://www.nice.org.uk/about/what-we-do/evidence-services/journals-and-databases/openathens

Advantages

- Shibboleth enables Single sign-on system.
- Shibboleth facilitates federated system.
- Protect data and user’s privacy

Limitations

- Non-proxy remote authentication fails. Many libraries struggle to create and preserve shibboleth.
- Global log out is Shibboleth's biggest difficulty. Shibboleth can't log out of all services at once, to show.
- Shibboleth's security risk is a major negative. Single Sign-On interface raises security issues because it's on both the management and client's side.
- Shibboleth implementation on proxy servers is more difficult than conventional servers.

References

- Mikesell, B. L. (2004, January 20). Anything, Anytime, Anywhere. *Journal of Library Administration*, *41*(1–2), 315–326. https://doi.org/10.1300/j111v41n01_22
- Kamal, P., Mustafiz, S., Rahman, F. M. A., & Taher, R. (2015). Evaluating the Efficiency and Effectiveness of a Federated SSO Environment Using Shibboleth. *Journal of Information Security*, *06*(03), 166–178. https://doi.org/10.4236/jis.2015.63018
- *About Inflibnet Centre*(2023). Inflibnet Centre. https://www.inflibnet.ac.in/index.php