Jurnal Elektronik Ilmu Komputer Udayana
Volume 12, No 4. May 2024

p-ISSN: 2301-5373
e-ISSN: 2654-5101

Single Sign on (SSO) Model Using Security Assertion Markup Language (SAML) and OAuth for authentication application of Universitas Pembangunan Nasional Yogyakarta (UPNVYK)

Ahmad Taufiq Akbar[a1], Hari Prapcoyo[a2], Rifki Indra Perwira[a3]

[a]Informatics Department, UPN "Veteran" Yogyakarta
Jl. Babarsari No 2, Tambakbayan 55281 Yogyakarta, Indonesia

[1]ahmadtaufiq.akbar@upnyk.ac.id
[2]hari.prapcoyo@upnyk.ac.id
[3]rifki@upnyk.ac.id (Corresponding author)

Abstract

Big companies have different systems both in terms of applications as well as the operating system, which requires each user to login to each different applications over and over again. With the SSO, users only need to remember one username and one password, but apply automatically universal across enterprise applications, so in this way it can be easier by using Security Assertion Markup language(SAML) for applications to be integrated without having to create a separate user validation. This SAML technology is an Extensible Markup Language(XML)-based framework and can guarantee the encryption of all or part of the data and then convey it to the end user. Moreover, it allows easy and secure data exchange between systems. The data exchange will be protected by authorization and authentication through tokens containing statements to pass data between users authorized by SAML. SAML can be supported by OAUTH as bearer protocol to provide extensive security when user access services along side on the Single Sign On(SSO) network.

(Justify, Arial 10)

Keywords: *Single Sign-On (SSO), Security Assertion Markup Language (SAML), authentication, OAuth (Open Athorization)*

(Minimum 5 keywords related to the content and separated by comma, italic)

1. Introduction

Large companies have numerous applications and services that handling day to day operational level for running the business. User used the application based on their role in organization to handle their jobs. In addition, they should remember username and password along those numerous applications. Furthermore, security and authentication are becoming major issues that should tackle in order to work effectively and efficiently for accessing in various systems. Meanwhile, those complications of application, user access, password, security, and authentication are needed solution for improvement data exchanged over the internet. Essentially, organization have to start within central authentication for handling their applications, web based, easy to configure, highly support security system and easily from user perspective [1]. So, the Secure of Single Sign On (SSO) method is needed for those case.

The SSO can be practically direct many users to log in to multi-application using one credential but it must be supported by security assertion protocol. One of technology that can be used for is Security Assertion Markup Language (SAML) that offers a secure system, SAML, Extensible Markup Language (XML), Simple Object Access Protocol (SOAP) and Hypertext Transfer Protocol (HTTP) protocol based for exchanging user security information among organization and a service provider. In general, the SAML standard provides framework guidelines and language rules for the data communication more elastic and permit customization data to be delivered to the service provider and provide SSO on enterprise systems. The other method is OAuth, JavaScript Object Notation (JSON) and HTTP protocol based and offer security for Application Programming Interface (API) authorization among the user applications [2].

The SSO concept has a fairly good level of security compared to other authentication concepts. The SSO model has been tested in telematika(computer centre) at University of Pembangunan Nasional Veteran Yogyakarta (UPNVYK) by penetration testing to determine the level of vulnerability. The results of this study were that from the seven stages of the penetration test conducted, 12 vulnerabilities were identified, consisting of 3 moderate vulnerabilities, 6 low vulnerabilities and 3 information vulnerabilities. Six cyber-attacks were carried out to exploit the vulnerability with 3 successful attacks and 3 failed attacks. This means that the single sign on concept has good accessibility transparency and can be audited at any time. SAML can also only run on browsers that already use the https protocol so that the security level is more guaranteed [3].

A number of previous studies have shown that SSO can increase ease of access with just one sign on or log in in using various integrated applications in a large company [4], and [5]. However, SSO still has a risk, namely that it can be breached by the man in the middle if there is no encryption framework for each session when accessing the application after the single sign on [6]. So for this reason SAML and Oauth are needed to provide security capabilities for each session of all access in the realm of single sign on [7]. SAML has generally been able to provide cross-domain authentication security with high mechanism efficiency [8]. But SAML can be integrated with OAuth to provide layered security, where SAML encrypted can be encrypted by Oauth running on Transport Layer Security (TLS) then it can achieve mutual authentication without the help of trusted third parties, [9].

The pervasiveness automation process in many organizations including higher education systems in UPNVYK also influence in maintenance and operational level to secure each stage of any academic procedures. By this condition, user credential is very important that must be managed as one set credential to access in multi-application across network securely so that can ease to process of many online academic processes. The implementation of SSO will make it easier for users to log in to the website without having trouble remembering their credentials such as username, NIM, and password. So that only by entering an email address that has been registered in the system, users will easily log in quickly to several information system domains within the UPNYK campus simultaneously without having to login one by one. Only by one email makes it easier to login on multiple domains. Its authentication method uses the OAuth 2.0 and SAML protocol which is integrated with the account using the official institutional ID (@upnyk) from the Gmail mail server.

There are several techniques is developed for data exchange and security authentication. In general, it can be seen from password authentication, Public Key Infrastructure (PKI), Secure Socket Layer (SSL), XML based services. PKI based service is highly complex structure, code and costly in development and maintenance. SSL extremely needs more resource such as need partial encryption in data. While XML based services provide more robust from penetration and free in data exchange. Compare the current existing system in security authentication and single sign on methods, SAML is based on XML services that more reliable, high flexibility, and good authentication with security systems [10].

The implementation of SSO will make it easier for users to log in to the website without having trouble remembering their credentials such as username, NIM, and password. So that only by entering an email address that has been registered in the system, users will easily log in quickly to several information system domains within the UPNYK campus simultaneously without having to login one by one. Although one email makes it easier to login on multiple domains. The authentication method used uses the OAuth 2.0 and SAML protocol which is integrated with the account using the official institutional ID (@upnyk) from the gmail mail server

2. Research Methods

2.1. The SAML Web SSO process

SAML web SSO process inititated by the Service Provider (SP) or the Identity Provider (IdP) in vice versa. A web SSO flow began with an identity provider called IdP-initiated, while a low that initiated at the service provider is titled SP-initiated. IdP initiated in SSO within several steps that illustrate the data exchange between the user and IdP provider. The first, the user acquaintances the IdP. Then, the user authenticates to the IdP. Following that, upon positive authentication, the IdP refers a SAML reply to service provider. Finally, SP proves the SAML response and authorizes the user's request. Definitely, the whole process of IdP initiated SSO can be seen in the Figure 1 below [11]

p-ISSN: 2301-5373
e-ISSN: 2654-5101

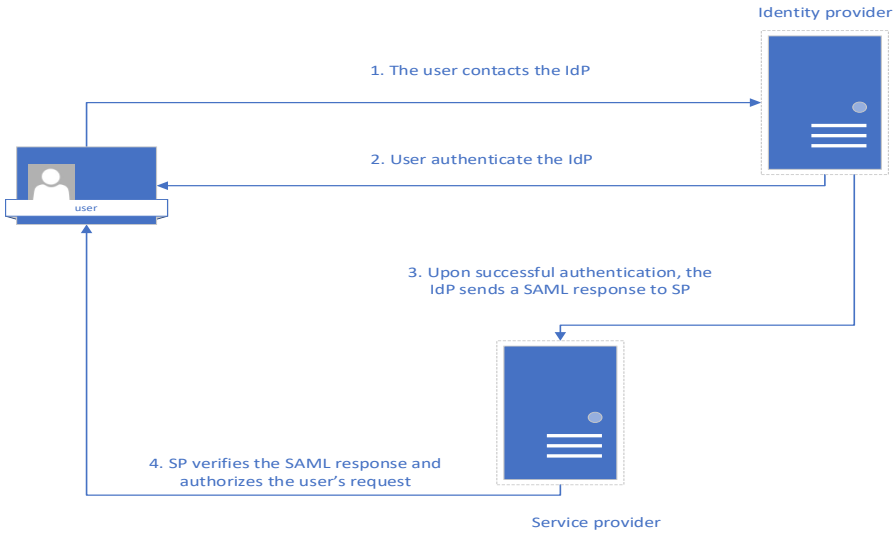

Fig. 1. The Flow of SSO that is initiated by IdP[12]

The user initiates the IdP with IdP-initiated SSO. The IdP guides the user to authenticate and displays (in the form menu) links to one or more of her SPs. Once the user is authenticated, the IdP generates her SAML response containing the authentication assertion and directs the user to the SP requested by the user. When a user tries to connect to an SP, it comes with the promise of authentication. The SP then analyzes the assertions and grants or denies access based on those assertions[11].

SP-initiated SSO as seen in Fig. 2, it begins with user send access to SP services. The SP will create a SAML authentication and then redirects to the authentication request. Following that user authentication to the IdP and send response to that includes assertion to verify SAML response also authorizes user's request.

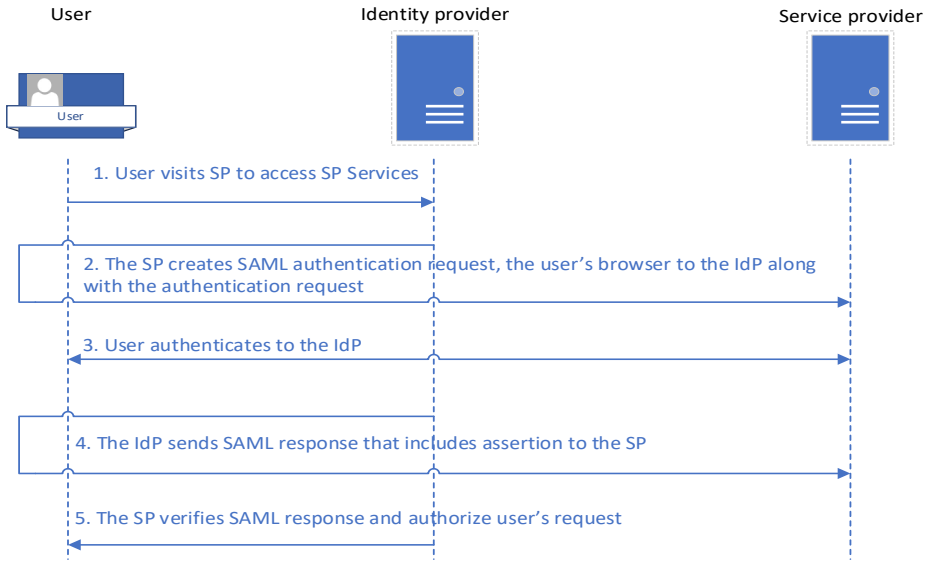

Fig. 2. The Flow of SSO that is initiated by SP[12]

First, the user goes to the SP, which directs the user to the IdP for authentication. SP-initiated SSO is a common configuration for SSO, so we'll cover it in detail.The IdP generates a SAML response in step 4. It contains authentication statements related to the user's security context. These confirmations are digitally marked and sent to the user's browser. Then forward the signed statement from the user's browser to the SP. The SP verifies the SP's digital signature and processes the contents of the statement. Next (if all requirements are met), create a "local" version of the security user context. After fulfillment, the user is registered with the SP and can access services within the SP[11].

2.2. OAuth Technology

To facilitate the implementation of authentication mechanisms, it can use services provided by application service providers (ASP). Google is one of the ASPs that dominate most users for Search engines and email services. One of the services provided by Google is Google Identity, that provides the ability to perform SSO using the OAuth 2.0 protocol. By using this service, users will soon be able to access services provided by Google APIs such as Google Calendar, Gmail, and more. However, users can not only use services provided by Google, but also use the Google Identity Service as an authentication and authorization server, so that can possibly do the SSO integration via Google [13](Senapartha, 2021). To keep the credentials safe, an access token is generated by the OAuth provider and passed to the client, and the access token has an expiration date. After the expiration date, user will need to request a new access token from his authentication provider or OAuth provider. The update token is a credential used to obtain an expired access token [14].

The OAuth 2.0 protocol is a widely used protocol for SSO due to its ease of implementation and ease of implementation. Lots of support from ASP for this protocol [15]. OAuth is an open standard for authorization that makes this possibility to the third-party applications for accessing resources on resource servers without sharing user credentials. Other available Protocol options are SAML and OpenID as open standard and decentralized authentication protocol, SAML is an XML-based protocol and Open ID is a modern protocol that runs on top of the OAuth 2.0 protocol. Previous research conducted as a result of the analysis shows that SAML has limited interoperability with mobile devices. It is considered immature for use as a standard authentication protocol and is therefore low among enterprises [16]. Therefore, any SSO implementation based on the OAuth 2.0 protocol can be used as the SSO authorization protocol in many systems. The OAuth is authorization method can provide authorization application on the web. Social network Googles plus, Facebook, Twitter use their authorization based on OAuth protocol in SSO and social sharing. This technology also uses an open standard platform to give a process for third-party application to get user's resources on servers without sharing login credentials. SSO is an identification technique that is allowing for website to use and confirm the users [15].

2.3. SSO using SAML and OAuth

The data collection method was carried out through observations on systems that did not use the single sign on method on the UPNYK campus and collected data from several Information and Communication (ICT) units, Computer Center or Directorate of Data Resources and Information (DSDI) from various universities, both public and private. Data from information sources that are very useful and can help provide input to researchers to use this single sign on method. In accordance with what was obtained during this observation, it can be indicated that the mechanism for students and users in logging in to be able to access campus information systems consisting of various domains such as Computer Base Information System, University web, Department web, and learning management system like SPADA adheres to conventional methods, namely students still it is necessary to remember the password and NIM (Student Identification Number) in order to be able to access the information system which students often neglect with their credentials.

SSO technology was developed to make it easier for users to access various applications, both mobile and web, in using various existing services. For example, a mail account from Google, where a user has logged in using an email account from Google can access all applications on Google without the need to log in again. SSO also allows authentication information and identify the subject strictly to avoid double login on a trusted system or system group. The SSO system can also centralize the management of the relevant system parameters at the same time and improve overall usability. Service users may prefer SSO systems over conventional sign-on systems. In implementing SSO, OAuth and SAML2 are used. As illustrated in Fig.3, the Client can obtain a SAML statement from the IdP and request the Authorization Server (IdP) to grant access to the Resource Server. The Authorization Server can then verify the user's identity and return an OAuth token in the HTTP header to access the protected resource. As an OAuth 2.0 Authorization Server, the Identity Server can

p-ISSN: 2301-5373
e-ISSN: 2654-5101

accept SAML2 Assertions from OAuth 2.0 clients as a means of authenticating and authorizing resource owners. Additionally, it can exchange it for an OAuth 2.0 access token to access protected resources on behalf of the resource owner.

The flow of SSO usage with SAML2 and OAuth 2 Protocol can be seen in Fig. 3.

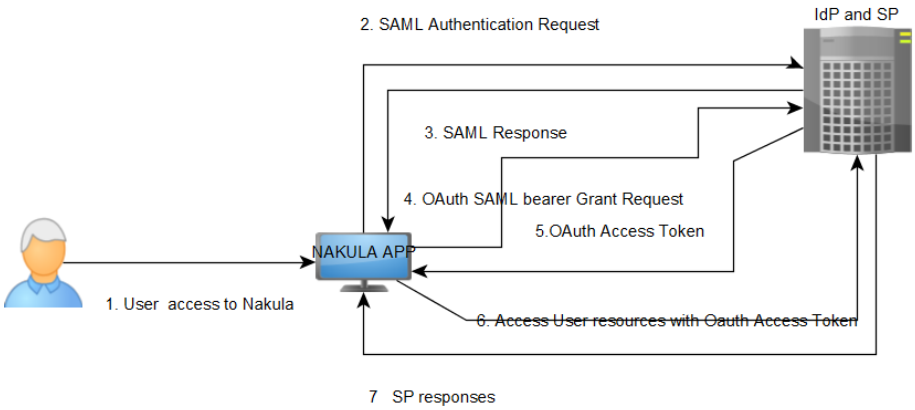

Fig. 3. The Flow of SSO using SAML and OAuth

3. Result and Discussion

The SSO application implemented on the Nakula App (Management Information System that have been developed by UPNVYK) can be accessed on android and web platforms. In Fig. 4 shows the application of SSO on the Android Front end by using the lecturer's NIDN credentials and password.

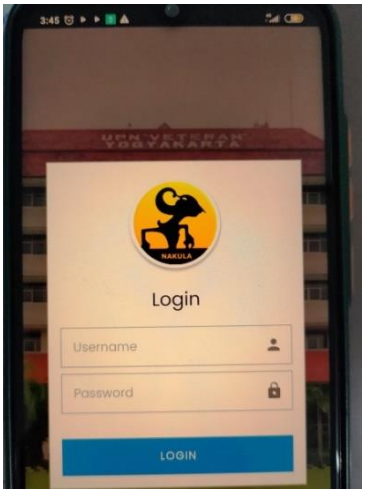

Fig. 4. The User Concern of Sign In using one Credential (gmail account)

While in web-based Nakula as seen in Fig. 5, users, especially lecturers, can choose to sign in with 1 of 2 types of credentials, namely NIDN and password or the registered institutional email username and password.

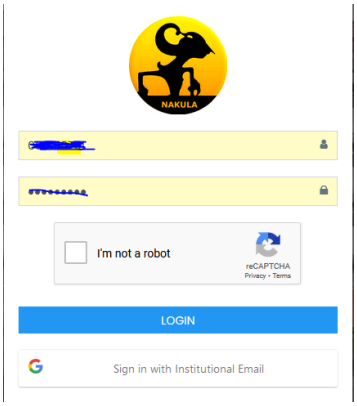

Fig. 5. Web Based Nakula Interface

If user use the first type of credential, the user will be immediately sent to the dashboard page which will bring up navigation to other sub domains without signing in again. Whereas if the user uses the second type of credential, then before going to the dashboard, the user will be asked to input the institutional email account and password that has been registered as a means of single sign on (Fig. 6).

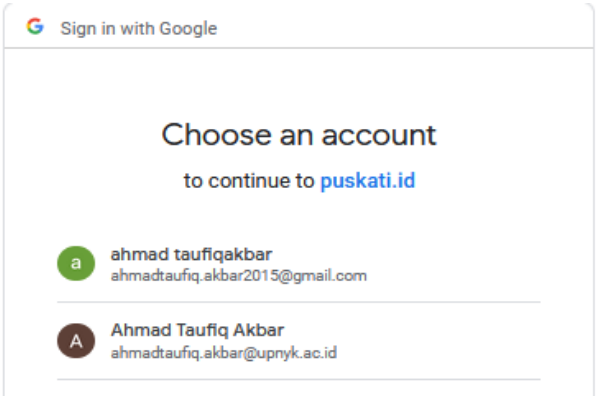

Fig. 6. The Web Based Nakula ask for gmail account as credential

Furthermore, after login process using email account credentials will also be delivered to the application dashboard as seen in Fig. 7. If user have reached the dashboard, they will no longer sign in or input credentials when accessing other sub domains (applications).

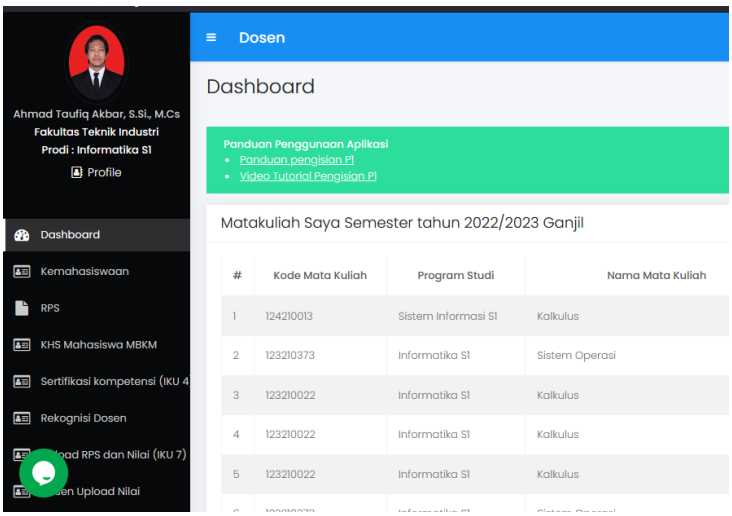

Fig. 7. The Dasboard Application after sign in Web Based Nakula using gmail account as credential

As long as the user is in the sub-domain application that has been accessed, the user can log out after returning to the dashboard as a one-stop media for single sign on. Immediately logged out the

p-ISSN: 2301-5373
e-ISSN: 2654-5101

user session has been deleted. The processing of every data transaction from the application to the server (including login and revoke token) is carried out on the HTTPS protocol as the transmission layer and data encryption. This ensures that the user data channel is secure and can use the OAuth SAML bearer token to access data from the desired SP. This bearer method protects sending tokens via Uniform Resource Locator (URL) from being accessed by other users via browser history.

4. Conclusion

Research has shown that the SSO method with OAuth and SAML bearer provides easy and secure access with 1 type of credential through the use of google accounts and the client server RESt architecture. The SSO application on Nakula which is based on android and web client server makes it easy for users to access sub domains or other applications without having to re-sign in every application that is accessed. The implementation of the refresh access token of the OAuth protocol will protect the validity of the access token used by the client that has been authorized by SAML, so this security is layered. Goggle identity service can speed up SSO while still focusing on securing data transmission while using SSO. By applying SSO method with OAuth and SAML the security level of authentication application have been improved, robust and more resilience from the network attacks.

References

(All of the references should be cited in the paper, it is recommended to use reference tools such as Mendeley or enote, Minimum 80% of the references are from journals and published within last 5 years, please cite one paper from this journal)

(Journal)

[1] K. D. Lewis, “Web single sign-on authentication using SAML,” *arXiv Prepr. arXiv0909.2368*, 2009.

[2] C. H. Rupa, R. Patan, F. Al-Turjman, and L. Mostarda, “Enhancing the access privacy of IDAAS system using SAML protocol in fog computing,” *IEEE Access*, vol. 8, pp. 168793–168801, 2020, doi: 10.1109/ACCESS.2020.3022957.

[3] S. U. Sunaringtyas and D. S. Prayoga, “Implementasi Penetration Testing Execution Standard Untuk Uji Penetrasi Pada,” *Edu Komputika J.*, vol. 8, no. 1, pp. 48–56, 2021.

[4] Q. Aini, U. Rahardja, and R. S. Naufal, “Penerapan Single Sign On dengan Google pada Website berbasis YII Framework Application Single Sign On with Google the Website Based on Yii Framework,” *J. Ilm. SISFOTENIKA*, vol. 8, no. 1, pp. 57–68, 2018.

[5] H. Ajie, M. Insan Rizky, and M. F. Duskarnaen, “Pengembangan Teknologi Single Sign On Pada Sistem Informasi Dosen dan Sistem Informasi Kurikulum di Universitas Negeri Jakarta,” *PINTER J. Pendidik. Tek. Inform. dan Komput.*, vol. 3, no. 1, pp. 32–37, 2019, doi: 10.21009/pinter.3.1.6.

[6] N. M. Karie, V. R. Kebande, R. A. Ikuesan, M. Sookhak, and H. S. Venter, “Hardening SAML by Integrating SSO and Multi-Factor Authentication (MFA) in the Cloud,” *ACM Int. Conf. Proceeding Ser.*, 2020, doi: 10.1145/3386723.3387875.

[7] S. Watini, P. Nursaputri, and M. Iqbal, “Comparison of CAS and Manage Oauth in Single Sign on (SSO) Client Applications,” *IAIC Trans. Sustain. Digit. Innov.*, vol. 1, no. 2, pp. 152–159, 2020, doi: 10.34306/itsdi.v1i2.147.

[8] A. J. Cui, W. Wang, H. F. Zhang, Y. H. Ma, C. Li, and X. M. Wang, “Cross-domain single sign-on authentication of information security in network environment,” *Int. J. Inf. Commun. Technol.*, vol. 18, no. 1, pp. 89–104, 2021, doi: 10.1504/IJICT.2021.111924.

[9] U. Joshi, S. Cha, and S. Esmaili-Sardari, “Towards adoption of authentication and authorization in identity management and single sign on,” *Adv. Sci. Technol. Eng. Syst.*, vol. 3, no. 5, pp. 492–500, 2018, doi: 10.25046/aj030556.

[10] M. Kang, C. S. Hong, H. J. Koo, and G. H. Lee, “An SAML based SSO architecture for secure data exchange between user and OSS,” *APNOMS 2005 - 8th Asia-Pacific Netw. Oper. Manag. Symp. Towar. Manag. Ubiquitous Inf. Soc. Proc.*, no. January, pp. 608–617, 2005.

[11] I. Rajapaksha, “No Title,” *medium.com*, 2019. https://is-rajapaksha.medium.com/single-sign-on-with-saml-e39dc3e72cf2 (accessed Oct. 16, 2022).

[12] I. Rajapaksa, “https://medium.com/single-sign-on-with-saml-e39dc3e72cf2,” 2019.

[13] I. K. D. Senapartha, “Implementasi Single Sign-On Menggunakan Google Identity, REST dan OAuth 2.0 Berbasis Scrum,” *J. Tek. Inform. dan Sist. Inf.*, vol. 7, no. 2, pp. 307–320, 2021, doi: 10.28932/jutisi.v7i2.3437.

[14] I. Kusuma, A. Susanto, and I. U. W. Mulyono, “Implementasi Restful Web Services Dengan Otorisasi Oauth 2.0 Pada Sistem Pembayaran Parkir,” *Simetris J. Tek. Mesin, Elektro dan Ilmu Komput.*, vol. 10, no. 1, pp. 391–404, 2019, doi: 10.24176/simet.v10i1.3026.

[15] N. Hossain, M. A. Hossain, M. Z. Hossain, M. H. I. Sohag, and S. Rahman, “OAuth-SSO: A Framework to Secure the OAuth-Based SSO Service for Packaged Web Applications,” *Proc. - 17th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. 12th IEEE Int. Conf. Big Data Sci. Eng. Trust. 2018*, pp. 1575–1578, 2018, doi: 10.1109/TrustCom/BigDataSE.2018.00227.

[16] N. Naik and P. Jenkins, “Securing digital identities in the cloud by selecting an apposite Federated Identity Management from SAML, OAuth and OpenID Connect,” *Proc. - Int. Conf. Res. Challenges Inf. Sci.*, pp. 163–174, 2017, doi: 10.1109/RCIS.2017.7956534.