Eduvest – Journal of Universal Studies
Volume 6 Number 5, May, 2026
p- ISSN 2775-3735- e-ISSN 2775-3727

Keycloak-Based Single Sign-On Implementation with QR Code Authentication Using OIDC PKCE

Arvin Demas Naryama*, Budi Suyanto
Universitas Pembangunan Nasional, Indonesia
Email: 1124230148@student.upnyk.ac.id*, budi.suyanto@upnyk.ac.id

Keywords
Single Sign-On; Keycloak; QR Code Authentication; OIDC PKCE; E-Government; Service Provider Interface

ABSTRACT
Regional government digital services face critical challenges in centralized identity management, including authentication inefficiency across multiple devices, lack of institutionally branded interfaces, and the absence of a self-service account management dashboard for civil servants. This study develops PemdaSSO, a Keycloak-based Single Sign-On system, by integrating a password less QR Code authentication feature via a custom Service Provider Interface extension, combined with the OpenID Connect Authorization Code Flow protocol secured with Proof Key for Code Exchange on a React JS Single Page Application dashboard, deployed at the Department of Communication and Information Technology of the Special Region of Yogyakarta. Methods: The system employs a three-tier architecture deployed via Docker Compose, comprising Keycloak as the Identity Provider, React JS as the Single Page Application frontend, Node.js as the backend API, PostgreSQL as the database, and MinIO as object storage. Black Box Testing was conducted on 59 test scenarios across 11 functional categories in accordance with ISO/IEC 25010 functional suitability criteria. The testing yielded a 100% pass rate. The implemented single-use token mechanism with a 30-second expiration directly mitigates the Reusable QrId and Unbound SessionId vulnerabilities identified in prior literature, while Proof Key for Code Exchange protects the Single Page Application from authorization code interception attacks. Compared to national-scale e-government Single Sign-On implementations relying on physical X.509 certificates, this approach is lighter, hardware-independent, and better suited to the mobility requirements of regional government personnel, thereby addressing a gap in the literature on modern Single Sign-On security implementation at the local government level.

INTRODUCTION

The implementation of an electronic government system demands efficient integration of digital services across local government agencies. However, as the number of information systems continues to grow, government officials and citizens are often required to authenticate repeatedly across separate applications. This fragmented access pattern not only increases users' cognitive burden but also encourages poor security practices, including password reuse across multiple platforms. From an operational perspective, decentralized credential management reduces work productivity and places a significant burden on information technology support teams. In many organizations, a large proportion of helpdesk requests are related to password recovery and reset procedures, which indicates an urgent need for a more

efficient identity management solution (Hermawan, 2023; Juwara & P Nyeleker, 2026; Naghmouchi et al., 2025; Pandey & Nisha, 2021; Zineddine et al., 2025). For this reason, a centralized Identity and Access Management approach is essential to simplify workflows while strengthening service security.

Experiences from the implementation of digital identity systems in several countries show that governance models are a decisive factor in success. FranceConnect, which is managed directly by public authorities, has successfully reached more than 40 million active users (Naghmouchi et al., 2025), whereas the United Kingdom's Verify project, which relied heavily on private vendors, attracted only 3.6 million users before being discontinued (Naghmouchi et al., 2025). Broader literature also shows that identity management is moving between federated, decentralized, and self sovereign models, and that governance choices strongly affect sustainability, trust, and interoperability (Manimaran et al., 2025; Sousa & Gonçalves, 2024; Supangkat et al., 2025). In Indonesia, the implementation of a Keycloak based Single Sign On system within the national electronic government framework has successfully integrated 15,000 users through X.509 digital certificate authentication (Hermawan, 2023). These cases indicate that self managed open source solutions operated by government institutions can offer a more sustainable approach for public sector identity services, particularly in complex public infrastructure environments (Juwara & P Nyeleker, 2026; Supangkat et al., 2025).

In the Special Region of Yogyakarta, the Department of Communication and Informatics has operated PemdaSSO, a Keycloak based system serving as a centralized Identity Provider for various digital services in the local government ecosystem. Nevertheless, the current system does not yet support an efficient alternative authentication method for cross device access, the existing interface does not reflect the visual identity of the local government, and a self service dashboard for centralized account management is still unavailable. An analysis using the PIECES framework, namely Performance, Information, Economics, Control, Efficiency, and Service, identifies these limitations as operational gaps that require a comprehensive solution. These gaps are not merely technical inconveniences, because they directly affect usability, administrative efficiency, and the overall security posture of public digital services. Similar challenges have also been reported in e government implementation studies, where interoperability, user adoption, and service continuity often become key obstacles in the public sector (Bunn, 2024; Juwara & P Nyeleker, 2026).

QR Code based authentication is a promising candidate for reducing friction in cross device login scenarios. It allows users to authenticate on a target device such as a desktop computer by scanning a code with an already authenticated mobile device, without manually entering credentials. However, recent research has shown that QR Code login is not inherently secure. Zhang et al. (Zhang & others, 2025) conducted an empirical security audit of 109 high ranked websites that implemented QR Code login and found that 43 percent were vulnerable to security attacks. They identified six fundamental implementation weaknesses, namely Unbound SessionId, Reusable QrId, Predictable QrId, Controllable QrId, Vulnerable Identity Verification, and Unintentional Privacy Leakage. These weaknesses can be exploited to launch Authorization Hijacking, Double Login, and Universal Account Takeover attacks (Zhang & others, 2025). This evidence shows that QR Code authentication must be designed with strong safeguards if it is to be deployed in public sector systems, especially where privacy and security

risks in Single Sign On environments remain significant (Shabi & Marie, 2024; Zineddine et al., 2025).

Passwordless authentication is another relevant direction because it seeks to eliminate the inherent weaknesses of traditional passwords, such as brute force attacks, credential stuffing, and phishing (Mitra & Ghosh, 2024; Yusop et al., 2025). Among current passwordless standards, FIDO2, which combines Web Authentication and the Client to Authenticator Protocol, is the most mature (Mitra & Ghosh, 2024). Even so, practical adoption in government environments remains limited because it requires dedicated physical hardware and introduces complex account recovery procedures (Owens et al., 2021; Yusop et al., 2025). Studies on multi factor authentication in secure digital systems also show that stronger authentication is increasingly treated as a baseline requirement rather than an optional enhancement (Tran-Truong et al., 2025). Owens et al. (Owens et al., 2021) reported that adoption continues to be constrained by concerns over device availability and the high friction of account recovery. These findings suggest that an alternative passwordless approach that is more suitable for large scale local government environments is still needed.

Recent studies in the related literature further show that the field remains fragmented. Divyabharathi demonstrated the flexibility of Keycloak through custom Service Provider Interface extensions (Divyabharathi & Cholli, 2020). Hardt (Hardt, 2012) and Sakimura (Sakimura et al., 2015) examined the importance of Proof Key for Code Exchange in protecting the OpenID Connect Authorization Code Flow for public clients. Hermawan et al. reported successful Keycloak integration in the Indonesian SPBE environment (Hermawan, 2023). Zhang et al. (Zhang & others, 2025) focused on QR Code login vulnerabilities rather than secure implementation. Owens et al. highlighted the usability barriers of FIDO2 in real world adoption (Owens et al., 2021). Other studies have also examined OAuth integration in mobile applications, SSO privacy and security, and privacy implications in OpenID Connect based systems, showing that secure identity design must consider both protocol safety and deployment context (Jaswanth Alahari et al., 2023; Shabi & Marie, 2024; Zineddine et al., 2025). At the governance level, FranceConnect and UK Verify illustrate how public and private models can produce very different outcomes in national identity systems (Naghmouchi et al., 2025). Taken together, these studies demonstrate important progress in individual components of identity management, but they do not yet provide an integrated solution that combines Keycloak as an Identity Provider, OpenID Connect with PKCE protection, and QR Code passwordless authentication within a single regional e government ecosystem.

Based on this gap, the present study develops PemdaSSO using Keycloak by integrating a passwordless QR Code authentication feature that is secured through a 30 second single use token mechanism. The feature is implemented through a custom Keycloak Service Provider Interface extension (Divyabharathi & Cholli, 2020) and combined with the OpenID Connect Authorization Code Flow together with Proof Key for Code Exchange protection (Hardt, 2012; Sakimura et al., 2015) to secure the authorization layer for React JS based client applications. This study aims to address the limitations of the current system by providing a centralized, secure, and more usable authentication mechanism for local government digital services. In general, the study seeks to enhance identity management efficiency in regional electronic government, and in particular, it seeks to improve cross device authentication, reduce helpdesk dependency, and strengthen access security.

METHOD

System Development Design

The development of PemdaSSO was carried out using an Agile approach based on the Scrum framework, which follows an iterative and incremental cycle. The work was organized into several sprints, each consisting of Project Vision, Release Planning, Sprint Planning, Sprint Implementation, Review, and Retrospect activities until the final product was ready for handover. The entire development process was completed over a two month period from January to February 2026 and included literature review, architectural design, feature implementation, testing, and the preparation of technical documentation.

System Architecture

PemdaSSO was designed using a three tier architecture consisting of a presentation layer, a business logic layer, and a data layer. All system components were deployed within a containerized ecosystem using Docker Compose to simplify service management and improve portability in both development and production environments. The first layer was a Keycloak based Identity Provider that served as the centralized authentication and authorization server for all digital services of the Special Region of Yogyakarta government. The Keycloak login interface was customized using a custom theme based on *FreeMarker Template Language* and CSS to consistently reflect the visual identity of the local government. The second layer was a dashboard application for account management built with React JS v19 and TypeScript, which functioned as a *Single Page Application* and as a *Relying Party* within the *OpenID Connect* ecosystem. The third layer was a Node.js backend API using Express, which mediated communication between the React frontend and the Keycloak Admin API, supported by PostgreSQL 15 and MinIO Object Storage.

QR Code Authentication Design

The QR Code authentication feature was implemented as a custom Keycloak extension through the *Service Provider Interface* mechanism, which made it possible to insert a new authentication module into the Keycloak authentication flow without modifying the core platform code (Divyabharathi & Cholli, 2020). The QR Code authentication flow was designed as follows. First, the target device, in this case a desktop computer, opened the login page and the system generated a single use QR token, or QrId, with a 30 second validity period, which was temporarily stored on the backend and bound to the session. Second, the user scanned the QR Code using an already authenticated mobile device and confirmed the login request. Third, the target device detected successful confirmation in real time through a hidden iframe polling mechanism every 3 seconds. Fourth, the system automatically redirected the target device to the dashboard. The lifecycle of the QR token was strictly designed to be single use and to expire automatically after 30 seconds in order to prevent exploitation of Reusable QrId and Unbound SessionId vulnerabilities (Zhang & others, 2025).

OIDC and PKCE Integration

Authentication communication between the React JS dashboard and Keycloak implemented the *OpenID Connect* Authorization Code Flow with *Proof Key for Code Exchange* security extension using the @react-keycloak/web library. The PKCE based authorization flow was implemented as follows. First, the React JS application generated a code_verifier as a random string with high cryptographic entropy and then calculated the

code_challenge using Equation 1. Second, the React JS application redirected the user to the Keycloak Authorization Endpoint by including the code_challenge parameter and code_challenge_method=S256. Third, after successful authentication, Keycloak returned an authorization_code through the redirect URI. Fourth, the React JS application exchanged the authorization_code together with the original code_verifier at the Keycloak Token Endpoint. Fifth, Keycloak validated that the SHA 256 hash of the received code_verifier matched the stored code_challenge. If the validation was successful, Keycloak issued an Access Token in JWT RS256 format, an ID Token, and a Refresh Token (Hardt, 2012; Sakimura et al., 2015). This design aligns with published findings on OAuth and OIDC security, including studies that emphasize both secure implementation practices and formal safety verification of OpenID Connect programs (Al Rahat et al., 2024; Jaswanth Alahari et al., 2023; Shabi & Marie, 2024).

Testing Scenario

Functional testing was conducted using the Black Box Testing method, which focuses on verifying whether the system output matches the given input without considering the internal implementation of the program code (Kinasih et al., 2026; Meliala et al., 2024). This method is aligned with the functional suitability aspect of the ISO/IEC 25010 standard. The test design consisted of 59 test scenarios grouped into 11 functional categories, namely QR Code authentication and login, account registration, password recovery, TOTP authenticator setup, profile management, active session monitoring, account security, document management, personal note management, login activity history, and the user administration panel (Kinasih et al., 2026; Meliala et al., 2024).

RESULT AND DISCUSSION

Implementation Results

The PemdaSSO system was successfully developed and deployed using Docker Compose with five containers running simultaneously: Keycloak as the Identity Provider, Node.js as the backend API, React JS as the frontend dashboard, PostgreSQL as the database, and MinIO as the object storage service. All components were integrated within a private internal Docker bridge network so that service communication remained secure and was not exposed directly to the public network. This deployment model supported modular maintenance, simplified service orchestration, and improved portability across development and production environments.

Figure 1 illustrates the customized PemdaSSO login page, which was designed using a Custom Theme based on *FreeMarker Template Language* and CSS to reflect the visual identity of the Special Region of Yogyakarta government consistently. The interface presents four authentication methods in a single entry point, namely username and password login, social login through Google and GitHub, passkey authentication, and a QR Code tab for cross device authentication. This design improves usability by reducing fragmentation at the login stage while preserving a unified institutional appearance.

Fig 1. PemdaSSO login page with a custom theme reflecting the visual identity of the Special Region of Yogyakarta government and four authentication methods.

Figure 2 presents the QR Code modal interface together with a 30 second countdown timer. When the token expires before being scanned, the system automatically displays a Refresh QR Code button to generate a new token. This short validity period and session binding mechanism directly implement mitigation against the Unbound SessionId and Reusable QrId weaknesses identified by Zhang et al. (Zhang & others, 2025).

Fig 2. QR Code modal window with a 30 second countdown and automatic refresh button when the token expires.

Figure 3 shows the React JS based account management dashboard, which provides seven functional modules in a unified interface. Users can manage their profile, configure 2FA and TOTP, monitor active sessions across devices, upload and download documents to MinIO, create personal notes, and review login activity history with timestamp, IP address, and device type information, all without requiring administrator assistance.

Fig 3. React JS account management dashboard with seven functional modules in a single integrated interface.

Testing Results

Functional testing was conducted using 59 test scenarios grouped into 11 functional categories. Table 1 summarizes the overall Black Box Testing results. The evaluation was aligned with the functional suitability criteria in the ISO/IEC 25010 standard (Kinasih et al., 2026; Meliala et al., 2024).

Table 1. Summary of Black Box Testing Results

No.	Testing category	Scenarios	Passed	Failed
1	QR Code authentication and login	10	10	0
2	Account registration	6	6	0
3	Password recovery	6	6	0
4	TOTP authenticator setup	4	4	0
5	Account profile dashboard	4	4	0
6	Active session dashboard	4	4	0
7	Account security dashboard	5	5	0
8	Document management	5	5	0
9	Personal note management	5	5	0
10	Login activity history	3	3	0
11	User administration panel	7	7	0
	Total	**59**	**59**	**0**
	Success rate		**100 percent**	**0 percent**

Source: Research Data Processed by the Authors (2026).

As shown in Table 1, all 59 test scenarios passed successfully, resulting in a 100 percent success rate. No scenario produced an output that deviated from the expected result. This success also covered critical security related tests, including magic bytes validation in the document management module to prevent malicious file uploads and Role Based Access Control protection in the user administration panel, which correctly rejected unauthorized access and returned HTTP 403 Forbidden when the panel was accessed without administrator privileges.

The implementation results indicate that the QR Code authentication feature, developed as a custom Keycloak *Service Provider Interface* extension, effectively addressed the main challenges identified in the PIECES analysis, particularly in the Efficiency and Performance dimensions. The implemented 30 second single use token mechanism directly mitigated two

of the six critical QR Code login weaknesses identified by Zhang et al. (Zhang & others, 2025), namely Reusable QrId and Unbound SessionId, without requiring additional hardware infrastructure that would increase institutional cost. This finding supports the practical value of integrating short lived session bound tokens into cross device authentication workflows in the public sector.

The open source approach based on self managed Keycloak also appears more sustainable than dependence on commercial vendors. The comparative study by Vereau Jacobo (Vereau Jacobo, 2025) reported that Keycloak has an 80 percent lower Total Cost of Ownership, estimated at USD 50,000 compared with USD 250,000 over a five year projection, while still maintaining 99.5 percent availability (Vereau Jacobo, 2025). In the context of regional government services, this cost profile is especially relevant because it allows institutions to build a centralized identity platform without creating long term dependency on proprietary licensing structures. The present study therefore extends that perspective by showing that Keycloak can also support a secure QR Code based passwordless flow when it is combined with a custom authentication extension.

The use of the *OpenID Connect* Authorization Code Flow with *Proof Key for Code Exchange* on the React JS application successfully secured the authentication process against authorization code interception, which is a common weakness of *Single Page Application* clients that operate as public clients (Clarke & Furnell, 2026; Hardt, 2012; Sakimura et al., 2015; Sharif et al., 2022). Compared with the national SPBE implementation reported by Hermawan et al. (Hermawan, 2023), which still relied on X.509 certificate based PKI authentication, the PKCE based approach in this study is lighter, does not require specialized cryptographic hardware, and can operate seamlessly through a standard web browser. This makes it more appropriate for broader local government adoption, especially in environments where budget constraints and device diversity are significant operational considerations.

The system also demonstrated that the additional dashboard functions contribute to service efficiency. By centralizing profile management, TOTP configuration, active session monitoring, document handling, personal notes, and login history within one interface, the system reduces user dependence on administrators and lowers routine support requests. This is consistent with the broader objective of improving digital service efficiency in public administration, where repeated authentication and scattered account management often create avoidable operational burden.

The main limitation of this study is that testing was still limited to Black Box functional testing and did not yet include formal load testing or penetration testing. Although the PKCE mechanism and the 30 second single use token are theoretically capable of mitigating the main attack vectors described by Zhang et al. (Zhang & others, 2025), the resilience of this custom SPI extension under very high traffic conditions and advanced session manipulation attacks, such as Authorization Hijacking, has not yet been comprehensively validated. Future research should therefore evaluate performance under load, security resistance under adversarial conditions, and user acceptance in a broader government deployment setting.

CONCLUSION

This study successfully developed a Keycloak based PemdaSSO system by integrating a passwordless QR Code authentication feature through a custom *Service Provider Interface*

extension and an *OpenID Connect* Authorization Code Flow protected by *Proof Key for Code Exchange* in a React JS dashboard environment at the Communication and Informatics Office of the Special Region of Yogyakarta. Black Box Testing across 59 test scenarios in 11 functional categories achieved a 100 percent success rate, confirming that all system functions, from cross device QR Code authentication and self service account management to *Role Based Access Control* protection on the administration panel, operated in accordance with the defined requirements. The implemented 30 second single use token mechanism effectively mitigated the Reusable QrId and Unbound SessionId weaknesses without requiring additional hardware, while PKCE protected the *Single Page Application* from authorization code interception attacks that are inherent to public clients. The choice of a self managed open source Keycloak architecture also proved financially relevant, with a Total Cost of Ownership 80 percent lower than commercial alternatives, while addressing a gap in the academic literature on modern SSO security implementation at the local government level. For future research, empirical validation should be expanded through formal load testing and penetration testing of the custom QR Code SPI extension, especially to assess resilience against Authorization Hijacking under high traffic conditions. In addition, integrating machine learning based anomaly detection into the Keycloak Authentication Flow could become a promising direction for strengthening the system's security posture proactively.

REFERENCE

Al Rahat, T., Feng, Y., & Tian, Y. (2024). AuthSaber : Automated Safety Verification of OpenID Connect Programs. *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security*, 2949–2962. https://doi.org/10.1145/3658644.3670318

Bunn, C. D. S. (2024). *Evaluating Performance Impacts in Identity Management Based on Keycloak and OpenID Connect*.

Clarke, N., & Furnell, S. (2026). Usable authentication: Are we there yet? *Computers & Security*, *162*, 104823. https://doi.org/10.1016/j.cose.2025.104823

Divyabharathi, D. N., & Cholli, N. G. (2020). A Review on Identity and Access Management Server (KeyCloak). *International Journal of Electrical and Power Engineering*, *14*(2), 17–22.

Hardt, D. (2012). *The OAuth 2.0 Authorization Framework* (Issue 6749).

Hermawan, W. (2023). Single Sign On Using Keycloak Integrated Public Key Infrastructure for User Authentication In Indonesia's Electronic Based Government System. *Advance Sustainable Science Engineering and Technology*, *5*(2), 0230204. https://doi.org/10.26877/asset.v5i2.15795

Jaswanth Alahari, Dasaiah Pakanati, Harshita Cherukuri, Om Goel, & Prof.(Dr.) Arpit Jain. (2023). Best Practices for Integrating OAuth in Mobile Applications for Secure Authentication. *Universal Research Reports*, *10*(4), 385–401. https://doi.org/10.36676/urr.v10.i4.1354

Juwara, M. M., & P Nyeleker, K. (2026). The Challenges of Implementing E-government in the Public Sector: A Case Study on The Gambia. *Journal of Governance Innovation*, *7*(2), 454–475. https://doi.org/10.36636/jogiv.v7i2.7197

Kinasih, S. A., Sahputra, R., & Anwar, C. (2026). Functional Suitability Testing of Web-Based

Warehouse Inventory Application Using Black Box Testing. *Ambidextrous Journal of Innovation Efficiency and Technology in Organization*, *3*(02), 138–154. https://doi.org/10.61536/ambidextrous.v3i02.391

Manimaran, P., Garrett, T., Jehl, L., & Vitenberg, R. (2025). Decentralization trends in identity management: From federated to Self-Sovereign Identity Management Systems. *Computer Science Review*, *58*, 100776. https://doi.org/10.1016/j.cosrev.2025.100776

Meliala, R. J., Anggraeni, A., Holik, W., Manik, J. S. R., Hakim, G. J. P., Mindara, G. P., & Wicaksono, A. (2024). Web-Based Financial Information System Testing of PT Perta Sakti Abadi Using the Black Box Testing Method. *International Journal of Computer Technology and Science*, *2*(1), 58–66. https://doi.org/10.62951/ijcts.v2i1.129

Mitra, A., & Ghosh, A. (2024). FIDO2: A comprehensive study on passwordless authentication. *International Journal of Engineering Research and Applications*, *14*(7), 58–63. https://doi.org/10.9790/9622-14075863

Naghmouchi, M., Laurent, M., Levallois-Barth, C., & Kaaniche, N. (2025). Perspectives on National Digital Identity Systems. *Blockchain: Research and Applications*, 100429. https://doi.org/10.1016/j.bcra.2025.100429

Owens, K., Anise, O., Krauss, A., & Ur, B. (2021, August). User Perceptions of the Usability and Security of Smartphones as FIDO2 Roaming Authenticators. *Proceedings of the Seventeenth Symposium on Usable Privacy and Security (SOUPS)*.

Pandey, P., & Nisha, T. N. (2021). Challenges in Single Sign-On. *Journal of Physics: Conference Series*, *1964*(4), 042016. https://doi.org/10.1088/1742-6596/1964/4/042016

Sakimura, N., Bradley, J., & Agarwal, N. (2015). *Proof Key for Code Exchange by OAuth Public Clients* (Issue 7636).

Shabi, M. Al, & Marie, R. R. (2024). Analyzing Privacy Implications and Security Vulnerabilities in Single Sign-On Systems: A Case Study on OpenID Connect. *International Journal of Advanced Computer Science and Applications*, *15*(4). https://doi.org/10.14569/IJACSA.2024.0150465

Sharif, A., Carbone, R., Sciarretta, G., & Ranise, S. (2022). Best current practices for OAuth/OIDC Native Apps: A study of their adoption in popular providers and top-ranked Android clients. *Journal of Information Security and Applications*, *65*, 103097.

Sousa, B., & Gonçalves, C. (2024). FedAAA-SDN: Federated Authentication, Authorization and Accounting in SDN controllers. *Computer Networks*, *239*, 110130. https://doi.org/10.1016/j.comnet.2023.110130

Supangkat, S. H., Firmansyah, H. S., Rizkia, I., & Kinanda, R. (2025). Challenges in Implementing Cross-Border Digital Identity Systems for Global Public Infrastructure: A Comprehensive Analysis. *IEEE Access*, *13*, 42083–42098. https://doi.org/10.1109/ACCESS.2025.3547373

Tran-Truong, P. T., Pham, M. Q., Son, H. X., Nguyen, D. L. T., Nguyen, M. B., Tran, K. L., Van, L. C. P., Le, K. T., Vo, K. H., Kim, N. N. T., Nguyen, T. M., & Nguyen, A. T. (2025). A systematic review of multi-factor authentication in digital payment systems: NIST standards alignment and industry implementation analysis. *Journal of Systems Architecture*, *162*, 103402. https://doi.org/10.1016/j.sysarc.2025.103402

Vereau Jacobo, E. W. (2025). Evaluation of Keycloak as an Identity Server Versus Commercial Solutions in Multiplatform Organizations. *Proceedings of the 5th LACCEI International*

Multiconference on Entrepreneurship, Innovation and Regional Development (LEIRD).
Yusop, M. I. M., Kamarudin, N. H., Suhaimi, N. H. S., & Hasan, M. K. (2025). Advancing Passwordless Authentication: A Systematic Review of Methods, Challenges, and Future Directions for Secure User Identity. *IEEE Access*, *13*, 13919–13943. https://doi.org/10.1109/ACCESS.2025.3528960
Zhang, X., & others. (2025, August). Demystifying the (In)Security of QR Code-based Login in Real-world Deployments. *Proceedings of the 34th USENIX Security Symposium*.
Zineddine, A., Belfaik, Y., Rehaimi, A., Sadqi, Y., & Safi, S. (2025). Single Sign-On Security and Privacy: A Systematic Literature Review. *Computers, Materials & Continua*, *84*(3), 4019–4054. https://doi.org/10.32604/cmc.2025.066139