Journal of Information Systems Engineering and Management
2025, 10(61s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

A Unified Authentication and Authorization Platform for Multi-Product SaaS: Design, Implementation, and Evaluation

Kalyan Inturi

Independent Researcher, USA

ARTICLE INFO

Received: 18 Sept 2025

Revised: 26 Oct 2025

Accepted: 06 Nov 2025

ABSTRACT

The fast practice of SaaS organizations by acquiring companies is causing significant issues of identity fragmentation in authentication flows and user management interfaces. Although this problem is common, there is limited documentation on methodologies of multi-product identity unification. This paper introduces a single authentication and authorization hub that aims at overcoming these issues in acquisitive SaaS systems. It uses the architecture based on a standards-based framework that includes an OIDC service, token-time claim enrichment, central identity storage, and an event-driven replication layer. The solution shows a great pace in integration cycles, a high level of economy due to the use of previous parts, a high level of security due to regular deprovisioning, and a high level of stability during migrations. Although the implementation yields concrete benefits, it also manages to circumvent a number of constraints, such as the vendor coupling risks, past integration challenges, and authorisation model limitations. The reported platform is a viable roadmap to SaaS entities aiming to integrate identity infrastructure among the purchased products without compromising security and operational quality.

Keywords: Identity Unification, Saas Acquisition Integration, Oauth 2.0, Event-Driven Identity Replication, Multi-Tenant Authentication

I. Introduction

The fast developmental pattern in Software-as-a-Service (SaaS) organizations often involves strategic acquisitions, which, though broadening the product portfolio, are bound to cause a challenge of identity fragmentation. This fragmentation is shown in authentication flows, user management interfaces, and session semantics- with a direct hit on customer experience and operations efficiency. In analyzing the patterns of post-acquisition integration, identity consolidation is always a thorn in the flesh, and heterogeneous authentication systems introduce a rift between the end-users and the administrators. Enterprise clients are demanding smooth product ones, which pressurizes SaaS vendors to consolidate identity infrastructure without interfering with existing offerings [1].

Although this challenge is common, there is still a substantial gap in the research on the reported methodologies of identity unification in multi-products. The academic literature is strong in analyzing single authentication protocols, but there is less information provided on how these protocols can be coordinated among acquired product ecosystems. The practice in

Journal of Information Systems Engineering and Management
2025, 10(61s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

the industry also has not come with a generalized approach, and integration teams tend to come up with their unique, one-off solutions, which cannot be generalized. The formal verification of security protocols such as OAuth 2.0 and OpenID Connect is evolving and is facilitated, but its application in multi-customer product-based environments continues to be unexplored in the security research [1].

An identity platform design is a solution to these problems with a standards-based design that finds a balance between the security requirements and the integration viability. This will reduce the complexity of integration without reducing security controls by maximizing the use of identity protocols and adding flexible orchestration layers. In the platform design, it is shown that identity standardization provides a platform to build faster technical integration and enhance security due to uniform deprovisioning mechanisms.

The context of the acquisition introduced in this case study gives useful information concerning the real-world application of identity unification in enterprise SaaS. The single identity platform allowed a simplified authentication process through numerous product lines without needing to segregate the necessary data between tenants- achieving substantial time reductions in integration projects and improving existing security posture instead of worsening it [1].

II. Background and Related Work

The modern authentication and authorization frameworks are based on enterprise identity standards. OAuth 2.0 has developed fundamental patterns of delegated authorization that have remained fundamental in ensuring secure API access in distributed applications. Research relating to formal verification has shown that implementation of these protocols, when done correctly, can offer high-quality security assurances, even in practice [1]. OpenID Connect is a continuation of OAuth 2.0 by adding standardized authentication, making it possible to have identity federation among platforms. Mathematical analysis of these protocols verifies their security properties under certain threat models, but deployments of protocols in the real world usually involve new complications.

The landscape of enterprise identity is a collection of various standards that deal with various facets of identity management. Although OpenID Connect is gradually replacing modern applications, SAML 2.0 is still deeply embedded in most enterprise systems, and it has been difficult to integrate into an acquisition. SCIM 2.0 offers standard provisioning capabilities, but implementation differences may make user lifecycle synchronization across systems complicated. Their interaction in complex environments can only be analyzed through further analysis, and formal verification methodologies can be used to analyze the security properties of these protocols in isolation [1].

The identity provider extensibility is another important feature of multi-product environments that allows contextual authentication without changing the core identity services. The token customization strategies permit the injection of tenant-specific or product-specific context when making identity assertions without violating protocol compliance. These extension mechanisms strike a balance between the standardization and customization requirements.

Journal of Information Systems Engineering and Management
2025, 10(61s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Standard	Purpose
OAuth 2.0	Authorization
OpenID Connect	Authentication
SAML 2.0	Enterprise SSO
SCIM 2.0	Provisioning
Extensions	Customization
HA Techniques	Reliability

Table 1: Identity Standards [1, 2]

Identity system migration requires high-availability methods, which will meet the high stakes of authentication services in current business enterprises. A study on the patterns of cloud-native deployment shows that the progressive delivery approaches are effective in mitigating risk when changing identity infrastructures to a cloud-native setting [2]. Traffic mirroring facilitates authentication flow validation without interfering with existing sessions, whereas blue-green deployment strategies offer rollback capabilities in real time. These strategies are also useful in identity services, where the availability directly affects all interactions with users. When changing the authentication infrastructure on which all system access is based, the development of near-zero downtime strategies becomes critical. Research shows that well-coordinated migrations can achieve 99.99% availability even when making major architectural changes [2].

III. System Architecture

The identity platform architecture combines the architecture of unified identity to use a layered architecture that decouples authentication mechanisms and identity management functions. Modern microservice-based identity architectures spread the functionality of specialised services instead of monolithic identity providers. With this model, the components of the system can be expanded in response to demand trends on an individual basis, and standardized interfaces allow the character of the integration of purchased products to be gradual. Studies investigating the identity architecture of enterprises prove that the decomposed authentication services are more resilient to traffic spikes than the monolithic ones [3].

There are three main components in the identity control plane implementation, which are used to handle authentication policy and identity lifecycle. The integration of the OIDC service is the main federation layer, which accepts authentication requests via standardized OpenID connections. The studies on federated authentication show that authorization code flow with suitable security extensions offers strong security against the typical authentication attacks whilst still being compatible with enterprise identity providers [3]. Policy enrichment service acts as a critical extension point, which allows contextual authorization decisions to be made without altering the underlying identity provider. The central identity store holds

Journal of Information Systems Engineering and Management
2025, 10(61s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

the record system of identity information, which adopts a relational type of data model, giving priority to referential and query performance to make authorization decisions.

The data plane elements are used to address the functionalities of identity validation and propagation throughout the ecosystem of integrated products. The API gateway will be the main token validation point, and it will use the standards-based signature validation, with proper caching to reduce the time of validation. The subsystem of token validation performs the cryptographic verification, having rotation of keys to find the balance of security and operational stability. The event-based replication layer distributes the identity updates to the downstream systems on dependable asynchronous messaging patterns. Enterprise integration patterns have been analyzed to show that event-driven architectures result in suitable decoupling of identity management and consuming systems, where independent evolution is made possible but eventual consistency is ensured [4].

Cross-cutting issues touch upon operational needs and security needs that are necessary in enterprise identity systems. The monitoring system will effectively instrument the authentication flows comprehensively to give insight into the performance aspects and security anomalies. The security controls will deploy the principles of defense-in-depth, and the sensitive credential data and cryptographic materials will be particularly secured [4].

IV. Implementation

The implementation of the authentication flow is based on the best practices of authorization and is also able to meet the practical needs of enterprise software. PKCE (Proof Key for Code Exchange) authorization code flow is the basis of the authentication procedure, which is selected due to its strong security characteristics and compatibility with both Web and mobile applications. Scholarly studies into the vulnerabilities of OAuth 2.0 as an implementation model suggest that the PKCE extension can be used effectively to prevent attackers of authorization code, without becoming complex to use [3]. Enrichment of token-time claims allows policy evaluation to be effectively performed during authentication, with contextual authorization information being injected, subject to the user, tenant, and system parameters. This design is consistent with the literature of security studies, which shows that just-in-time claim generation minimizes token bloat and also requires fine-grained authorization. The edge validation method applies distributed verification to a proper key distribution mechanism by balancing both security and performance constraints.

The identity data model initiates a normalized relational schema and is meant to support a multi-tenant and multi-product environment and ensure the right data isolation between tenants. The entity of organization is the main tenant boundary, and it is one where hierarchical relationships are applied, akin to the enterprise organizational structures. User entity stores basic identity attributes that have proper normalization in order to facilitate cross-product recognition. The studies of identity schema design focus on the value of logical decoupling between relationship metadata and core identity attributes to accommodate a changing authorization policy [4]. The membership relationship model applies many-to-many relationships between users and groups with extra metadata of role-based access control. Product account relationships use this model to support product-specific entitlements and provide polymorphic associations to support product needs.

Journal of Information Systems Engineering and Management
2025, 10(61s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Layer	Component	Function
Control	OIDC Service	Authentication
	Policy Service	Authorization
	Identity Store	Data management
Data	API Gateway	Edge validation
	Token Validation	Verification
	Replication	Propagation

Table 2: Architecture Components [3, 4]

The replication architecture provides consistent propagation protocols in distributing identity changes between integrated products. The directed acyclic graph (DAG) orchestration methodology is a declarative model that defines the dependencies between identity consumers and executing the updates in the correct sequence, as well as allowing multiple use of parallel processing where dependencies allow it. The change event propagation applies the publish-subscribe pattern with guaranteed-delivery semantics to ensure that identity updates are delivered to all downstream systems, even in the case of intermittent connectivity. Scholarly discussion on the distributed identity synchronization has established that eventual consistency models with riskful conflict management strategies provide the balance needed between availability and consistency to enterprise identity systems running on many products [4].

V. Benefits to the Industry

The adoption of single identity architectures provides organizations that expand by acquisition with quantifiable gains in adoption speed. The studies that investigate the incorporation of technology within mergers and acquisitions indicate that identity integration is a significant path constraint that directly influences the time-to-value realization [5]. The quantification method of these benefits is analytical in nature, whereby not only the integration costs of a delayed market synergy are considered, but also the opportunity costs as a result. Time-to-value formula is a methodology that offers a systematic way of determining the financial impact of financial benefits accounted for in the preservation of revenue and efficiency in operations. Firms using standardized identity platforms show condensed integration schedules over those using customized strategies. This acceleration has impacts on the engineering efficiency and the customer retention metrics in the transition periods because the longer the integration time, the higher the churn risk. According to market research, the satisfaction of customers during acquisition transitions is much better in case the continuity of identities is provided at the very beginning [5].

Journal of Information Systems Engineering and Management
2025, 10(61s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The financial benefits of the integration projects in terms of cost profile and operational efficiency related to unified identity platforms are powerful financial benefits beyond the accelerated integration. Research on enterprise architecture related to technology standardization finds that there is high potential for savings in terms of cost due to the removal of duplicate identity infrastructures [6]. Companies with centralized identity architecture also receive fewer integration engineering demands due to the commoditization of standardized components that do not require special integration interface development. The benefits of efficiency go beyond integration in the current processes, and the support incidents would be dramatically reduced after consolidation. Studies researching microservice architecture patterns confirm that identity service standardization eases the operational model by providing uniform monitoring, deployment, and scaling strategies [6].

Improvement of security and compliance are important benefits that is not directly cost-related. A study on the vulnerability of access control systems finds fragmented identity management as the root cause of the security gap [5]. A major benefit of centralized deprovisioning in identity provider integration is the minimization of orphaned accounts risks. Constructions to support access by limited impersonation functions are solutions to operational needs and provide reasonable security constraints and detailed audit trails. Single authentication systems make it easy to comply with various regulatory regimes because of the ability to ensure that there are similar controls on authentication, authorization, and revocation of access [5].

Category	Impact	Area
Adoption	Integration speed	Acquisition
Cost	Engineering	Development
Cost	Infrastructure	Operations
Security	Session handling	Access control
Security	Deprovisioning	Lifecycle
Stability	Migration	Continuity

Table 3: Benefits to Industry [5, 6]

Mechanisms of operational stability are vital elements of enterprise-scale identity platforms, especially in terms of transition. Studies of continuity strategies see authentication services as the baseline elements that must be deployed using specific strategies [6]. The progressive delivery methodologies that are customized to identity services make them highly reliable at the time of architectural transitions. Parallel validation with production traffic mirroring offers empirical validation but does not subject users to the possibility of disruption. Automated rollback systems are important risk mitigation systems that can go a long way in minimizing the possible business impact in case of unforeseen integration failure [6].

Journal of Information Systems Engineering and Management
2025, 10(61s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

VI. Challenges and Constraints

In spite of these powerful advantages, there are major challenges to the implementation of unified identity platforms. The risk of vendor coupling and the control plane is the main issue when outsourcing authentication services. Legal and economic studies analyzing the dependence of technologies establish dimensions of vendor risk that need to be systematically considered such as the effects of market concentration and switching costs involved with identity infrastructure [7]. Firms that embrace single platforms should decide on the tolerable degrees of reliance, especially when these services are used as key facilities of all interactions with customers. Examples of effective mitigation strategies found in the literature involve contractual safeguarding with definite service degree guarantees, architectural patterns with functional separation, and operational protocols with authentication functionality throughout interruptions by providers.

Complexities in integration: Legacy integrations are technically difficult, especially when the acquired systems use divergent authentication methods. Studies of models of enterprise federation point to heterogeneity of SAML implementations, where custom extensions and non-standard attribute mappings form a major barrier to integration [7]. Such variations require the development of adapters to normalize authentication assertions, which raises the engineering requirements in addition to testing complexity. Several authentication flows, numerous federation options, and edge cases of session management make authentication testing requirements outweigh common API verification strategies. Economics have shown that authentication standardization is more expensive in the short run than other integration areas, but it generates significant long-term payoff in the form of less complexity and enhanced security.

Limitations of the authorization model are a continuous issue in the implementation, even on mature systems. Studies concerning authorization structures determine inherent conflicts between engineering and situational decision-making [8]. Authorization gaps that are policy-based occur when application-specific models of permissions are changed to unified models, since, in many cases, application product-specific contexts are not available to the identity provider model. This shortcoming impacts the gaining of centralized decisions, necessitating a hybrid structure between standardization and situational awareness. New models that solve the shortcomings of the present-day methods are attribute-based access control and graph-based permission engines, which are in a position to model intricate organizational affiliations.

VII. Evaluation

Detailed assessment tools will offer the requisite authentication of the identity platform application, ensuring technical efficiency and business value realization. Integration velocity is one of the key indicators of evaluating the performance of the platform, and it has a direct effect on business results in the process of acquisition integration [8]. The analysis of the academic sources determines some indicators, such as the improvement of the successful time-to-value realization and efficiency within engineering. Standardized platforms show a significant reduction in integration schedules relative to customized strategies, so that integrated customer experiences can be dispatched quickly. Such acceleration is based on uniform patterns of integration, extensive documentation, and reusable elements that

Journal of Information Systems Engineering and Management
2025, 10(61s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

minimize custom engineering needs. Studies have highlighted the fact that standardized methods not only decrease the processes of integration but also enhance quality outcomes as a result of uniform implementation patterns.

Cost performance analysis is an objective form of validating the economic advantages of unified methods of identity. Studies investigating the economics of technology standardization also determine various dimensions of cost avoidance, such as direct engineering savings, benefits of infrastructure consolidation, and continued operation enhancement [7]. Economic analysis shows that identity standardization has a tendency to pay back beginning in the first year of operation and continuing into the life cycle of integrated products. The evaluation of costs should be done in a comprehensive way by taking into consideration the integration savings in the short run and operational benefits in the long run to be able to fully evaluate the economic impact of unified platforms.

The improvements in security posture are very important non-financial gains of unified identity implementations. A study on authentication architectures suggests that there are a number of security improvements that are achieved due to standardized identity management [8]. The session handling enhancements also allow uniform authentication controls across integrated products and synchronized session termination over serious vulnerabilities to fragmented conceptions. Similar improvements are seen with privileged access controls that demonstrate time-rated, scoped access with extensive audit trails. Security analysis focuses on the fact that single solutions not only simplify operations, but also directly overcome the frequent authentication vulnerabilities inherent in a distributed architecture.

Category	Challenge	Mitigation	Impact
Risk	Vendor coupling	Contracts	Dependency
Technical	Legacy systems	Adapters	Integration
Model	Authorization limits	Hybrid approach	Flexibility
Metrics	Integration speed	Standardization	Time-to-value
Context	Organization size	Adaptation	Generalizability
	Regulatory needs	Compliance	Security

Table 4: Challenges & Evaluation [7, 8, 9, 10]

The validation of reliability and user experience is based on the results of operational stability. The studies of the methods of technology migration have determined a number of strategies that can be used to maintain continuity in authentication as the infrastructure changes [8]. Progressive delivery plans provide the possibility of verifying identity requests by processing in parallel and detecting possible compatibility problems in advance, before exposing the customer to them. The methods ensure the availability of authentication during migration phases and ensure that the functionality of legacy services and modernized services can be validated. User experience metrics do not change or increase when identity

Journal of Information Systems Engineering and Management
2025, 10(61s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

transitions have been implemented successfully, and the need to support reduces after standardization.

VIII. Ethics and Disclosure

The research ethics framework that will be employed in this research will be applied to have transparent disclosure mechanisms, and at the same time, have the right boundaries of the proprietary information. Recent studies looking into disclosure practices in a technology case study indicate that it is crucial to balance transparency and deference to valid commercial interests, especially when the research is of applied technology implementations as opposed to an exclusively academic exercise [9]. This study practices partial identification, revealing the names of main organizations but not providing a finer description of the systems within the company and its internal structure. The ethics framework also highlights the need to explain the source of data and limitations, especially in cases where the research involves a combination of public data and internal documentation. This research is based on publicly available documentation as well as duly anonymized project reports, with recommended approaches to the utilization of commercial information in research applied.

The responsible research practice needs to state the presence of evaluation limitations on interpretation and generalizability. The recent literature that focuses on assessing the evaluation models of enterprise architecture projects highlights that organizational attributes largely determine the implementation strategies as well as the achieved results [10]. The implementation described is an experience in a particular organizational setting having certain features of the technical debt, engineering capabilities, and architecture underpinnings. Organizations with radically different natures could have different obstacles and advantages with respect to employing the same strategies.

The industry factors make the generalizability in various business areas come with extra considerations. A study that investigates the implementations of identity management in industries finds wide differences in the requirements depending on the regulatory landscape, the nature of customers, and the modes of delivery [10]. Organizations operating in the highly regulated industries have supplementary compliance requirements that play a major role in identity architecture decisions. The multi-tenant SaaS service delivery model under consideration has certain architectural requirements that vary from the single-tenant model and on-premises deployment models. Although architectural patterns can be of great help when used in different fields, there are cases where unique implementation strategies must be adopted depending on the industry-related needs and limitations.

Conclusion

The described unified identity platform forms a viable strategy towards the resolution of authentication and authorization issues within an acquiring SaaS environment. Through standards-based architecture and flexible orchestration layers, the platform facilitates expedited integration schedules in addition to augmenting security disposition through steady controls. The indicated advantages in the adoption speed, the price cut, the security improvement, and the stability of the operations confirm the solution as the possible one in case of multi-product SaaS companies. The issues, such as the need to maintain a close

relationship with the vendor, the complexities involved in integrating the legacy, and the drawbacks of the authorization model, point to the issues that need to be carefully considered during the implementation. The offered patterns of architecture apply to a wide scope of SaaS organizations in the process of their growth, with the involvement of acquisition, yet the adaptation to the context is required depending on the organizational peculiarities and the needs of the industry. The next step is investigations in the field of attribute-based authorization models, more extensive capabilities in contextual decisions, and additional development of integration patterns to make the implementation of various authentication systems even simpler.

References

[1] Gerasimos Charizanis et al., "Data-Driven Decision Support in SaaS Cloud-Based Service Models," MDPI, 2025. [Online]. Available: https://www.mdpi.com/2076-3417/15/12/6508

[2] Antra Malhotra et al., "Evaluate Solutions for Achieving High Availability or Near Zero Downtime for Cloud Native Enterprise Applications," ResearchGate, 2023. [Online]. Available: https://www.researchgate.net/publication/373027597_Evaluate_Solutions_for_Achieving_High_Availability_or_Near_Zero_Downtime_for_Cloud_Native_Enterprise_Applications

[3] Aisha Saeed, "Authentication and Authorization Modules for Open Messaging Interface (O-MI)," Aalto University, 2018. [Online]. Available: https://aaltodoc.aalto.fi/server/api/core/bitstreams/002d50fc-c76d-4541-a370-fc04b6c74d7e/content

[4] Matthew Benjamin, "Microservices Architecture for Scalable Enterprise Applications," ResearchGate, 2025. [Online]. Available: https://www.researchgate.net/publication/389817361_Microservices_Architecture_for_Scalable_Enterprise_Applications

[5] Karolis Andriuskevicius, "M&A Performance and Economic Impact: Integration and Critical Assessment of Methodological Approach," VUT, 2017. [Online]. Available: https://journals.vut.cz/index.php/trends/article/view/578

[6] Tri Hoang Vo et al., "Identity-as-a-Service: An Adaptive Security Infrastructure and Privacy-Preserving User Identity for the Cloud Environment," MDPI, 2019. [Online]. Available: https://www.mdpi.com/1999-5903/11/5/116

[7] Ashutosh Ahuja, "A Detailed Study on Security and Compliance in Enterprise Architecture," SSRN, 2025. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5114289

[8] Anna Kotonen, "Data-Driven Product Portfolio Process Development - Navigating Growth and Strategic Decision-Making," Aalto University, 2025. [Online]. Available: https://aaltodoc.aalto.fi/items/01247336-ae1c-45b4-a23d-aed0c84034ce

[9] Sujata Singh, "Corporate Responsibility: Transparency and Disclosure," SSRN, 2025. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5094766

[10] Anniina Saari et al., "Best practices for blockchain-driven digital transformation in cross-industry settings," ScienceDirect, 2025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2666954425000225