African Journal of Advanced Pure and Applied Sciences (AJAPAS)
Online ISSN: 2957-644X
Volume 5, Issue 3, 2026
Page No: 1-19
Website: https://aaasjournals.com/index.php/ajapas/index
ISI 2025: 1.126 **SJIFactor 2024: 6.752** **معامل التأثير العربي: 1.62**

Enterprise Integration Challenges in Libya's Digital Transformation Journey: A Government Service Bus Perspective

Abdunnaser A. Diaf [1 *], Hajir O. Asmeea [2], Ramzi H. Elghanuni [3]
[1,2,3] Dept. of Internet Technology, Faculty of IT, University of Tripoli, Tripoli, Libya

تحديات التكامل المؤسسي في مسيرة التحول الرقمي في ليبيا: منظور قائم على ناقل الخدمات الحكومية (*GSB*)

عبد الناصر ضياف [1*]، هاجر اسميع [2]، رمزي القانوني [3]
[3،2،1] قسم تقنيات الإنترنت، كلية تقنية المعلومات، جامعة طرابلس، طرابلس، ليبيا

*Corresponding author: aadiaf@uot.edu.ly

Received: April 14, 2026	Accepted: June 20, 2026	Published: July 01, 2026

Abstract:
Government digital transformation initiatives increasingly depend on secure and governed interoperability among public-sector institutions. Yet fragmented information systems, organizational silos, and the absence of common integration standards continue to impede the delivery of integrated government services—challenges particularly pronounced in emerging digital government environments such as Libya. This paper presents a Government Service Bus (GSB) reference architecture grounded in Enterprise Architecture principles and evaluates its practical applicability through the *Nawa* interoperability pilot, a GSB-based proof-of-concept connecting four Libyan governmental institutions: the Tax Authority, Commercial Registry, Central Bank of Libya, and Customs Authority. Implemented by a five-member team within approximately one month using exclusively open-source technologies, the pilot successfully deployed 23 cross-agency services supporting taxpayer verification, compliance assessment, and tax-clearance workflows. The solution demonstrated that a standards-based interoperability platform can substantially reduce integration complexity. For the four participating institutions, the required integration links were reduced from six point-to-point connections to four governed interfaces while preserving institutional autonomy and existing information systems. The proposed solution was subsequently awarded first place in a national interoperability hackathon organized under the patronage of the General Information Authority and Expertise France in Libya. The findings indicate that successful interoperability initiatives require governance structures, regulatory modernization, and organizational readiness alongside technical integration capabilities. The paper further discusses governance, organizational, and regulatory considerations, together with a phased roadmap for scaling GSB adoption within Libya's emerging digital government ecosystem.

Keywords: Enterprise Architecture (EA), Government Service Bus (GSB), Government Interoperability, Digital Government, Service-Oriented Architecture (SOA), E-Government Interoperability, API Governance, Open-Source Integration, Public Sector Digital Transformation, Libya.

الملخص
تعتمد مبادرات التحول الرقمي الحكومي بصورة متزايدة على تحقيق تشغيل بيني آمن ومحكوم بين مؤسسات القطاع العام. ومع ذلك، لا تزال الأنظمة المعلوماتية المتباينة، والصوامع المؤسسية، وغياب معايير التكامل الموحدة تشكل عوائق رئيسية أمام تقديم خدمات حكومية متكاملة، وهي تحديات تزداد وضوحًا في بيئات الحكومات الرقمية الناشئة، مثل ليبيا. تقدم هذه الورقة معمارية مرجعية لناقل الخدمات الحكومية (GSB) تستند إلى مبادئ هندسة المؤسسات (EA)، كما تقيّم قابليتها للتطبيق عمليًا من خلال مشروع نواة، وهو نموذج إثبات فكرة قائم على ناقل الخدمات الحكومية، يربط أربع مؤسسات حكومية ليبية هي: مصلحة الضرائب، والسجل التجاري، ومصرف ليبيا المركزي، ومصلحة الجمارك. وقد نُفِّذ المشروع بواسطة فريق مكوّن من خمسة أعضاء خلال مدة تقارب شهرًا واحدًا، اعتمادًا بالكامل على تقنيات مفتوحة المصدر، حيث

تم نشر 23 خدمة للتشغيل البيني على متن الناقل دعمت عمليات التحقق من بيانات الممولين وتقييم الامتثال الضريبي وإجراءات إصدار شهادات السداد الضريبي. وأظهرت النتائج أن منصة تشغيل بيني قائمة على المعايير القياسية يمكنها الحد بصورة ملحوظة من تعقيد عمليات التكامل؛ إذ انخفض عدد وصلات التكامل المطلوبة بين المؤسسات الأربع المشاركة من ست وصلات ربط مباشر (نقطة-إلى-نقطة) إلى أربع واجهات تكامل محكومة، مع المحافظة على الاستقلالية المؤسسية واستمرار عمل الأنظمة المعلوماتية القائمة. كما حصد الحل المقترح المركز الأول في هاكاثون وطني للتشغيل البيني أُقيم برعاية الهيئة العامة للمعلومات ومؤسسة خبراء فرنسا في ليبيا. وتشير نتائج الدراسة إلى أن نجاح مبادرات التشغيل البيني لا يعتمد على القدرات التقنية وحدها، وإنما يتطلب أيضًا أطرًا فعّالة للحوكمة، وتحديثًا للتشريعات، وجاهزية تنظيمية ومؤسسية داعمة. كما تناقش الورقة الجوانب المتعلقة بالحوكمة والتنظيم والأطر التشريعية، وتقترح خارطة طريق مرحلية لتوسيع تبني ناقل الخدمات الحكومية ضمن منظومة الحكومة الرقمية الناشئة في ليبيا.

الكلمات المفتاحية: هندسة المؤسسات، ناقل الخدمات الحكومية، التشغيل البيني الحكومي، الحكومة الرقمية، المعمارية الموجهة نحو الخدمات، التشغيل البيني للحكومة الإلكترونية، حوكمة واجهات برمجة التطبيقات، التكامل باستخدام البرمجيات مفتوحة المصدر، التحول الرقمي في القطاع العام، ليبيا.

1. Introduction

Governments worldwide are pursuing ambitious digital transformation initiatives aimed at improving service delivery, enhancing operational efficiency, increasing transparency, and enabling data-driven decision making. As public institutions evolve from isolated administrative entities toward interconnected digital ecosystems, they face growing challenges associated with organizational complexity, fragmented information systems, duplicated data, and inconsistent service delivery mechanisms. This fragmentation frequently requires citizens and businesses to repeatedly submit identical information and supporting documents to multiple public-sector institutions, even when such information already exists elsewhere within the public sector.

Addressing these challenges requires more than the deployment of individual technologies or standalone applications. It requires a structured approach that aligns organizational objectives, business processes, information assets, applications, and technology platforms within a coherent governance framework. This need has led to the widespread adoption of Enterprise Architecture (EA) as a foundational discipline for planning, governing, and evolving complex organizational environments. EA provides a holistic view of the enterprise and establishes a common framework through which strategic objectives can be translated into business capabilities, information systems, and supporting technologies [1]. Through architectural principles, standards, and governance mechanisms, EA enables organizations to reduce complexity, improve interoperability, promote reuse of shared capabilities, and ensure that technology investments remain aligned with institutional goals.

Although EA frameworks vary in terminology and methodology, they generally organize architectural concerns into four closely related domains: Business Architecture, which defines organizational objectives, capabilities, processes, stakeholders, and governance structures; Application Architecture, which describes the systems and services that support business operations and deliver organizational capabilities; Data Architecture, which governs the structure, ownership, quality, exchange, and lifecycle management of information assets; and Technology Architecture, which encompasses the infrastructure, networks, platforms, security mechanisms, and technical services upon which applications and data depend [1]. Collectively, these domains provide a comprehensive architectural blueprint that enables organizations to manage change systematically while maintaining consistency across business and technology initiatives. The relationships among the principal EA domains and their supporting governance mechanisms are presented in Fig. 1. The figure shows how the four principal EA domains collectively contribute to organizational objectives while operating under common governance principles and architectural standards.

Together, these domains provide a structured framework that aligns business capabilities, information assets, applications, and technology infrastructure under a common governance model. Within the public sector, EA assumes particular significance because governmental organizations typically operate through multiple ministries, agencies, authorities, and administrative units, each possessing distinct responsibilities, information systems, and operational procedures. While such institutional specialization is necessary for governance, it often results in fragmented digital landscapes that hinder information sharing and complicate the delivery of integrated public services [2], [3]. Citizens and businesses, however, interact with government as a unified service provider rather than as a collection of independent organizations. Consequently, modern digital government strategies increasingly emphasize interoperability, data sharing, service integration, and whole-of-government service delivery models [2], [4].

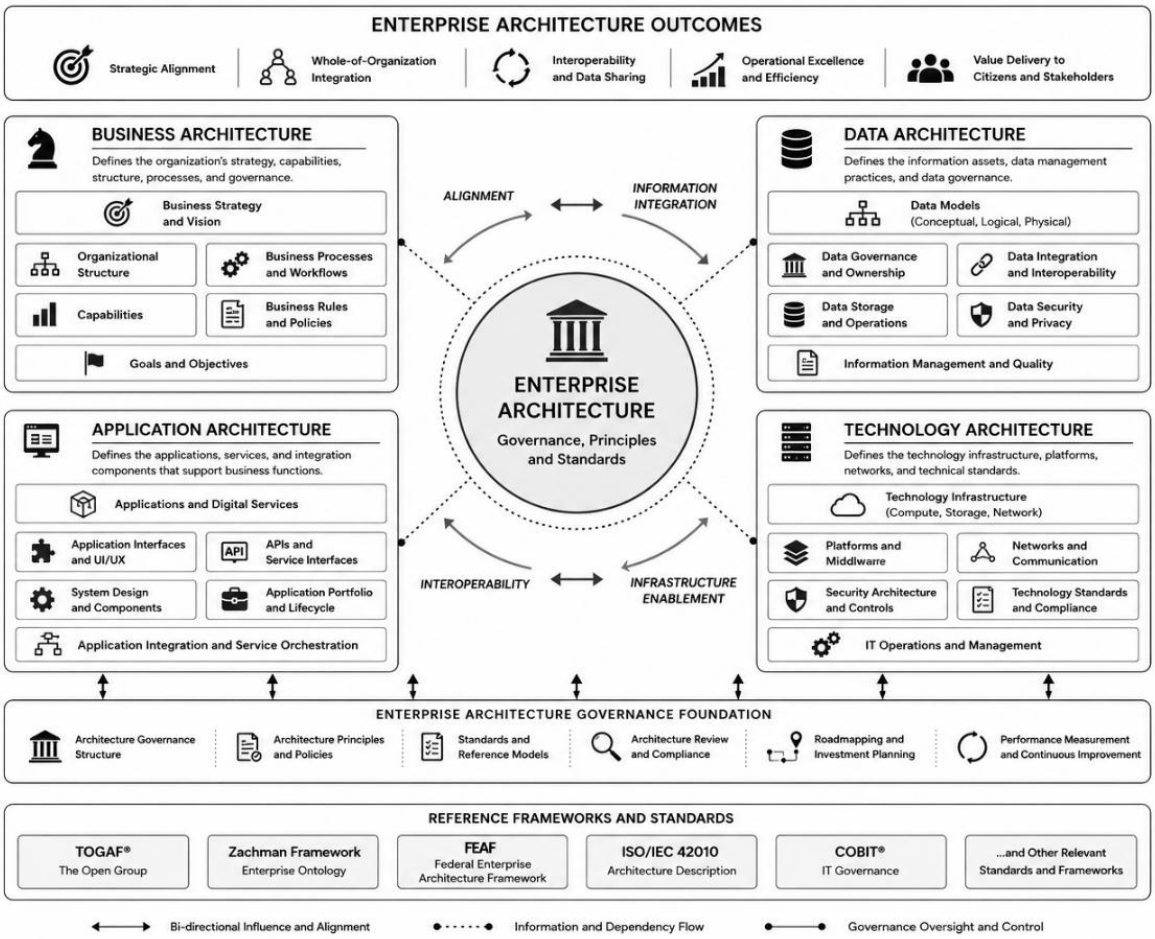

Fig. 1. *Conceptual view of Enterprise Architecture domains and their interrelationships within a governance-driven digital transformation framework.*

This architectural discipline provides the strategic and governance foundation necessary to achieve these objectives. By establishing common standards, architectural principles, data models, and integration policies, it creates the conditions under which heterogeneous systems can operate as components of a unified digital ecosystem rather than isolated technological silos [1], [2]. However, achieving interoperability in practice requires more than architectural guidance alone; it demands integration capabilities capable of enabling secure, standardized, and scalable communication among diverse systems and institutions.

Against this backdrop, modern government architectures increasingly incorporate dedicated integration platforms that facilitate information exchange and service orchestration across organizational boundaries [2], [4]. Such platforms represent the operational realization of the interoperability objectives established by EA and constitute a critical component of contemporary digital government ecosystems. Among the architectural approaches commonly adopted to address these integration requirements is the Government Service Bus (GSB), which provides a standardized mechanism for connecting heterogeneous systems, enabling service interaction, and supporting government-wide digital integration.

The main contributions of this paper can be summarized as follows:

- It identifies and analyzes key interoperability barriers affecting digital transformation initiatives in the Libyan public sector.
- It proposes GSB reference architecture grounded in EA principles and public-sector interoperability requirements.
- It presents the design and implementation of the *Nawa* pilot as a practical proof-of-concept demonstrating cross-agency information exchange among four governmental institutions.
- It discusses governance, organizational, and regulatory considerations relevant to the nationwide adoption of interoperability capabilities within Libya's emerging digital government ecosystem.

1.1 Research Approach

This study adopts an applied case-study approach to investigate the practical applicability of a GSB for improving interoperability within the Libyan public sector. The research combines a qualitative analysis of interoperability

challenges with the architectural design, implementation, and evaluation of the *Nawa* pilot, which involved four governmental institutions participating in a national interoperability initiative. Rather than proposing a purely conceptual framework, the study validates the proposed architecture through the implementation of a real-world proof of concept. The evaluation focuses on the resulting interoperability model, integration complexity, architectural feasibility, implementation outcomes, and organizational implications observed during the pilot. The findings are interpreted in light of EA principles and contemporary digital-government interoperability practices.

The remainder of this paper examines the role of the GSB within the broader EA context and evaluates its potential contribution to overcoming interoperability barriers and enabling secure, scalable, and integrated digital government services.

2. Related Work

2.1 Enterprise Architecture in Digital Government

EA has become a widely recognized discipline for managing complexity and guiding digital transformation initiatives within both public- and private-sector organizations. In government environments, EA provides a structured framework for aligning organizational objectives, business processes, information assets, applications, and technology infrastructure under a common governance model [1]. Numerous studies have identified EA as a key enabler of digital government transformation due to its ability to support strategic alignment, interoperability, service integration, and organizational modernization. By establishing common architectural principles, standards, and governance mechanisms, EA assists public institutions in reducing fragmentation, improving coordination among agencies, and promoting the reuse of shared capabilities [2], [4].

Within the public sector, EA assumes particular importance because government services frequently span multiple institutions, each operating under distinct mandates, information systems, and administrative procedures. Consequently, digital government initiatives increasingly rely on EA frameworks to facilitate cross-agency collaboration, data sharing, and integrated service delivery. Frameworks such as TOGAF, the European Interoperability Reference Architecture (EIRA), and various national EA initiatives have emphasized the role of architecture-driven governance in supporting whole-of-government approaches to digital transformation [1], [2].

A recurring theme in the literature is that interoperability challenges are rarely attributable to technology alone. Rather, they often arise from a combination of organizational, semantic, procedural, and regulatory factors. EA addresses these challenges by providing a common language through which stakeholders can model business capabilities, define information exchange requirements, establish governance structures, and coordinate technology investments across institutional boundaries [4]. Despite the broad recognition of EA as a strategic enabler of digital government, the practical realization of interoperability objectives requires integration mechanisms capable of supporting secure and governed information exchange among heterogeneous systems. This requirement has led many governments to complement EA initiatives with interoperability platforms and GSB infrastructures designed to operationalize architectural principles at the implementation level.

2.2 Government Service Bus Initiatives

Over the past two decades, numerous governments have adopted interoperability platforms and GSB-like architectures as foundational components of their digital transformation strategies. Although implementation approaches vary according to institutional, legal, and technological contexts, these initiatives share a common objective: enabling secure, standardized, and scalable information exchange among public-sector institutions while reducing fragmentation and duplication of effort.

One of the most frequently cited examples is Estonia's X-Road, which provides a secure distributed data exchange layer connecting public-sector institutions and private-sector organizations through standardized interoperability mechanisms. The platform has played a central role in Estonia's digital government ecosystem and is widely regarded as a benchmark for national interoperability infrastructures [5], [6]. In the Middle East, Saudi Arabia established the Yesser e-Government Program to promote interoperability and coordinated digital service delivery across government agencies. The initiative introduced common standards, shared services, and integration capabilities intended to support nationwide digital transformation objectives [7]. Similar interoperability initiatives have emerged in other regions. Serbia implemented a GSB platform to facilitate information exchange among public institutions and support the delivery of integrated electronic services. Likewise, Greece developed its Interoperability Center as a national integration infrastructure enabling secure communication and data exchange among governmental entities [8], [9]. Jordan has also pursued interoperability through its e-Government Program, which emphasizes service integration, data sharing, and institutional coordination as key enablers of digital government development [10].

Despite differences in governance models and technical implementations, these initiatives consistently demonstrate the importance of interoperability platforms in enabling whole-of-government service delivery. They further illustrate how EA principles can be operationalized through integration infrastructures that support secure information exchange, service reuse, and cross-agency collaboration [3].

2.3 Research Gap

While previous studies have examined interoperability frameworks and national GSB initiatives in mature digital government environments, limited attention has been given to interoperability adoption challenges within emerging digital government ecosystems such as Libya. Furthermore, relatively few studies have documented practical interoperability pilots implemented under the organizational, regulatory, and technological constraints commonly encountered in developing-country contexts. This paper seeks to address this gap by examining interoperability challenges in the Libyan public sector and presenting the *Nawa* pilot as a practical GSB-based interoperability model involving four governmental institutions.

3. Interoperability Challenges in Digital Government Ecosystems

Interoperability challenges in digital government environments extend beyond technology platforms and system integration mechanisms. While technical capabilities constitute an essential enabler of digital transformation, successful nationwide interoperability also depends on governance structures, institutional readiness, regulatory adaptation, and organizational alignment. Consequently, understanding the barriers that inhibit interoperability requires a broader examination of organizational, procedural, legal, and technological factors.

3.1 The Digital Transformation Paradox

Over the past two decades, governments worldwide have invested heavily in digitization initiatives, deploying information systems, automating administrative processes, and introducing online portals for citizen services. These efforts have improved operational efficiency and expanded access to public services. Nevertheless, many governments continue to face significant challenges in delivering integrated and seamless digital services despite substantial investments in information and communication technologies. A key explanation for this phenomenon lies in the distinction between digitization and digital transformation. Digitization primarily focuses on converting paper-based processes into electronic workflows, whereas digital transformation seeks to fundamentally redesign service delivery through organizational integration, process reengineering, and data-driven decision making. Consequently, the successful automation of individual institutions does not necessarily result in an integrated digital government ecosystem [4].

In many cases, ministries, agencies, and public authorities have independently modernized their internal operations while remaining largely disconnected from one another. Although such initiatives often improve institutional efficiency, they frequently lead to citizen-facing fragmentation, where individuals must interact separately with multiple agencies to complete a single life event, such as registering a business, obtaining permits, or applying for social benefits. This fragmentation is compounded by multiple registrations of identical information and repeated verification procedures across different institutions.

Furthermore, service delivery frequently remains siloed, with agencies offering technologically advanced digital services that lack institutional interoperability. Consequently, modern digital government strategies increasingly emphasize interoperability, data sharing, service integration, and whole-of-government service delivery models [2], [4]. The challenge therefore lies not in the absence of digital systems but in the inability of those systems to operate as a coherent government-wide ecosystem.

3.2 Institutional and Technical Interoperability Barriers

To understand why digitization has not matured into comprehensive digital transformation, it is necessary to examine the barriers that inhibit interoperability across organizational boundaries. Consistent with international interoperability frameworks, these barriers can be classified into organizational, semantic, technical, and legal/regulatory categories [2].

Organizational Barriers

Public institutions typically operate within well-defined administrative boundaries characterized by distinct mandates, governance structures, budgets, and operational priorities. While such specialization is necessary for effective governance, it often results in institutional silos that limit collaboration and impede information sharing. Weak cross-agency governance mechanisms, unclear ownership of shared data assets, and resistance to organizational change further complicate interoperability initiatives.

Semantic Barriers

Interoperability requires not only technical connectivity but also a common understanding of exchanged information. Different institutions frequently employ divergent definitions, classifications, and representations of identical real-world entities. For example, the same individual may be represented as a Citizen, National ID Holder, Taxpayer, Beneficiary, or Student, depending on the institutional context. Without harmonized data definitions and canonical information models, duplication, inconsistency, and misinterpretation inevitably emerge.

Technical Barriers
Many government organizations continue to rely on heterogeneous technology environments consisting of legacy systems, proprietary platforms, and independently developed applications. These systems often utilize incompatible communication protocols, data formats, and interface standards. Historically, interoperability requirements have frequently been addressed through direct point-to-point integrations, which become increasingly difficult to maintain and scale as the number of participating systems grows.

Legal and Regulatory Barriers
Interoperability initiatives must also address legal and regulatory considerations associated with privacy protection, data ownership, information governance, and institutional mandates. Ambiguities regarding data stewardship responsibilities and information-sharing authority often discourage collaboration, even when technical integration capabilities are available. The absence of comprehensive interoperability policies further reinforces fragmentation across the public sector. Taken together, these barriers demonstrate that interoperability is not merely a technical challenge but a multidimensional governance issue requiring coordinated organizational, semantic, technical, and regulatory responses.

3.3 Interoperability Challenges in the Libyan Context

Legacy Information Systems
The Libyan public sector has witnessed increasing adoption of information systems across various governmental institutions. However, many of these systems have been developed independently over extended periods, often by different vendors and using diverse technologies. The resulting heterogeneity has produced a fragmented technology landscape characterized by varying architectural approaches, inconsistent integration capabilities, and limited interoperability support.

Fragmented Data Ownership
Critical national information assets—including citizen records, business registration information, taxation data, educational records, and land-related information—are distributed across multiple institutions. While such specialization reflects organizational responsibilities, it frequently limits the ability to establish a unified view of citizens, businesses, and government operations.

Limited Integration Standards
A further challenge arises from the limited availability of common integration standards and governance mechanisms. In the absence of a national interoperability framework, canonical data models, standardized API policies, and shared integration guidelines, interoperability initiatives are often implemented on a case-by-case basis, increasing complexity and reducing opportunities for reuse.

Governance and Procedural Challenges
Beyond technological considerations, interoperability initiatives depend heavily on the existence of clear governance structures, standardized procedures, and formally documented administrative processes. In many public-sector environments, operational practices have historically evolved through institutional convention and accumulated experience rather than through comprehensive, formally maintained procedural frameworks. The absence of unified process documentation, standardized operating procedures, and authoritative implementation guidelines can result in variations in interpretation and execution across institutions. Such variations complicate efforts to harmonize business processes, establish common service models, and implement interoperable digital solutions. As a consequence, integration initiatives frequently encounter difficulties in defining authoritative workflows, identifying ownership responsibilities, and ensuring consistent service delivery across organizational boundaries.

Legislative and Regulatory Modernization Challenges
A further challenge concerns the alignment of legislative and regulatory frameworks with contemporary digital government requirements. Many administrative laws and regulations were originally developed for paper-based operating environments and may not adequately address emerging issues such as digital identity, electronic transactions, data sharing, interoperability governance, API-based service delivery, and cross-agency information exchange [3]. In addition, the pace of technological innovation often exceeds the rate at which regulatory frameworks evolve. This gap may create uncertainty regarding data-sharing responsibilities, digital service ownership, and institutional authority for information exchange. Consequently, modernization of interoperability capabilities frequently requires not only technological transformation but also corresponding legal and regulatory adaptation capable of supporting contemporary digital government objectives.

Digital Leadership and Institutional Capacity
Successful digital transformation initiatives require leadership structures capable of aligning technology strategy with organizational objectives. International experience suggests that large-scale interoperability programs are more likely to succeed when decision-making processes are supported by multidisciplinary expertise spanning public administration, EA, information governance, cybersecurity, and digital service delivery. Where such expertise is insufficiently represented within strategic planning and governance processes, interoperability initiatives may face challenges related to prioritization, coordination, architectural consistency, and long-term sustainability.

Duplication of Citizen Data
Citizens and businesses are frequently required to repeatedly provide identical information, including national identification details, family records, business registration information, and contact information, to multiple public-sector institutions. Such duplication increases administrative burden while simultaneously increasing the likelihood of inconsistencies across information systems.

Operational Consequences
The cumulative impact of these challenges includes delays in service delivery, increased operational costs, reduced data quality, and limited decision-support capabilities. These issues hinder the realization of integrated public services and constrain the broader objectives of digital transformation. Consequently, improving interoperability represents a strategic prerequisite for establishing an effective and sustainable digital government ecosystem in Libya. Overall, achieving nationwide interoperability in Libya should be viewed not merely as a technology modernization effort, but as a broader institutional transformation initiative encompassing governance, legislation, organizational processes, and leadership capacity.

3.4 Limitations of Traditional Integration Approaches

Manual Data Exchange
In many organizational environments, information exchange continues to rely on manual mechanisms such as spreadsheets, email attachments, and paper-based documentation. While these approaches may provide short-term operational flexibility, they remain vulnerable to delays, inconsistencies, duplication, and human error. Moreover, they are incapable of supporting real-time service integration.

Database-to-Database Links
Direct database connectivity is another frequently adopted integration mechanism. Although it may facilitate information sharing between selected systems, it introduces tight coupling, security concerns, and governance challenges. Changes within one system can directly affect dependent systems, increasing maintenance complexity and reducing organizational agility.

Integration Complexity
Point-to-point integration approaches suffer from fundamental scalability limitations. As the number of participating systems increases, the number of required integration links grows according to:

$$Integration\ Complexity\ L \approx \frac{N(N-1)}{2}$$

where (N) denotes the number of participating systems and (L) represents the number of integration links.
This relationship illustrates how integration complexity grows disproportionately as government ecosystems expand, making maintenance, monitoring, governance, and change management increasingly difficult. For the four institutions participating in the *Nawa* pilot, a traditional point-to-point integration approach would require six separate integration links. As commonly observed in enterprise integration environments, the number of integration links grows rapidly as additional systems are introduced, resulting in increased maintenance and governance complexity [11], [12]. In contrast, the GSB model requires each institution to establish a single connection to the interoperability platform, resulting in only four institutional connections. As the number of participating entities grows, the reduction in integration complexity becomes increasingly significant.

Concluding Statement
Traditional integration mechanisms do not scale adequately to satisfy nationwide interoperability requirements. They increase operational complexity, reinforce institutional fragmentation, and hinder the realization of integrated digital services. These limitations highlight the need for a strategic integration architecture capable of supporting secure, standardized, and scalable information exchange across organizational boundaries, a role increasingly fulfilled by GSB architectures in modern digital government ecosystems.

3.5 Toward a GSB-Based Integration Strategy

The analysis presented in the preceding subsections demonstrates that interoperability remains a principal obstacle to integrated digital government services. Organizational fragmentation, semantic inconsistencies, heterogeneous technology environments, and regulatory constraints collectively impede effective information exchange across institutional boundaries, causing public-sector organizations to operate as isolated digital entities despite continued investments in digitization and systems modernization. These challenges are particularly evident where information systems have evolved independently, ownership of information assets is distributed across multiple agencies, and common interoperability standards are lacking. Under such conditions, traditional integration approaches—including manual information exchange, direct database connectivity, and point-to-point integration—become increasingly difficult to govern, maintain, and scale. Consequently, a more systematic and sustainable integration strategy becomes essential.

To address these limitations, governments worldwide have increasingly adopted centralized interoperability platforms that enable secure, standardized, and governed information exchange across public-sector institutions [2], [4]. Among these, the GSB has emerged as one of the most widely adopted architectural approaches for establishing a shared integration backbone among heterogeneous information systems. Rather than replacing existing applications or databases, a GSB introduces a standardized interoperability layer through which organizations can expose services, exchange information, enforce security policies, and participate in coordinated cross-agency business processes while preserving institutional autonomy and protecting existing technology investments.

Although Libya has made tangible progress toward digital transformation, interoperability barriers continue to limit the delivery of integrated public services. Existing information systems remain largely fragmented across institutional boundaries, resulting in duplicate data, inconsistent service delivery, and limited information exchange among public-sector institutions. Against this backdrop, this paper investigates the extent to which a GSB, implemented within an EA framework, can provide a practical foundation for improving interoperability and enabling government-wide digital integration.

4. GSB Architecture and Design Principles

The GSB is a nationwide interoperability platform that enables secure, standardized, and governed information exchange among public-sector institutions. Rather than relying on numerous point-to-point integrations among government institutions, the GSB provides a shared integration backbone through which services can be exposed, discovered, consumed, governed, and monitored under common architectural standards and policies [13].

From an EA perspective, the GSB is not merely middleware. It constitutes the architectural realization of interoperability requirements, providing the technical and governance capabilities required to transform fragmented information systems into a coherent digital government ecosystem. By decoupling service providers from consumers and enforcing common integration policies, the GSB enables institutions to collaborate while preserving institutional autonomy and protecting existing technology investments.

4.1 Concepts

Historically, many of the technical concepts underlying GSB architectures originated from Enterprise Application Integration (EAI), Service-Oriented Architecture (SOA), and Enterprise Service Bus (ESB) approaches developed within enterprise computing environments. SOA promotes the exposure of business capabilities through standardized service contracts, encouraging interoperability, service reuse, abstraction, and loose coupling among heterogeneous systems [14]. ESB platforms subsequently emerged as a practical realization of many SOA principles by providing mediation, routing, transformation, and integration capabilities across distributed services [11], [15].

More recently, Event-Driven Architecture (EDA) paradigms have further influenced the design of modern interoperability platforms by enabling asynchronous, scalable, and loosely coupled interactions among distributed systems [16]. However, while ESB platforms primarily address technical integration challenges within organizational boundaries, GSB architectures extend these concepts to support nationwide interoperability, incorporating additional requirements related to governance, security, accountability, policy enforcement, and cross-agency information exchange.

Service-Oriented Integration

The GSB adopts a service-oriented integration model in which participating institutions expose capabilities through standardized service interfaces. Under this model, government systems publish and consume services based on formally defined contracts rather than direct implementation dependencies. This abstraction enables agencies to evolve their internal systems independently while maintaining interoperability with other participants [13]. In practical terms, service-oriented integration transforms government information systems into reusable organizational assets that can support multiple business processes and institutions. This approach promotes service reuse, reduces duplication, and improves the consistency of public-service delivery.

Message Brokering and Mediation
A central concept of the GSB is message mediation. Rather than communicating directly with one another, participating systems exchange information through the bus using structured messages. The GSB assumes responsibility for message routing, protocol conversion, validation, transformation, and delivery [17]. This mediation layer introduces an important level of abstraction that shields institutions from the technical complexities of partner systems while simplifying integration governance and operational management.

Canonical Data Model
Interoperability requires more than connectivity; it also requires a shared understanding of information. Government agencies frequently maintain different representations of common entities such as citizens, businesses, properties, and geographic locations. To address this challenge, GSB implementations often employ a canonical data model that provides a common representation of shared information assets [18]. By mapping institutional data structures to canonical representations, agencies can exchange information without requiring numerous bilateral transformations. The canonical model therefore serves as a semantic foundation for interoperability across the government ecosystem.

Event-Driven Integration
Contemporary digital government services increasingly rely on event-driven interactions in addition to traditional request-response communication models. Events such as citizen registrations, business licensing approvals, tax filings, or social benefit approvals often trigger actions across multiple institutions. The GSB can support event-driven architectures by enabling systems to publish and subscribe to business events in real time. This capability improves responsiveness, reduces coupling, and supports the implementation of cross-agency workflows that react dynamically to changes in shared state [16], [19].

Governance and Policy Enforcement
A distinguishing characteristic of government interoperability platforms is the integration of governance capabilities directly into the architecture. Beyond technical connectivity, the GSB provides mechanisms for enforcing access policies, security classifications, service ownership responsibilities, compliance requirements, and audit obligations [13]. Consequently, the GSB functions not only as an integration platform but also as a governance platform through which interoperability policies are operationalized and enforced.

4.2 Components
Although implementations vary across jurisdictions, mature GSB architectures generally comprise a set of common functional components that collectively support integration, security, governance, and operational management.
Figure 2 presents a high-level conceptual architecture of a GSB. The architecture illustrates the principal integration layers, governance mechanisms, and interoperability services typically found in modern cross-government integration platforms. As shown, the GSB operates as an intermediary layer between service providers and service consumers, while simultaneously enforcing security policies, managing service exposure, supporting message mediation, and providing monitoring and governance capabilities.

Service Registry and Repository
As illustrated in Fig. 2, the Service Registry and Repository serves as the authoritative catalog of services available through the bus. It maintains metadata describing service interfaces, endpoint locations, supported protocols, ownership information, security requirements, and lifecycle status. This component enables service discovery, promotes reuse, and supports governance activities such as version management and dependency tracking [17].

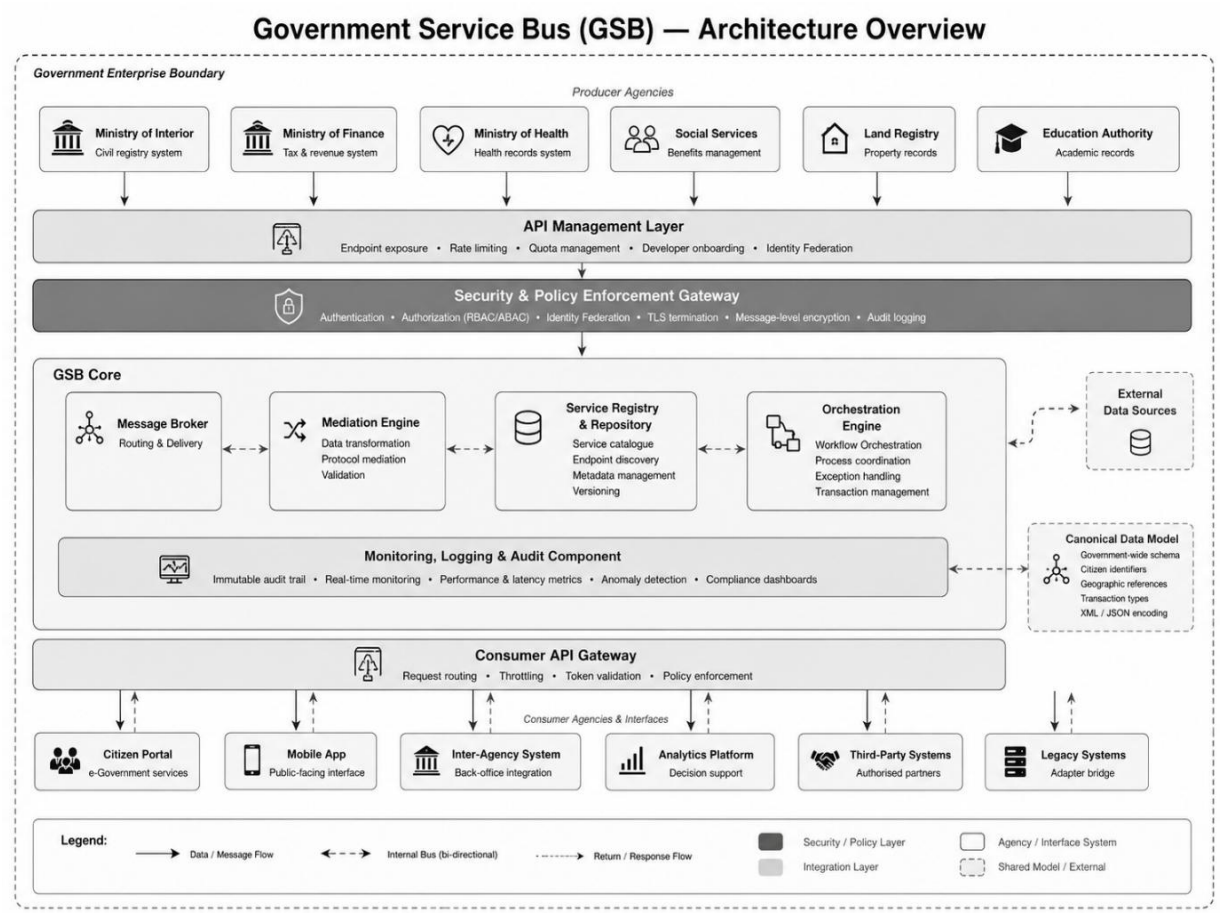

Fig. 2. *Reference GSB architecture illustrating service exposure, security enforcement, mediation, orchestration, governance, and interoperability capabilities within a cross-government integration environment.*

API Management Layer

The API Management Layer provides controlled exposure of services to consuming applications, agencies, and authorized third parties. Typical capabilities include API publication, developer onboarding, access control, throttling, quota management, and usage analytics. This layer extends interoperability beyond internal government systems and supports broader digital ecosystem participation [2], [20].

Message Broker

The Message Broker constitutes the operational core of the GSB. It receives, routes, and delivers messages between participating systems while supporting both synchronous and asynchronous communication patterns. By centralizing communication management, the broker reduces integration complexity and enables scalable information exchange across large government environments [17].

Mediation and Transformation Engine

The Mediation and Transformation Engine resolves differences in communication protocols, message structures, and data representations. It converts messages between source-specific formats and canonical representations while performing validation, enrichment, and content-based routing operations. This component is particularly important in government environments characterized by heterogeneous legacy systems and independently developed applications [21].

Security and Policy Enforcement Gateway

Security represents a foundational requirement for government interoperability platforms. The Security and Policy Enforcement Gateway shown in Fig. 2 provides authentication, authorization, encryption, and policy enforcement capabilities that protect information exchanges across institutional boundaries. Modern implementations increasingly incorporate zero-trust security principles, ensuring that every interaction is authenticated, authorized, and continuously monitored regardless of network location [22].

Orchestration and Process Engine
Many public services involve business processes that span multiple agencies and information systems. The Orchestration and Process Engine coordinate these processes by managing workflow execution, service invocation sequences, exception handling, and process state management. Through orchestration, the GSB enables the implementation of end-to-end digital services that transcend organizational boundaries [21].

Monitoring, Logging, and Audit Services
Operational transparency and accountability are essential characteristics of government interoperability initiatives. Monitoring, logging, and audit components provide visibility into service availability, performance, transaction volumes, security events, and compliance indicators. Comprehensive audit trails support regulatory compliance, incident investigation, operational diagnostics, and performance management [23].

Security Considerations
Security constitutes a fundamental requirement for government interoperability platforms. The proposed architecture incorporates authentication, authorization, API gateway controls, secure service exposure, audit logging, and encrypted communication channels. Participating institutions exchange information through governed service interfaces rather than direct database connectivity, thereby reducing the attack surface while preserving institutional ownership of information assets. In large-scale national deployments, these controls can be complemented by public key infrastructure (PKI), digital certificates, and advanced trust-management mechanisms.

4.3 Design Principles
The architectural components shown in Fig. 2 collectively support the design principles discussed in this section, including interoperability, loose coupling, security by design, governance, and technology neutrality. The effectiveness of a GSB depends not only on its functional capabilities but also on the architectural principles that govern its design, deployment, and evolution. These principles ensure that interoperability solutions remain sustainable, secure, scalable, and aligned with EA objectives.

Interoperability by Design
Interoperability should be treated as a primary architectural objective rather than an afterthought. The GSB therefore promotes the adoption of open standards, technology-neutral interfaces, and common information exchange models that facilitate communication among heterogeneous systems [13], [15].

Loose Coupling and Service Independence
Participating systems should remain operationally independent and should not depend on the internal implementation details of other systems. Loose coupling improves adaptability, simplifies maintenance, and enables institutions to evolve their systems without disrupting external integrations [17].

Reusability and Shared Services
Cross-government integration initiatives should maximize the reuse of common services and information assets rather than encourage the repeated development of equivalent capabilities across institutions. The GSB promotes reuse by providing a standardized mechanism through which services can be discovered, consumed, and governed across organizational boundaries. This principle reduces duplication, lowers implementation costs, and accelerates the delivery of new digital services.

Security and Compliance by Design
Security and regulatory compliance must be embedded throughout the architecture. Authentication, authorization, confidentiality, integrity, auditability, and policy enforcement should be treated as foundational architectural requirements rather than optional operational controls [22].

Reliability and Guaranteed Delivery
Government transactions frequently involve legal, financial, and administrative consequences. The architecture should therefore provide appropriate delivery guarantees, fault tolerance mechanisms, redundancy strategies, and recovery capabilities to ensure dependable service operation [17].

Scalability and Extensibility
As digital government ecosystems expand, the integration architecture must accommodate increasing transaction volumes, new services, and additional participating institutions without requiring fundamental redesign. Horizontal scalability and modular extensibility therefore constitute essential architectural objectives [16], [19].

Observability and Accountability
Government interoperability initiatives must support transparency and accountability through comprehensive monitoring, tracing, logging, and auditing capabilities. Observability enables operational visibility while ensuring that information exchanges remain verifiable and auditable [23].

Technology Neutrality and Long-Term Sustainability
Public-sector integration infrastructures should avoid unnecessary dependence on specific vendors, products, or proprietary technologies. Technology neutrality preserves institutional flexibility, reduces vendor lock-in, and supports long-term digital sovereignty objectives [2].

Incremental Adoptability
Recognizing the complexity of government transformation programs, GSB implementations should support gradual adoption and coexistence with legacy systems. Incremental migration strategies reduce implementation risk and enable institutions to participate in interoperability initiatives without requiring wholesale replacement of existing systems [24]. Taken together, these principles establish the foundation upon which a GSB can function as a strategic interoperability enabler within a broader EA framework. By combining standardized integration mechanisms with governance, security, and operational oversight capabilities, the GSB provides a practical approach to transforming fragmented information systems into an integrated digital government ecosystem.

5. Case Study: The GSB-Based Interoperability Pilot "*Nawa*"
To investigate the practical applicability of GSB concepts within the Libyan public-sector environment, a pilot interoperability initiative was developed under the project subsequently designated as *Nawa*. The name *Nawa* is derived from the Arabic word for core, seed, or foundation, and was deliberately chosen to reflect the pilot's intended role as the foundational nucleus of a future national GSB ecosystem. The initiative sought to demonstrate how heterogeneous government institutions could securely exchange information through a standards-based interoperability platform while preserving institutional autonomy and existing information systems.
Unlike purely conceptual interoperability frameworks, the proposed pilot was implemented and evaluated within a competitive national environment involving multiple public-sector stakeholders. The resulting solution provided a practical demonstration of how EA principles and GSB concepts can be combined to support government-wide information exchange, service integration, and digital transformation objectives.

5.1 Competition Context and Objectives
The pilot was originally developed as a response to a national interoperability hackathon organized by the General Information Authority (GIA) under the patronage of Expertise France in Libya. The competition aimed to explore practical approaches for improving information sharing among government institutions and to identify viable interoperability models capable of supporting future digital government initiatives. Participating teams represented a diverse range of organizations, including universities, information centers, software development teams, and public-sector institutions. The challenge focused on designing and demonstrating a secure, scalable, and governable information-sharing mechanism among four governmental entities selected to form the experimental interoperability environment.
The primary objective of the pilot was to demonstrate how a GSB architecture could enable trusted information exchange while minimizing institutional disruption, preserving data ownership, and reducing the integration complexity typically associated with cross-agency communication.
The proposed solution, its implementation approach, and its operational interoperability model were subsequently awarded first place in the competition and received the grand prize in January 2025.

5.2 Participating Institutions and Roles
The experimental environment consisted of four public-sector institutions representing different administrative domains and information assets. Together, these institutions formed a representative interoperability ecosystem capable of demonstrating real-world information exchange requirements.
Unlike symmetrical integration models in which all participants perform identical functions, the pilot adopted a business-driven interoperability approach centered on the operational requirements of the Tax Authority. The Tax Authority served as the primary beneficiary and consumer of information services exposed by the other participating institutions. Simultaneously, it acted as a provider of tax compliance services to the broader ecosystem. The remaining entities operated primarily as authoritative data providers responsible for exposing trusted information services through the interoperability platform. Table I summarizes the institutional roles within the pilot environment.

TABLE I
PARTICIPATING INSTITUTIONS AND INTEROPERABILITY ROLES

Institution	Role
Tax Authority	Primary Consumer and Service Provider
Commercial Registry	Authoritative Data Provider
Central Bank of Libya	Authoritative Data Provider
Customs Authority	Authoritative Data Provider

5.3 *Nawa* Reference Architecture

The proposed architecture adopted a GSB model as the central interoperability mechanism responsible for mediating information exchange among participating institutions. The architecture was designed according to SOA principles and emphasized loose coupling, standards-based communication, security, and institutional autonomy. Rather than allowing direct point-to-point integrations between agencies, all information exchange interactions were routed through the GSB layer. This approach significantly reduced integration complexity while providing a centralized mechanism for service discovery, routing, authentication, monitoring, and governance enforcement. Each participating institution retained ownership and operational control of its internal information systems and databases. Consequently, institutional autonomy was preserved while controlled access to selected information assets was provided through standardized service interfaces and governed interoperability contracts.

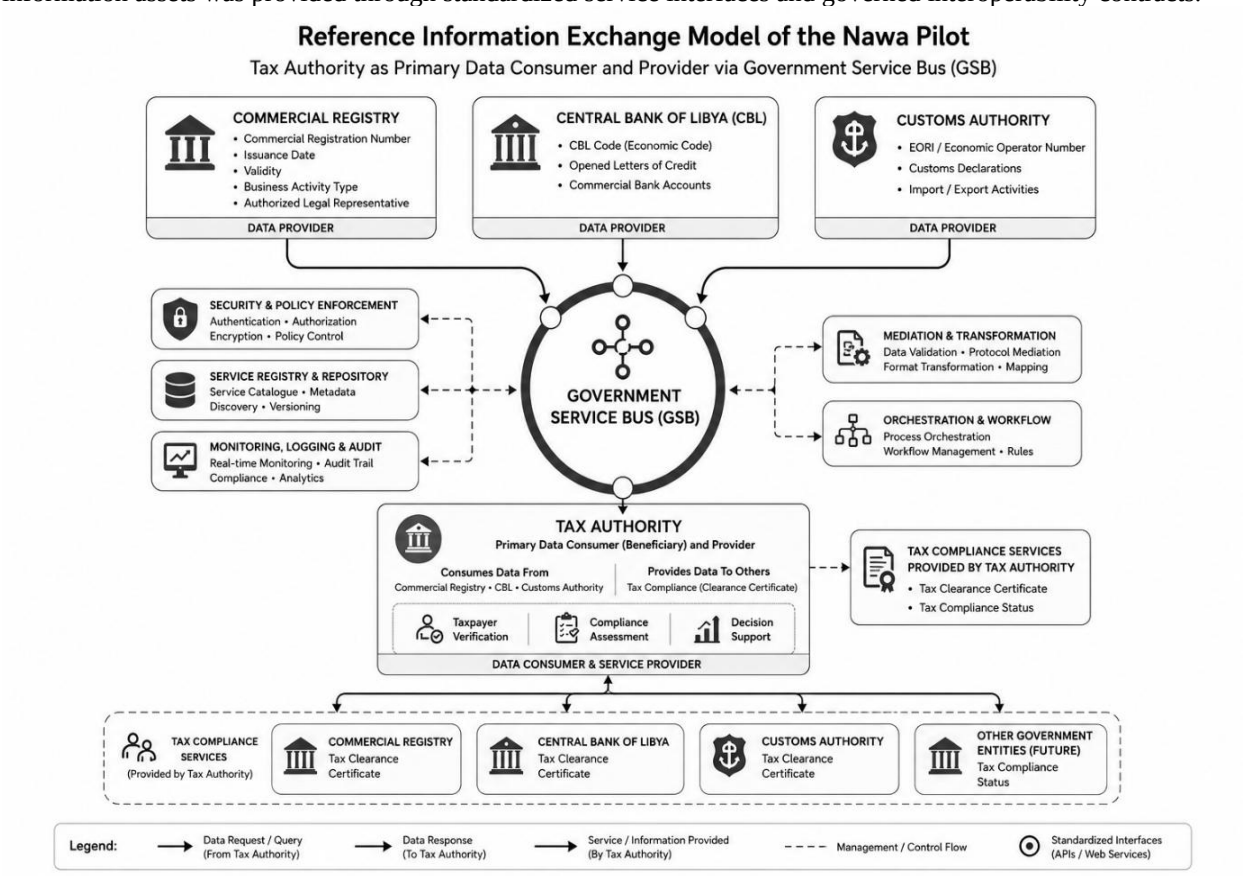

Fig. 3. *Reference information exchange model of the Nawa pilot, illustrating the role of the GSB in mediating secure information exchange between participating institutions and supporting tax-compliance services.*

Information exchange occurred through governed service interfaces rather than direct database access, allowing institutions to evolve their internal implementations independently while maintaining agreed interoperability contracts. This approach reduced integration dependencies, minimized the impact of internal system changes on external stakeholders, and supported long-term sustainability of the interoperability ecosystem. Figure 3 illustrates the high-level architecture (the operational interoperability model) adopted by the *Nawa* pilot. The Tax Authority acts as the primary consumer of authoritative information exposed by the Commercial Registry, Central Bank of Libya, and Customs Authority through the GSB while simultaneously providing tax-compliance services to

participating institutions. The model demonstrates how standardized service interfaces enable secure information exchange without requiring direct database connectivity.

The adopted architecture represents an implementation-oriented instantiation of the reference GSB architecture presented in Fig. 2. While the reference architecture defines the generic interoperability components and governance mechanisms of a GSB platform, the *Nawa* architecture adapts these concepts to the operational requirements of the participating institutions and the information exchange scenarios considered within the pilot.

5.4 Business-Oriented Information Exchange Model

The pilot was designed around a business-oriented interoperability model in which information exchange services were organized according to operational requirements rather than technical system boundaries.

When evaluating taxpayer/funder records, the Tax Authority retrieves authoritative information from participating institutions through the GSB. Each institution remains responsible for maintaining the accuracy and integrity of its own data while exposing selected services for authorized consumption.

The Commercial Registry provides information related to business registration and legal existence. Services exposed through the interoperability platform include the commercial registration number, registration date, registration validity status, business activity classification, and authorized legal representative information. The Central Bank of Libya provides financial and regulatory information relevant to commercial activities. Available services include the Central Bank code used for letters of credit, information concerning opened letters of credit, and registered commercial banking relationships. The Customs Authority provides customs-related information, including the Economic Operator Registration and Identification (EORI) number and customs declaration records associated with import and export activities. In the opposite direction, the Tax Authority exposes services that enable participating institutions to verify taxpayer compliance status. The primary service offered by the authority consists of the Tax Clearance Certificate service, which provides information regarding the tax compliance status of businesses and economic operators.

This information-sharing model enables institutions to access authoritative information directly from its source while avoiding data duplication and maintaining clear ownership responsibilities.

5.5 Implementation Stack and Technology Choices

A deliberate design objective of the pilot was to demonstrate that government interoperability platforms can be implemented using open-source technologies and internationally recognized standards without dependence on proprietary software ecosystems.

The pilot was implemented using Jakarta EE as the primary enterprise application framework and deployed on Payara Community Server as the application runtime environment. JavaServer Faces (JSF) was utilized for administrative interfaces, while Java Message Service (JMS) provided asynchronous communication capabilities supporting loose coupling among services. Service exposure and interoperability contracts were implemented according to OpenAPI specifications, enabling standardized service documentation and facilitating future integration efforts. Authentication and authorization mechanisms relied on JSON Web Tokens (JWT), while API Gateway technologies were employed to control service exposure, traffic management, and security enforcement. The persistence layer was implemented using MySQL, while the overall architecture adhered to SOA principles and emphasized modularity, interoperability, and long-term maintainability.

The exclusive use of open-source technologies was intended to maximize sustainability, reduce acquisition costs, minimize vendor lock-in risks, and facilitate future adoption across government institutions.

5.6 Outcomes and Lessons Learned

Before discussing the implementation outcomes, it is useful to summarize the overall characteristics of the *Nawa* pilot. Table II provides an overview of the implementation scope, the principal interoperability technologies adopted, and the project's execution profile. Collectively, these characteristics demonstrate that the pilot progressed beyond a conceptual prototype to deliver a functional GSB proof of concept under realistic development constraints.

As summarized in Table II, the pilot successfully interconnected four governmental institutions through twenty-three interoperable services while incorporating key interoperability capabilities, including REST APIs, API Gateway management, JMS messaging, service discovery, and OpenAPI-based service documentation. The solution was implemented by a five-member team within approximately one month using exclusively open-source technologies, demonstrating the practical feasibility of rapidly developing standards-based interoperability platforms for government environments.

TABLE II
SUMMARY OF THE *NAWA* PILOT IMPLEMENTATION CHARACTERISTICS

Characteristic	Value
Participating Institutions	4
Implemented Services	23
REST APIs	Implemented
API Gateway	Implemented
JMS Messaging	Implemented
Service Registry	Implemented
OpenAPI Documentation	Published
Demonstration Type	Live Demonstration
Development Duration	Approximately One Month
Team Size	5 Members

To further assess the architectural implications of the proposed solution, Table III compares the implemented GSB approach with a traditional point-to-point integration model. Although the pilot was not designed as a quantitative benchmarking study, the comparison highlights the principal qualitative advantages of the GSB approach, including reduced integration complexity, improved governance, greater service reuse, and enhanced institutional autonomy. These advantages become increasingly significant as additional governmental entities participate in the interoperability ecosystem.

TABLE III
QUALITATIVE COMPARISON OF INTEGRATION APPROACHES

Dimension	Point-to-Point	GSB-Based Approach
Integration Links	$N(N-1)/2$	N Connections to GSB
Scalability	Limited	High
Service Reuse	Low	High
Governance Enforcement	Decentralized	Centralized and Governed
Monitoring and Auditing	Fragmented	Centralized
Institutional Autonomy	Moderate	High
Maintenance Effort	High	Reduced
Integration Consistency	Variable	Standardized
Cross-Agency Expansion	Complex	Incremental

The pilot demonstrated that GSB principles can be successfully applied within the Libyan public-sector context to address interoperability challenges without requiring wholesale replacement of existing information systems.

Several observations emerged from the implementation experience. First, interoperability initiatives are fundamentally organizational endeavors rather than purely technical projects. While the GSB provided the technical infrastructure necessary for information exchange, successful integration depended equally on institutional cooperation, service ownership definition, and governance arrangements.

Second, the use of open standards and open-source technologies proved sufficient for implementing a secure and scalable interoperability platform capable of supporting real-world government information exchange scenarios.

Third, the pilot confirmed that business-driven interoperability models provide greater practical value than technology-driven integration initiatives. Organizing services around operational requirements such as taxpayer verification and compliance assessment produced a clear value proposition for participating institutions and simplified stakeholder engagement.

Finally, the pilot highlighted the importance of governance, data stewardship, and institutional readiness as prerequisites for broader interoperability adoption. These observations reinforce the argument that digital

transformation requires not only technological modernization but also organizational, procedural, and regulatory evolution.

Although the pilot was not designed as a formal performance-benchmarking study, it successfully validated several interoperability capabilities, including service discovery, API-based information exchange, asynchronous messaging, service governance, institutional autonomy, and standards-based service documentation through OpenAPI specifications. The implementation therefore demonstrated the practical feasibility of applying GSB principles to support controlled information exchange among independent governmental entities.

The pilot demonstrates that GSB-based interoperability is not merely theoretically sound but practically achievable within Libya's public-sector constraints.

6. Discussion and National Adoption Considerations

The results of the *Nawa* pilot demonstrate the practical feasibility of implementing GSB concepts within the Libyan public-sector environment. Beyond the technical success of the prototype, the pilot provides valuable insights into the architectural, governance, organizational, and regulatory factors that must be addressed in order to support nationwide interoperability initiatives.

While the pilot focused on a limited set of participating institutions and information exchange scenarios, the observations obtained from its design and implementation offer a useful foundation for evaluating broader adoption strategies. This section discusses the implications of the pilot from an EA perspective and examines the key considerations associated with scaling interoperability capabilities across the national digital government ecosystem.

6.1 Alignment with Enterprise Architecture

The proposed *Nawa* interoperability model demonstrates strong alignment with the fundamental principles of EA discussed earlier in this paper. Rather than introducing isolated integration mechanisms, the solution establishes a structured interoperability layer that supports business objectives while preserving institutional autonomy and existing information systems.

From a Business Architecture perspective, the pilot enables public-sector institutions to collaborate around shared operational objectives such as taxpayer verification and compliance assessment. The information exchange services implemented through the GSB support business processes that span multiple institutions while maintaining clear ownership and accountability boundaries.

At the Application Architecture level, the solution promotes service reuse and loose coupling by exposing institutional capabilities through standardized service interfaces. This approach reduces direct dependencies among systems and simplifies future integration efforts.

From a Data Architecture perspective, the pilot encourages the use of authoritative information sources and reduces unnecessary duplication of government data. Information remains under the ownership of the originating institution while being made available to authorized consumers through governed exchange mechanisms.

Finally, the Technology Architecture layer is supported through standards-based integration mechanisms, security controls, and monitoring capabilities that facilitate interoperability and reduce implementation complexity.

Taken as a whole, these characteristics demonstrate how EA principles can be translated into operational interoperability capabilities through a GSB implementation.

6.2 Governance Requirements

The pilot confirms that interoperability initiatives cannot be sustained through technology alone. Long-term success requires governance structures capable of coordinating participating institutions, defining responsibilities, managing service lifecycles, and enforcing interoperability policies. A national interoperability program would therefore require the establishment of a centralized governance framework responsible for defining technical standards, service publication procedures, data-sharing policies, security requirements, and operational oversight mechanisms.

Particular attention should be given to service ownership and accountability. Every information service exposed through the interoperability platform must have a clearly designated owner responsible for data quality, service availability, version management, and regulatory compliance. Governance mechanisms should also include formal processes for onboarding new institutions, resolving cross-agency disputes, managing service changes, and monitoring compliance with interoperability standards. Without such structures, technical interoperability platforms risk evolving into fragmented collections of services that reproduce many of the challenges they were intended to eliminate.

Consequently, interoperability governance should be regarded as a strategic capability operating alongside the technical platform itself rather than as an administrative afterthought.

6.3 Legal and Regulatory Considerations

The pilot also highlights the importance of regulatory modernization as a prerequisite for large-scale interoperability initiatives. Many existing administrative procedures, reporting obligations, and information-

sharing practices were originally developed for paper-based operating environments and may not adequately address contemporary digital government requirements.

Future interoperability programs would benefit from a comprehensive review of legislation related to electronic transactions, digital identity, information exchange, data ownership, privacy protection, records management, and institutional accountability. Such a review would help eliminate ambiguities that often discourage data sharing and limit cross-agency collaboration. Equally important is the establishment of a formal interoperability policy framework defining the legal basis for information exchange among government institutions. Clear regulatory guidance can improve institutional confidence, reduce operational uncertainty, and facilitate the adoption of shared digital services.

The findings of the pilot suggest that legal and regulatory adaptation should progress in parallel with technical implementation efforts to ensure that interoperability capabilities remain both operationally effective and legally sustainable.

6.4 Organizational Readiness

The implementation experience revealed that organizational readiness is a critical determinant of interoperability success. Effective information exchange requires institutions to adopt collaborative operating models that extend beyond traditional organizational boundaries.

One important consideration concerns leadership and strategic sponsorship. Large-scale interoperability initiatives require sustained executive support capable of aligning institutional priorities, allocating resources, and resolving cross-agency coordination challenges. Without visible leadership commitment, interoperability efforts frequently struggle to move beyond pilot-stage implementations. Capacity development represents an additional requirement. Government institutions participating in interoperability programs must possess sufficient expertise in EA, information governance, cybersecurity, API management, and service lifecycle management. Investments in professional development and specialized training programs are therefore essential components of national interoperability strategies.

The pilot further demonstrated the importance of institutional ownership. Participating organizations must view interoperability not as an externally imposed technical project but as a shared capability that directly contributes to their operational objectives. Establishing this sense of ownership is critical for ensuring long-term sustainability and continuous service improvement.

6.5 Future Work and National Expansion

The interoperability model demonstrated by the *Nawa* pilot provides a foundation upon which broader cross-government integration initiatives can be progressively constructed. Rather than pursuing large-scale transformation through a single implementation effort, a phased adoption strategy is likely to offer lower risk and greater institutional acceptance.

A logical next phase would involve the inclusion of additional authoritative information providers whose data assets support multiple government services. Examples include the Civil Registry, Social Security Fund, and municipal administration systems. Integrating these entities would significantly enhance identity verification, eligibility determination, and public-service delivery capabilities. Subsequent phases could extend interoperability capabilities to strategic sectors such as healthcare, education, and the financial ecosystem. Such expansion would enable the development of increasingly sophisticated digital services built upon trusted information exchange mechanisms. From a technical perspective, future expansion should prioritize standardized APIs, common data models, shared security frameworks, and reusable service components. From an institutional perspective, expansion should proceed according to clearly defined governance criteria and interoperability maturity requirements.

Ultimately, a nationally deployed GSB has the potential to evolve into a foundational component of Libya's digital government ecosystem, enabling secure information exchange, reducing administrative fragmentation, improving service delivery, and supporting evidence-based decision making across the public sector.

Future work should also explore the development of advanced digital government services built upon the interoperability foundation established by the GSB. By leveraging the GSB as a secure integration backbone, future initiatives could support citizen-centric and business-centric service delivery models, enabling the implementation of one-stop government portals, life-event services, proactive public services, and cross-agency digital workflows that extend the value of interoperability beyond institutional information exchange.

7. Conclusion

Digital transformation initiatives increasingly require governments to move beyond isolated digitization efforts toward integrated digital ecosystems capable of supporting secure, reliable, and efficient information exchange. However, as discussed throughout this paper, interoperability challenges frequently extend beyond technology itself and encompass organizational fragmentation, procedural inconsistencies, regulatory limitations, and governance constraints. These challenges are particularly acute in emerging digital government ecosystems such

as Libya's, where institutional silos and heterogeneous information systems continue to impede integrated public-service delivery.

This paper examined the role of EA as a strategic framework for addressing these challenges and enabling interoperability across government institutions. By aligning business objectives, information assets, application services, and technology infrastructure under a common governance model, EA provides the foundation necessary for coordinated digital transformation and sustainable interoperability initiatives. Building upon this foundation, the paper explored the GSB as an architectural mechanism for operationalizing interoperability requirements. The analysis demonstrated how GSB architectures combine integration capabilities, governance mechanisms, security controls, service management, and standardized information exchange models to support collaboration among heterogeneous public-sector systems while preserving institutional autonomy and data ownership.

To evaluate the practical applicability of these concepts, the paper presented the *Nawa* pilot as a case study of a GSB-based interoperability model involving the Tax Authority, Commercial Registry, Central Bank of Libya, and Customs Authority. The pilot demonstrated how authoritative information sources can be integrated through a governed interoperability platform to support taxpayer verification, compliance assessment, and cross-agency information exchange. The implementation further illustrated the feasibility of adopting open-source technologies and standards-based integration approaches within the Libyan public-sector environment. The findings demonstrate that GSB architectures provide a practical and scalable foundation for addressing interoperability challenges within emerging digital government ecosystems. The *Nawa* pilot demonstrates that EA principles, when combined with governed interoperability platforms, can support secure information exchange while preserving institutional autonomy and existing investments. As Libya continues its digital transformation journey, the adoption of a national interoperability framework is expected to contribute significantly to the development of integrated, citizen-centric government services.

Rather than representing an isolated technical prototype, the *Nawa* pilot demonstrates how EA and GSB concepts can provide a realistic and scalable foundation for nationwide digital government interoperability in Libya.

Acknowledgment

The authors gratefully acknowledge the support and cooperation of the Libyan Tax Authority and ARJ Information and Communications Technology Company during the development and evaluation of the *Nawa* interoperability pilot. Their contributions provided valuable operational, technical, and organizational perspectives that supported the practical realization of the proposed interoperability model. The authors also acknowledge the General Information Authority and Expertise France in Libya for facilitating the interoperability innovation initiative within which the pilot was developed and demonstrated.

Compliance with ethical standards

Disclosure of conflict of interest

The authors declare that they have no conflict of interest.

References

[1] The Open Group, "The TOGAF Standard, 10th Edition," 2022.
[2] I. Europe, "European interoperability reference architecture (eira)," 2024.
[3] M. Janssen and Y. Dwivedi, "Interoperability in government information systems: Challenges and perspectives," Government Information Quarterly, vol. 29, no. S1, pp. S1–S8, 2012.
[4] O. for Economic Co-operation and Development, "Digital government index 2023 results and key findings," OECD, Tech. Rep., 2024.
[5] A. Kalja, A. Reitsakas, and T. Saarepera, "egovernment interoperability through the x-road infrastructure," Electronic Government, pp. 412–421, 2005.
[6] Nordic Institute for Interoperability Solutions (NIIS), "X-road: Data exchange layer for digital government," https://x-road.global, 2024, accessed: 2026-06-21.
[7] Yesser e-Government Program, "National e-government program (yesser)," https://www.yesser.gov.sa, 2024, accessed: 2026-06-21.
[8] Office for Information Technologies and eGovernment, Republic of Serbia, "Government service bus and national interoperability platform," https://www.ite.gov.rs, 2024, accessed: 2026-06-21.
[9] Ministry of Digital Governance, Hellenic Republic, "Interoperability center (ked): National government interoperability infrastructure," https://www.gov.gr, 2024, accessed: 2026-06-21.
[10] Ministry of Digital Economy and Entrepreneurship, Jordan, "Jordan e-government and digital transformation initiatives," https://modee.gov.jo, 2024, accessed: 2026-06-21.
[11] D. Chappell, Enterprise Service Bus. O'Reilly Media, 2004.

[12] G. Hohpe and B. Woolf, Enterprise Integration Patterns: Designing, Building, and Deploying Messaging Solutions. Addison-Wesley, 2004.
[13] European Parliament and Council of the European Union, "Interoperable europe act," Official Journal of the European Union, vol. L 2024/903, Mar. 2024, Regulation (EU) 2024/903. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202400903
[14] T. Erl, Service-Oriented Architecture: Concepts, Technology, and Design. Prentice Hall, 2005.
[15] W. Z. et al., "Soa-based enterprise service bus," in Proc. IEEE Int. Conf. on e-Business Engineering (ICEBE), 2008, pp. 1–6.
[16] H. C. et al., "On the impact of event-driven architecture on performance: An exploratory study," Future Generation Computer Systems, vol. 153, Apr. 2024. [Online]. Available: https://www.researchgate.net/publication/368431218
[17] B. Erl, A. Karimi, and R. Merson, "Enterprise service bus," in Encyclopedia of Cloud Computing. Hoboken, NJ, USA: Wiley/IEEE Press, 2016, ch. 12. [Online]. Available: https://www.sciencedirect.com/topics/computer-science/enterprise-service-bus
[18] A. A.-Z. et al., "Government services bus (gsb): Opportunity to improve the quality of data entry," Int. J. of Semantic Web and Information Systems, vol. 17, no. 3, pp. 1–20, Jul. 2021.
[19] P. Mishra, "The role of event-driven architectures in enterprise digital transformation initiatives," Int. J. of Emerging Trends in Computer Science and Information Technology, vol. 5, no. 3, 2024. [Online]. Available: https://ijetcsit.org/index.php/ijetcsit/article/view/625
[20] European Commission, Directorate-General for Informatics, "Serbia 2024 digital public administration factsheet," Interoperable Europe Portal, Tech. Rep., 2024. [Online]. Available: https://interoperable-europe.ec.europa.eu/sites/default/files/inline-files/NIFO_2024%20Supporting%20Document_Serbia_vFINAL.pdf
[21] E. T. et al., "Service orchestration using enterprise service bus for real-time government executive dashboard system," ResearchGate, Jun. 2017. [Online]. Available: https://www.researchgate.net/publication/304412463
[22] P. Phiayura and S. Teerakanok, "A comprehensive framework for migrating to zero trust architecture," IEEE Access, vol. 11, pp. 19 487–19 511, 2023.
[23] S. K. R. Basireddy, "Securing the digital public sector: Cloud transformation of government infrastructure," Int. J. of Computational and Experimental Science and Engineering, vol. 11, no. 4, Dec. 2025. [Online]. Available: https://ijcesen.com/index.php/ijcesen/article/view/4409
[24] A. A. et al., "Event-driven architectures for microservices: A framework and migration challenges," IEEE Access, vol. PP, no. 99, pp. 1–1, 2023. [Online]. Available: https://www.researchgate.net/publication/373151876

