ISSN: 2583-9888
DOI: doi.org/10.51219/JAIMLD/raghavendar-akuthota/608

URF PUBLISHERS
connect with research world

Journal of Artificial Intelligence, Machine Learning and Data Science

https://urfpublishers.com/journal/artificial-intelligence

Vol: 1 & Iss: 1

Research Article

Implementing Non-Repudiation Mechanisms in IBM Sterling File Transfers: Ensuring Data Integrity and Sender

Raghavendar Akuthota*

Citation: Akuthota R. Implementing Non-Repudiation Mechanisms in IBM Sterling File Transfers: Ensuring Data Integrity and Sender. *J Artif Intell Mach Learn & Data Sci 2022* 1(1), 2921-2924. DOI: doi.org/10.51219/JAIMLD/raghavendar-akuthota/608

Received: 02 October, 2022; **Accepted:** 18 October, 2022; **Published:** 20 October, 2022

***Corresponding author:** Raghavendar Akuthota, USA, E-mail: araghavendar@gmail.com

ABSTRACT

Non-repudiation is a critical requirement in enterprise file transfer systems, ensuring that neither the sender nor the recipient can deny their involvement in a transaction. IBM Sterling File Gateway (SFG) provides a secure, centralized platform for exchanging files across heterogeneous systems, but the integration of message-level security features remains essential for guaranteeing data integrity and sender authenticity. This paper explores strategies for implementing non-repudiation in IBM Sterling file transfers through digital signatures, hashing, encryption and certificate-based authentication. A review of related literature highlights the evolution of secure file transfer protocols and standards. The study identifies practical challenges such as scalability, certificate management and compliance, followed by potential solutions for integrating non-repudiation mechanisms within Sterling's architecture. Recommendations are provided to strengthen enterprise adoption of non-repudiation measures, ensuring security, compliance and trust in digital transactions.

Keywords: Non-repudiation, IBM Sterling file gateway, Secure file transfer, Message-level security, Digital signatures, Data integrity

1. Introduction

As enterprises increasingly depend on digital ecosystems for exchanging mission-critical data, secure file transfer has become indispensable for maintaining trust, compliance and operational continuity. Traditional security measures such as encryption ensure the confidentiality of data during transit, while hashing mechanisms help verify that the content has not been altered. However, these measures alone do not prevent a sender or receiver from denying participation in a transaction. To address this gap organizations must enforce non-repudiation - a security principle that guarantees the authenticity of the sender and the integrity of the transmitted data, leaving verifiable proof that cannot later be denied.

IBM Sterling File Gateway (SFG) is a widely adopted enterprise solution for managing large-scale, multi-protocol file transfers across diverse trading partners. Its flexibility makes it suitable for industries such as banking, healthcare, supply chain management and logistics, where data authenticity and regulatory compliance are paramount. In these sectors, the absence of non-repudiation can expose organizations to disputes, fraud and non-compliance with mandates such as HIPAA, PCI DSS or GDPR.

Message-level non-repudiation, achieved through mechanisms such as Public Key Infrastructure (PKI), Secure/Multipurpose Internet Mail Extensions (S/MIME) and digital signatures, provides an additional layer of assurance beyond traditional encryption. These frameworks ensure that each transmitted file carries cryptographic evidence of its origin, while also validating that the content has not been altered. In IBM Sterling, integrating non-repudiation involves configuring certificate-based signing, trusted certificate chains and audit trails that preserve evidence of transactions.

The growing emphasis on digital trust, regulatory requirements and secure data exchange in global business ecosystems makes non-repudiation not just an optional enhancement but an operational necessity. This paper explores the practical strategies for implementing non-repudiation in IBM Sterling File Gateway, evaluating both technical configurations and compliance benefits. The discussion highlights how enterprises can leverage IBM Sterling's built-in capabilities, combined with industry-standard cryptographic protocols, to ensure accountability, protect sensitive data and foster reliable business partnerships.

2. Literature Review

Non-repudiation in B2B file exchange is commonly realized through digital signatures and receipt mechanisms embedded in application-layer protocols. AS2, standardized by the IETF, defines secure business data exchange over HTTP with options for signed payloads and signed Message Disposition Notifications (MDNs) to provide proof of origin and delivery[1]. Building on web-services stacks, the OASIS AS4 profile of ebMS 3.0 carries forward AS2's evidentiary concepts (signatures, receipts) while adding pull messaging and web-services alignment, making it attractive for modern partner ecosystems[2]. Together, these protocols establish a foundation for message-level integrity, authenticity and evidentiary trails beyond transport security.

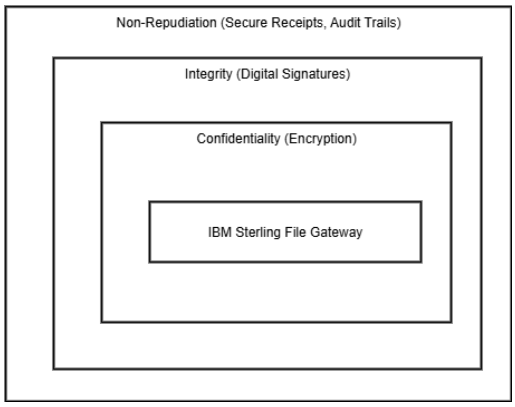

Figure 1: Message-Level Security Framework in IBM Sterling.

The cryptographic underpinnings of non-repudiation in these protocols derive from long-standing standards. CMS (Cryptographic Message Syntax) specifies the encapsulation used for digital signatures and signed receipts, enabling verifiable proof that a specific private key holder originated a message[3]. S/MIME 3.2 formalizes secure MIME packaging and explicitly states that signatures provide authentication, integrity and non-repudiation with proof of origin[4]. For durable evidence, trusted timestamping per RFC 3161 is frequently combined with signatures so that proofs remain valid even as certificates rotate, supporting long-term verification requirements[5].

Operational guidance for key lifecycles is critical, since non-repudiation assurances depend on sound key management. NIST SP 800-57 Part 1 provides prescriptive recommendations for key generation, usage periods, rollover and revocation-practices that directly affect the reliability of digital signatures and the verifiability of audit evidence[6]. In IBM Sterling deployments, vendor materials emphasize AS2's use of certificates, encryption, signatures and non-repudiation and describe how MDNs attest to successful, unaltered delivery, aligning implementation details with these standards[7,8].

Within IBM Sterling specifically, product documentation and field advisories detail configuration patterns that preserve evidentiary value at scale. For example, asynchronous MDN routing must be engineered so the MDN returns to the originating data center-otherwise the cryptographic linkage between message and receipt is broken, undermining non-repudiation guarantees[9]. In addition, IBM Redbooks on Sterling Managed File Transfer provide architectural practices for integrating certificate stores, logging and governance components, which together support auditability and dispute resolution across heterogeneous partner communities[10].

Overall, the literature converges on a layered model: standardized application protocols with signed payloads and receipts (AS2/AS4), cryptographic packaging (CMS/S/MIME), long-term evidence via trusted timestamps and disciplined key management. IBM Sterling operational guidance maps these standards into deployable controls—signed MDNs, certificate lifecycle hygiene and topology-aware routing, so that enterprises can produce durable, verifiable proofs of origin and delivery across their B2B exchanges.

3. Problem Statement

3.1. Lack of message-level authentication

Enterprises deploying IBM Sterling File Gateway often rely primarily on transport-level encryption protocols such as SSL/TLS or SSH. While these mechanisms safeguard confidentiality during transmission, they provide limited assurance once the file has been delivered to the application layer. In this scenario, there is no verifiable proof linking the sender to the transmitted data beyond the session itself. This gap exposes organizations to potential repudiation risks, where a sender may deny initiating a transaction or a receiver may claim not to have received a specific file. The absence of message-level authentication undermines trust in business-to-business (B2B) data exchanges and prevents organizations from meeting stringent non-repudiation requirements.

3.2. Weak evidence of delivery

Another critical challenge is the limited evidence of successful delivery within Sterling's default configurations. Although transport protocols confirm file transfer completion, they do not generate verifiable receipts or cryptographic evidence that the receiver accepted and processed the file. This lack of proof creates ambiguity in cases of transaction disputes, particularly in regulated industries where a clear audit trail is mandatory. For example, in healthcare and financial services, missing or incomplete delivery evidence could result in compliance violations, customer disputes or even legal liabilities. Without signed acknowledgments or secure logging mechanisms, enterprises cannot conclusively demonstrate the integrity of end-to-end file transactions.

3.3. Certificate and key management challenges

Non-repudiation frameworks rely heavily on digital certificates and cryptographic key pairs, but managing these assets within Sterling File Gateway introduces operational complexity. Enterprises must regularly issue, revoke and renew certificates to maintain compliance with Public Key Infrastructure (PKI) standards. Additionally, keeping revocation lists updated and ensuring seamless key rollover processes are prone to administrative errors that can compromise both

security and availability. A misconfigured or expired certificate may disrupt critical business transactions, while inconsistent key management practices increase vulnerability to fraud or unauthorized access. As the number of trading partners and protocols grows, the scalability of Sterling's certificate and key management becomes a persistent challenge for IT administrators.

3.4. Compliance and audit limitations

Organizations operating in regulated sectors face an increasing demand to prove the authenticity, integrity and accountability of file transactions. Frameworks such as HIPAA, GDPR, PCI DSS and SOX require organizations to maintain tamper-proof audit logs and evidence of non-repudiation. However, Sterling's native logging and reporting features, while extensive, do not always provide cryptographically verifiable proof of transaction authenticity. This limitation forces organizations to rely on supplementary tools or manual interventions, increasing both costs and operational risks. The inability to fully satisfy audit requirements exposes enterprises to compliance gaps, potential penalties and reputational damage, emphasizing the urgent need for robust non-repudiation mechanisms within Sterling's deployment.

4. Solution

4.1. Message-level digital signatures

One of the most effective solutions for implementing non-repudiation in IBM Sterling File Gateway is the use of message-level digital signatures. Unlike transport-layer encryption, which only secures data during transmission, digital signatures bind authenticity to the message itself. By using asymmetric cryptography, senders can sign outgoing files with their private key, while receivers validate the signature with the corresponding public key. This ensures that the sender cannot later deny authorship of the message. In the IBM Sterling environment, digital signatures can be enabled through the integration of PKI-based frameworks, ensuring compliance with standards such as S/MIME and XML Digital Signatures.

4.2. Signed receipts and acknowledgments

To strengthen delivery evidence, IBM Sterling can be configured to generate signed receipts using protocols such as AS2 or AS4. A signed receipt provides verifiable proof that the receiving party not only obtained the message but also validated its integrity. These receipts act as non-repudiation tokens, preventing either party from denying that a transaction occurred. In highly regulated industries such as finance or healthcare, such receipts serve as legal evidence during audits or dispute resolution. IBM Sterling supports Message Disposition Notifications (MDNs), which can be signed to enhance evidentiary value.

4.3. Certificate lifecycle management

Non-repudiation in Sterling also relies on effective certificate and key management. Organizations must establish automated processes for certificate issuance, renewal and revocation. Sterling's integration with external certificate authorities (CAs) allows enterprises to manage these lifecycles within a centralized PKI framework. Regular rollover policies mitigate risks of key compromise, while revocation lists ensure invalid certificates are not used for signing or verification. Automation tools and monitoring dashboards within Sterling can help reduce administrative errors, which are often a source of non-repudiation failures.

4.4. Transaction logging and audit trails

Implementing immutable transaction logs is another core solution. Sterling can be configured to maintain tamper-resistant audit trails that capture details of each file transfer, including timestamps, sender and receiver identities and signature validation results. Storing these logs in write-once-read-many (WORM) systems or blockchain-based ledgers further enhances evidentiary strength. Comprehensive logging not only supports internal investigations but also ensures that organizations can present verifiable proof of transactions to regulators, auditors or legal entities **(Figure 2)**.

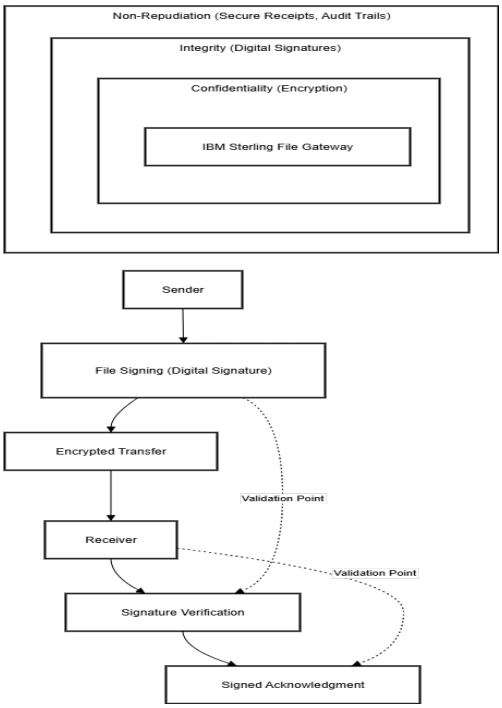

Figure 2: Non-Repudiation Workflow for File Transfers.

5. Recommendations

5.1. Adopt a hybrid security model

Organizations should move beyond transport-only encryption and adopt a layered security model that combines message-level signatures, hashing and receipts. This approach ensures that data integrity and authenticity are preserved throughout the file lifecycle, including at rest and during audits. By embedding non-repudiation tokens directly into files and receipts, enterprises can meet stricter compliance requirements.

5.2. Standardize certificate policies

Enterprises should develop standardized policies for certificate usage, covering issuance, renewal, revocation and rollover. Aligning with industry standards such as X.509 ensures interoperability across partners and systems. Training IT staff on PKI practices, combined with Sterling's certificate automation capabilities, can mitigate human error and strengthen trust.

5.3. Strengthen compliance readiness

Organizations in regulated industries should configure Sterling to align with compliance frameworks such as GDPR, HIPAA and SOX. This involves enabling signed

receipts, maintaining immutable logs and regularly auditing configurations. Periodic penetration testing and compliance audits ensure that non-repudiation mechanisms function effectively under real-world conditions.

5.4. Integrate with enterprise security ecosystems

IBM Sterling should not operate in isolation. Integrating its non-repudiation features with enterprise security tools such as SIEM (Security Information and Event Management) systems, identity and access management platforms and blockchain-based verification services strengthens overall resilience. Centralizing monitoring and alerting ensures that anomalous file transfer behaviors or certificate misuse are quickly detected and addressed.

6. Conclusion

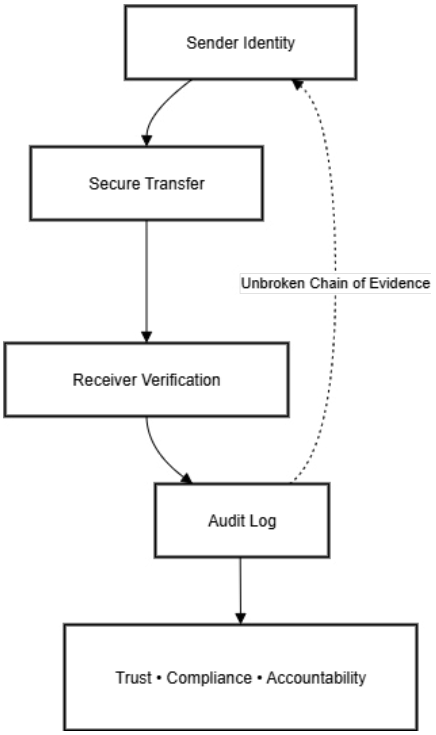

Figure 3: End-to-End Accountability Model.

Non-repudiation is a cornerstone of secure digital file exchange, ensuring that neither senders nor receivers can deny their participation in a transaction. While IBM Sterling File Gateway already provides strong capabilities for encryption, protocol handling and compliance alignment organizations often face challenges in extending these features to achieve full message-level assurance. This paper has highlighted the key gaps, including limited authentication beyond transport layers, weak evidence of delivery, certificate management complexities and compliance limitations and proposed strategies to address them.

The solutions discussed, such as implementing digital signatures, enabling secure receipts, strengthening certificate lifecycle management and enhancing audit trails, provide a comprehensive framework for embedding non-repudiation into Sterling environments. Recommendations emphasize the need for a layered security approach, the adoption of standardized PKI frameworks and investment in automation for certificate governance.

By aligning IBM Sterling configurations with established standards and industry best practices, enterprises can not only meet regulatory demands but also reinforce trust across digital ecosystems. Ultimately, embedding non-repudiation safeguards business integrity, reduces the risk of disputes and ensures that critical data transfers remain verifiable, accountable and secure.

7. References

1. https://datatracker.ietf.org/doc/html/rfc4130.
2. https://docs.oasis-open.org/ebxml-msg/ebms/v3.0/profiles/AS4-profile/v1.0/os/AS4-profile-v1.0-os.pdf.
3. https://datatracker.ietf.org/doc/html/rfc5652.
4. https://www.rfc-editor.org/rfc/rfc5751.html.
5. https://www.ietf.org/rfc/rfc3161.txt.
6. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf.
7. https://www.ibm.com/docs/SSYJCD_1.0.0/com.ibm.help.meigV100.doc/com.ibm.help.meg.welcome.doc/meg_as2_overview.html.
8. https://www.ibm.com/docs/en/b2b-integrator/6.2.0?topic=manager-async-mdn-configuration-as2.
9. https://public.dhe.ibm.com/software/commerce/doc/sb2bi/v5r2/Stds801_UsingAS2_book.pdf.
10. https://www.ibm.com/support/pages/as2-performance-sterling-integrator-hints-and-tips.