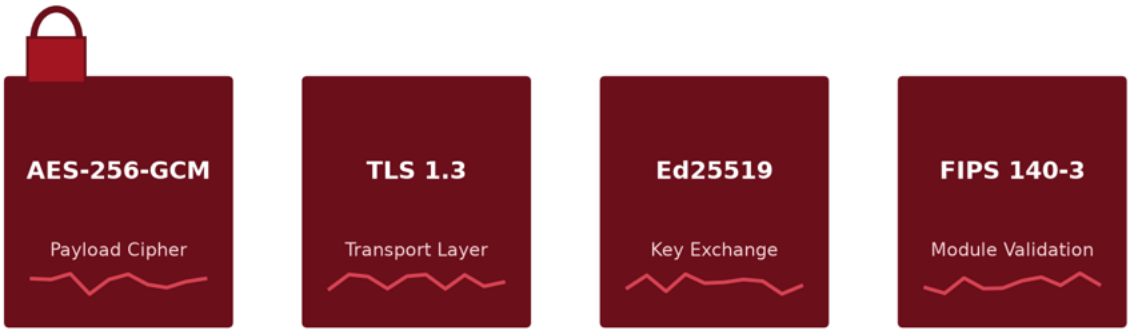
iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

ENCRYPTED DATA-IN-TRANSIT FRAMEWORKS FOR ENTERPRISE HCM: EXTENDING CRYPTOGRAPHIC FILE TRANSFER BEYOND MOVEIT

A LAYERED PROTOCOL AND KEY MANAGEMENT FRAMEWORK FOR SECURING INBOUND AND OUTBOUND HCM DATA MOVEMENT ACROSS VENDORS AND INTEGRATION PLATFORMS



Ujwal Dyasani
Lead Software Engineer Integrations, USA

ABSTRACT
Managed file transfer platforms, most notably MOVEit, have served for years as the default mechanism for moving sensitive human capital management data between enterprise HCM tenants and external vendors, payroll processors, and benefits administrators. Widely reported security incidents affecting managed file transfer platforms in 2023 prompted many organizations to reexamine whether a single, centralized file transfer product should continue to serve as the sole encrypted data in transit mechanism for their HCM integration landscape, or whether a more diversified, layered framework spanning multiple protocols and cryptographic mechanisms would better limit exposure to any single platform's vulnerability. This article develops an encrypted data in transit framework for enterprise HCM environments that extends beyond reliance on a single managed file transfer product, structured around a six layer defense in depth stack spanning network perimeter control, key exchange and certificate validation, transport layer encryption, application layer payload encryption, audit logging, and governance. Drawing on established cryptographic protocol standards, transport layer security specifications, and documented integration platform security capabilities, the article presents a protocol and cryptographic module selection framework, a comparative security property analysis across five transfer mechanisms, and an illustrative throughput and latency comparison. The findings indicate that no single protocol or platform choice is uniformly superior across all integration patterns, and that a mature encrypted data in transit posture instead depends on matching protocol choice to counterparty regulatory profile and integration pattern, while applying the full defense in depth stack consistently regardless of which specific protocol is selected for a given flow. The article concludes with a phased migration approach and governance recommendations for organizations reducing reliance on any single managed file transfer platform.

Keywords:
encryption in transit; managed file transfer; cryptographic protocols; TLS; key management; human capital management security; defense in depth; secure file transfer; Studio integration security; data protection.

1. INTRODUCTION
For much of the past decade, managed file transfer platforms have occupied a central, often unquestioned position in enterprise HCM integration architecture. A single platform, most commonly MOVEit, would be configured once, connected to dozens of vendor endpoints, and treated thereafter as a solved problem rather than an area requiring ongoing architectural attention. This pattern reflected a reasonable engineering instinct: centralizing file

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

transfer logic in one well understood platform reduces duplication of effort relative to building bespoke transfer logic for every vendor relationship individually.

That instinct came under significant scrutiny following widely reported vulnerabilities affecting managed file transfer platforms in 2023, which demonstrated a specific structural risk inherent to architectural centralization: when the majority of an organization's sensitive data movement flows through a single platform, a vulnerability in that platform becomes a single point of exposure affecting the entire integration landscape simultaneously, rather than a contained, isolated incident affecting one vendor relationship (Cybersecurity and Infrastructure Security Agency, 2023). This article does not focus on the specific incidents themselves, which are well documented elsewhere, but instead uses the structural lesson those incidents surfaced as the motivation for developing a more diversified, layered encrypted data in transit framework.

This article develops such a framework for enterprise HCM environments, addressing how organizations can extend their encrypted file transfer posture beyond reliance on any single managed file transfer product. The research questions guiding this study are as follows.

- RQ1: What structural lessons from managed file transfer platform security incidents should inform a more resilient encrypted data in transit architecture for HCM integrations?
- RQ2: What defense in depth layers should a comprehensive encrypted transfer framework include, beyond transport layer encryption alone?
- RQ3: How should protocol and cryptographic module selection vary by counterparty regulatory profile and integration pattern, and what are the comparative security and performance trade-offs across available options?
- RQ4: What migration approach and governance practices allow an organization to reduce reliance on a single managed file transfer platform without disrupting existing vendor integrations?

The remainder of this article proceeds as follows. Section 2 reviews related literature on cryptographic protocols and transport security. Section 3 examines lessons from managed file transfer platform incidents. Section 4 details the research methodology. Sections 5 through 13 present the core framework, including the defense in depth stack, protocol selection guidance, comparative analysis, topology design, key management, Studio specific patterns, and audit logging. Sections 14 and 15 address migration and governance. Sections 16 through 20 discuss pitfalls, limitations, recommendations, future research, and conclusions.

2. Background and Related Work

2.1 Foundational Cryptographic and Transport Security Standards

The Transport Layer Security protocol, most recently formalized in version 1.3, provides the foundational specification for the transport layer encryption discussed throughout this article, defining the handshake, cipher negotiation, and forward secrecy properties that any modern encrypted transfer mechanism should incorporate (Rescorla, 2018). The Advanced Encryption Standard, particularly in its Galois Counter Mode configuration, provides the foundational specification for the application layer payload encryption discussed in Section 5, offering both confidentiality and integrity protection in a single authenticated encryption construction (National Institute of Standards and Technology, 2007; Dworkin, 2007).

2.2 FIPS Validation and Regulated Data Handling

Federal Information Processing Standards validation, specifically FIPS 140 series requirements for cryptographic modules, provides the compliance basis for the module selection guidance developed in Section 7, particularly for HCM data flows involving regulated financial or healthcare counterparties where FIPS validated modules are frequently a contractual or regulatory expectation (National Institute of Standards and Technology, 2019).

2.3 Managed File Transfer Security Literature

Security advisory literature addressing managed file transfer platform vulnerabilities has documented a recurring pattern in which internet facing file transfer applications, by virtue of their necessary exposure to external vendor traffic, represent an attractive target surface distinct from the risk profile of internally facing systems, and has recommended defense in depth practices that do not rely solely on the file transfer application's own security controls (Cybersecurity and Infrastructure Security Agency, 2023; SANS Institute, 2022).

2.4 Integration Platform Encryption Capabilities

Documented guidance on Studio based integration development addresses connector level support for mutual TLS, certificate based authentication, and payload level encryption options available within the integration runtime, positioning the platform itself as capable of directly supporting several of the defense in depth layers developed in this article, rather than requiring encryption to be handled entirely by an external file transfer product (Workday, Inc., 2021a; Workday, Inc., 2023b).

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

2.5 Positioning of This Study

While TLS and AES standards, FIPS validation requirements, and managed file transfer security advisory literature each independently address components of the problem, comparatively little published material synthesizes these into a structured, layered framework specifically addressing how enterprise HCM organizations should diversify their encrypted data in transit architecture beyond a single managed file transfer platform. This article's contribution is that synthesis, together with comparative protocol analysis and a phased migration approach.

3. Lessons From Managed File Transfer Platform Incidents

Without focusing on any single incident's technical specifics, this section extracts four structural lessons from the pattern of managed file transfer platform vulnerabilities publicly documented in 2023, each of which directly motivates a specific element of the framework developed later in this article.

Table 1. Structural lessons from managed file transfer platform incident patterns and corresponding framework elements.

Structural Lesson	Description	Framework Element Motivated
Centralization Creates Concentrated Exposure	A single platform handling the majority of transfer volume becomes a single point of failure affecting many vendor relationships simultaneously	Protocol diversification across multiple mechanisms (Section 7)
Internet Facing Applications Carry Elevated Target Risk	File transfer applications necessarily exposed to external traffic face a different threat profile than internal systems	Network perimeter and endpoint allowlisting layer (Section 5, Layer 1)
Application Level Vulnerabilities Bypass Transport Encryption Alone	A vulnerability in the file transfer application itself can be exploited regardless of transport layer encryption strength	Application layer payload encryption as an independent layer (Section 5, Layer 4)
Delayed Detection Extends Impact Window	Extended time between compromise and detection allowed broader data exposure across affected organizations	Audit logging and non repudiation layer (Section 5, Layer 5; Section 13)

The application level vulnerabilities lesson in Table 1 deserves particular emphasis, because it directly counters a common but mistaken assumption: that strong transport layer encryption alone is sufficient protection for a file transfer flow. Transport layer encryption protects data while it moves between two endpoints, but does not protect against a vulnerability in the endpoint application itself, which is precisely the vulnerability class that affected managed file transfer platforms in 2023. This is the specific rationale for treating application layer payload encryption as an independent, additional layer rather than a redundant one.

4. Research Methodology

This study employs a design framework and illustrative comparative analysis methodology, synthesizing foundational cryptographic and transport security standards (Rescorla, 2018; National Institute of Standards and Technology, 2007; Dworkin, 2007), FIPS validation guidance (National Institute of Standards and Technology, 2019), managed file transfer security advisory literature (Cybersecurity and Infrastructure Security Agency, 2023; SANS Institute, 2022), and documented Studio integration platform encryption capabilities (Workday, Inc., 2021a; Workday, Inc., 2023b) into the six layer defense in depth stack presented in Section 5. The comparative illustrations in Sections 8 and 9 use figures constructed to demonstrate directional relationships consistent with the underlying cryptographic and networking principles, rather than measurements audited against a specific production deployment.

Table 2. Summary of research methodology components.

Methodology Component	Method	Purpose
Incident Lesson Extraction	Synthesis of managed file transfer security advisory literature	Establish structural lessons motivating the framework (Section 3)

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

Defense in Depth Framework Development	Synthesis of TLS, AES, and FIPS standards with platform capability documentation	Establish the six layer stack and protocol selection guidance
Comparative Security Property Illustration	Directional estimate construction consistent with cryptographic protocol properties	Illustrate expected security property differences across mechanisms (Section 8)
Performance Illustration Construction	Directional estimate construction consistent with protocol overhead characteristics	Illustrate expected throughput and latency trade-offs (Section 9)

5. The Six Layer Defense in Depth Stack

This article proposes a six layer defense in depth stack for encrypted data in transit, structured so that a weakness in any single layer does not compromise the overall security posture of a given transfer flow.

FIGURE 3: SIX-LAYER DEFENSE-IN-DEPTH STACK FOR ENCRYPTED FILE TRANSFER

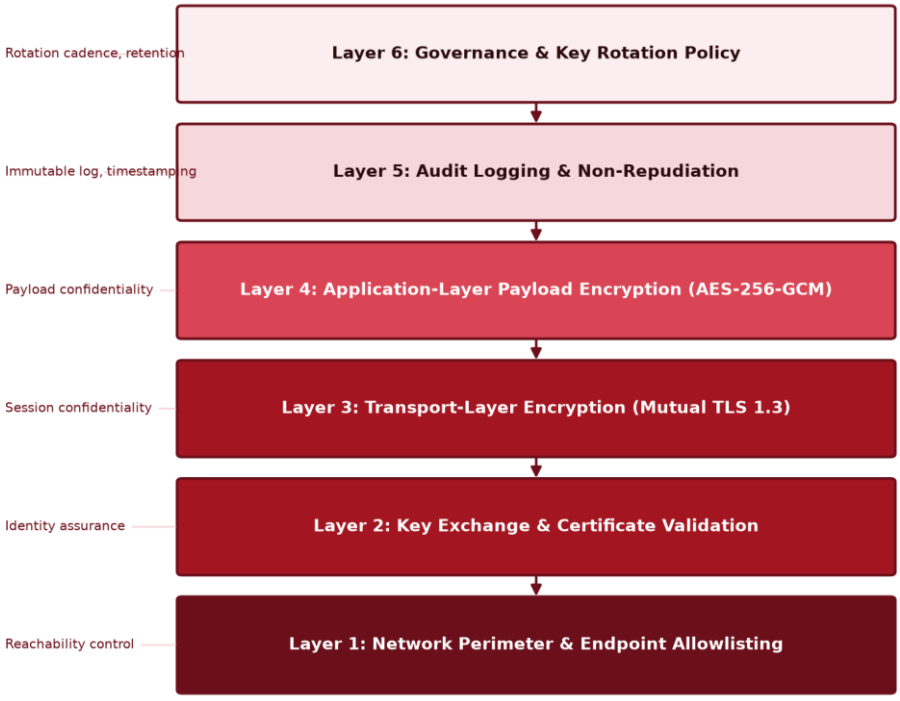


Figure 1. The six layer defense in depth stack for encrypted file transfer, spanning network perimeter control through governance and key rotation policy.

Table 3. The six layer defense in depth stack for encrypted data in transit, with representative controls and addressed failure modes.

Layer	Primary Concern	Representative Control	Failure Mode Addressed
Layer 1: Network Perimeter and Endpoint Allowlisting	Reachability control	IP allowlisting, network segmentation	Unauthorized network level access to the transfer endpoint
Layer 2: Key Exchange and Certificate Validation	Identity assurance	Mutual certificate validation, certificate pinning where appropriate	Impersonation of a legitimate counterparty endpoint

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

Layer 3: Transport Layer Encryption (Mutual TLS 1.3)	Session confidentiality	Mutual TLS 1.3 handshake with forward secrecy	Interception of data while in transit between endpoints
Layer 4: Application Layer Payload Encryption	Payload confidentiality	AES-256-GCM encryption of the payload itself, independent of transport	Compromise of the transfer application exposing unencrypted payload content
Layer 5: Audit Logging and Non Repudiation	Accountability	Immutable, timestamped transfer logs with cryptographic signing	Delayed or absent detection of unauthorized transfer activity
Layer 6: Governance and Key Rotation Policy	Sustained assurance	Scheduled key and certificate rotation, periodic policy review	Gradual erosion of cryptographic strength through stale keys or lapsed certificates

Layers 3 and 4, transport layer encryption and application layer payload encryption, are frequently conflated in practice, with organizations assuming that strong TLS configuration alone constitutes complete encryption in transit coverage. As discussed in Section 3, this assumption does not hold once the specific failure mode under consideration is a vulnerability in the transfer application itself rather than interception of data on the network, which is precisely why the framework treats these as two distinct layers rather than a single combined layer.

6. End to End Encrypted Transfer Sequence

To illustrate how the six layers in Section 5 combine operationally, this section walks through a representative end to end encrypted transfer sequence spanning five distinct actors, from initial file staging at a source system through final delivery confirmation at the HCM tenant boundary.

FIGURE 1: END-TO-END ENCRYPTED TRANSFER SEQUENCE (MULTI-ACTOR)

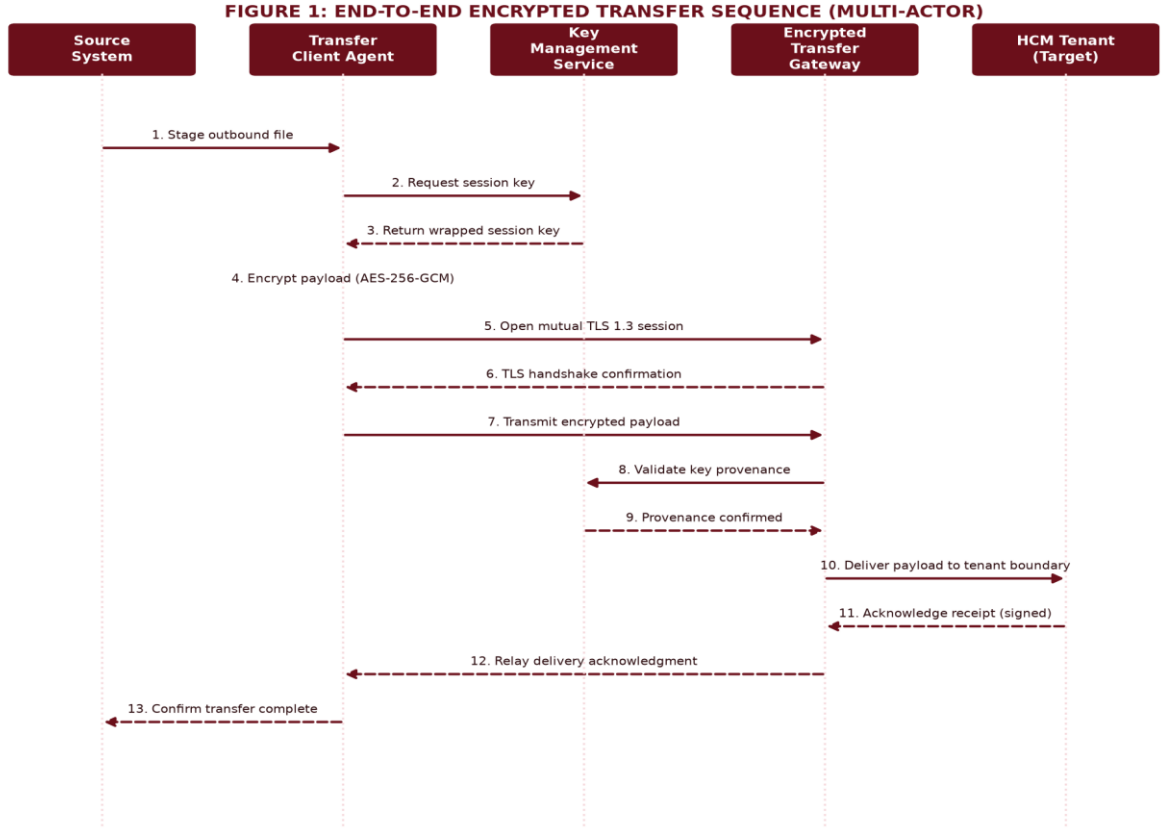


Figure 2. End-to-end encrypted transfer sequence across five actors, illustrating key exchange, mutual TLS session establishment, payload transmission, and signed delivery acknowledgment.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

Table 4. Mapping of the end-to-end transfer sequence steps to the six defense in depth layers.

Sequence Step	Actors Involved	Defense Layer(s) Exercised
1-4: Staging, key request, and payload encryption	Source System, Transfer Client Agent, Key Management Service	Layer 4 (payload encryption), Layer 6 (key issuance policy)
5-7: Mutual TLS session and encrypted payload transmission	Transfer Client Agent, Encrypted Transfer Gateway	Layer 2 (certificate validation), Layer 3 (transport encryption)
8-9: Key provenance validation	Encrypted Transfer Gateway, Key Management Service	Layer 2 (identity assurance), Layer 6 (governance)
10-11: Tenant delivery and signed acknowledgment	Encrypted Transfer Gateway, HCM Tenant	Layer 5 (non repudiation)
12-13: Acknowledgment relay and completion confirmation	Encrypted Transfer Gateway, Transfer Client Agent, Source System	Layer 5 (audit logging)

This mapping illustrates an important structural property of the framework: a single transfer operation exercises multiple layers concurrently rather than passing through them sequentially as independent gates. Steps 8 and 9, key provenance validation, for example, draw on both the identity assurance provided by Layer 2 and the governance policy established in Layer 6 simultaneously.

7. Protocol and Cryptographic Module Selection Framework

Given the six layer stack established in Section 5, this section addresses a practical decision point: which specific protocol and cryptographic module combination is appropriate for a given transfer flow, given that counterparty regulatory profile and integration pattern both materially affect that decision.

FIGURE 4: PROTOCOL AND MODULE SELECTION DECISION TREE

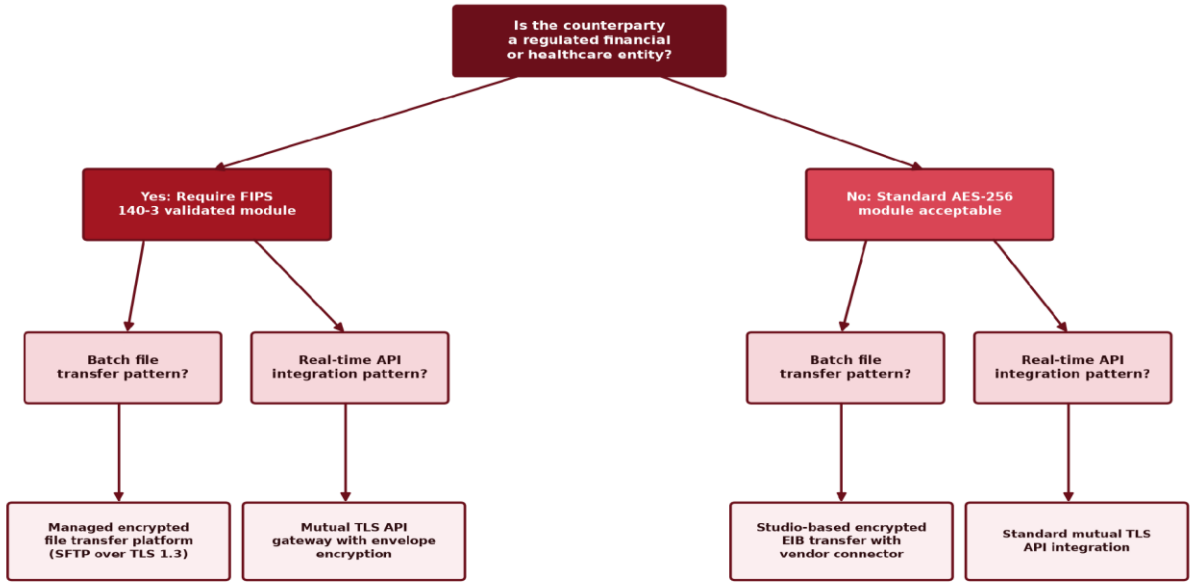


Figure 3. Protocol and cryptographic module selection decision tree, branching on counterparty regulatory profile and integration pattern.

Table 5. Decision factors informing protocol and cryptographic module selection for a given transfer flow.

Decision Factor	Question	Implication for Selection
Counterparty Regulatory Profile	Is the counterparty a regulated financial or healthcare entity	Regulated counterparties generally require FIPS 140-3 validated modules; unregulated

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

	subject to specific cryptographic module requirements	counterparties can generally accept standard AES-256 modules
Integration Pattern	Does the flow follow a batch file transfer pattern or a real time API integration pattern	Batch patterns favor managed encrypted file transfer platforms or Studio encrypted EIB transfer; real time patterns favor mutual TLS API gateways
Data Sensitivity Classification	Does the flow carry highly sensitive fields such as national identifiers or compensation detail	Higher sensitivity classifications favor combining Layer 3 and Layer 4 encryption rather than transport encryption alone
Vendor Technical Capability	Does the counterparty's own platform support mutual TLS 1.3 and modern cipher suites	Limited vendor capability may require a managed intermediary platform rather than direct mutual TLS integration

As Figure 3 illustrates, the decision tree does not converge on a single recommended protocol across the entire organization. Instead, it produces four distinct recommended configurations depending on the combination of regulatory profile and integration pattern, reflecting this article's central argument that protocol diversification, rather than uniform reliance on a single platform, is itself a risk reducing design choice.

8. Comparative Security Property Analysis

This section presents an illustrative comparative analysis of security properties across five transfer mechanisms, spanning legacy unencrypted FTP through modern Studio based encrypted transfer patterns.

FIGURE 5: ILLUSTRATIVE SECURITY PROPERTY COMPARISON ACROSS TRANSFER PROTOCOLS

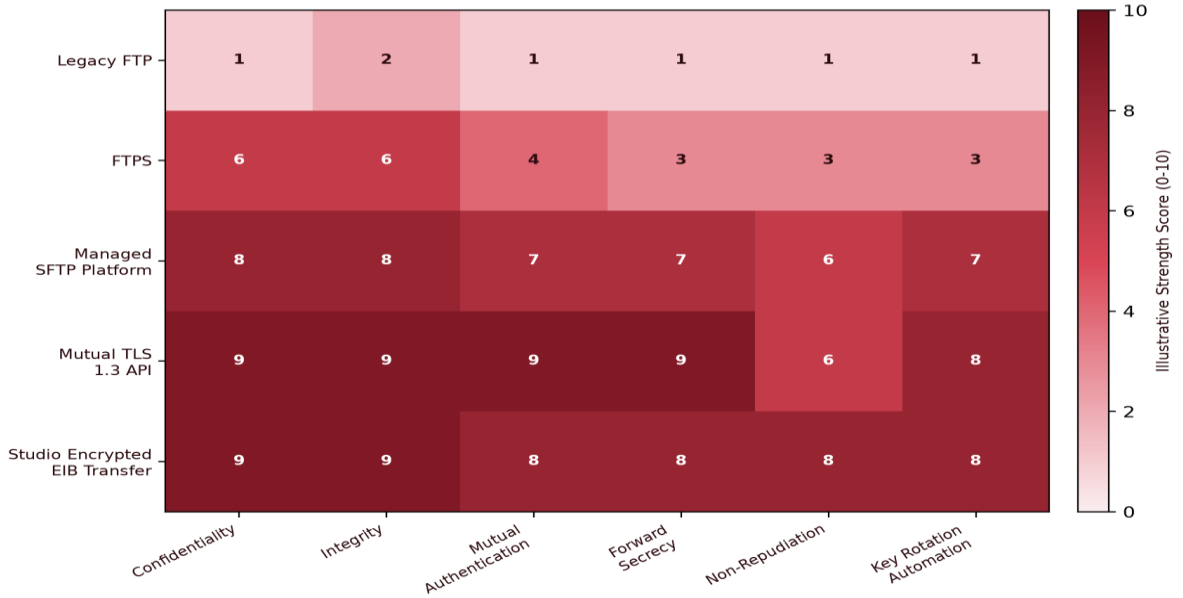


Figure 4. Illustrative security property comparison across five transfer protocols, scored across confidentiality, integrity, mutual authentication, forward secrecy, non-repudiation, and key rotation automation.

Table 6. Illustrative overall security posture and primary limiting property by transfer mechanism.

Transfer Mechanism	Illustrative Overall Security Posture	Primary Limiting Property
Legacy FTP	Very Low	No confidentiality or integrity protection of any kind
FTPS	Low-Moderate	Limited forward secrecy and non-repudiation support

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

Managed SFTP Platform	Moderate-High	Key rotation automation and non-repudiation depend on platform configuration maturity
Mutual TLS 1.3 API	High	Non-repudiation weaker than dedicated audit logging mechanisms absent additional signing
Studio Encrypted EIB Transfer	High	Requires disciplined connector configuration to realize full property coverage

The comparative figures in Table 6 and Figure 4 reinforce a theme carried throughout this article: even the strongest mechanisms examined, mutual TLS 1.3 API integration and Studio encrypted EIB transfer, show a residual limitation in at least one property, underscoring why the defense in depth stack in Section 5 treats non-repudiation and governance as independent layers rather than assuming they are automatically provided by strong transport encryption alone.

9. Performance Considerations: Throughput and Latency

Security property strength is not the only relevant consideration in protocol selection. This section presents an illustrative throughput and handshake latency comparison across the same five transfer mechanisms examined in Section 8.

FIGURE 6: ILLUSTRATIVE THROUGHPUT AND HANDSHAKE OVERHEAD BY TRANSFER PROTOCOL

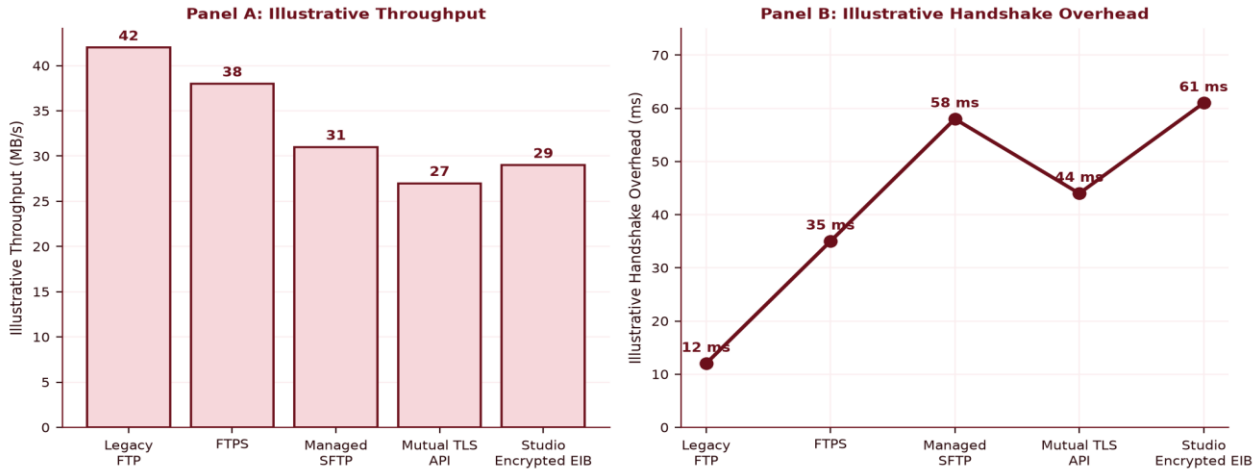


Figure 5. Illustrative throughput and handshake overhead comparison across five transfer protocols, shown as two panels.

Table 7. Illustrative throughput and handshake overhead by transfer mechanism, with practical implications.

Transfer Mechanism	Illustrative Throughput (MB/s)	Illustrative Handshake Overhead (ms)	Practical Implication
Legacy FTP	42	12	Highest throughput and lowest overhead, but security posture is unacceptable for HCM data
FTPS	38	35	Moderate overhead increase relative to FTP for a modest security improvement
Managed SFTP Platform	31	58	Overhead reflects mature session negotiation;

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

			acceptable for scheduled batch patterns
Mutual TLS 1.3 API	27	44	Handshake overhead is amortized across session reuse in sustained API integration patterns
Studio Encrypted EIB Transfer	29	61	Highest overhead among viable options, generally acceptable given typical batch scheduling tolerance

The throughput figures in Table 7 indicate a general, expected pattern: stronger security properties correlate with somewhat higher handshake overhead and modestly lower raw throughput. For the batch oriented and moderate volume integration patterns typical of HCM data flows, this trade-off is generally acceptable, since the absolute overhead differences shown remain small relative to typical batch processing windows, a point addressed further in the protocol selection guidance in Section 7.

10. Encrypted Transfer Topology for a Multi Vendor HCM Landscape

A single HCM tenant typically maintains encrypted transfer relationships with a substantial number of distinct external and internal endpoints simultaneously. This section illustrates a representative topology spanning ten endpoints, demonstrating how the protocol diversification principle from Section 7 applies across a realistic, multi-vendor landscape rather than a single point to point connection.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

FIGURE 2: ENCRYPTED TRANSFER MESH TOPOLOGY ACROSS TEN ENDPOINTS

Figure 6. Encrypted transfer mesh topology spanning the HCM core tenant, external vendor endpoints, internal support services, and auxiliary legacy nodes.

Table 8. Endpoint categories within the illustrative multi vendor topology and typical protocol assignment.

Endpoint Category	Representative Endpoints	Typical Protocol Assignment
External Vendor Endpoint	Payroll Vendor A, Payroll Vendor B, Benefits Admin, Background Check Provider	Managed SFTP platform or mutual TLS API, per the decision tree in Section 7
Internal Support Service	Time and Attendance, Regional HCM Replica, Key Management Service	Studio encrypted EIB transfer or mutual TLS, given common administrative control
Auxiliary or Legacy Node	Legacy Staging Zone, Audit Log Sink	Managed SFTP platform, pending eventual decommission per the migration approach in Section 14

The topology in Figure 6 makes visually explicit a structural benefit of protocol diversification: because different endpoint categories connect through different protocol assignments, a vulnerability affecting one specific protocol or platform does not simultaneously expose every connection in the topology, directly addressing the centralization lesson documented in Section 3.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

11. Key Management and Rotation Practice

Layer 6 of the defense in depth stack, governance and key rotation policy, depends on a specific, well defined key management practice to be operationally meaningful rather than aspirational. This section documents recommended key management practices supporting the framework.

Table 9. Recommended key management practices supporting the governance and key rotation policy layer.

Key Management Practice	Description	Recommended Frequency
Session Key Rotation	Session keys used for application layer payload encryption are generated fresh for each transfer session	Per transfer session, without exception
Certificate Renewal	TLS certificates used for mutual authentication are renewed before expiration with sufficient lead time	Per certificate validity period, with renewal initiated at least thirty days before expiration
Key Provenance Validation	Every session key's issuing authority is validated before use, per the sequence step documented in Section 6	Every transfer session
Emergency Key Revocation Capability	A defined, tested process exists to revoke and reissue keys rapidly if a compromise is suspected	Tested quarterly; executed immediately upon suspected compromise
Key Management Service Redundancy	The key management service itself is deployed with sufficient redundancy to avoid becoming a single point of failure	Continuous, architectural requirement

The key management service redundancy practice in Table 9 deserves specific attention, because it represents a subtle risk: if every layer of the defense in depth stack ultimately depends on a single key management service instance, that service itself becomes exactly the kind of concentrated point of exposure the overall framework is designed to avoid, echoing the centralization lesson from Section 3 at a different architectural layer.

12. Studio Integration Specific Encryption Patterns

Studio based integration pipelines occupy a specific position within the overall framework, since they can directly implement several defense in depth layers natively rather than depending entirely on an external file transfer product.

Table 10. Studio integration platform capabilities supporting specific defense in depth layers.

Studio Capability	Defense Layer Supported	Configuration Consideration
Connector Level Mutual TLS Support	Layer 3 (transport layer encryption)	Confirm the specific connector version supports TLS 1.3 rather than an older, deprecated version
Certificate Based Authentication	Layer 2 (key exchange and certificate validation)	Maintain certificate inventory and renewal tracking specifically for Studio managed certificates
Custom Payload Encryption Logic	Layer 4 (application layer payload encryption)	Apply consistent AES-256-GCM implementation across all pipelines rather than ad hoc, pipeline specific encryption logic
Integration Event Logging	Layer 5 (audit logging and non-repudiation)	Confirm logging captures sufficient detail to support the non-repudiation requirements in Section 13

The custom payload encryption logic row in Table 10 highlights a specific governance risk: because Studio allows integration developers to implement custom encryption logic directly within a pipeline, absent a governed, shared implementation standard, different pipelines built by different developers may implement payload encryption inconsistently, undermining the uniformity the framework otherwise assumes across Layer 4.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

13. Audit Logging and Non Repudiation

Layer 5 of the defense in depth stack directly addresses the delayed detection lesson documented in Section 3, requiring that every transfer produce a durable, tamper evident record sufficient to reconstruct what occurred after the fact, independent of whether the transfer itself succeeded, failed, or was later found to be unauthorized.

Table 11. Audit logging and non-repudiation requirements supporting Layer 5 of the defense in depth stack.

Audit Requirement	Description	Rationale
Immutable Log Storage	Transfer logs are written to storage that prevents after the fact modification or deletion	Preserves evidentiary value if a compromise is later discovered
Cryptographic Timestamping	Log entries include a cryptographically verifiable timestamp	Establishes precise sequencing for incident reconstruction
Signed Delivery Acknowledgment	The receiving endpoint returns a cryptographically signed confirmation of receipt	Provides non-repudiation of successful delivery, as illustrated in step 11 of Figure 2
Retention Aligned to Regulatory Requirement	Log retention periods meet or exceed applicable regulatory and contractual requirements for the data involved	Supports compliance obligations and extended incident investigation windows

14. A Phased Migration Approach

Organizations reducing reliance on a single managed file transfer platform rarely do so through a single, simultaneous cutover. This article proposes a nine task, phased migration timeline.

FIGURE 7: ILLUSTRATIVE MIGRATION TIMELINE FROM LEGACY TRANSFER TO ENCRYPTED FRAMEWORK

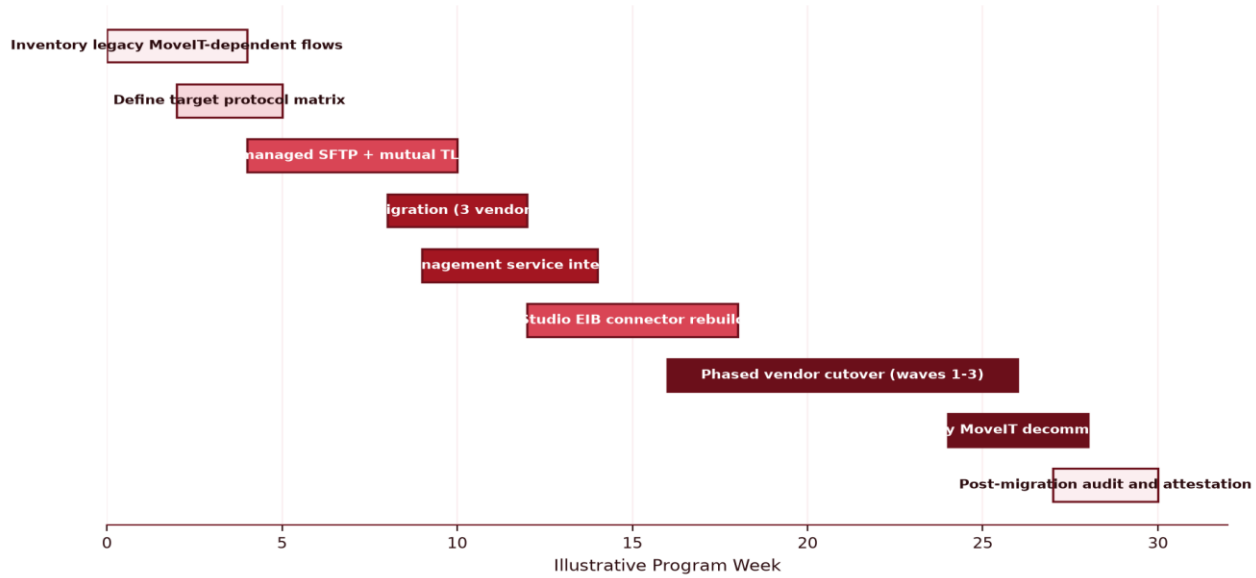


Figure 7. Illustrative migration timeline from legacy managed file transfer reliance to a diversified encrypted transfer framework.

Table 12. Illustrative nine task migration timeline from legacy managed file transfer reliance to a diversified framework.

Migration Task	Illustrative Start Week	Illustrative Duration (Weeks)	Primary Dependency
Inventory legacy platform dependent flows	Week 0	4	None; foundational task
Define target protocol matrix	Week 2	3	Partial completion of inventory task

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

Stand up managed SFTP and mutual TLS gateway	Week 4	6	Target protocol matrix substantially defined
Pilot migration across three vendor flows	Week 8	4	Gateway infrastructure operational
Key management service integration	Week 9	5	Gateway infrastructure operational
Studio EIB connector rebuild	Week 12	6	Key management service integration underway
Phased vendor cutover across three waves	Week 16	10	Pilot migration validated successfully
Legacy platform decommission	Week 24	4	Substantial completion of phased cutover
Post migration audit and attestation	Week 27	3	Decommission substantially complete

The overlapping task durations visible in Figure 7 and Table 12, particularly the parallel execution of key management service integration and Studio EIB connector rebuild, reflect a practical migration principle: tasks that do not share a direct sequential dependency should generally proceed in parallel, since sequencing every task strictly one after another would extend the overall program timeline well beyond what is operationally necessary.

15. Governance for Sustained Encryption Posture

Sustaining the framework's security posture after initial migration requires ongoing governance structure, since new vendor relationships and integration flows continue to be added after the migration program concludes.

Table 13. Recommended governance practices for sustaining encryption posture after initial migration.

Governance Practice	Purpose	Recommended Review Cadence
New Vendor Protocol Assignment Review	Confirm every newly onboarded vendor is assigned a protocol per the decision tree in Section 7 rather than an ad hoc default	Prior to every new vendor onboarding
Certificate and Key Inventory Audit	Confirm all active certificates and keys remain within validity and rotation policy	Quarterly
Protocol Diversification Ratio Review	Monitor the proportion of transfer volume concentrated in any single platform, to detect re-concentration over time	Semi-annual
Audit Log Completeness Check	Confirm audit logging coverage remains complete across all active transfer flows	Quarterly
Incident Response Plan Rehearsal	Test the emergency key revocation and incident response process under simulated conditions	Annual

The protocol diversification ratio review deserves particular attention, since it directly monitors whether the centralization risk the entire framework was designed to reduce is gradually reaccumulating over time, for example if operational convenience leads new vendor onboarding to default back toward a single dominant platform absent explicit governance attention.

16. Common Pitfalls in Encrypted Transfer Adoption

Table 14. Recurring pitfalls in encrypted data in transit adoption and recommended corrections.

Pitfall	Description	Recommended Correction
Conflating Transport and Payload Encryption	Organization assumes strong TLS configuration alone provides complete encryption in transit coverage	Apply both Layer 3 and Layer 4 independently, per Section 5

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

Re-Concentration After Migration	Operational convenience gradually shifts new vendor onboarding back toward a single dominant platform	Monitor the protocol diversification ratio per Section 15
Inconsistent Studio Payload Encryption Implementation	Different pipelines implement custom encryption logic inconsistently	Establish a governed, shared implementation standard per Section 12
Key Management Service as an Unrecognized Single Point of Failure	The key management service itself lacks redundancy despite every layer depending on it	Apply the redundancy practice documented in Section 11
Uniform Protocol Selection Regardless of Counterparty	The same protocol is applied to every vendor regardless of regulatory profile or integration pattern	Apply the decision tree in Section 7 rather than a single default choice

17. Limitations of the Study

Several limitations should be considered when interpreting this article's findings. First, the comparative security property and performance figures presented in Sections 8 and 9 are illustrative estimates constructed to demonstrate expected directional relationships consistent with established cryptographic and networking principles, rather than measurements audited against a specific production deployment. Second, this study addresses encrypted data in transit specifically for HCM integration flows and does not directly examine encryption at rest, which is a related but distinct concern outside this article's scope. Third, the migration timeline in Section 14 reflects a synthesized, illustrative sequencing rather than outcomes empirically tracked across multiple organizations completing a comparable migration program. Fourth, this article does not address the specific technical details of the 2023 managed file transfer platform incidents in depth, focusing instead on the structural lessons those incidents illustrate.

Table 15. Summary of study limitations and suggested mitigations for future research.

Limitation	Potential Effect on Findings	Suggested Mitigation for Future Studies
Illustrative, not audited, comparative figures	Absolute figures may not generalize across organizations	Controlled empirical study across multiple production integration landscapes
Encryption in transit scope only	Findings do not address encryption at rest considerations	Extension study addressing a combined in transit and at rest framework
Unvalidated migration timeline	Actual migration duration and sequencing may vary considerably by organization	Longitudinal tracking of organizations completing a comparable migration program
Limited incident specific technical detail	Framework motivated by general lessons rather than a detailed technical post-mortem	Dedicated technical case study drawing on detailed incident forensic data where available

18. Recommendations

- Apply the full six layer defense in depth stack to every transfer flow, treating transport layer and application layer encryption as independent, complementary layers rather than a single combined control.
- Diversify protocol and platform selection across the vendor landscape according to the decision tree in Section 7, rather than defaulting every counterparty to a single platform for operational convenience.
- Monitor the protocol diversification ratio on an ongoing basis to detect and correct gradual re-concentration toward a single dominant platform.
- Establish a governed, shared implementation standard for Studio based payload encryption logic, rather than allowing inconsistent, pipeline specific implementations to proliferate.
- Deploy the key management service itself with sufficient redundancy, recognizing that it underpins every other layer of the framework.
- Sequence migration tasks with attention to genuine dependencies, running independent tasks in parallel rather than in an unnecessarily long strict sequence.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

- Rehearse the emergency key revocation and incident response process at least annually, rather than assuming a documented process alone is sufficient preparation.

19. Future Research Directions

This study suggests several directions for further research. First, an empirical study measuring actual security posture, throughput, and latency across organizations that have implemented the six layer framework would strengthen the illustrative findings presented in Sections 8 and 9 with statistically validated figures. Second, research extending this framework to address encryption at rest in combination with encryption in transit would provide a more complete data protection picture for HCM environments. Third, comparative research examining post quantum cryptographic algorithms and their eventual integration into the transport and application layers of this framework would help organizations plan for the long term evolution of cryptographic standards. Finally, longitudinal research tracking organizations across the full duration of a migration program away from a single managed file transfer platform would provide deeper insight into which specific sequencing and governance choices most reliably predict a successful, sustained outcome.

20. Conclusion

This article has presented a six layer defense in depth framework for encrypted data in transit in enterprise HCM environments, developed specifically to address the structural lesson that widely reported managed file transfer platform incidents made clear: concentrating the majority of an organization's sensitive data movement in a single platform creates a concentrated exposure that a layered, diversified architecture is better positioned to avoid. The comparative analyses in Sections 8 and 9 indicate that no single protocol or platform choice is uniformly superior across every integration pattern, and that a mature posture instead depends on matching protocol selection to counterparty regulatory profile and integration pattern through the decision framework in Section 7, while consistently applying the full six layer stack regardless of which specific protocol is chosen for a given flow. The phased migration approach in Section 14 and the governance practices in Section 15 further underscore that reducing reliance on a single platform is not a one time architectural change but a sustained discipline, requiring ongoing monitoring to prevent the same concentration risk from gradually reaccumulating after migration concludes. Organizations seeking to strengthen the security posture of their HCM data movement are best served by adopting the full framework presented in this article, recognizing that protocol diversification, layered encryption, and sustained governance are mutually reinforcing elements of a single coherent strategy rather than independently sufficient measures on their own.

REFERENCES

1) Cybersecurity and Infrastructure Security Agency. (2023). Advisory on exploitation of managed file transfer software vulnerabilities. U.S. Department of Homeland Security.
2) Dworkin, M. (2007). Recommendation for block cipher modes of operation: Galois/Counter Mode (GCM) and GMAC (NIST Special Publication 800-38D). National Institute of Standards and Technology.
3) National Institute of Standards and Technology. (2007). Advanced Encryption Standard (AES) (Federal Information Processing Standards Publication 197). U.S. Department of Commerce.
4) National Institute of Standards and Technology. (2019). Security requirements for cryptographic modules (Federal Information Processing Standards Publication 140-3). U.S. Department of Commerce.
5) Rescorla, E. (2018). The Transport Layer Security (TLS) protocol version 1.3 (RFC 8446). Internet Engineering Task Force.
6) SANS Institute. (2022). Securing managed file transfer platforms: A practitioner's guide. SANS Institute Reading Room.
7) Workday, Inc. (2021a). Workday Studio integration development guide. Workday, Inc. Product Documentation.
8) Workday, Inc. (2023b). Workday integration encryption and connector security reference guide. Workday, Inc. Product Documentation.

Appendix A: Glossary of Terms

Table A-1. Glossary of key terms used throughout this article.

Term	Definition

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

Managed File Transfer (MFT)	A category of software platform providing centralized, typically encrypted file transfer capability across an organization
Transport Layer Security (TLS)	A cryptographic protocol providing communication security over a network, most recently formalized in version 1.3
AES-256-GCM	Advanced Encryption Standard with a 256 bit key, operated in Galois Counter Mode, providing both confidentiality and integrity
FIPS 140-3	A Federal Information Processing Standard specifying security requirements for cryptographic modules
Mutual TLS (mTLS)	A TLS configuration in which both the client and server present and validate certificates, rather than only the server
Forward Secrecy	A cryptographic property ensuring that compromise of a long term key does not compromise past session keys
Non-Repudiation	A property ensuring that a party cannot credibly deny having performed a specific action, typically achieved through cryptographic signing
Defense in Depth	A security strategy employing multiple independent layers of protection so that a failure in one layer does not compromise overall security
Key Provenance	Verifiable evidence establishing the legitimate origin and issuing authority of a cryptographic key
Protocol Diversification	The practice of distributing data transfer flows across multiple distinct protocols or platforms rather than a single mechanism

Appendix B: Supplementary Data Tables

This appendix provides additional illustrative data tables supporting the analysis in the main body of the article, including an extended cipher suite reference and a consolidated certificate lifecycle timeline.

B.1 Extended Cipher Suite Reference for TLS 1.3

Table B-1. Extended TLS 1.3 cipher suite reference with recommended use cases.

Cipher Suite	Key Exchange	Authenticated Encryption	Recommended Use
TLS_AES_256_GCM_SHA384	Ephemeral Diffie-Hellman	AES-256-GCM	Recommended default for regulated and high sensitivity flows
TLS_AES_128_GCM_SHA256	Ephemeral Diffie-Hellman	AES-128-GCM	Acceptable for lower sensitivity flows with performance sensitivity
TLS_CHACHA20_POLY1305_SHA256	Ephemeral Diffie-Hellman	ChaCha20-Poly1305	Preferred on platforms lacking AES hardware acceleration

B.2 Illustrative Certificate Lifecycle Timeline

Table B-2. Illustrative certificate lifecycle timeline supporting Layer 6 governance practice.

Lifecycle Stage	Illustrative Timing	Responsible Party
Certificate Issuance	Initial vendor onboarding	Key Management Service Administrator
Mid-Validity Health Check	Fifty percent of validity period elapsed	Automated monitoring system
Renewal Initiation	Thirty days before expiration	Key Management Service Administrator

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

Renewal Completion and Deployment	Fifteen days before expiration	Integration Engineering Team
Post-Renewal Validation	Within forty eight hours of deployment	Integration Engineering Team

B.3 Illustrative Protocol Volume Distribution Target

Table B-3. Illustrative target protocol volume distribution supporting the diversification ratio governance practice in Section 15.

Transfer Mechanism	Illustrative Target Share of Total Transfer Volume	Rationale
Managed SFTP Platform	35 percent	Retained for established batch relationships with limited vendor technical capability
Mutual TLS 1.3 API	30 percent	Preferred for real time integration patterns and technically capable vendors
Studio Encrypted EIB Transfer	30 percent	Preferred for internally controlled flows and batch patterns within the platform
Other or Emerging Mechanisms	5 percent	Reserved capacity for pilot evaluation of new protocols or platforms

