Mission-Critical Demands: Why Mainframe Certificates Require Strategy, Not Just Software

How Ensono combines its own z/OS certificate discovery and lifecycle automation intellectual property with a Certificate Life Cycle Manager (CLM) to run mainframe certificates as a governed, evidenced managed service.

Jane Bradshaw, Security Product Management, Leader
Nikita Hissaria Presales, Senior Solution Architect

©2026 Ensono, LLC. All rights reserved.

CONFIDENTIAL - INTERNAL USE ONLY

47 days	8x	199%	30 days
Maximum public TLS validity from 15 March 2029, reached in steps of 200 and 100 days	Renewal events per certificate by year five against one annual renewal today	Five-year ROI on avoided labor alone, before any outage-avoidance credit	To a complete, evidenced certificate and key ring inventory across the estate

Audience: CIO, CISO, Head of Mainframe and Infrastructure Operations, Audit and Risk, Finance
Version 1.0 | September 2026 | Written to be read on its own

Executive summary

The option to manage certificates manually has been removed. Maximum publicly trusted TLS validity fell to 200 days for certificates issued on or after 15 March 2026, falls to 100 days on 15 March 2027, and falls to 47 days on 15 March 2029, when domain validation data reuse also drops to 10 days.[1] These are adopted dates in the CA/Browser Forum Baseline Requirements, not a proposal.[2] Renewal events per certificate move from roughly one a year to about eight.

For distributed estates this is a tooling problem, and the market has answered it with agents and orchestration. For the mainframe it is an operating-model problem. A z/OS certificate is not a file on a server. It is an object inside the external security manager, connected to one or more key rings under a specific owning identity, and consumed by subsystems that only pick up the change when a particular operator or policy refresh action is taken.[3] Renewal is a privileged, multi-step, multi-team transaction with a real blast radius – exactly the work that does not scale by adding events to a calendar.

> **Ensono closes the mainframe gap with its own intellectual property and uses a commercially available CLM for what a certificate authority platform should do. Neither half works alone.**

Ensono Mainframe Certificate Management as a Service is built on three layers with deliberately separate responsibilities. A CLM is the lifecycle engine, policy authority, and issuance path, and exposes the enrollment, replacement, renewal, and revocation actions Ensono automation calls.[4] The ITSM is the system of record for change authority and retained evidence. Between them sits the part no external platform provides: Ensono-developed z/OS intellectual property that reads the authoritative certificate and key ring inventory out of the security manager, maps every consuming subsystem, and then executes the privileged renewal path to a validated live endpoint.

---

[1]CA/Browser Forum, Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates (Ballot SC-081v3 validity schedule), https://cabforum.org/working-groups/server/baseline-requirements/requirements/

[2]DigiCert, "TLS Certificate Lifetimes Will Officially Reduce to 47 Days", https://www.digicert.com/blog/tls-certificate-lifetimes-will-officially-reduce-to-47-days

[3]IBM, "Digital Certificates on z/OS: From Concept to Implementation" (RACDCERT functions, key rings), https://public.dhe.ibm.com/eserver/zseries/zos/racf/pdf/r14_digital_certificates_on_zos_from_concepts_to_implementation_part_1.pdf

[4]Sectigo, "Understanding REST endpoints", Sectigo Certificate Manager administrator documentation, https://docs.sectigo.com/scm/scm-administrator/understanding-rest-endpoints.html

CONFIDENTIAL - INTERNAL USE ONLY

Six points to take from this paper

- **The deadline is dated and non-negotiable.** No mainframe team is staffed for eight renewal events per certificate per year.
- **A Structured Approach to Mainframe Certificate Governance.** The difficulty is key ring topology, owning identities, hardware-protected keys, and subsystem refresh authority.
- **Ensono IP supplies what platforms cannot.** Authoritative internal inventory that network discovery cannot see, plus a governed privileged execution path with evidence and rollback.
- **The control boundary is the design.** Discovery is provably read-only. Write authority is scoped to named rings, gated, and enabled only after the client accepts the inventory and signs the lifecycle policy.
- **Commitments follow authority.** Ensono warrants outcomes only where it holds the authority to complete them, and says so explicitly through the disposition model.
- **The funding case stands on labor, not fear.** On the reference estate, labor avoidance alone returns 199% over five years and cuts five-year total cost of ownership by 67%. Avoided outage value is upside.

Reference figures are from Ensono's controlled Mainframe CMaaS model on a 600-certificate, 120-domain estate, dated September 2026.

The forcing function is a set of dates

Certificates Issued	Maximum Validity	Domain And IP Validation Data Reuse	Renewal Events Per Certificate Per Year
Before 15 Mar 2026	398 days	398 days	About 1
15 Mar 2026 to 14 Mar 2027	200 days	200 days	About 2
15 Mar 2027 to 14 Mar 2029	100 days	100 days	About 4
On or after 15 Mar 2029	47 days	10 days	About 8

Two consequences matter more than the headline. Validation data reuse collapsing to 10 days makes domain control validation a recurring automated activity rather than an annual task.[5] And the arithmetic compounds with scale: an enterprise holding 1,000 public TLS certificates moves toward roughly 8,000 issuances and 40,000 domain validations a year.[6]

Mainframe certificate failure can halt entire business. In independent survey work, more than one third of organizations had a service outage caused by an expired certificate in the past year, nearly three quarters

[5]CA/Browser Forum, Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates (Ballot SC-081v3 validity schedule), https://cabforum.org/working-groups/server/baseline-requirements/requirements/

[6]DigiCert, "Research Finds Certificate Failures Are a Six-Figure Infrastructure Risk" (Omdia survey), https://www.digicert.com/news/digicert-research-finds-certificate-failures-are-a-six-figure-infrastructure-risk

CONFIDENTIAL - INTERNAL USE ONLY

reported at least five hours of certificate-related downtime, and nearly one in four said their most significant certificate incident cost more than $250,000. Only around 10% had automation already in place.[7]

Regulation points the same way. PCI DSS v4.0.1 requires a maintained inventory of cryptographic cipher suites and protocols, and of the trusted keys and certificates protecting account data in transit.[8] NIST IR 8547 sets the cryptographic horizon: classical 112-bit signatures deprecated after 2030 and disallowed after 2035, which makes a rehearsed mass-reissue capability a stated expectation rather than a good intention.[9]

> **An organization that cannot produce a current certificate inventory on demand has a compliance finding today and an availability incident scheduled for later.**

Why mainframe certificates require cross-functional governance

On the mainframe, the challenge is not primarily about lacking tools, but rather about the organizational and operational structure required to manage certificates safely. The challenge is operational dependencies which are scattered across multiple domains. A single certificate change in the security manager can ripple across 5–10 different operational systems simultaneously. Yet there's no integrated governance model that treats these dependencies as a single, coordinated change. Each domain owns its piece independently.

Dimension	Distributed Estate	z/OS Estate
Where it lives	A file or store on the host, or a cloud key store	An object in the external security manager, connected to one or more key rings under a specific owning identity
How it is discovered	Network scan plus host agent enumeration	Network scan sees the listener only. The authoritative record requires privileged extraction from the security manager
Who can renew it	Platform or application team, often with delegated automation	Scoped privileged authority in the security manager, plus separate operator authority to refresh the consumer
How the consumer picks it up	Service reload or container restart	A specific action per subsystem: policy agent refresh for AT-TLS, SSL rebuild for CICS, security refresh for MQ, node cycle for managed file transfer
Key custody	Usually exportable software keys	Keys may be generated in and bound to cryptographic hardware and cannot be exported, which removes some renewal paths entirely
Blast radius	Usually one application	A shared key ring can serve several subsystems and business services at once

[7]DigiCert, "Research Finds Certificate Failures Are a Six-Figure Infrastructure Risk" (Omdia survey), https://www.digicert.com/news/digicert-research-finds-certificate-failures-are-a-six-figure-infrastructure-risk

[8]Encryption Consulting, "PCI DSS v4.0.1 Requirement on CBOM" (Requirements 12.3.3 and 4.2.1.1 cryptographic and certificate inventory), https://www.encryptionconsulting.com/pci-dss-v4-requirement-on-cbom/

[9]NIST IR 8547 (initial public draft), Transition to Post-Quantum Cryptography Standards, https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf

CONFIDENTIAL - INTERNAL USE ONLY

Three of these are where generic certificate lifecycle management quietly fails. Network discovery cannot enumerate key rings, owning identities, trust status or default designation, because none of it is exposed on the wire — so any inventory built from scanning alone under-reports the mainframe and omits the internal certificates that most often cause the outage.[10] Installing and connecting a renewed certificate is only the middle of the job; the consuming subsystem must be told to pick it up, and that authority often sits with a different team.[11] And where private keys are non-exportable because they were generated in hardware, the renewal path must be decided by certificate class at design time. Discovering that during a live renewal window is the most common cause of a stalled mainframe certificate program.

The architecture: three layers, one control boundary

The separation of responsibilities is what makes the service auditable, and it is what a client security team should examine first.

Layer	Component	Responsibility
Lifecycle platform	Certificate Lifecycle Manager	Certificate authority agnostic issuance from public, private or client existing certificate authority paths; certificate profiles constraining validity, key type, and subject alternative name policy; network discovery; validity-based renewal triggers; enrollment, replacement, renewal, and revocation through REST endpoints using low-privilege credentials
Mainframe intellectual property	Ensono z/OS certificate discovery (read-only) and Ensono z/OS lifecycle execution (scoped write)	Authoritative extraction of certificates, key rings, owning identities, and mappings from the external security manager; dependency and blast-radius mapping to consuming subsystems; execution of the privileged renewal path from certificate signing request to validated live endpoint; evidence capture and rollback
Workflow and record	ITSM	Certificates and key rings as configuration items; standard changes for like-for-like automated renewals and normal changes for shared rings and restarts; pre-routed tasks to network, CICS, MQ and file transfer towers; approvals, timestamps, and retained evidence

> **Neither the CLM nor the ITSM touches the external security manager. That is Ensono intellectual property, and its authority is scoped, gated, and evidenced.**

[10]IBM, "Configuring a TLS connection with RACF key rings", z/OS Connect documentation, https://www.ibm.com/docs/en/zos-connect/3.0.0?topic=arci-configuring-tls-connection-racf-key-rings

[11]IBM, "Leveraging z/OS Communications Server Application Transparent TLS" (AT-TLS policy and key ring configuration), https://public.dhe.ibm.com/s390/zos/racf/pdf/share_2013_02_leveraging_zos_at_tls.pdf

CONFIDENTIAL - INTERNAL USE ONLY

Certificate Lifecycle Manager: the lifecycle engine

The CLM provides certificate authority agnostic lifecycle management across public and private certificates from one interface.[12] It does four jobs here. It holds the policy, with certificate profiles constrained to what the mainframe security manager can actually produce, so an automated renewal cannot be issued in a shape the platform cannot install. It is the issuance path across public, private and client certificate authority hierarchies. It carries the validity-based renewal trigger that drives the operating calendar. And it exposes the automation interface: enrollment REST endpoints support enrollment, replacement, renewal, and revocation with no administrator present, using accounts scoped to specific organizations and departments and requiring only outbound TCP 443.[13]

The CLM Ensono works with, gives Ensono a true multi-tenancy with isolated tenants, separate certificate inventories, separate administrator controls and separate usage and billing per end client[14] – tenant isolation as a platform property rather than a promise about internal process discipline.

Ensono mainframe intellectual property

Two capabilities carry the mainframe side and stay logically separate. One reads. One writes. That separation is the security argument.

Discovery (read-only)

Produces a machine-readable, authoritative inventory across every logical partition, then loads and enriches those records in the CLM and ITSM:

- **Certificate attributes –** label, owning identity, subject and issuer distinguished name, serial, validity dates, key algorithm, and size, whether the key sits in the security manager database or the cryptographic hardware, and trust status.
- **Key ring topology –** ring name, owning identity, the full certificate-to-ring connection map, usage designation, default flags, and identity mappings.
- **Both forms of orphaning –** certificates connected to no ring, and rings referencing missing or untrusted certificates.
- **Consumer dependencies –** AT-TLS policy rules, CICS key ring and TCP/IP service definitions, MQ queue managers and channels, managed file transfer nodes, IMS Connect, distributed data facility, directory services, file transfer and terminal listeners, and shadow key stores under Unix System Services.

The property that matters is negative: discovery holds list-level read authority only, with no authority to generate, alter or delete. It is designed to be provably incapable of mutation, which is what lets it run at the start of an engagement without a change freeze. Its outputs are what the rest of the service is contracted against – the certificate register, the dependency and blast-radius map, a twelve-month expiry heat map, and risk findings covering expired-but-connected certificates, weak keys, deprecated algorithms, self-signed client-facing endpoints, unrelated services sharing a ring, and hardware-bound keys with no defined renewal path.

---

[12]Sectigo, Certificate Manager product overview, https://www.sectigo.com/enterprise-solutions/certificate-manager

[13]Sectigo, "Understanding REST endpoints", Sectigo Certificate Manager administrator documentation, https://docs.sectigo.com/scm/scm-administrator/understanding-rest-endpoints.html

[14]Sectigo, "Sectigo Introduces Industry-First Multi-Tenant Partner Platform for Certificate Lifecycle Management" (24 March 2026), https://www.sectigo.com/resource-library/sectigo-partner-platform-clm

CONFIDENTIAL - INTERNAL USE ONLY

Lifecycle Execution (Scoped Write)

Carries the renewal transaction end to end and returns evidence. Three design decisions define it: authority is scoped to named rings and owning identities in the statement of work and never estate-wide; write authority is provisioned but disabled through discovery and enabled only after the client accepts the inventory and approves the dispositions; and where subsystem refresh authority is withheld, the certificate is reclassified rather than assumed.

Why a distributed lifecycle agent only is not the answer

The distributed pattern — install an agent, let it enumerate local stores, replace files, and reload the service — does not transfer. Agents do not enumerate external security manager key rings, and third-party agents are rarely permitted on z/OS in regulated estates.[15] The fallback most organizations use is a spreadsheet, a quarterly report and a senior engineer performing each renewal by hand. That is affordable at one renewal a year. It is not affordable at eight.

The renewal transaction, step by step

This is the sequence for a certificate classified as fully automated. It is written out deliberately, because the credibility of a mainframe certificate service rests on describing the whole path rather than the issuance step.

1. **Trigger.** The validity-based trigger fires and creates an ITSM request and change with the dependency map attached, so the approver sees the blast radius before approving.
2. **Certificate signing request.** A PKCS#10 request is generated against the incumbent certificate, preserving the registered subject and subject alternative names, or with a fresh key pair where rotation policy requires it.
3. **Issuance.** The request is submitted through the CLM enrollment REST endpoint against the assigned profile.
4. **Installation.** The signed leaf and chain are retrieved, correctly encoded, transferred and added under the correct owning identity and label, with chain certificates added as certificate authority entries.
5. **Connection.** The certificate is connected to every registered key ring with correct usage and default handling, followed by a security manager class refresh.
6. **Consumer refresh.** The specific action for each mapped consumer is executed or coordinated — policy agent refresh for AT-TLS, SSL rebuild for CICS, security refresh for MQ, node cycle for managed file transfer, or a listener restart where nothing lighter exists.
7. **Validation.** Ring and certificate state are re-read, trust and default state confirmed, a handshake performed against every consuming endpoint, and the serial presented live matched to the platform record.

---

[15]IBM, "Digital Certificates on z/OS: From Concept to Implementation" (RACDCERT functions, key rings), https://public.dhe.ibm.com/eserver/zseries/zos/racf/pdf/r14_digital_certificates_on_zos_from_concepts_to_implementation_part_1.pdf

CONFIDENTIAL - INTERNAL USE ONLY

8. **Evidence and rollback rehearsal.** An evidence pack is written to the ITSM change and the platform, and the rollback path is exercised inside the change window.

A change is closed on validated evidence, never on task completion alone.

The authority model, in outline

Function	Discovery (read-only)	Lifecycle execution (scoped write)
Enumeration and extract	List-level read authority, plus read access to the security manager database unload or authority to run it on a schedule	Inherits read for validation only
Generate, alter, delete	Explicitly none – provably incapable of mutation	Scoped to request generation, add, ring creation, connect, alter, and delete, limited to rings and owning identities named in the statement of work
Class refresh	None	Authority to refresh the certificate, ring, and mapping classes
Hardware key operations	None	Only where private keys are generated in hardware, with the renewal path documented per certificate class
Consumer subsystem refresh	None	Operator authority where granted, otherwise an explicit client handoff that changes the certificate's disposition

Two properties follow. Discovery can begin early because it cannot change anything. And write authority is a negotiated, documented artefact rather than a standing administrative account, which is normally what internal audit wants to see.

Operating model: gated onboarding to steady state

Onboarding is gated so neither party carries a commitment before the facts are agreed. No service level begins to measure until the client has accepted the certificate register.

CONFIDENTIAL - INTERNAL USE ONLY

Gate	Exit condition	Deliverables
0 – Readiness	Scope, tenancy model, certificate authority hierarchy, counterparts, and authority model agreed	Readiness checklist; service design document
1 – Access	Ensono can read the security manager and reach the platform. Write authority provisioned but disabled	Authority model and connectivity evidence
2 – Discovery acceptance	Three-pass discovery reconciled and signed accurate by client mainframe security	Certificate register; dependency and blast-radius map; risk findings; expiry heat map
3 – Governance	Lifecycle policy and dispositions approved; ITSM live; write authority enabled	Platform records, profiles, approval workflow, change and task templates
4 – Pilot	A non-production, single-consumer, software-key certificate completes the full evidence loop, then one low-blast-radius production repeat under an attended bridge	Pilot evidence pack; rollback rehearsal record
5 – Commencement	Migration waves complete and the legacy spreadsheet and quarterly report process retired	Signed exception register and remediation roadmap; runbooks

Discovery deliberately runs from two directions and is then reconciled: Ensono extracts the authoritative internal record, the platform scans network-visible endpoints, and Ensono reconciles the two and maps dependencies. That is where the interesting findings appear – certificates that terminate somewhere unexpected, endpoints nobody owns, and rings serving unrelated business services.

Classification before automation

Every certificate in the accepted register is assigned a disposition, so automation depth matches key custody, refresh authority, blast radius, and ownership rather than being forced uniformly across the estate.

Disposition	What Ensono Does	What Ensono Commits To
Automate	Full zero-touch path: issuance, installation, ring connection, security manager refresh, and dependent subsystem refresh	Prevention of expiry on in-scope production certificates, and renewal completion with validated evidence
Assisted	Issues, installs, and connects, then hands off to the client or a named third party for subsystem refresh or restart	A handoff a defined number of days before expiry, not automated completion. The remaining step is not Ensono's to warrant
Exception	Governance and monitoring only – non-exportable hardware-bound keys, vendor-embedded certificates, client-declined automation	Expiry visibility and inventory currency, with the exception recorded, approved, and aged
Retire	Removal after client approval – orphaned, duplicated or decommissioned	Excluded from service levels once approved

CONFIDENTIAL - INTERNAL USE ONLY

The assisted disposition is the load-bearing concept. It is what keeps the service levels honest.

Two further constructions do most of the operating work. The renewal trigger is expressed as a percentage of issued validity rather than a fixed number of days, so the operating calendar adjusts automatically at each validity step instead of being renegotiated three times before 2029. And migration waves are ordered by blast radius — non-production single-consumer first, then production internal, then client-facing public TLS, then shared multi-consumer rings requiring coordinated multi-tower change. The first certificate in every wave is attended.

Evidence, validation and recovery

A renewal is complete only when all three conditions hold. Any weaker definition allows a ticket to close while an endpoint still presents the old certificate.

Condition	Test
Correct certificate present	Present, trusted, and default where applicable, on every mapped key ring
Consumer actually using it	A functional handshake, or equivalent confirmation, against every mapped consuming endpoint
Records agree with reality	The serial presented by the live endpoint matches the platform record

Each renewal attaches the raw security manager checks, handshake result, serial match, approvals and timestamps, error and remediation detail, and rollback proof to the ITSM change and the platform record. That is what turns an audit request from a reconstruction exercise into a query. Four runbooks are maintained and tested — normal renewal, emergency replacement, revocation, and mass reissue for certificate authority compromise or algorithm deprecation. The mass-reissue drill is deliberately specific: reissue every certificate on a nominated key ring inside a single change window, which is the concrete answer to the cryptographic agility question the board will eventually ask.[16]

Service levels follow authority

The schedule covers prevention of expiry for automated certificates, renewal execution, assisted handoff, emergency replacement, expiry visibility, severity-one acknowledgement and restoration, revocation, discovery currency, register accuracy, drift detection, reporting, audit evidence on demand, the cryptographic agility drill, and platform availability pass-through. Three constructions matter: service levels apply only to certificates in the register the client has signed, using the agreed disposition; an initial measurement-only window establishes real baselines before credits apply; and platform availability is passed through rather than warranted by Ensono. Numeric targets sit in the service catalogue and the client statement of work.

[16]NIST IR 8547 (initial public draft), Transition to Post-Quantum Cryptography Standards, https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf

CONFIDENTIAL - INTERNAL USE ONLY

Six outcomes, and how each is measured

Each outcome is a claim with a target and a named evidence source. If Ensono cannot show the evidence, the outcome is not being delivered.

Outcome	Target	Evidence
A complete and continuously accurate certificate inventory	Complete evidenced inventory within 30 days, then maintained	Certificate register and dependency map, plus a monthly variance report showing additions, removals, and drift
No expiry-driven outages on in-scope production certificates	Zero	Incident record, renewal lead-time distribution, and count of certificates inside their at-risk window
Renewal capacity without adding headcount	Residual client effort at roughly 10% of the manual path; about 2.3 full-time equivalents at year-five volumes against about 15.1 unmanaged	Renewal volume and engineer-hours per renewal, reported monthly
Audit and regulatory evidence as a by-product	An audit-ready pack produced on request rather than reconstructed before an audit	Ownership, key strength, issuing authority, full renewal history, and approved exceptions with age
Cryptographic agility and a quantum-safe path	A costed, sequenced reissue plan with a rehearsed drill	Algorithm and key-length distribution, plus mass-reissue rehearsal throughput
Senior mainframe skills returned to higher-value work	Around 12.8 full-time equivalents of capacity released at 2029 reference volumes	Before-and-after effort measurement with explicit capacity reallocation

Executives see this on a fixed cadence. Monthly: renewal success rate, automation coverage, mean time to renew, out-of-process renewals and exception burn-down. Quarterly: policy review, cryptographic agility drill status, and algorithm and key-length posture mapped to the client's applicable frameworks. The CFO view is five-year total cost of ownership, labor savings, return on investment, and payback; the audit view is time to produce evidence, register accuracy and exception age.

The financial case

The reference estate is 600 in-scope mainframe certificates and 120 billable domains, with manual effort of 210 minutes per renewal plus 90 minutes for deployment, refresh, verification, and evidence, 12% rework, a $95 loaded hourly rate, and renewals rising 1 / 2 / 4 / 6 / 8 across five years — 12,600 renewal events in total, reaching 27,180 hours or 15.1 full-time equivalents in year five. Managed cost is a $90,000 annual platform base plus $600 per domain per year, $150,000 of implementation amortized across five years, 0.75 of an Ensono oversight full-time equivalent, and 10% retained client effort. Separating base from per-domain charging means rising renewal volume does not inflate subscription cost.

CONFIDENTIAL - INTERNAL USE ONLY

Case	Manual Five-Year Cost	Managed Five-Year Cost	Result
Conservative – labor only, no outage credit	$6.846M	$2.286M	• $4.560M saved • 199% ROI • 67% TCO reduction
Headline – includes avoided outage value	$12.272M	$3.100M	• $9.172M saved • 296% ROI • 75% TCO reduction • $6.416M NPV at 10% • Payback in year one

The saving is not a claim that certificate work disappears. In the manual path, effort scales with renewal events, which multiply eight-fold. In the managed path, the renewal loop runs unattended for automated certificates and human effort concentrates on exceptions, shared-ring coordination, and governance, which grow far more slowly than event volume. The framing is avoided recruitment of scarce z/OS specialists, not reduction of existing staff.

Sector fit

The control problem is the same everywhere. The consequence of failure is not.

Sector	What Breaks When A Mainframe Certificate Expires	Evidence And Regulatory Pressure
Financial services	Digital and core banking, payments, clearing, trading, and partner and API integration paths	PCI DSS cryptographic and certificate inventory requirements, SOX, GLBA and FFIEC expectations, and DORA for European operations
Insurance	Policy administration, claims intake and settlement, broker and agent integration, billing, and policyholder access	NAIC model expectations, state, and multi-jurisdiction examination evidence, NYDFS, and DORA where applicable
Government and public sector	Citizen services, public safety, tax, health and licensing platforms, and interagency exchange	CJIS and NIST SP 800-53 control evidence, with public-trust consequences that outlast the incident
Healthcare payers	Claims and enrolment processing, member and provider portals, and clearinghouse connectivity	HIPAA controls, authentication requirements, and timed recovery and evidence obligations

Ensono positions certificate, key management, and encryption services as part of a complete data security framework spanning data at rest and in transit.[17] Mainframe CMaaS is the operational execution layer underneath it: the part that keeps those certificates current, evidenced and governed.

[17]Ensono, Certificate, Key Management and Encryption Services, https://www.ensono.com/offerings/certificate-key-management-encryption/

CONFIDENTIAL - INTERNAL USE ONLY

Getting started: a 30-day baseline

Period	Activity	Client Receives
Days 1 to 5	Scope agreement, read-only authority provisioning, connectivity	Readiness checklist and agreed authority model
Days 6 to 20	Three-pass discovery and reconciliation across in-scope partitions	Draft certificate register, dependency and blast-radius map, twelve-month expiry heat map
Days 21 to 30	Risk findings, draft dispositions, and the financial model rebuilt on measured client inputs	Risk findings pack, draft disposition set, and a client-specific business case replacing every reference figure

At the end of 30 days the client owns an evidenced inventory of its mainframe certificates. That artefact has standalone compliance value regardless of what is decided next.

CONFIDENTIAL - INTERNAL USE ONLY