GOVERNED TEMPLATE RENDERING REFERENCE: PAYMENT SECURITY & PCI SPEC DEFAULT V2 (DRAFT)

definition f9576552…c689

PAYMENT SECURITY & PCI SPEC · PROJECT ARTIFACT

SPECIRA

Payment Security & PCI Spec: Dispatch Modernization

Meridian Field Services: instructional example, not project evidence

DRAFT · WATERMARK POLICY: DRAFT_ONLY

template payment_security_pci v2 · pack: specira_default_delivery

the cheapest control is the cardholder data you never touch

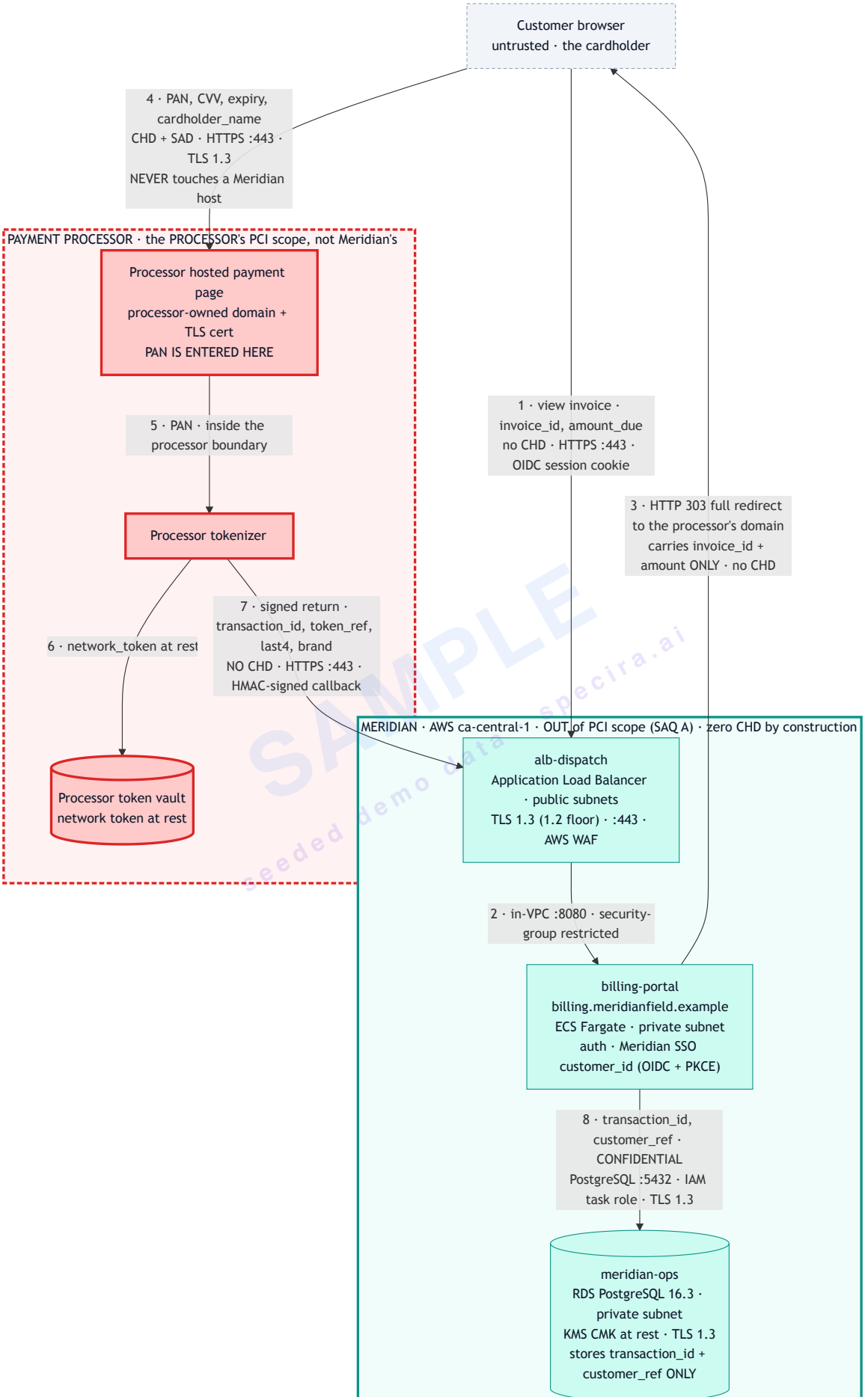
§1 Cardholder Data Scope

mandatory | 1 decision | 1 evidence rule

validators: saq_type_decision_justified_by_scope · saq_decision_made_before_architecture_not_backfilled · cde_boundary_diagram_present · no_pan_stored · sad_never_stored_post_auth

Scope first, because scope decides everything downstream. The dispatch core takes ZERO cardholder data; the compliance matrix excluded payment-card standards for the pilot (applicable regulations[1]); this artifact engages ONLY for the phase-two customer-portal billing surface (the portal's commercial extension[2]), designed now because scope minimization is decided before the architecture, not backfilled to justify what got built.

> **DECISION: SAQ A VIA A FULL REDIRECT**
>
> over a vendor-hosted iframe and direct handling. *Why considered*: a full redirect means zero cardholder data touches Meridian systems (the browser goes to the processor and returns); the iframe keeps SAQ A only if Meridian controls no element of the payment page, and the portal's branded styling risks that line dropping it to SAQ A-EP; direct handling is SAQ D, the full twelve-requirement catch-all, disproportionate for invoice payment. *Findings*: the redirect wins, the cheapest defensible SAQ, no cardholder data on merchant systems (payment scope decision[3]). *Who*: E. Sandoval (engineering) with N. Duval (compliance).



The cardholder-data environment boundary. Red is the processor's PCI scope, where cardholder data actually exists; teal is Meridian, which is PAN-free by construction. Fallback text: (1) the customer views an invoice (invoice_id, amount_due, no cardholder data) through alb-dispatch over TLS 1.3; (2) the load balancer forwards in-VPC to billing-portal on port 8080, security-group restricted; (3) the portal answers with an HTTP 303 full redirect to the processor's own domain, carrying only invoice_id and amount; (4) the customer types PAN, CVV, expiry, and cardholder_name into the PROCESSOR's hosted page over TLS 1.3, which never touches a Meridian host; (5) the processor tokenizes the PAN inside its own boundary; (6) the network token rests in the processor's vault; (7) the processor returns an HMAC-signed callback carrying transaction_id, token_ref, last4, and brand (no cardholder data); (8) billing-portal writes transaction_id and customer_ref to meridian-ops over TLS 1.3 with an IAM task role. The redirect severs the path rather than proxying it, so nothing is pulled into scope by connectivity.

The boundary, node by node

Node	Runs on	Auth · encryption	Card data held
`alb-dispatch`	Application Load Balancer · public subnets · AWS ca-central-1 (register[12])	TLS 1.3 terminated, 1.2 floor · WAF · 443 only	**None**; the redirect never carries it
`billing-portal` `billing.meridianfield.example`	ECS Fargate · private subnet · no public address	Meridian SSO customer_id, OIDC + PKCE (identity model[6]) · TLS 1.3	**None**; holds transaction_id + customer_ref only
`meridian-ops`	RDS PostgreSQL 16.3 · private subnet	IAM task role only · TLS 1.3 · KMS customer-managed key at rest	**None**; transaction_id, customer_ref
`Processor hosted page`	**The processor's** domain and certificate, the processor's	Processor-owned · TLS 1.3	`PAN, CVV, expiry`, entered here

Node	Runs on	Auth · encryption	Card data held
	PCI scope, not Meridian's		
Processor vault	The processor's infrastructure	Processor-owned	`Network token` at rest

Why the arrows name fields rather than "payment data." The entire scope argument turns on *which field crosses which boundary*. PAN, CVV, expiry, and cardholder_name cross only into the red zone. transaction_id, token_ref, last4, and brand are all that ever come back. An assessor who cannot follow the cardholder data across a diagram places the whole environment in scope by default, so the diagram either earns SAQ A or costs it.

No-store law: Meridian stores NO PAN (there is none to store) and NO sensitive authentication data, ever; the transaction id it retains is not cardholder data. Were PAN ever stored it would be rendered unreadable and masked to first-six-last-four on display, but the redirect model means that clause never fires.

§2 PCI Controls

mandatory · 1 decision · 1 evidence rule

validators: every_pci_requirement_cited_maps_to_saq_subset · every_cited_requirement_maps_to_sr_id · no_control_restates_sr_implementation · omitted_requirements_carry_saq_rationale

SAQ A asks a REDUCED set, not all twelve. The table restates only what the redirect model demands, each mapped to the security requirement that implements it; the mechanism lives in the security requirements, cited here, never re-described.

Requirement	Applicability under SAQ A	Mechanism (cites)	Status
Req 6: secure the redirect page	Script-integrity on the portal; exact-match redirect target	SR-006[4], exact-match redirects[5]	`Compliant`
Req 8: identify portal users	The portal's customer_id audience	identity model[6]	`Compliant`
Req 9: protect physical media	Not applicable: no cardholder-data media exists	SAQ omits; rationale recorded	`N/A`

Requirement	Applicability under SAQ A	Mechanism (cites)	Status
`Req 11: test the redirect integrity`	Quarterly script-integrity check	testing gates[7]	`Compliant`
`Req 12: maintain a policy`	The payment-security policy cites this artifact	This spec	`Compliant`

Omitted requirements carry the rationale: Reqs 3 and 4 (protect stored, and encrypt transmitted, cardholder data) do not apply, since no cardholder data is stored or transmitted by Meridian under the redirect model. Every cited requirement maps to the SAQ A subset AND to an SR id; no control re-describes an SR's implementation.

§3 Tokenization

mandatory · 1 decision · 1 evidence rule

validators: tokenization_vault_segmented_from_cde · tokenization_flow_shows_pan_location_and_lifetime · encryption_alone_does_not_descope

Where PAN exists, and for how long. Capture happens on the PROCESSOR's page (the redirect target), not a Meridian one; the processor tokenizes and returns a transaction id plus, for repeat billing, a network token stored in the PROCESSOR's vault.

> **DECISION: NETWORK TOKENS OVER GATEWAY TOKENS**
>
> for the repeat-billing case: higher authorization rates and automatic card-lifecycle updates. *Who*: E. Sandoval. The de-scoping condition is met either way: Meridian stores only the transaction id and the processor's customer reference, both segmented from any vault (there is no Meridian vault), so the portal stays out of scope.

PAN's location and lifetime on Meridian systems: never. The flow marks the merchant boundary as PAN-free by construction. Encryption alone would NOT de-scope; the point is that no cardholder data reaches Meridian to encrypt. Tokenization removes a system from scope only when it is segmented from the vault and the cardholder-data environment and stores only tokens, which the portal satisfies trivially, holding no token vault at all.

§4 Incident Playbook

mandatory · 1 decision · 1 evidence rule

validators: incident_playbook_cites_brand_notification_timelines · forensic_obligations_named · playbook_cites_detection_prediction_and_tracking

The realistic incident on a redirect surface is a compromised redirect or a skimming script injected into the portal page, not a Meridian cardholder-data breach, since there is none. Roles: N. Duval owns compliance notification, E. Sandoval owns containment.

Notification step	Timeline	Source
Merchant → acquirer	`Within 24 hours of suspicion`	card-brand response program[8]
Acquirer → card brand	`Within the brand's stated window`	card-brand response program[8]
Forensic investigator initial report	`On the brand's business-day deadline`	card-brand response program[8]
Compromised-account delivery	`On the brand's clock`	card-brand response program[8]

Forensic obligations: when a payment-card forensic investigator is engaged, evidence is preserved (the portal's page-integrity logs, the redirect telemetry), the investigator is granted system access, and the report cadence is met. **Cross-links**. Detection: the script-integrity alert (alert catalog[9]) and the e-skimming path the model predicted (attack surface: the public portal edge[10]); a realized incident becomes a risk-register issue (governance[11]). Tested annually; evolves from lessons.

§5 Open Questions

mandatory · 1 decision

Question	Owner	Answer by	Blocks
Does the phase-two portal's branded styling keep the redirect on SAQ A, or does any styled element on the payment page drop it to SAQ A-EP (a scope question the processor's integration guide answers)?	E. Sandoval with N. Duval	`At the portal integration design`	The SAQ-type confirmation only; the redirect model holds either way

Refs References & Package Contents

In the Specira workspace

specira	[1] Compliance matrix: the payment-card exclusion for the pilot app.specira.ai/projects/dispatch-modernization/artifacts/compliance-matrix#exclusions
specira	[2] Multi-tenant design: the portal's commercial extension, isolation strategy app.specira.ai/projects/dispatch-modernization/artifacts/multi-tenant-design
specira	[3] Decision log: the payment-scope decision app.specira.ai/projects/dispatch-modernization/artifacts/decision-log#payment-scope
specira	[4] Security requirements: SR-006 input validation app.specira.ai/projects/dispatch-modernization/artifacts/security-requirements#sr-006
specira	[5] API contracts: the exact-match redirect rule the portal reuses app.specira.ai/projects/dispatch-modernization/artifacts/api-contracts#redirects
specira	[6] Auth & authorization policy: the portal's customer_id identity model app.specira.ai/projects/dispatch-modernization/artifacts/auth-authz-policy#identity
specira	[7] CI/CD pipeline: the quarterly script-integrity testing gate app.specira.ai/projects/dispatch-modernization/artifacts/cicd-pipeline#testing
specira	[9] Observability: the script-integrity alert in the catalog app.specira.ai/projects/dispatch-modernization/artifacts/observability-monitoring#alerts
specira	[10] Threat model: the public portal edge, the e-skimming path app.specira.ai/projects/dispatch-modernization/artifacts/threat-model#attack-surface
specira	[11] Risk register: where a realized breach becomes a tracked issue app.specira.ai/projects/dispatch-modernization/artifacts/risk-register
specira	[12] Infrastructure & deployment: the network topology register (AWS ca-central-1, the load balancer, the private subnets, the RDS instance) app.specira.ai/projects/dispatch-modernization/artifacts/infrastructure-deployment#network-topology

External standards

external	[8] The card brand's account-data-compromise response program: the merchant, acquirer, forensic-investigator, and compromised-account notification timelines the acquirer's published card-brand response requirements