Secure PAN Decryption — Serverless PrivateLink Pattern (PCI Compliant)

Author: Mahesh Devendran — Cloud Architect, AWS | Serverless | DR | AI Automation | Compliance

Executive Summary

This paper presents a serverless, multi-account AWS architecture that secures PAN decryption using PrivateLink and AWS KMS, ensuring no plaintext PAN leaves the decryption boundary. It outlines the multi-account segmentation, security design, compliance alignment, and technical standards such as RSA-OAEP-SHA256 and SigV4, with an optional CloudHSM integration for hardware key custody.

1. Architecture Overview

The architecture adopts a multi-account segmentation model across Shared Services, Source (EKS), Security, Crypto (HSM), and Observability accounts. Each account serves a unique purpose — key distribution, PAN encryption, decryption, key custody, and compliance analytics. PrivateLink ensures secure, private communication between accounts without internet exposure.

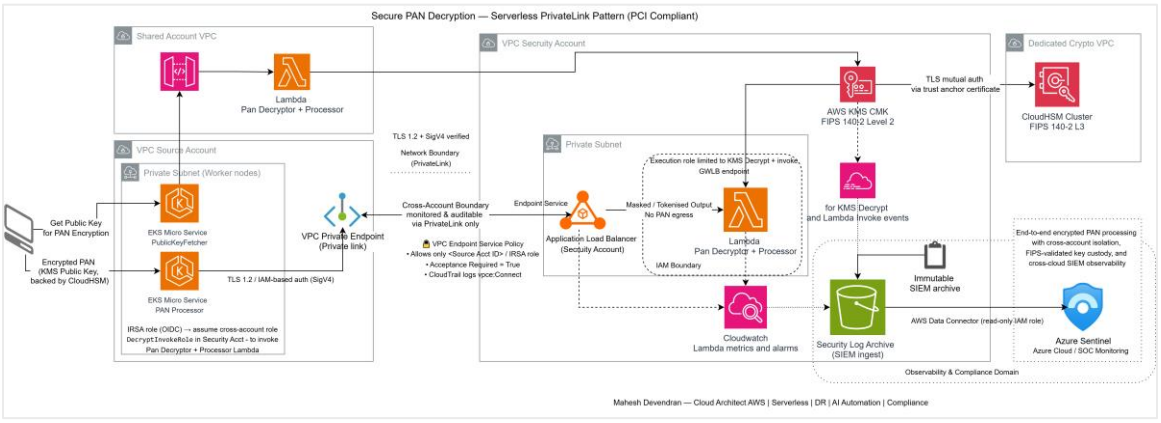

Figure 1: Secure PAN Decryption — Serverless Private Link Architecture (Client ingress via ALB + ACM omitted for simplicity)

Ingress and TLS Termination

For simplicity, the diagram does not depict the **Application Load Balancer (ALB)** and **AWS Certificate Manager (ACM)** components. In the production implementation, all client traffic to the EKS microservices is routed through a **secure HTTPS path** terminated at the **ALB Ingress Controller**, using **ACM-managed TLS certificates** to enforce encryption and certificate rotation. This design ensures full encryption in transit, centralized certificate management, and alignment with **PCI DSS 4.1 (Transmission Encryption)** requirements.

Data Flow Summary

Stage	Component	Key Functions

Client	Browser / App	Fetch KMS public key; encrypt PAN via RSA-OAEP-SHA256
Source	EKS Microservice	Handles encrypted PAN; calls Security Account via PrivateLink
Shared Services	Lambda KeyDistributor	Fetches KMS public key via AssumeRole
Security	Lambda Decryptor	Decrypts PAN using KMS; returns masked result
Observability	Azure Sentinel	Ingests audit and compliance logs

2. Security and Compliance Design

Encryption lifecycle ensures PAN data remains encrypted from client to decryption boundary. Client-side RSA encryption prevents plaintext exposure in transit or storage. PrivateLink provides TLS 1.2+ encryption within AWS backbone, and all decrypt operations occur within AWS KMS, optionally backed by CloudHSM for hardware assurance. Logs from all layers feed into CloudWatch, CloudTrail, and Azure Sentinel for full compliance visibility.

Compliance Alignment

Framework	Control ID	Coverage
PCI DSS 4.0	3.4–3.6	Encryption, key protection, lifecycle management
ISO 27001	A.10.1, A.12.4	Cryptographic controls, event logging
DORA	Article 9	ICT risk & operational resilience
FIPS	140-2 L2/L3	Hardware cryptography assurance (KMS/CloudHSM)

3. Business Benefits

The model delivers end-to-end encryption, cost-efficient scalability, and clear compliance mapping. It isolates decryption within the Security Account, enforces least privilege, and integrates native observability

for audits. Designed to evolve with CloudHSM, it provides PCI/DORA-ready architecture without additional compute overhead.

4. AWS Service–Compliance Mapping and Control Alignment

AWS Service	Primary Function	PCI DSS	ISO 27001	DORA	FIPS
AWS KMS	Encryption key management and PAN decryption	3.4–3.6: Encryption, key lifecycle	A.10.1: Cryptographic controls	Data protection & integrity	Level 2
AWS CloudHSM	Hardware key custody (CryptoAdmin/SysAdmin)	3.5: Key protection	A.10.1: Secure key storage	Segregation of duties	Level 3
AWS Lambda	Stateless compute for key ops	3.4: Data isolation	A.12.1: Controlled execution	Operational resilience	FIPS endpoints
API Gateway (Private)	Private API access via PrivateLink	3.6: Key exchange	A.10.1.2: Key exchange	Controlled comms	FIPS TLS
AWS PrivateLink	Private VPC-to-VPC connection	3.4: Encrypted transmission	A.10.1.1: Encryption in transit	ICT continuity	TLS 1.2
Amazon EKS	PAN processing (encrypted payload only)	3.4: No plaintext stored	A.12.4: Controlled env	Risk segmentation	KMS encryption
AWS IAM & STS	Role-based, temporary auth (SigV4)	3.6.6: Restrict key access	A.9.2: Access control	Least privilege auth	FIPS validated
CloudWatch	Operational monitoring	12.10.5: Security tracking	A.12.4: Logging	ICT monitoring	N/A
CloudTrail	Audit & API logging	10.2–10.3: Audit trails	A.12.4.3: Audit review	Resilience traceability	N/A
Amazon S3 (Archive)	Immutable log retention	3.4.1: PAN protection	A.12.3.1: Backup protection	Evidence retention	AES-256 FIPS
Azure Sentinel	Cross-cloud SIEM analytics	10.6: Audit correlation	A.12.7: Event correlation	Monitoring ICT risk	TLS 1.2

Each AWS service aligns to specific compliance and security objectives. KMS enforces encryption lifecycle; CloudHSM provides hardware-level custody; PrivateLink ensures zero internet exposure. IAM and STS secure cross-account access via SigV4, while CloudWatch, CloudTrail, and S3 maintain immutable audit trails. Azure Sentinel extends observability for DORA resilience monitoring. Together, they deliver a defense-in-depth architecture where encryption, access control, and compliance operate as integrated layers of trust.

5. Technical Glossary & Standards Explained

RSA-OAEP-SHA256: Asymmetric encryption algorithm using RSA key pairs. OAEP adds secure padding and SHA-256 ensures integrity, protecting PAN data even if intercepted.

SigV4 (AWS Signature Version 4): AWS's secure request signing protocol using temporary IAM credentials to authenticate API calls. Prevents replay or tampering without static keys.

FIPS 140-2 Level 2 and Level 3: NIST cryptographic security certifications. Level 2 adds role-based access and tamper evidence (AWS KMS). Level 3 enforces tamper-resistance and dual-control (CloudHSM).

PCI DSS 3.4–3.6: Payment Card Industry requirements for encryption, key management, and key lifecycle protection, implemented through KMS and IAM controls.

ISO 27001 A.10: Cryptographic control framework ensuring confidentiality and integrity through managed key protection using KMS and IAM.

DORA Article 9: EU regulation focusing on ICT risk management and operational resilience, achieved through multi-account segregation and SIEM visibility.