Sensible data tokenization and encryption for bank processing

Solution white Paper

Challenge

Challenge

- Financial technology companies, which handle vast volumes of sensitive customer and transactional data, face the critical challenge of securing confidential information such as:
  - — personally identifiable information (PII);
  - — payment card data;
  - — authentication credentials;
  - — employee records.
- Data encryption methods provide strong information protection through robust algorithms and secure management of cryptographic keys, making information inaccessible to unauthorized access.
- Tokenization effectively replaces sensitive data with secure equivalents, minimizing risks in data storage and transmission.
- Implementing either of these solutions significantly enhances data security:
  - — at rest;
  - — in transit;
  - — during processing.
- It is important to ensure smooth integration of the technology into:
  - — business processes;
  - — system scalability;
  - — staff training for maximum implementation effectiveness.

Goals and priorities

Business Goals

Sensitive data requiring protection via encryption and tokenization includes:

1. Personal Identifiable Information (PII)

Names, addresses, phone numbers, dates of birth, government-issued IDs.

2. Financial Data

Credit card primary account numbers (PAN), CVV codes, bank account details, transaction histories.

3. Employee Data

Payroll records, salaries, tax information.

4. Confidential Business Data

Contractual terms, internal financial calculations, sensitive communications.

5. Authentication Data

Passwords, one-time passwords (OTP), biometric identifiers.

6. API Keys and Access Tokens

Used for secure authentication and integration with banking and fintech services.

Tokenization & encryption key benefits

- Tokenization replaces sensitive data with tokens that hold no exploitable value on their own, significantly reducing exposure if data stores are compromised.
- Encryption scrambles data to make it unreadable without keys, protecting data during:
  - — storage;
  - — transmission.
- The combined use of these technologies creates layered defense: tokenization secures data privacy at rest by minimizing clear-text exposure, while encryption protects data:
  - — in transit;
  - — during processing.
- This layered protection framework helps financial institutions maintain regulatory compliance with standards such as:
  - — PCI DSS;
  - — GDPR.
- It reduces the impact of potential data breaches and safeguards the privacy and integrity of customer and employee data while preserving business operational effectiveness.

Solution overview

Here is a list of examples of fintech sensitive data protection solutions using tokenization and encryption, including types, architectures, and pricing where possible. These options provide a range from fully tailored projects in Kazakhstan to global solutions adaptable for CIS fintech environments. Pricing is often dependent on scale and customization, with local integrators playing a key role in adaptation and support.

Each solution's unique characteristics address specific fintech data protection challenges based on geography, deployment model, innovation level, and compliance requirements.

Here is a fit&gap analysis table for the five proposed products articulating how each fits fintech and sensitive data protection needs, and where gaps or trade-offs exist:

Criteria	HashiCorp Vault	QAZTECH Alliance Cryptographic Solutions	CAC Kazakhstan (Groupe CIS)	TokenEx / Thales CipherTrust	Fintech Regulatory Sandbox Projects (Kazakhstan)
Tokenization Description	Vault-based tokenization, with future potential for vaultless.	Vault-based tokenization tightly integrated with sovereign / local compliance.	Vault-based tokenization, customized for regional requirements.	Both vault-based and emerging vaultless tokenization options.	Hybrid blockchain / tokenization; project-based experimental use.
Pros	Centralized secret management. Dynamic secrets and auto-revocation. Strong API support.	Complete sovereign control with strong compliance. High security.	Flexible hybrid-on-prem / cloud deployments. Regional expertise.	Certified globally (PCI DSS, GDPR). Fast SaaS integration. Scalable cloud-native architecture.	Supports rapid innovation. Enables regulatory sandboxing and experimentation.
Cons	Complex to configure. Risk of misconfigured access policies (requires experience).	High initial cost. Requires specialized expertise.	Variable pricing. Scaling complexity in projects.	Relies on global SaaS infrastructure. Less localized customization.	Immature technology. Regulator dependent. Limited scalability.
Use Case Fit	Enterprises requiring flexible secret management across environments.	Large banks requiring sovereign control over sensitive data.	Regionally focused banks needing hybrid security architectures.	Fintechs seeking rapid, compliant SaaS adoption and scale.	Fintech startups and projects within regulatory frameworks.

Fit & gap analysis table for proposing products

Criteria	HashiCorp Vault	QAZTECH Alliance Cryptographic Solutions	CAC Kazakhstan (Groupe CIS)	TokenEx / Thales CipherTrust	Fintech Regulatory Sandbox Projects (Kazakhstan)
Encryption Technologies	AES symmetric, HSM-backed on-demand encryption.	AES symmetric, RSA asymmetric, HSM key management.	AES symmetric, RSA asymmetric encryption.	AES symmetric, hybrid encryption schemes.	Standard encryption, with blockchain cryptography options.
Vaultless Tokenization	Not currently, planned future support.	No.	No.	Yes.	Potential via blockchain-based pilots.
Scalability & Performance	Highly scalable via microservices and distributed architecture.	Enterprise scale limited by vault-based design.	Enterprise scale with hybrid deployment flexibility.	Cloud-native SaaS designed for high volume and rapid scaling.	Dependent on pilot scope; high innovation potential.
Integration Flexibility	Robust API and authentication integration.	Custom developed for local banking workflows.	Modular and flexible hybrid-cloud deployments.	Rich SDK, API and multi-cloud support.	Experimental APIs, designed for sandbox regulatory tests.
Cost Profile	Free community edition, enterprise starting ~ $1,000/month.	High upfront investment, project-based.	Variable, scope-dependent.	License starting ~ $15,000/year, scalable pricing.	Grant / subsidy supported, minimal direct costs initially.
Compliance and Auditing	Detailed audit logs and strict policy control.	Strong local audit and regulatory compatibility.	Regional compliance with extensive audit capabilities.	PCI DSS, GDPR certified, enterprise-grade auditing.	Focus on regulatory reporting and sandbox monitoring.

HashiCorp Vault

Platform designed for secure storage, dynamic generation, and lifecycle management of sensitive information such as:

— API keys;
— credentials;
— tokens;
— encryption keys.

Type

Open-source and commercial solution.

Architecture

- HashiCorp Vault provides centralized secrets management with dynamic secrets generation and encryption as a service.
- It securely stores and manages sensitive information such as API keys, passwords, and certificates through encryption at rest and in transit.
- Vault supports identity-based access control with:
  - — multiple authentication methods (tokens, LDAP, GitHub, AppRole);
  - — fine-grained policy enforcement;
  - — dynamic key management;
  - — secret leasing with automatic expiration;
  - — comprehensive audit logging for compliance.
- It can integrate with hardware security modules (HSMs) for enhanced protection.
- Vault exposes APIs for seamless integration into:
  - — fintech applications;
  - — backend systems.

1. **Tokenization Technologies:** Relies on Vault's Transform Secrets Engine, which uses AES256-GCM96 encryption to tokenize data such as API keys or confidential IDs, providing maximum resistance against data breaches.
2. **Encryption Technologies:** Deploys Vault's Transit Secrets Engine for encrypting data in transit and at rest (symmetric AES encryption), without storing the plaintext data, suitable for encrypting sensitive data on-the-fly.

Pricing

- Free open-source version available.
- Commercial enterprise starts approximately at $1,000/month for small to midsize usage.
- Higher tiers for large organizations with dedicated support and advanced features.
- **Influencing factors:**
  - — number of users;
  - — secrets stored;
  - — high availability features;
  - — HSM integration;
  - — support plans.

Solution key benefits

- Provides a dynamic, policy-driven secret management platform with :
  - — robust API support;
  - — balancing tokenization's irreversibility with on-demand encryption /decryption.
- Its dynamic secret leasing minimizes exposure windows, combined with detailed audit logs ensuring governance and traceability.

Tokenization & encryption key benefits

QAZTECH Alliance Cryptography Solutions (KZ)

Focus on increasing local tech expertise and compliance; tailored for Kazakhstan's banking and finance sectors.

Type

Custom / local fintech cryptographic solutions.

Architecture

Cryptographic protection designed for fintech workflows; uses secure token vaults and encrypted channels; meets local regulatory standards with government cooperation.

1. **Tokenization Technologies:** Vault-based tokenization maps tokens to original data, ensuring controlled access and audit, suitable for banking requirements.
2. **Encryption Technologies:** Symmetric AES encryption for fast, bulk data protection and swift encryption / decryption.

Pricing

Custom contracts starting from 10k+ USD for enterprise cryptographic systems.
Influencing factors: Deployment scope, customization, integration complexity, support, maintenance, data processing scale.

Solution key benefits

Sovereign locally developed cryptosystems integrated with Kazakhstan's laws, ensuring data residency and national security compliance. Tokenization preserves data formats reducing app changes; encryption secures data with national-grade algorithms.

CAC Kazakhstan (Groupe CIS)

Emphasis on regional market customization and compliance.

Type

Systems integrator providing innovative fintech security.

Architecture

Modular integration with banking and cloud systems; offers end-to-end encryption with tokenization.

1. **Tokenization Technologies:** Secure vault modules dynamically create and manage tokens, replacing sensitive data like passports or payments.
2. **Encryption Technologies:** Uses symmetric (AES) and asymmetric (RSA) encryption for data in transit and at rest.

Pricing

Project-based, starting around $20K enterprise-level.
Influencing factors: Bank size, data workflows, deployment type (hybrid / on-prem), SLA.

Solution key benefits

Tailored modular security solutions combining tokenization and encryption designed for CIS banks' heterogeneous IT infrastructures.

Enables flexible hybrid cloud or on-premises deployment meeting regional compliance, with strong focus on minimizing operational disruption during integration.

Sensitive data protection solutions

Commercial Products (Familiar global tools adapted)

Emphasis on national and regional market customization and compliance.

Type

Systems integrator offering innovative fintech security solutions.

Architecture

Modular integration with banking infrastructure and cloud; provides end-to-end encryption and tokenization for sensitive data.

1. **Tokenization Technologies:** Secure vault modules dynamically generate and manage tokens, replacing sensitive info like passports or payments.
2. **Encryption Technologies:** Uses symmetric (AES) and asymmetric (RSA) encryption for secure data transit and storage.

Pricing

Generally starting from $15,000 to $50,000 annually depending on transaction volume and integration complexity.
Influencing factors: Bank size, data workflows, deployment (hybrid cloud/on-prem), SLA levels.

Solution key benefits

Cloud-native, high-assurance tokenization and encryption platform with proven PCI DSS certification and global multi-tenant SaaS architecture. Scales easily with transaction volume and provides seamless developer integration tools for rapid fintech innovation globally, including CIS.

Kazakhstan Regulatory Sandbox Fintech Projects

Focused on regulatory support to accelerate fintech security adoption.

Type

Pilot and experimental custom fintech security projects.

Architecture

Enables rapid fintech innovation with blockchain tokenization and cryptography; integrates API gateways for secure data access.

1. **Tokenization Technologies:** Blockchain-backed tokenization generating tokens representing assets, banking data, or identities.
2. **Encryption Technologies:** Uses AES encryption and secure key management for fast prototyping.

Pricing

Startup pilots range $3,000–$30,000; larger regulated pilots cost more based on scale and customization.
Influencing factors: Project scope, innovation, blockchain use, regulator involvement.

Solution key benefits

Fast-iterating platform for secure digital asset tokenization under regulatory supervision, combining standard encryption to protect live data and lower startup entry barriers.

Solution architecture (tokenization)

Tokenization integration

Sensitive employee data is extracted from operational, HR, and banking systems using Airbyte and Airflow. During transformation with Spark and dbt, sensitive fields go to a Tokenization API, which creates tokens and stores originals securely in a vault like HashiCorp Vault or processes them cryptographically without a vault.

Tokenized data is stored in a Data Lake like MinIO. BI tools query this data and request detokenization via API. HashiCorp Vault replaces sensitive data with tokens, reducing exposure. It ensures encrypted storage, strict access control, secure detokenization, audits, compliance, and enables secure analytics without compromising privacy.

Integration into Data Entry / Onboarding Flow

1. Data Interception

During employee onboarding in HRIS, sensitive inputs such as salary are routed to the Tokenization Service API via real-time API calls or hooks.

2. Token Generation

The API returns a format-preserving token stored in HRIS, while securely storing the original data in the vault.

3. Flow Update

Original flow: HR enters data → Save to DB. Integrated: HR enters data → API tokenizes → Save token in DB, original in vault. This adds minimal latency (<50ms).

Integration into Storage and Management Flow

1. Token Storage

Tokens replace PII in operational databases, reducing the compliance scope since tokenized data is not considered PII.

2. Update Handling

Updates like salary changes are handled by sending the token to the API for detokenization and vault update; a new token may be generated.

3. Flow Update

Original: Update → Overwrite DB. Integrated: Update via token → API detokenizes and updates vault → New token stored. Immutable logs can be maintained via blockchain technologies like Hyperledger for audit trails.

Solution architecture (tokenization)

Integration into Processing (e.g., Payroll)

1. Authorized Detokenization

- Payroll systems request originals via authenticated API calls using tokens (e.g., to get exact salary numbers).

2. Secure Processing

- Operations occur in secure memory enclaves; results are re-tokenized before storage.

3. Flow Update

- Original: Pull data → Process.
- Integrated: Pull token → API detokenizes → Process → Re-tokenize output.
- Third-party vendors see only tokens, improving security.

Integration into Analytics and Reporting

1. Tokenized Analytics

- Tokens are stored in Data Warehouse / Data Lake for analysis.

2. Aggregate Detokenization

- For aggregates (e.g., average salaries), the API detokenizes data in a secure backend and returns results without exposing individual data.

3. Flow Update

- Original: Export data → Analyze.
- Integrated: Export tokens → API for aggregated detokenization → Analyze.
- Format-preserving tokens ensure numeric compatibility for analytics.

Tokenizing Existing Data in Operational DB and Warehouse

1. Export

Extract PII from operational DB and data warehouse via ETL or SQL.

2. Batch Processing

Feed PII batches to Tokenization Service API for tokenizing and original data vault storage.

3. Data Replacement

Replace sensitive fields in operational DB with tokens using SQL updates.

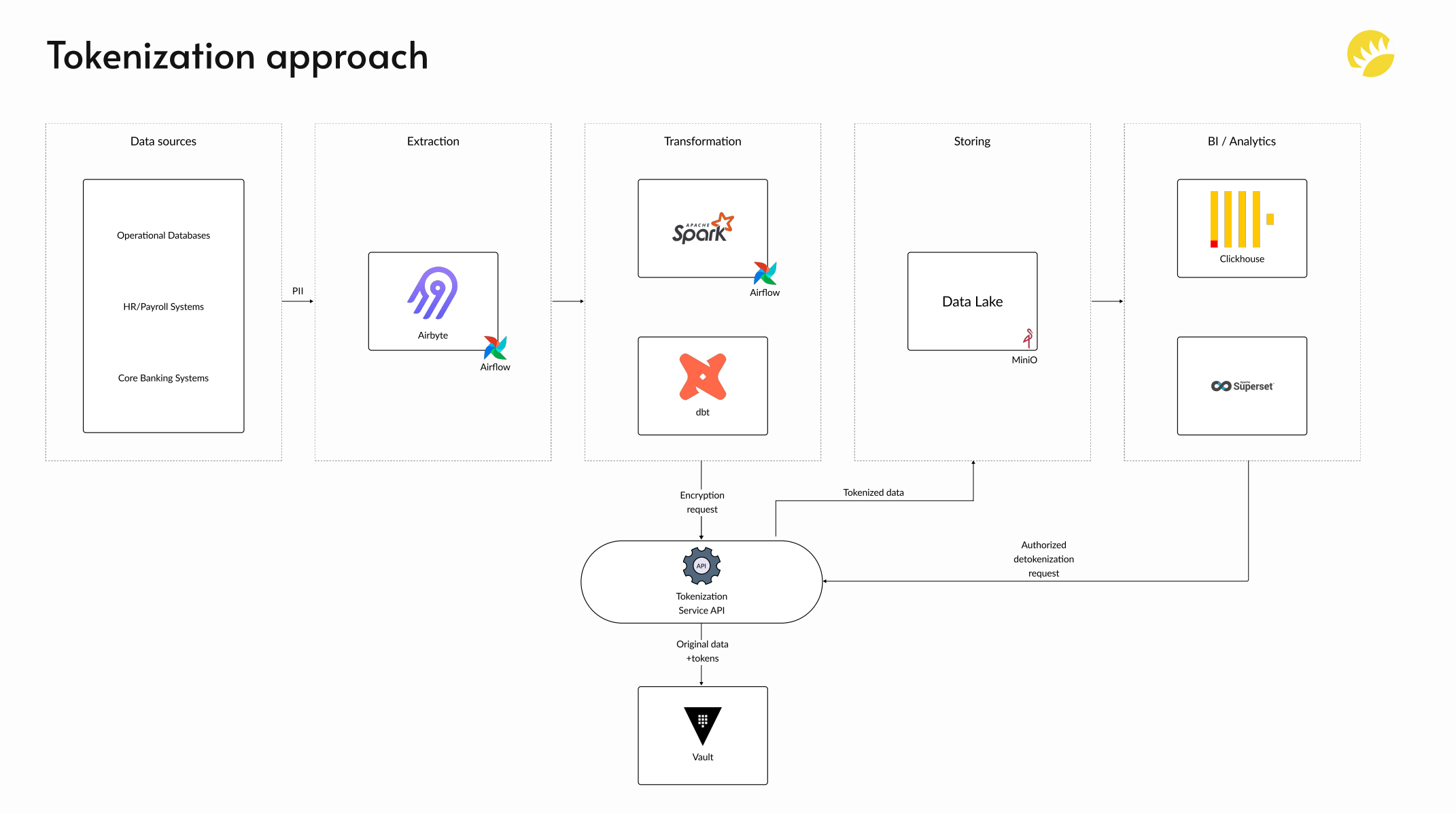
4. Warehouse Update

Update historical tables in Data Lake using ETL.

5. Validation

Run checks to ensure data integrity and correctness post tokenization.

Tokenization approach



Solution architecture (encryption)

Encryption integration

Sensitive employee data from operational databases, HR/Payroll, and core banking platforms is extracted via Airbyte and orchestrated by Airflow. During transformation, Spark and dbt send data to an Encryption Service API that performs encryption and manages keys via a dedicated Key Management System.

Encrypted data is stored in a Data Lake (MinIO). For analytics and BI, tools like ClickHouse and Superset access encrypted data and submit authorized decryption requests to the Encryption Service API as needed.

Integration into Data Entry / Onboarding Flow

1. Data Interception

When entering data in the HRIS or operational system, sensitive fields are intercepted in the extraction layer (Airbyte + Airflow) and routed to the transformation stage.

2. Data Encryption

During transformation (Spark/dbt), values are encrypted via the Encryption Service API. The encrypted results are then saved to storage or the original system.

3. Flow Update

Original flow: Enter data → Save to DB. With integration: Enter data → API encrypts values → Save encrypted values to DB. Symmetric encryption (e.g., AES) is recommended for performance.

Integration into Storage and Update Management

1. Encryption at Rest

Data is encrypted before storage in the Data Lake (MinIO) using the Encryption Service API, or using native field-level encryption features of the database.

2. Update Handling

For data changes, an authorized decryption request is made via the API, the record is updated, and re-encrypted.

3. Flow Update

Original: Update → Overwrite DB. Integrated flow: API decrypts → Update → API re-encrypts → Save.

Solution architecture (encryption)

Integration into Processing (e.g., Payroll)

1. Authorized Detokenization

- Payroll or processing modules retrieve encrypted data and request decryption from the API.

2. Secure Processing

- Processing is performed in memory, and the results are re-encrypted before storage.

3. Flow Update

- Original: Pull data → Process.
- Integrated: Pull encrypted values → API decrypts → Process → API re-encrypts and save.

Integration into Analytics and Reporting

1. Encrypted Analytics

- Encrypted values are sent to the data warehouse and BI tools (ClickHouse, Superset).

2. Homomorphic Encryption

- For certain use cases, homomorphic schemes can be used, enabling computation on encrypted data (such as salary analysis) without prior decryption. Only final aggregates may be decrypted if necessary.

3. Flow Update

- Original: Export data → Analyze.
- Integrated: Export encrypted data → Homomorphic Encryption computations (e.g., mean salary) → Analyze results. API decrypts aggregates on request.

Encrypting Existing Data in Source Systems and Data Warehouse

1. Export from Sources

Use ETL tools (Airbyte) or SQL queries to extract PII from operational databases and warehouses.

2. Encryption Processing

Feed batch data to the Encryption Service API for encryption.

3. Operational DB

Replace sensitive values in operational databases with encrypted strings via SQL UPDATE.

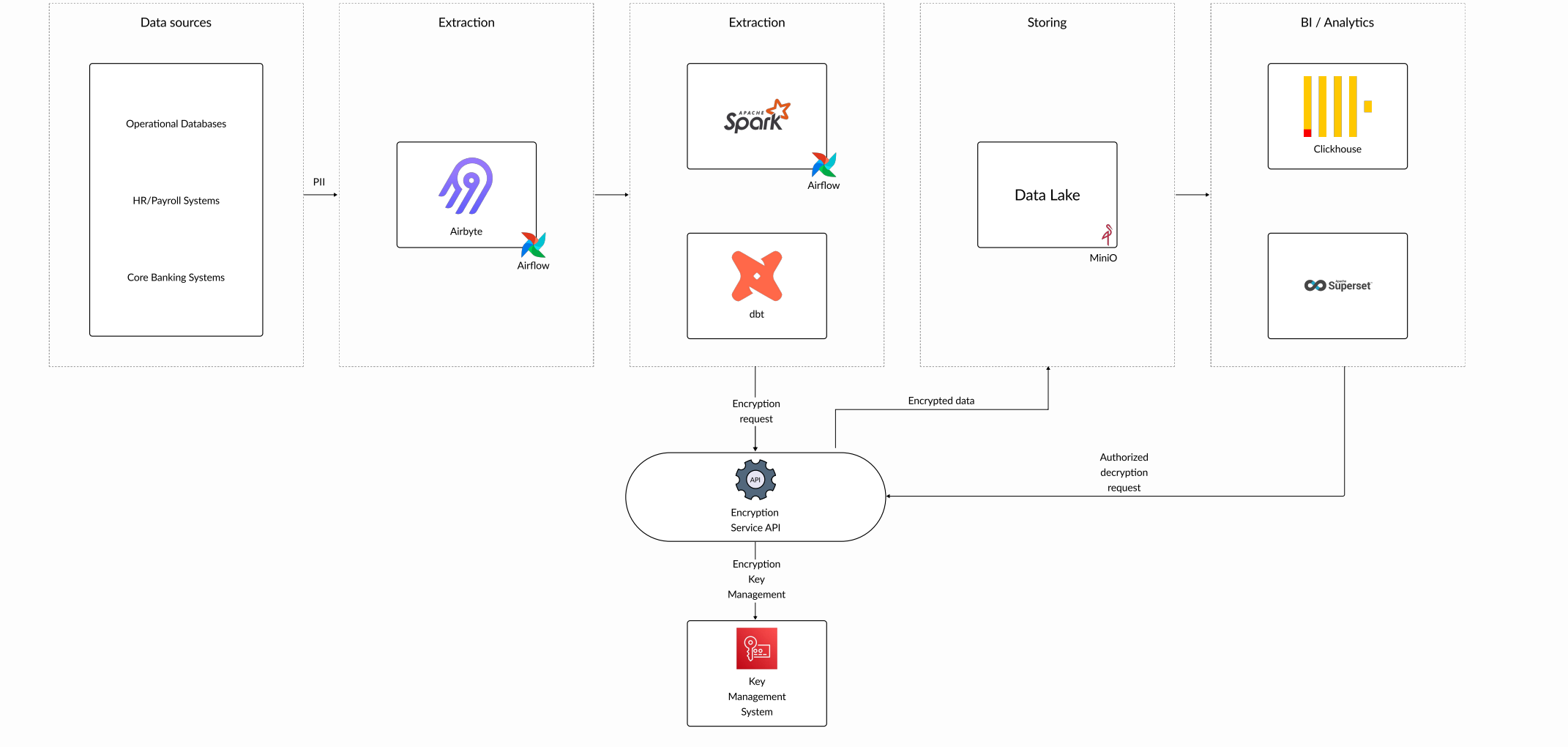
4. Data Warehouse

Update warehouse tables (e.g., Data Lake) via ETL.

5. Validation

Ensure data integrity and correctness post-migration.

Encryption approach



Customer Success Story I

Vaultless Tokenization Implementation

Duration
9 months

Resourses
8 specialists

Estimated budget alignment
~ USD 100K (Costs for tokenization is approximately $0.005 per token request)

Technologies
Vaultless Tokenization API, Cloud-native encryption services, HSM integration

Challenge

Our client, a leading European digital payments provider, sought to rapidly scale transaction throughput globally while maintaining PCI DSS compliance and minimizing infrastructure costs. The existing vault-based tokenization system caused latency and posed a bottleneck during peak loads. They needed a highly scalable, low-latency tokenization solution to support instant payments with real-time fraud monitoring without compromising security.

Executive Solution Overview

Andersen implemented a Vaultless Tokenization platform that generates cryptographic tokens dynamically within distributed cloud environments, eliminating the need for a centralized token vault. This reduced latency and infrastructure costs while enhancing system availability and fault tolerance. Coupled with hardware security modules (HSMs) and standard encryption, the solution ensured data protection and regulatory compliance. The vaultless approach enabled seamless integration with payment rails and fraud systems, accelerating innovation and customer satisfaction.

Customer Success Story I

Executive Solution Overview:

Vaultless tokenization was proposed in the case primarily because of its key advantages in speed, scalability, security, and reduced operational overhead. This logic includes:

- Faster Processing & Scalability: Vaultless tokenization generates tokens directly within the application or distributed servers, eliminating the need for communication with a central vault.
- Enhanced Security: Without a central token vault, the attack surface is significantly reduced.
- Lower Cost & Operational Complexity: Eliminating the need for expensive vault appliances massively cuts infrastructure and maintenance costs.
- Regulatory & Compliance Benefits: Vaultless solutions often reduce PCI DSS scope because raw data is never stored in a central vault or unprotected form.
- Resilience & Reliability: Distributed, vaultless systems provide higher availability and fault tolerance, as they do not rely on a central vault system that could become a bottleneck or single point of failure.

Key Architectural Decisions:

- Vaultless architecture optimizes for throughput and resilience, ideal for instant payment environments.
- Integration with HSM ensures key security without central token storage vulnerability.
- Microservices and event-driven design provide modular scalability and maintainability.

Architecture Solution Overview:

The core architecture features a distributed processing layer implementing stateless vaultless token generation algorithms leveraging AES-FF3-1 encryption and ephemeral keys controlled by HSMs. Tokens are produced on demand without persistent lookups, enabling linear scalability across multi-cloud data centers:

- Token Generation Service: Stateless microservices producing format-preserving tokens, integrated via secure API.
- Encryption Module: HSM-backed encryption of session keys and sensitive intermediate data.
- API Gateway: Secure entry point managing authentication, token lifecycle, and monitoring.
- Monitoring and Audit: Real-time fraud detection feeding back into token generation rules with comprehensive audit trails for compliance

Customer Success Story 2

Vault-Based Tokenization & Encryption Implementation

Duration
12 months

Resourses
10 specialists

Estimated budget alignment
~ USD 100K (Tokenization cost per transaction is up to $0.01)

Technologies
HashiCorp Vault, AES encryption, Kubernetes, REST APIs

Challenge

Our client, a North American engineering company in the oil and gas sector, required a reliable solution to protect confidential data throughout the complex project lifecycle. Strict industry regulations demanded strong control over sensitive engineering designs, procurement, contracts, and communications. Existing fragmented systems did not ensure consistent data protection, traceability, and auditability. The client needed a unified tokenization strategy integrated with encryption to safeguard data both at rest and in transit, complying with security and audit requirements.

Executive Solution Overview

Andersen implemented a comprehensive project lifecycle management framework based on tokenization using HashiCorp Vault. Tokenization replaced sensitive data with secure tokens, reducing exposure risks. HashiCorp Vault was chosen for its mature secret management capabilities, centralized storage, encryption, and strict policy-based access control.
This ensured uniform security policies, audit trails, and governance across CRM, ERP, and engineering tools, improving collaboration, reducing errors, and supporting regulatory traceability and digital twin handover.

Customer Success Story 2

Architecture Solution Overview

The architecture was designed with tokenization as a foundational mechanism embedded deeply in all data exchanges and storage points:

- Vault-Based Tokenization via HashiCorp Vault:
  Serves as the secure central token vault generating, storing, and mapping tokens to original data.
  Provides encryption at rest and in transit, secured with hardware security modules (HSM), ensuring no cleartext sensitive data is persisted or transmitted outside controlled environments.
- Service-Based Architecture (SBA):
  Facilitates modular integration of tokenization capabilities into engineering workflows, procurement, and supplier portals, enabling auditable and scalable data protection.
- Event-Driven Communication:
  Ensures real-time updates and synchronization of tokenized data, aligning with operational needs like forecasting and scheduling.
- Role-Based Access Control (RBAC) and Audit Logging:
  Protect tokens and secrets with fine-grained access policies, comprehensive audit logs for regulatory compliance, and operational security.

Vault-based tokenization was chosen because the client's environment required centralized, strict governance over token access and lifecycle, corresponding to high regulatory standards in Oil & Gas.

HashiCorp Vault was selected for its:
— proven enterprise-grade security features;
— dynamic secret management;
— seamless integration capabilities with APIs and cloud infrastructure;
— ability to enforce fine access controls and auditability.

This combination allowed the client:
— to meet compliance requirements;
— protect intellectual property;
— maintain operational efficiency with a centralized, secure tokenization backbone.

Customer Success Story 3

Tokenization as Proxy for SaaS Data Exchange in Restricted Cloud Environments

Duration
10 months

Resourses
7 specialists

Estimated budget alignment
~ USD 120K

Technologies
Tokenization Proxy, API Gateway, On-prem Data Vault, Secure Data Exchange Protocols

Challenge

Our client, a major banking institution in Central Asia, faced significant regulatory and operational challenges due to restrictions on the use of major public cloud providers (such as AWS, Azure, GCP, Oracle) and widely adopted SaaS platforms like Salesforce and Microsoft Dynamics in their country. Local regulations prohibit sensitive customer and employee data from leaving national borders or being processed on unauthorized cloud infrastructure.
The client needed to leverage modern SaaS solutions for CRM, analytics, and customer engagement without violating strict data residency and PII protection laws.

Executive Solution Overview

Andersen implemented an advanced real-time tokenization proxy system situated between the client bank's internal systems and external SaaS services. This proxy intercepts every API call and data transfer, replacing sensitive data elements with tokens before information crosses the organizational boundary and leaves the local environment. This design ensures strict adherence to local data residency and PII protection regulations, preventing unmasked sensitive data escape.

Customer Success Story 3

Architecture Solution Overview

- Tokenization Proxy Layer: Real-time interception and tokenization of inbound and outbound SaaS data.
- On-Premises Vault (HashiCorp Vault): Highly secured token and key vault ensuring encrypted storage, access control, and compliance auditing.
- API Gateway & Security: Handles secure token exchange, authentication, encryption, and rate-limiting with logging.
- Compliance Dashboard: Aggregates tokenization events and access audit trails for regulatory review.
- Data Exchange Manager: Adapts token formats and protocols specific to SaaS provider API requirements.

Technically, the solution's backbone is a highly secure, on-premises vault implemented using HashiCorp Vault.

This vault serves as the centralized token store and key manager, providing both token-to-data mapping and encryption key lifecycle management. HashiCorp Vault's strengths in secret management, policy-driven access control, dynamic secrets, and HSM integration made it the ideal choice.

It guarantees tokens and cryptographic keys are protected with strong encryption both at rest and in transit, while flexible API support allows seamless integration with tokenization proxy, API gateway, compliance dashboard, and SaaS vendor APIs.

Key Architectural Decisions

- Adoption of a centralized centralized, hardened HashiCorp Vault key and token store to adhere to local data protection mandates while enabling SaaS integration.
- Strict role-based policies and hardware security module (HSM) backed encryption ensure key security during lifecycle.
- Real-time tokenization proxy architecture balances privacy, security, and SaaS functionality without exposing PII outside controlled boundaries.

The use of HashiCorp Vault allowed the client to maintain full control over sensitive data lifecycle and access policies within their sovereign infrastructure, reducing cloud SaaS risks and compliance burdens.

The vault's audit logging capabilities support stringent regulatory reporting and incident analysis. Meanwhile, the secure API gateway orchestrates tokenization and validation workflows with scale, reliability, and real-time performance.

Thank you!

Let's build seamless solutions together!