CAIBE

A Cryptographically Verifiable Identity, Encryption, and Trust Platform

Version 1.0

12/18/2025

Executive Summary

Modern enterprises depend on Identity and Access Management (IAM) systems to secure workforce and customer access. However, traditional IAM platforms rely on centralized trust, password-based authentication, and vendor-controlled cryptographic keys—creating systemic security, privacy, and resilience risks.

CAIBE (Certificate Authority + Identity-Based Encryption) introduces a fundamentally different approach. Built on decentralized identity, passwordless authentication, Identity-Based Encryption (IBE), and an internally governed Certificate Authority (CA), CAIBE delivers cryptographically verifiable, zero-trust identity assurance without vendor lock-in. The platform supports both CIAM and Workforce IAM use cases, integrates seamlessly with legacy enterprise systems through a SAML Bridge, and provides mathematically enforceable security guarantees anchored on-chain.

CAIBE replaces implicit trust with provable trust, shifting identity security from policy promises to cryptographic facts.

---

1. The Problem with Traditional IAM

Enterprise IAM platforms such as Okta and Ping were designed for perimeter-based security models that no longer reflect modern distributed systems.

Key Limitations

- **Passwords and shared secrets** remain primary authentication factors, enabling phishing and credential theft
- **Centralized trust architectures** create single points of failure and systemic breach risk
- **Vendor-managed cryptographic keys** limit transparency and control
- **Off-chain operations** prevent independent cryptographic verification
- **Vendor lock-in** restricts portability and long-term resilience
- **Complex federation** increases operational overhead and misconfiguration risk
- **Privacy exposure** through centralized identity data stores

These constraints make traditional IAM costly, brittle, and increasingly incompatible with zero-trust and privacy-first security requirements.

---

2. CAIBE Overview

CAIBE is a hybrid identity platform combining: - Internet Identity passwordless authentication - Identity-Based Encryption with session-level key rotation - An internally governed Certificate Authority - Cryptographically enforced zero-trust policies -

On-chain auditability and verification - SAML-based federation for legacy and partner systems

The platform serves both **Customer IAM (CIAM)** and **Workforce IAM**, while enabling secure partner federation and third-party SSO.

Two role-isolated portals provide secure separation of duties: - **Admin Portal** for governance, CA administration, federation, and policy management - **User Portal** for personal identity, session, and encryption key visibility

Compliance Overview

CAIBE can significantly improve compliance posture rather than complicate it. Because all identity operations are cryptographically verifiable and recorded on-chain, CAIBE naturally provides auditable identity events that satisfy GDPR, SOC 2, and ISO 27001 logging requirements. The zero-trust, passwordless Internet Identity authentication model also eliminates credential breach risks, aligning strongly with NIST 800-63 and FIDO2 standards.

Furthermore, the builtin internal Certificate Authority (CA) ensures certificate issuance and revocation policies are enforceable within corporate PKI frameworks. Overall, CAIBE simplifies compliance by replacing opaque, centralized controls with transparent, verifiable cryptographic identity assurance.

---

3. Architectural Differentiation

3.1 Passwordless, Decentralized Authentication

CAIBE integrates Internet Identity to eliminate passwords entirely. Authentication relies on WebAuthn, biometrics, and hardware-backed cryptographic credentials.

Benefits: - No credential databases - No phishing vectors - No password reuse risk - Strong cryptographic identity binding

---

3.2 Identity-Based Encryption (IBE)

CAIBE embeds IBE as a first-class security primitive.

Key properties: - Automatic key rotation on every session start - Session-synchronized encryption material (8-hour lifespan) - Client-side private key ownership - No server-side private key storage

Encryption is bound directly to identity, ensuring end-to-end confidentiality enforced at the protocol level.

3.3 Internal Certificate Authority with CA–IBE Trust

CAIBE includes a fully internal Certificate Authority that bridges traditional PKI trust models with modern IBE encryption.

The CA: - Issues and manages certificates for users and services - Signs SAML assertions for federation - Certifies public IBE identities **without ever accessing private keys**

This CA–IBE trust relationship allows enterprises to retain PKI assurance while benefiting from modern, privacy-preserving encryption.

3.4 Zero-Trust by Construction

CAIBE enforces zero-trust principles cryptographically: - Continuous identity verification - Session-bound access decisions - Mandatory fresh encryption keys per session - Network boundary isolation between internal and external entities

Trust is never assumed; it is proven repeatedly through cryptographic validation.

3.5 On-Chain Verifiability

All identity operations are verifiable on the Internet Computer blockchain: - Immutable audit trails - Tamper-evident logs - Consensus-backed identity assertions

This enables independent verification for security audits, compliance, and forensic analysis.

---

4. Federation and Enterprise Integration

4.1 SAML Bridge

To ensure enterprise compatibility, CAIBE provides a SAML Bridge that enables: - Workforce SSO into existing SaaS platforms - Partner federation with external organizations - Role and attribute translation

Legacy systems gain cryptographic identity assurance without requiring redesign.

4.2 Partner Federation

CAIBE supports secure federation across organizational boundaries: - CA-signed SAML assertions - Strict internal/external network separation - Federated identity lifecycle management

Trust between partners is established cryptographically rather than contractually.

---

5. Governance, Administration, and Auditability

5.1 Administrative Controls

Administrators manage: - CA initialization and trust hierarchy - Certificate policies and lifecycles - CA–IBE trust parameters - SAML configurations - Zero-trust and session policies

Once configured, CAIBE automates certificate issuance, rotation, and enforcement.

5.2 Comprehensive Activity Logging

Every security-relevant action is logged: - Authentication and session events - IBE key rotations - Certificate operations - Role and policy changes - Federation activity

Logs are cryptographically verifiable and exportable for compliance and audit.

---

6. Security and Compliance Benefits

Organizations adopting CAIBE gain:

- **Stronger security** through passwordless, cryptographic identity
- **Privacy guarantees** through user-controlled encryption keys
- **Compliance readiness** via immutable audit trails
- **Operational resilience** through vendor independence
- **Reduced costs** by eliminating per-user IAM licensing

CAIBE replaces trust assumptions with mathematical proof.

---

7. Use Cases

- Enterprise Workforce IAM
- Customer Identity (CIAM)
- High-assurance partner federation

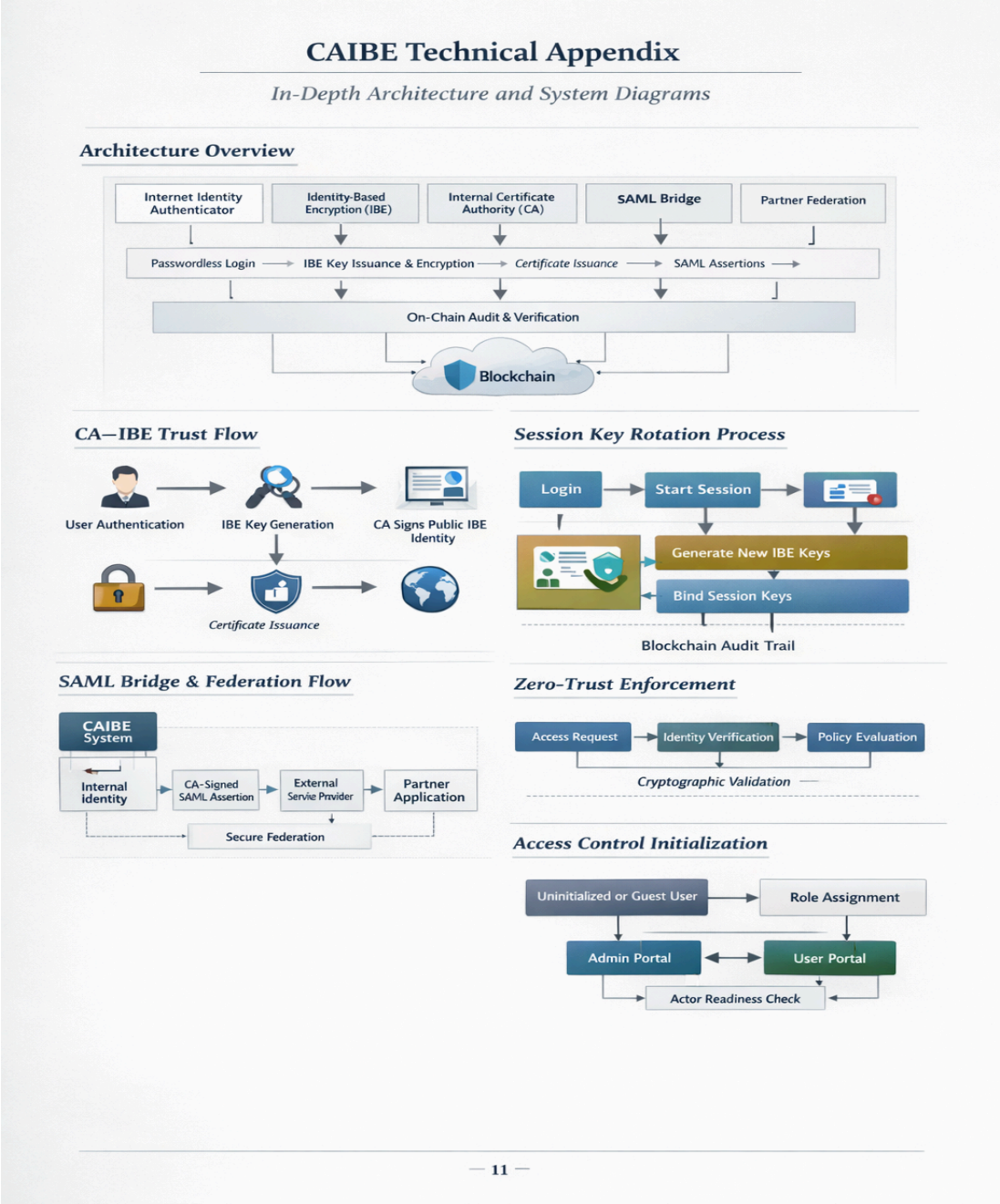
- Regulated industries requiring auditability
- Zero-trust modernization initiatives

---

8. Technical Appendix

8.1 Architecture Overview Diagram

Architecture Overview



8.2 CA–IBE Trust Flow

Refer to the diagram above: user authentication → IBE key generation → CA signs public IBE identity → certificate issuance → blockchain verification.

8.3 Session Key Rotation Process

Login → start session → generate fresh IBE keys → bind session keys → 8-hour expiry → reauthentication.

8.4 SAML Bridge & Federation Flow

Internal identity → CA-signed SAML assertion → external partner application → secure federation and role mapping.

8.5 Zero-Trust Enforcement

Access request → continuous identity verification → policy evaluation → cryptographic validation → network boundary enforcement.

8.6 Access Control Initialization

Uninitialized/guest user → role assignment → admin/user portal redirection → actor readiness check.

8.7 Backend Storage & Logging Architecture

Tracks user identity, role storage, certificate & IBE metadata, session lifecycle, rotation logs, and audit trails integrated on-chain.

---

9. Conclusion

CAIBE represents a next-generation identity platform designed for a decentralized, zero-trust world. By combining passwordless authentication, Identity-Based Encryption, internal PKI governance, and on-chain verifiability, CAIBE delivers identity assurance that is provable, private, and future-proof.

As identity becomes the new perimeter, CAIBE ensures that perimeter is cryptographically sound.

CAIBE — Verifiable Trust for the Modern Enterprise