Aretiico CA in a Box

Enabling Sovereign Operation of Certificate Authorities

Overview

Aretiico CA in a Box is a sovereign, comprehensive turnkey Certificate Authority (CA) solution designed to enable organisations to establish, manage, and operate their own Public Key Infrastructure (PKI). Delivered as a fully integrated platform, it provides the core components, policy frameworks, and operational controls required to implement and govern PKI services without reliance on third-party certificate issuance.

The platform supports both public and private certificate issuance across a wide range of use cases, including TLS certificates. It is designed with cryptographic agility at its core, supporting the phased adoption of post-quantum cryptography as standards evolve, while maintaining interoperability and operational continuity.

Key Features of Aretiico CA in a Box

Turnkey Solution

Pre-configured Setup

Comes with pre-configured settings and components, significantly reducing the complexity of initial setup.

Accreditation Framework

Provides a structured technical and operational foundation capable of supporting future accreditation paths, subject to appropriate governance and audit.

Crypto-Agile Certificate Profiles

Policy-driven support for classical, hybrid, and post-quantum certificates, enabling controlled algorithm transition without infrastructure replacement.

Ease of Deployment

Offers a straightforward installation process, allowing for quick deployment of a secure and sovereign CA.

Core Platform Components

- **CA Software:**
  Includes next-generation PKI software to issue and manage digital certificates.
- **Role-Based Management Portals:**
  Secure portals for subscribers and operators to request, approve, and manage certificates.
- **Logging and Auditability:**
  Ensure comprehensive logging and audit trails for regulatory compliance and security monitoring.
- **DevOps Integration:**
  Seamlessly integrate with DevOps practices for continuous delivery and deployment.
- **Hardware Security Module (HSM) Support:**
  Secure key generation, storage, and cryptographic operations backed by industry-standard Hardware Security Modules.
- **Authentication Workflows:**
  Streamline authentication processes for enhanced security and user experience.
- **Security Architecture:**
  Layered security controls designed to protect key material, certificate data, and operational processes.
- **Infrastructure as Code:**
  Implement and manage infrastructure using “as code”, ensuring consistency and scalability across environments.

Security and Compliance

- **Cryptographic Agility and Assurance**
  Supports policy-driven algorithm selection, hybrid cryptography, and controlled cryptographic rollover in line with recognised standards and guidance.
- **Regulatory Compliance:**
  Helps organisations and public-sector operators meet regulatory and industry standards for PKI and digital certificates, such as GDPR, HIPAA, and PCI DSS.

Scalability

- **Flexible Architecture:**
  Designed to scale with organisational growth and expanding service requirements.
- **Hybrid Deployment Options:**
  Blends both on-premise and cloud-based deployment options to fit various infrastructure needs.

Automation and Integration

- **Automated Processes:**
  Automates routine tasks such as certificate issuance, renewal, and revocation, reducing administrative overhead.
- **API Integration:**
  Provides APIs for seamless integration with existing IT systems and workflows, enhancing operational efficiency.

Support and Maintenance

- **Vendor Support:**
  Includes expert support services from Aretiico to assist with deployment, maintenance, and troubleshooting, ensuring smooth operation.
- **Regular Updates:**
  Ensures that the CA system is kept up to date with the latest security patches and features, maintaining robust security over time.

Technology, Policy, and Legal Frameworks

- **Advanced Technology:**
  Built on established PKI standards and enterprise-grade technologies.
- **Legal Compliance:**
  Designed to comply with various international legal frameworks and standards, ensuring the solution meets legal requirements for digital certification.
- **Policy Framework:**
  Comprehensive policy management to enforce security and operational policies within the PKI environment.

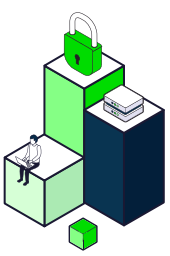
Why Organisations Choose to Operate Their Own Certificate Authority

01 Sovereignty and Control

Digital Independence: Establishing an internally governed CA enables organisations to control their digital trust infrastructure and reduce reliance on externally operated trust services.
Policy Enforcement: Organisations can define and enforce their own certificate policies and security standards aligned to governance and risk requirements.

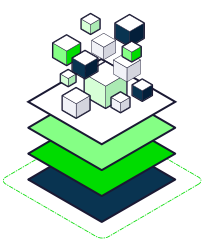
02 Enhanced Security and Trust

Secure Communications: Issuing both public and private certificates enables secure communication channels across systems, users, services, and devices.
Trusted Digital Identity: Certificates verify the identity of individuals, organisations, and devices, strengthening trust across digital interactions.



03 Operational and Strategic Control

Direct control over cryptographic policy, certificate lifecycle management, and trust decisions reduces dependency on third-party issuance and enhances resilience.



04 Regulatory and Standards Alignment

Standards Compliance: Supports alignment with applicable international standards and regulatory frameworks.
Governance Alignment: Enables adherence to organisational, contractual, and regulatory security obligations.

05 Operational Efficiency and Scalability

Automated Management: Streamlined certificate lifecycle processes reduce administrative overhead and operational risk.
Scalability: Designed to scale in line with organisational growth and evolving service requirements.

Use Cases for Aretiico CA in a Box

International Compliance

International Trust Frameworks: Supports alignment with recognised international trust frameworks and sector-specific standards, including aviation (e.g., ICAO), payments (e.g., EMV), and web PKI ecosystems.

Cross-Border Trust Requirements:
Designed to support participation in international digital trust environments while maintaining governance control.

Digital Identification

Enterprise Identity Enablement:
Supports digital identity verification and credential issuance across organisational ecosystems.

User and Device Credentials: Manages digital credentials for users, devices, and services.

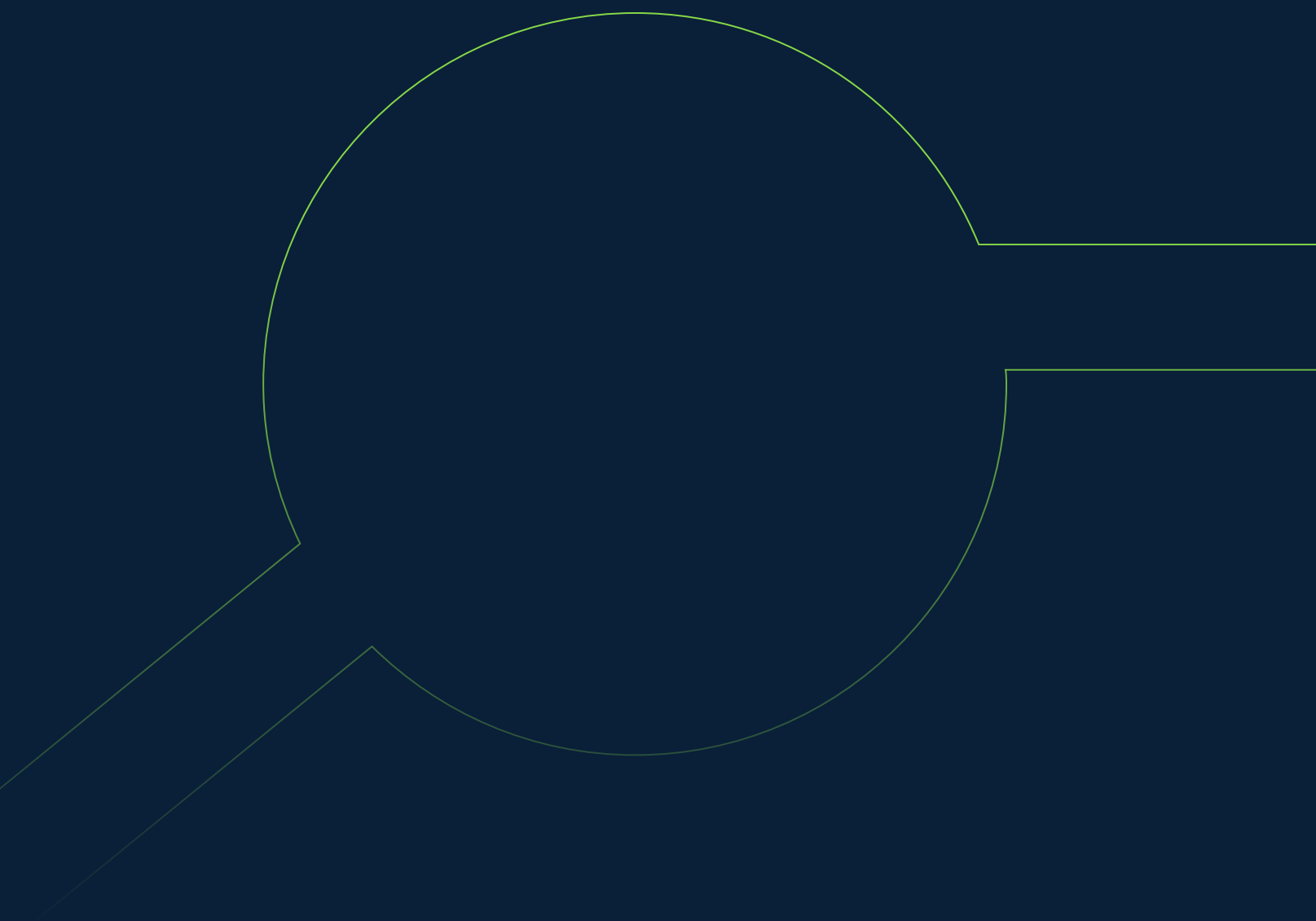
Trust Ecosystem Compatibility

Public Trust Alignment:
Capable of supporting public certificate issuance aligned with recognised trust frameworks (e.g., CA/Browser Forum Baseline Requirements, Adobe Approved Trust List), subject to applicable accreditation and acceptance.

Private Certificates:
Issues private certificates for internal use, ensuring secure communications and data integrity within the organisation.

International Standards Support:
Supports alignment with applicable international trust and payment standards (e.g., IATF, EMV) where required.

Aretiico CA in a Box is designed to support long-term cryptographic resilience, including the controlled adoption of post-quantum cryptography as standards and operational requirements evolve.



Discover more on our website **aretiico.com**