Keytos EZCA Services

Certification Practice Statement (CPS)

Version 2.0.0

February 02, 2023

Table of Contents

1 Introduction

1.1 Purpose

This Certification Practice Statement (CPS) is established by Keytos for our EZCA platform, a comprehensive solution for managing Certificate Authorities (CAs) on behalf of our customers. EZCA utilizes Azure Key Vault for our basic plan and Azure Managed Hardware Security Modules (HSMs) for our premium plans, offering scalable and secure management of digital certificates.

The purpose of this CPS is to define the practices and policies that govern the operation of CAs under the EZCA platform, ensuring the integrity, trustworthiness, and security of the digital certificates issued. This CPS aims to:

1.1.1 Facilitate Secure Certificate Management

Provide a robust and secure framework for the issuance, management, and revocation of digital certificates, enhancing the security of digital transactions and communications for our customers.

1.1.2 Outline Operational Procedures

Detail the operational procedures of EZCA, encompassing the lifecycle of digital certificates from issuance to revocation, and the use of Azure cloud infrastructure in these processes.

1.1.3 Ensure Compliance and Reliability

Ensure adherence to industry standards and regulatory requirements, fostering trust and reliability in the digital certificates managed by EZCA.

1.1.4 Explain the Leverage Azure Cloud Technologies

Highlight the use of Azure Key Vault and Azure Managed HSMs in our services, providing advanced security features, scalability, and reliability for key management and cryptographic operations.

1.1.5 Clarify Roles and Responsibilities

Define the roles and responsibilities of Keytos, our customers, and other stakeholders in the management and use of CAs and digital certificates. Although Keytos manages the underlying infrastructure and technology, customers retain control over the creation and access management of their CAs.

1.1.6 Promote Transparency and Trust

Offer transparency in our practices to customers and relying parties, ensuring a clear understanding of the security measures, operational procedures, and policies in place.

1.1.7 Support Diverse Digital Security Needs

Cater to a wide array of digital security requirements across different industries by offering tailored solutions through EZCA, ranging from basic to premium plans, depending on the security and operational needs of our customers.

This CPS represents a commitment by Keytos to uphold the highest standards of security and reliability in managing CAs through the EZCA platform. It is subject to regular review and updates to align with evolving technology, security challenges, and legal requirements.

1.2 Overview

This document serves as the Certification Practice Statement (CPS) for Keytos's EZCA solution. It defines the procedural and operational requirements governing the lifecycle management of Certificate Authorities (CAs) under the EZCA solution, catering to affiliated entities, Applicants, Subscribers, and Relying Parties. Keytos mandates adherence to this CPS for all entities involved in issuing and managing digital certificates within the EZCA solution's Public Key Infrastructure (PKI) hierarchy. This adherence extends to all services managed directly by Keytos.

Each PKI service under the EZCA umbrella is required to operate in accordance with an associated CPS, which, in turn, aligns with the overarching Certificate Policy (CP). Integral to this CPS are companion documents, including the CP and the Subscriber and Relying Party Agreements. Keytos reserves the right to publish additional Certificate Policies or Certification Practice Statements as necessary to delineate the guidelines for other product or service offerings.

This CPS is crafted in compliance with the Internet Engineering Task Force (IETF) RFC 3647 standards, which provide guidelines for the creation of Certificate Policy (CP) and Certification Practices Statement (CPS) documents. Furthermore, this CPS adheres to the current Baseline Requirements for the Issuance and Management of Certificates (“Baseline Requirements”).

In instances of any inconsistency between this CPS and the prevailing industry requirements or standards, the latter shall take precedence. This ensures that Keytos' EZCA solution remains aligned with the most current and rigorous standards in digital certificate management and security.

2. General Provisions

2.1 Obligations

2.1.1 CA Obligations

Keytos, as the provider of the EZCA solution, assumes the responsibility for the secure and reliable operation of the infrastructure for the Certificate Authorities under its management. This includes adhering to the practices outlined in this CPS, ensuring the accuracy and integrity of all issued certificates, and maintaining the confidentiality and security of the cryptographic keys.

2.1.2 RA Obligations

Registration Authorities (RAs), when applicable, are responsible for verifying the identity and legitimacy of applicants for digital certificates. They must comply with the identification and authentication procedures as specified in this CPS.

2.1.3 Subscriber Obligations

Subscribers are entities that have been issued a certificate by the EZCA-managed CA. They are responsible for safeguarding their private keys, using their certificates within the defined scope, and promptly notifying their CA owner of any changes that might affect the validity of their certificates.

2.1.4 Relying Party Obligations

Relying parties are those who trust and use the certificates issued by the EZCA-managed CA. They must verify the status of a certificate before relying on it and use it in accordance with the terms stated in the relying party agreement.

2.2 Liability

2.2.1 Platform Liability

Keytos assumes responsibility for safeguarding the Azure resources that host the EZCA platform, except in cases where the customer agreement specifies alternative arrangements, such as 'bring your own HSM' (Hardware Security Module) or 'bring your own infrastructure' plans. In these instances, the liability for protecting the infrastructure shifts in accordance with the terms outlined in the respective customer agreements.

2.2.2 CA Liability

PKI (Public Key Infrastructure) Administrators, who manage and operate their own Certificate Authorities within the EZCA platform, bear the responsibility for their secure management and operation. It is incumbent upon them to promptly inform Keytos of any security breaches or incidents within their infrastructure that could potentially impact the integrity or security of the EZCA platform

2.2.3 Subscriber and Relying Party Liability

Subscribers, who are entities issued certificates by the EZCA-managed CAs, and Relying Parties, who trust and utilize these certificates, are both responsible for adhering to best practices in the protection and use of their cryptographic keys. This includes the careful verification of certificate-based authentication and the obligation to immediately notify their PKI Administrators of any suspected or actual compromise of their certificates.

2.3 Privacy and Confidentiality

2.3.1 Privacy Policy

EZCA, as a solution provided by Keytos, adheres to the privacy policy outlined at https://www.keytos.io/legal/privacypolicy. This policy reflects our commitment to protect the personal and sensitive information of our customers and users. Our practices are designed to uphold the highest standards of privacy and data protection, in alignment with our SOC2 compliance framework.

2.3.2 Confidentiality

Keytos is dedicated to maintaining the confidentiality of customer information. In line with industry best practices, we implement robust data classification protocols, encryption of data at rest, and encryption of data in transit. These measures are part of our commitment to safeguarding customer information and are continuously reviewed and enhanced to align with evolving industry standards and our SOC2 compliance.

2.3.3 Information Disclosure

Keytos discloses customer information only when legally mandated. Such disclosure is conducted in strict compliance with legal procedures and is limited to the extent required by law. We are committed to transparency and will inform affected customers of any legal requests for their data, subject to legal restrictions.

2.4 Compliance with Applicable Law

Keytos, in its operation of the EZCA solution, is fully committed to complying with all applicable laws and regulations in the jurisdictions where it operates. This commitment encompasses adherence to data protection laws, electronic transaction regulations, and other relevant legal and regulatory requirements. Our compliance is further reinforced by our SOC2 certification, which demonstrates our adherence to high standards of security, confidentiality, and privacy. We continuously monitor legal developments to ensure our services remain in compliance with these requirements, thereby safeguarding our customers and their data.

2.5 Policy Administration

2.5.1 CPS Administration

The administration of this Certification Practice Statement (CPS) is a responsibility that Keytos takes seriously. We ensure that the CPS is regularly reviewed and updated to reflect the evolving landscape of digital security, legal requirements, and operational best practices. The process for updating this CPS includes a thorough review by our legal and security teams, ensuring alignment with industry standards and regulatory compliance. Version control measures are in place to maintain a clear record of amendments. Keytos commits to transparent communication with all stakeholders regarding any significant changes to this CPS. Stakeholders will be notified of updates through official communications from Keytos, and the latest version of the CPS will always be accessible on our website.

2.5.2 Contact Information

For any inquiries, concerns, or complaints related to this CPS or the operation of the EZCA solution, stakeholders are encouraged to reach out to us via email at security@keytos.io. This dedicated channel is monitored by our security team, ensuring timely and appropriate responses to all queries. We welcome feedback and are committed to addressing any concerns promptly and effectively.

3. Identification and Authentication

3.1 Naming

3.1.1 Certificate Naming Policy

Certificates issued by the EZCA platform are named in accordance with the information provided by the customer or identity information provided by the customer's Azure Active Directory (AD) associated with their Microsoft tenant. This ensures that each certificate can be uniquely linked to the identity of the entity it represents within the customer's organization.

3.1.2 Unique Identifiers

Each certificate includes unique identifiers, such as a serial number, which are generated by the EZCA platform to ensure distinctiveness and traceability.

3.2 Initial Identity Validation

3.2.1 Azure AD Authentication

For identity validation, EZCA leverages the customer's Azure AD identity. This method relies on the security and authentication mechanisms of Azure AD, assuming that the identity information provided through this service is accurate and validated by the customer's own IT infrastructure.

3.2.2 SCEP Certificate Issuance

When utilizing Simple Certificate Enrollment Protocol (SCEP), EZCA assumes validity based on the presence of the correct SCEP secret. This method presumes that the entity requesting the certificate is authorized to do so, provided they possess the correct SCEP secret.

3.2.3 ACME Protocol

For domain validation, EZCA supports the Automated Certificate Management Environment (ACME) protocol through a customer-managed agent. This agent is responsible for validating domain ownership within the customer's network. EZCA will issue certificates based on requests from this agent, under the assumption that the agent's domain validation is accurate.

3.3 Identity Proofing

3.3.1 Responsibility of Identity Proofing

The responsibility for identity proofing lies with the customer. Customers must ensure that the identity data provided via Azure AD, SCEP, or the ACME agent is accurate and represents valid entities within their organization or domain.

3.3.2 Security of the Customer-Managed Agent

Customers utilizing the ACME protocol are responsible for the security and integrity of their domain validation agent. EZCA will issue certificates based on the requests from this agent; therefore, it is imperative that customers maintain strict security controls over the agent to prevent unauthorized certificate issuance.

3.3.3 Verification Process

The EZCA platform does not independently verify the identity of entities. Instead, it relies on the customer's internal processes and the security measures in place within Azure AD, the SCEP protocol, and the ACME agent to ensure that only valid and authorized entities are issued certificates.

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Self-Service in Portal

PKI administrators set up self-service options in the EZCA portal. This allows users to apply for certificates based on domain ownership. Domains are allocated on a first-come, first-serve basis, though administrators can establish approval processes or restrict domain ownership to specific user groups.

4.1.2 API and Portal Requests

Applications for certificates can also be made through an API or directly in the portal. Users are responsible for providing the Certificate Signing Request (CSR).

4.1.3 Azure Key Vault Integration

For enhanced security, EZCA offers integration with Azure Key Vault, where the CSR is created, and the certificate installed directly in the Key Vault. This option includes automatic renewal of certificates.

4.1.4 SCEP and ACME Protocol Applications

SCEP applications rely on the correct SCEP secret for validation, while ACME protocol applications are processed through a customer-managed agent validating domain ownership.

4.2 Certificate Issuance

4.2.1 Validation Checks

Prior to issuance, EZCA performs validation checks based on the method of application. For portal and API requests, the provided CSR is verified. In the case of Azure Key Vault integrations, EZCA ensures secure communication with the client's Key Vault.

4.2.2 Issuance via SCEP and ACME

Certificates requested via SCEP and ACME protocols undergo validation based on the SCEP secret and domain ownership verification, respectively.

4.3 Certificate Acceptance

4.3.1 Acceptance Process

Upon issuance, the subscriber is notified, and the certificate must be accepted as per the instructions provided in the portal or via email. For Azure Key Vault integration, the certificate is automatically deployed and acceptance is implicit.

4.4 Key Pair and Certificate Usage

4.4.1 Responsibility of Users

Users are responsible for the secure usage of key pairs and certificates. This includes safeguarding private keys and using certificates within their intended scope.

4.4.2 Guidelines

EZCA provides guidelines on best practices for key pair management and certificate usage, available through the portal.

4.5 Certificate Renewal, Suspension, and Revocation

4.5.1 Renewal

Certificates can be renewed manually through the portal or API, or automatically when integrated with Azure Key Vault, SCEP, or ACME.

4.5.2 Suspension and Revocation

PKI administrators and domain owners can revoke certificates through the EZCA portal. The revocation status is then propagated to the Certificate Revocation List (CRL) and/or made available via EZCA's managed Online Certificate Status Protocol (OCSP) service.

4.5.3 Settings and Notifications

Administrators have the option to configure settings in response to certain events.

4.6 Certificate Status Services

4.6.1 OCSP

EZCA provides an OCSP service for checking the real-time status of certificates.

4.6.2 CRL Distribution

CRLs are updated regularly with revoked certificate information and are made publicly accessible. The location of the CRL distribution point is specified within each certificate. CRL uptime is closely monitored by a health checker that runs every 5 minutes and automatically fixes any CRL with detected issues.

5. Facility, Management, and Operational Controls

5.1 Physical Security Controls

5.1.1 Azure Datacenter Security

Keytos hosts all servers within Azure datacenters, which employ rigorous physical security measures. These measures include multi-factor authentication for datacenter access, continuous surveillance, and a secured perimeter. Azure datacenters are designed to withstand various physical threats and natural disasters, ensuring the continuous operation and security of the infrastructure hosting Keytos services.

5.2 Operational Security Controls

5.2.1 Security Best Practices

Keytos adheres to stringent operational security practices, encompassing regular security assessments, system monitoring, and comprehensive network security protocols.

5.2.2 Personnel Security

Our staff with access to sensitive systems undergo thorough security screenings and are provided with continuous security training to uphold the integrity and security of our operations.

5.3 Azure Managed HSM Usage

5.3.1 Key Ceremony Protocol

Keytos conducts a key ceremony for Azure Managed HSMs that adheres to strict security protocols. This ceremony involves multiple layers of security, including the generation of cryptographic keys in a controlled environment, secure handling and storage of key material, and maintaining a detailed chain of custody. The specific details of the ceremony are proprietary and are designed to ensure the highest levels of security and confidentiality.

5.3.2 FIPS 140-2 Level 3 Compliance

The Azure Managed HSMs used by Keytos are compliant with FIPS 140-2 Level 3 standards. This compliance indicates a high degree of security, including robust physical tamper-resistance features, identity-based authentication, and stringent cryptographic module specifications. The FIPS 140-2 Level 3 certification ensures that the HSMs provide a secure cryptographic environment for key management and operations.

5.3.3 Secure Key Management

The keys generated and managed within Azure Managed HSMs are protected by state-of-the-art security mechanisms, ensuring that cryptographic operations are performed within a highly secure and compliant framework. This approach is fundamental to maintaining the confidentiality, integrity, and availability of sensitive key material.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Automated Key Generation

Key pairs are automatically generated by the EZCA service through calls to Azure Managed HSM APIs. This process is entirely automated, with no human involvement from the Keytos team, ensuring a high level of security and consistency.

6.1.2 Secure Installation

Once generated, key pairs are securely installed in their respective environments, adhering to strict protocols to maintain cryptographic integrity and confidentiality.

6.2 Key Management

6.2.1 Infrastructure Protection

Although key pair generation is automated, Keytos employs robust security measures to protect the infrastructure. This includes the use of isolated devices (PAWs), passwordless authentication systems isolated from the corporate tenant, and access control gated by Azure PIM.

6.2.2 Monitoring

The infrastructure is monitored by Azure Cloud Defender and Cloud Watcher, with the latter specifically designed to alert any changes in Azure RBAC, enhancing the security posture of the key management environment.

6.2.3 HSM Security

Keys are managed within Azure Managed HSMs, which comply with FIPS 140-2 Level 3 standards, ensuring strong protection against unauthorized access and tampering.

6.3 Public Key Infrastructure (PKI) Token

6.3.1 Token Usage

If PKI tokens are used, they comply with high-security standards for the storage and management of cryptographic keys and credentials, ensuring secure access and operational integrity.

6.4 CA and Subscriber Key Usage

6.4.1 CA Key Usage

CA keys, used for signing certificates and CRLs, are managed under stringent security protocols to uphold the integrity and trustworthiness of the CA function.

6.4.2 Subscriber Key Usage

Subscribers are responsible for the secure usage of their keys. Keytos provides guidelines on best practices to aid subscribers in the secure handling of their certificates.

6.5 End of Life Key Management

6.5.1 Automated Deletion Process

Customer keys are automatically deleted from the HSMs three months after the associated CA is decommissioned. This automated process ensures that no residual key material is retained beyond the necessary period.

6.5.2 Compliance and Audit

The key deletion process aligns with industry best practices and is subject to compliance auditing and thorough documentation, reflecting Keytos' commitment to security and transparency.

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profiles

7.1.1 Specification Overview

The certificates issued by Keytos' EZCA solution adhere to a detailed specification that ensures compatibility and security. This includes the use of industry-standard algorithms, key sizes, and formats.

7.1.2 Content and Extensions

Each certificate contains necessary information, such as the subscriber's name, public key, issuer details, validity period, and unique serial number. Extensions are used to specify certificate usage, constraints, and other critical attributes.

7.1.3 Algorithm Standards

The certificates comply with current cryptographic standards, including RSA and ECDSA algorithms, with key lengths that meet or exceed industry best practices.

7.1.4 Format and Encoding

Certificates are encoded in X.509 v3 format, ensuring interoperability across various systems and applications.

7.2 CRL Profiles

7.2.1 CRL Generation and Distribution

The Certificate Revocation List (CRL) is regularly generated and updated by Keytos' EZCA platform to include all revoked certificates. The CRL is distributed via publicly accessible repositories for relying parties to verify the revocation status of certificates.

7.2.2 CRL Fields

Each entry in the CRL includes the serial number of the revoked certificate and the revocation date. Additional details may be included as necessary, in line with industry standards.

7.2.3 Update Frequency

The CRL is updated at regular intervals (by default every 7 days, however this can be changed by the PKI administrator when creating the Certificate Authority), ensuring timely dissemination of revocation information.

7.3 OCSP Profiles

7.3.1 OCSP Functionality

Keytos' EZCA solution offers an Online Certificate Status Protocol (OCSP) service that allows for real-time verification of the revocation status of certificates.

7.3.2 Response Profiles

OCSP responses include the certificate's status (good, revoked, or unknown), the time of the status check, and the next update time. The response is digitally signed by a dedicated OCSP responder certificate for validation.

7.3.3 Security and Reliability

The OCSP service is designed to be highly available and secure, with measures in place to prevent unauthorized access and ensure the integrity of the responses.

8. Compliance Audit and Other Assessments

8.1 Frequency and Scope of Compliance Audits

8.1.1 Audit Schedule

Keytos undergoes regular compliance audits to ensure adherence to industry standards and regulatory requirements. These audits are scheduled annually, with additional interim reviews if significant changes occur in the operational environment or regulatory landscape.

8.2.1 Scope of Audits

The scope of the audits encompasses all aspects of Keytos infrastructure and business practices, including technical security controls, operational procedures, and adherence to industry standards. This comprehensive approach ensures that every facet of the service aligns with best practices and regulatory mandates.

8.2 Identity/Qualifications of Auditor

8.2.1 Auditing Firm

Keytos' compliance audits are conducted by Prescient Assurance, a reputable and independent auditing firm with extensive experience in assessing security and compliance in the cloud services domain.

8.2.2 Auditor Qualifications

Auditors from Prescient Assurance possess necessary certifications and qualifications, including expertise in information security, cloud services, and regulatory compliance. Their knowledge and experience ensure a thorough and reliable audit process.

8.3 Auditor's Relationship to Audited Party

8.3.1 Independence and Objectivity

Prescient Assurance is an independent entity with no affiliations or conflicts of interest with Keytos. This independence is critical to maintaining the objectivity and impartiality of the audit process.

8.3.2 Conflict of Interest Disclosure

Any potential conflicts of interest or relationships that might affect the impartiality of the audit are disclosed in accordance with industry best practices and ethical guidelines. Keytos is committed to transparency in its audit processes and ensures that the audit firm adheres to the highest standards of professional conduct.

9 Incident Response Procedures

9.1 Introduction

The Incident Response Procedures outlined in this section are designed to effectively manage and mitigate any security incidents affecting the Azure infrastructure hosting Keytos' EZCA platform. It is important to note that while Keytos is responsible for the security of the Azure infrastructure, customers are responsible for the security of their Certificate Authorities (CAs) and the security of their Azure AD accounts managing these CAs.

9.2 Detection

9.2.1 Keytos Responsibilities

Keytos will continuously monitor the Azure infrastructure for signs of security incidents, including unauthorized access, system breaches, and unusual activities.

9.2.2 Customer Responsibilities

Customers are responsible for monitoring their own CAs and Azure AD accounts. They should promptly report any suspicious activities or perceived security incidents to Keytos.

9.3 Reporting

9.3.1 Incident Reporting Protocol

Any detected security incidents, either by Keytos or the customer, should be immediately reported to the designated Keytos Incident Response Team via [specified email/communication channel].

9.3.2 Information to Include in Reports

Reports should include a description of the incident, the time it was discovered, the systems or services affected, and any other relevant information.

9.4 Response

9.4.1 Initial Assessment and Categorization

Upon receiving a report, the Keytos Incident Response Team will assess and categorize the incident based on its severity and potential impact.

9.4.2 Containment and Mitigation

Immediate steps will be taken to contain the incident and mitigate any potential damage. This may include temporary suspension of services, isolation of affected systems, and implementation of emergency patches or fixes.

9.5 Recovery

9.5.1 System Restoration

Once the incident is contained and mitigated, efforts will be made to restore any affected services to full functionality.

9.5.2 Customer Communication

Keytos will keep affected customers informed about the status of the incident response and recovery efforts.

9.6 Post-Incident Analysis

9.6.1 Investigation

A thorough investigation will be conducted to understand the cause of the incident, the extent of the impact, and the effectiveness of the response.

9.6.2 Lessons Learned

Findings from the investigation will be used to improve future incident response procedures and overall security posture.

9.7 Roles and Responsibilities

9.7.1 Keytos Incident Response Team

Responsible for overall management of security incidents related to the Azure infrastructure.

9.7.2 Customer

Responsible for managing security incidents within their own CAs and Azure AD accounts.

9.8 Communication Plan

9.8.1 Regular Updates

Keytos will provide regular updates to affected customers throughout the incident response process.

9.8.2 Post-Incident Report

A detailed report will be provided to customers after the resolution of the incident, including a summary of the incident, actions taken, and recommendations for future prevention.

10 Business Continuity and Disaster Recovery Plans

10.1 Introduction

Keytos is committed to ensuring high availability and resilience of the EZCA platform. Our business continuity and disaster recovery plans are designed to maintain operations and minimize service disruption in the event of a disaster or significant business disruption. This includes robust data backup, system redundancy, and efficient recovery procedures.

10.2 System Redundancy

10.2.1 Redundant Infrastructure

Depending on the service instance selected by the customer, Keytos provides redundant infrastructure across multiple regions. This multi-region deployment ensures that, in the event of a regional outage, there is a failover mechanism in place to maintain service continuity.

10.2.2 Load Balancing and Failover Procedures

We employ advanced load balancing and automatic failover procedures to distribute traffic evenly across our servers and to switch operations to backup systems seamlessly in case of a primary system failure.

10.3 Data Backup

10.3.1 Regular Data Backups

Keytos performs regular backups of all critical data, including certificate data, configuration settings, and system logs. These backups are stored in geographically dispersed locations to protect against regional disasters.

10.3.2 Backup Testing

Backup integrity is regularly tested to ensure that data can be effectively restored in the event of data loss.

10.4 Disaster Recovery

10.4.1 Disaster Recovery Plan

We have a comprehensive disaster recovery plan in place, which is reviewed and updated regularly. This plan includes detailed procedures for responding to various types of disasters, including natural disasters, cyber-attacks, and system failures.

10.4.2 Rapid Recovery Capabilities

Our infrastructure is designed to enable rapid recovery of services. In case of a disaster, we aim to restore critical operations within a minimal time frame, as defined in our service level agreements (SLAs) with customers.

10.5. High Availability

10.5.1 Availability Zones

Services are hosted in multiple availability zones within each region, further ensuring high availability and fault tolerance.

10.5.2 Monitoring and Alerts

Continuous monitoring of system performance and automated alerts help in early detection of potential issues, allowing for proactive management and prevention of service disruptions.

10.6. Communication Plan

10.6.1 Customer Communication

In the event of a disaster or significant disruption, we will promptly inform our customers about the status of their services and expected recovery times. Communication channels include email, service status pages, and direct customer support lines.

10.6.2 Regular Updates

Throughout the recovery process, we will provide regular updates to our customers until full-service functionality is restored.

11 Subcontractor and Third-Party Trustworthiness

11.1 Introduction

At Keytos, we prioritize the security and integrity of our EZCA platform. To maintain the highest levels of trust and reliability, we have a firm policy against outsourcing any critical aspects of our operations, particularly code writing and infrastructure management.

11.2 Code Development and Management

11.2.1 Internal Development Teams

All code writing for the EZCA platform is carried out by our in-house development teams. This approach ensures that only trusted, vetted, and skilled Keytos employees are involved in the development and maintenance of our software.

11.2.2 Quality Assurance and Security

Our internal development process includes stringent quality assurance and security testing. Regular code reviews, vulnerability assessments, and penetration testing are integral parts of our development lifecycle.

11.3 Infrastructure Management

11.3.1 Direct Control Over Infrastructure

We maintain direct control over all aspects of our infrastructure management. This hands-on approach allows us to enforce the highest security standards and respond promptly to any potential threats or vulnerabilities.

11.3.2 Continuous Monitoring and Improvement

Our internal teams are responsible for the continuous monitoring of our infrastructure. We regularly update our systems and incorporate the latest security best practices to ensure the ongoing protection and reliability of our services.

11.4 No Reliance on External Subcontractors

11.4.1 Policy Against Outsourcing

Consistent with our commitment to security and control, Keytos does not rely on external subcontractors for any critical operational tasks. This policy helps us maintain complete oversight and accountability over every aspect of our service.

11.4.2 Vendor Selection and Management

While we may utilize third-party vendors for non-critical services, our vendor selection process is rigorous, emphasizing security and trustworthiness. We conduct thorough assessments of all third-party vendors to ensure they meet our high standards for security and reliability.

12. Legal Matters

12.1 Governing Law

12.1.1 Jurisdiction

This Certification Practice Statement (CPS) and the operations of Keytos's EZCA solution are governed by the laws of the Commonwealth of Massachusetts, United States. As a Boston-based organization, Keytos operates under the legal framework and jurisdiction of Massachusetts, ensuring compliance with local, state, and federal laws.

12.1.2 Applicability

The governing law encompasses all legal aspects related to the issuance, management, and use of digital certificates provided by Keytos, including but not limited to, liability, privacy, and intellectual property rights.

12.2 Compliance with Applicable Law

12.2.1 Regulatory Compliance

Keytos is committed to full compliance with all applicable laws and regulations pertaining to its operations and services. This includes adherence to digital security standards, data protection laws, and electronic transaction regulations.

12.2.2 Regular Legal Review

Keytos undertakes regular reviews of its CPS and operational practices to ensure ongoing compliance with evolving legal and regulatory requirements, especially those specific to the operation of digital certificate authorities and cloud services.

12.3 Dispute Resolution Mechanisms

12.3.1 Initial Resolution Efforts

In the event of a dispute arising from the use of Keytos' EZCA solution or related to this CPS, parties are encouraged to seek an initial resolution through direct communication with Keytos. This approach aims to resolve disputes amicably and efficiently.

12.3.2 Formal Proceedings

If a dispute cannot be resolved through direct communication, formal proceedings will be governed by Massachusetts law. Disputes will be addressed through arbitration or legal proceedings, as deemed appropriate, in the competent courts of Massachusetts.

12.3.3 Contact Information for Disputes

Parties wishing to initiate a dispute resolution process can contact Keytos through the designated legal contact channels provided on Keytos' website or as stated in the relevant agreements.

13 Acronyms

Term	Definition
CA	Certificate Authority
CPS	Certification Practice Statement
CP	Certificate Policy
CRL	Certificate Revocation List
DNS	Domain Name Service
ACME	Automated Certificate Management Environment
HSM	Hardware Security Module
PKI	Publik Key Infrastructure
FIPS	(US Government) Federal Information Processing Standard.
API	Application Programing Interface
SCEP	Simple Certificate Enrollment Protocol
OCSP	Online Certificate Status Protocol

14 Revisions

Revision Date	Revision Explanation	Revision Number	Supersedes
11/03/2021	Established	1.0	NA
02/02/2023	Updated to support ACME and SCEP certificate issuance.	2.0	1.0