

Pikachu Digital Certificate Trust Network Certificate Policy

1. Introduction

This Pikachu Digital Certificate Trust Network Root CA Certificate Policy (referred to as the CPS hereafter) aims to govern the use and management of digital certificates issued by the Pikachu Certificate Trust System (referred to as the CA hereafter). This policy applies to all certificates issued by the Pikachu Certificate Trust System.

2. Definitions

2.1 Certification Authority (CA): Refers to the Pikachu Certificate Trust System responsible for issuing and managing digital certificates.

2.2 Certificate Holder: Refers to an individual, organization, or entity that obtains a digital certificate issued by the Pikachu Certificate Trust System.

2.3 Certificate Applicant: Refers to an individual, organization, or entity that submits a digital certificate application to the Pikachu Certificate Trust System.

3. Certificate Issuance

3.1 Certificate Application

3.1.1 Certificate applicants must provide accurate, complete, and truthful information.

3.1.2 Certificate applicants must provide identity verification information to validate their identity and qualifications.

3.1.3 Certificate applicants must adhere to the application process and requirements set by the Pikachu Certificate Trust System.

3.2 Certificate Verification

3.2.1 The Pikachu Certificate Trust System will verify the identity of the certificate applicant to ensure its legitimacy and authenticity.

3.2.2 The Pikachu Certificate Trust System will verify the qualifications of the certificate applicant to ensure they are authorized to obtain the requested certificate.

3.3 Certificate Issuance

3.3.1 Upon successful verification of identity and qualifications, the Pikachu Certificate Trust System will issue a digital certificate to the qualified certificate applicant.

3.3.2 The issued digital certificate will contain necessary certificate information, such as the certificate holder's name, certificate validity period, etc.

4.Certificate Usage

4.1 Certificate holders must securely store their digital certificates to prevent loss, leakage, or misuse.

4.2 Certificate holders should only use the digital certificate for lawful and authorized purposes.

4.3 Certificate holders must comply with relevant laws, regulations, and industry standards to ensure the legal use of the digital certificate.

5.Certificate Renewal

5.1 Certificate Renewal

5.1.1 Certificate holders can apply to the Pikachu Certificate Trust System to renew their digital certificates and extend their validity period.

5.1.2 Certificate holders must apply for renewal before the expiration of their digital certificates.

6.Certificate Revocation

6.1 Certificate Revocation

6.1.1 The Pikachu Certificate Trust System has the authority to revoke a digital certificate if the certificate holder violates this policy or relevant laws and regulations.

6.1.2 The Pikachu Certificate Trust System will promptly notify the certificate holder and relevant parties upon certificate revocation.

7.Security Measures

7.1 The Pikachu Certificate Trust System will implement appropriate security measures to protect the private keys and related information of the certificates.

7.2 The Pikachu Certificate Trust System will periodically review and update security policies and measures to address security threats and vulnerabilities.

8.Legal and Dispute Resolution

7.1 This policy is subject to applicable laws.

7.2 Any disputes related to this policy should be resolved through negotiation and mediation. If a consensus cannot be reached, the matter should be submitted to the relevant judicial authorities for resolution.