Getting Started

Applications and uploads are managed through the Zoho Desk customer support portal at https://desk.zoho.com/portal/cryptocertify/home. Applicants are encouraged to create an account and submit an inquiry through this portal. For any application questions, either use the support portal or email apply@cryptocertify.com.

Upload Security

For your security, put all documentation into a single PDF file and encrypt the PDF file before uploading. Use a **strong and unique** password. If you wish to encrypt source code files, you may use GnuPG (https://www.gnupg.org/), available for Mac (https://gpgtools.org/) and Windows (http://www.gpg4win.org/). As part of the application process, we will arrange a secure channel to transmit the document password directly to us. For best security, do not email the files and especially **do not email the files and password together**. To protect your privacy, we never decrypt documentation files except for read-only purposes. We always keep documents and their passwords stored separately and encrypted.

Submission Materials

Developer ID

Submit Legal Proof of Identity

1. Copy of government issued identification with no information redacted **and**
2. Any of
   - Notarized proof of identity
   - Copy of birth certificate
   - Copy of passport

Submit Brief Summary of Relevant Experience

1. Programming skills
2. Previous projects and roles in those projects

Note: We do not warrant developers, and therefore do not offer a “proof of developer” or “developer certification”. However, we require identification for purposes of due diligence, on the way to Code or Deployment Certification.

Certified Code & Deployment

Developers must submit

- The crypto-currency specifications (emission schedule, money supply, staking parameters).
- Repository commit identifier or source bundle for the code being certified.

Certification Criteria

Certified Code

Prerequisites

1. Certified Code must have a Certified Developer.
2. The Certified Developer must state what roles they have in the crypto-coin that is submitted for certification.
3. The Certified Developer must demonstrate exclusive control over the code repository, or all direct contributers to the repository must be Certified Developers.

Codebase Criteria

1. Certified Code must not reveal evidence of any malicious behavior.
2. Have emission, money supply and staking characteristics that agree with the coin specifications, including no hidden premines or emission anomalies.
3. Be free of obvious security holes or exploits.

Certified Deployment

Prerequisites & Behavior

1. The deployment executables must be built by the CryptoCertify team.
2. The deployment must be crash-free during live testing.
3. The deployment must meet the coin specifications provided during code certification.
4. The deployment must not show any evidence of malicious activity during testing.