CryptoCurrency Security Standard Auditor (CCSSA) Glossary

Auditing Terms

Audit Documentation

The record of audit procedures performed, relevant audit evidence obtained, and conclusions the auditor reached.

CCSSA

CryptoCurrency Security Standard Auditor

CCSSA-PR

CryptoCurrency Security Standard Auditor Peer Reviewer

CoC

Certificate of Compliance

CoC Listing information

Entity website, entity contact, system audited, listing fee, and entity logo at least 500x500 pixels in size.

https://cryptoconsortium.org
Version 2.3-2022-12-1

Continually

Constant and Uninterrupted.

Listing Fee

The Listing Fee is the cost paid to C4 by the CCSSA for each completed audit. The Listing Fee covers:
1. listing an entity's CoC on C4's website
2. providing the CCSSA with an entity's CoC and Audit Badge.

Periodically

As determined to be sufficient by the auditor

PROL

Peer Review Options List

QSP

Qualified Service Provider

Regularly

Annually

SRoC

Summary Report on Compliance

Technical Definitions

Actor

An actor is a person, organization, system, or service that (for the purposes of this specification) makes direct use of a cryptographic key or seed (or shard of a key or seed as might be the case.) An actor is also called a key holder.

Address

A cryptocurrency address is (usually) an encoded form of a public key from a wallet that can be used as the recipient of a transaction. In multi-signature schemes, an address may be an encoding of information including several public keys and/or other information as in the case of a bitcoin P2SH address.

Approved Communication Channels

A communication channel that provides high confidence of the identities of the communicating parties. This could be a voice call where the sound of their known voice is verified, a digitally-signed message (using strong encryption such as PGP/GPG or S/MIME), or a combination of multiple separate channels that are unlikely to be simultaneously compromised, such as an email + an SMS message + an instant message via Slack.

Clients' Assets Custodied

This is the total amount of assets custodied by the entity on their clients behalf, as determined by the CCSSA at the beginning of the audit.

Comparable Control

A control put in place by the entity which provides equivalent or comparable protection to the control defined in the CCSS. The CCSSA can use their professional judgment where organizational controls do not meet CCSS controls descriptions but provide a similar level of protection.

Deterministic Random Bit Generator (DRBG)

A kind of PRNG that can produce some number of values (usually keys) from a single seed. DRBGs are primarily useful due to their ability to limit a system's reliance on secure sources of entropy.

Digital Signature

A mathematical scheme for verifying the authenticity of digital messages or documents. A valid digital signature, where the prerequisites are satisfied, gives a recipient very strong reason to believe that the message was created by a known sender (authentication), and that the message was not altered in transit (integrity).

Dirty Signature

A dirty signature is a signature where any part of the cryptographic and signature process does not conform to industry standards and best practices. Examples of this would be predictable nonces, nonce reuse, predictable signature variables, re-used signature variables (k, r), non-compliant deterministic random bit generators. A dirty signature attack is one in which attackers are able to recover a private key that was used to compute a digital signature.

Entropy

Randomness, usually collected from hardware, environmental factors (time of execution), or external sources (user-input). Wikipedia

Factor of Authentication

Multi-factor authentication schemes require multiple demonstrations of identity. The most common example is a username and password combination, where each input is a factor of authentication. To access protected information in this scheme, an actor must provide those two pieces of information. Additional factors generally (although with diminishing returns) increase the security of the system. Common examples include:

- A TOTP token may be required, where the token can only be obtained from a device seeded with the TOTP secret (Google Authenticator), which effectively requires the actor be in possession of a specific pre-authorized device.
- An OTP can be delivered to a phone number via SMS, MMS, or a voice call.
- A biometric scan may be required - although this is usually only useful if the access point is in a controlled and trusted environment.

Colloquially, a username is not considered a factor of authentication since usernames are not commonly secret information. The same applies to email addresses, phone numbers, and other pieces of data which only “identify” actors. The requirement imposed by a factor of authentication should only be satisfiable by the actor identified.

Full System

A system that can reach quorum independently. Full systems have some control over funds. An entity may have more than one system. Each system must be audited individually.

Hierarchical Deterministic Wallet

A wallet that uses a cryptographically secure key derivation function (e.g. PBKDF2) to create an arbitrarily large number of unique addresses from a single master seed. These are beneficial as only the master seed needs to be backed up to protect against loss. Some HD wallet software can also support multi-signature configurations where multiple master seeds are combined when creating addresses. HD wallets generally organize addresses into an n-ary tree structure, where each address is associated with a path through the tree. The first HD wallet standard adopted by many applications in the Bitcoin community was BIP32 as proposed by Pieter Wuille. BIP44 introduced additional functionality allowing sub-paths to be shared without compromising the security of the entire wallet.

Identity Verification

Identity verification is a tiered process by which an organization or system attempts to confirm the authenticity of an actor's claim to be a given individual or organization.

Typical methods of identity verification for individuals include:

- one or more forms of government-issued identification (driver’s license, passport, etc.)
- one or more proofs of residency at the individual’s home (utility bills, bank statements, etc.)
- successful completion of challenge questions through a reputable identity-verification service operating in the individual’s country of residence (e.g. Equifax)

In cases of an organization, the supporting records can include:

- Employer Identification Number (“EIN”), Business Number, or similar identifier based on jurisdiction
- D-U-N-S Number
- Articles of Incorporation

In either case, enough supporting documentation should be provided and verified to support the actor’s identity claim.

Key

A cryptographic key is an input to a cryptographic function (Wikipedia). In public-key cryptography a public key is used to encrypt data that can only be decrypted using a corresponding private key. Similarly, the private key can be used to generate irreproducible signatures for arbitrary data which the public key can verify. In cryptocurrency, a private key may often include additional application-specific information such as bitcoin's chain code. In such cases, the term key can apply to extended key information OR partial information which might be used to reconstruct a full key as both are sensitive, private information.

Key Compromise Protocol

A document that outlines the specific actions that are to be taken by every actor in an Information System in order to regenerate the system's set of keys in the event that a key may have been compromised.

Key Holder

A (key/seed) holder is a person, organization, system, or service that (for the purposes of this specification) makes direct use of a cryptographic key or seed (or shard of a key or seed as might be the case.) A key holder is also called an actor.

Multi-signature

A common security feature of cryptocurrency wallet applications is to require multiple signatures from different keys to create a valid transaction.

Not Applicable

A requirement can be marked as Not Applicable if a requirement does not apply to the assessed entity's environment. CCSSA's must provide evidence that testing was undertaken to confirm that the assessed entity's environment does not support or provide a facility that would meet the requirements intent when marking a control as Not Applicable.

One-Time Password

A one-time password is any token (often used as a factor of authentication) that is valid for one and only one use. OTP tokens are generally as secure as the weakest of:

1. The channel used to deliver the OTP to the intended user, if any.
2. The system where the OTP is generated and stored until “redeemed.”

Operator

An operator is the person that generates the key/seed, holds that private key, and is responsible for securing this backup. Operators are actors, but actors are not always operators.

Proof of Reserve

According to the CCSS, demonstration that an organization has access to all funds to which it claims ownership is called a Proof-of-Reserve. Cryptocurrencies based on a public ledger (blockchain) enable proofs of reserve to be conducted and publicly verified.

Pseudo-Random Number Generator

An algorithm, program, or system used to produce arbitrary difficult-to-guess values for cryptographic applications. Typically seeded with some source of entropy, PRNGs are used, among other things, to generate cryptographic keys. (Wikipedia)

Sometimes: CSPRNG (Cryptographically Secure PRNG).

See related: DRBG (Deterministic Random Bit Generator).

Qualified Service Provider

Systems that, by design, can not reach quorum without an additional system. QSPs do not control funds.

Seed

A slice of entropy typically used to initialize a PRNG/DRBG or other crypto-system (e.g. HD Wallets, deterministic signatures).

Strong Encryption

A system for encrypting data using an industry-standard encryption or key derivation algorithm with an encryption key or password *such that* modern cryptanalysis techniques would require the estimated global combined computing power and 1,000x more time than the expected life of the key or seed to decrypt the encrypted data. An example of an encryption algorithm that would provide the necessary level of security at the time of this writing is ES-256. An example of a password-based key derivation function is PBKDF2 as described in BIP39. (Wikipedia)

Trusted Environment

For the purposes of this specification, trusted environment is defined as the physical location, hardware, and software used in any private key related operations.

Wallet

In the context of most cryptocurrencies, a wallet is a public-private keypair, where some encoding of the public key (an address) can be used in transaction outputs to transfer funds. The private key can then be used to generate a valid signature for a transaction spending those funds. In practice, however, 'wallet' usually refers to an application that manages a large number of these keypairs, allowing a new address to be used for each transaction. Wallet applications generally fall into one of two categories:

- JBOK (Just a Bunch of Keys) Wallets where the wallet uses a PRNG to generate each keypair and stores them for use.
- HD (Hierarchical Deterministic) Wallets which derives an arbitrary number of keypairs from one random seed.

Wallet software can introduce additional complexity, for example by combining multiple keypairs into single addresses, as in the case of a multi-signature wallet. For the purposes of this document, the term 'wallet' refers to some *collection* of cryptocurrency addresses.