RedTeam Security

Cryptocurrency Security Standards Checklist

Use this checklist to assess your compliance with the CryptoCurrency Security Standard (CCSS).

RedTeam Security
redteamsecure.com
sales@redteamsecure.com
twitter.com/redteamsecure

214 4th Street E., #140
St. Paul, MN 55101

© Copyright 2019 RedTeam Security Corporation. All rights reserved.

About This Resource

The CryptoCurrency Security Standard (CCSS) is a set of requirements designed to govern all information systems that store, accept or transact with cryptocurrencies like Bitcoin and Ethereum.

CCSS is created collaboratively by a group of developers, researchers and security experts with the goal of giving users a safe and secure means of handling cryptocurrencies including Bitcoin, Ethereum, Litecoin, and many others. It is not meant to be a standalone governing document; rather, it should be used in tandem with existing best practices for information security.

This checklist was developed directly from the CCSS guidelines and is and supported by RedTeam's broad cryptocurrency security expertise. The 10 aspects of cryptocurrency security this checklist addresses are used as a scoring system, with the culminating total determining an organization's overall level of security on a scale of one to three. Level I is the lowest level and offers strong security measures, while Level III is the highest and offers the most comprehensive measure of security. These security levels are assigned based on the lowest common rating among all categories. So, for example, if a Level I organization meets some, but not all Level II criteria, it will retain a Level I rating until all Level II criteria are met.

For a more customized explanation of CCSS that speaks to your organization's unique needs, we invite you to **book a complimentary one-on-one consultation** with our team.

Here's What We'll Cover

I. Key/Seed Generation
II. Wallet Creation
III. Key Storage
IV. Key Usage
V. Key Compromise Policy
VI. Keyholder Grant/Revoke Policies and Procedures
VII. Third-Party Security Audits/Pen Tests
VIII. Data Sanitization Policy
IX. Proof of Reserve
X. Audit Logs

© Copyright 2019 RedTeam Security Corporation. All rights reserved.

I. Key/Seed Generation

There are two factors that contribute to the secure creation of cryptographic keys and seeds used in a cryptocurrency system: confidentiality and unguessable numbers. Confidentiality ensures that newly created keys or seeds are not obtained by an unintended party, while the use of unguessable numbers ensures that the key or seed cannot be guessed by someone other than the intended key/seed holder.

Level I

- ☐ Are the cryptographic keys and seeds created by the actor who will be using them?
- ☐ In cases where an automated agent will make use of a cryptographic key/seed, does the administrator of that system generate the key/seed on a suitable offline system with sufficient entropy, have this key/seed transferred securely onto the target device, and then securely delete the key/seed using CCSS-compliant data sanitization techniques (for more on data sanitization, see section VII)?
- ☐ Are cryptographic secrets that are transferred for backup purposes transmitted and stored in a strongly encrypted format?
- ☐ Are cryptographic keys and seeds created on a system with sufficient entropy to ensure the keys are not created with any bias towards a reduced range of values, or other deterministic properties?

Level II

- ☐ Is the key or seed generation methodology validated prior to use?
- ☐ Is a digital signature generated and published after the software has been audited?
- ☐ In cases where keys or seeds are created without the use of software (e.g. dice, a deck of cards, or other non-digital source of entropy), is the creation methodology validated to ensure determinism is not present (i.e. there are no weighted dice, each card in the deck is unique, etc.)?

Level III

- ☐ Is the key or seed generated using a Deterministic Random Bit Generator (DRBG) that conforms to NIST SP 800-90A and has been seeded with at least two separate cryptographically secure sources of entropy that have been combined in a cryptographically secure manner (e.g. SHA256[UnguessableFactor1 + UnguessableFactor2])?

© Copyright 2019 RedTeam Security Corporation. All rights reserved.

II. Wallet Creation

There are many different key signing methodologies that can be used during the creation of cryptocurrency wallets. This aspect covers best practices in wallet creation to maintain the integrity of the wallet in the face of various risks, like lost or stolen keys or the unintentional disclosure of the wallet holder's identity.

Level I

- ☐ Are unique addresses generated by the wallet for every transaction?

Level II

- ☐ Does any address generated by a wallet require a minimum of 2 signatures in order to spend funds, with a separate actor holding each signing key?
- ☐ Are redundant keys assigned to each wallet for recovery purposes?
- ☐ Are all addresses assigned deterministically based on seeds that are kept private?
- ☐ Are any keys that have signing authority on a single wallet stored in different locations?

Level III

- ☐ Are any keys that have signing authority on a single wallet stored by multiple organizational entities?

© Copyright 2019 RedTeam Security Corporation. All rights reserved.

III. Key Storage

To maximize the confidentiality of cryptocurrency keys and seeds, they should be stored as securely as practically possible using means such as encryption, secret sharing, and physical locks where appropriate. To maximize the integrity of keys/seeds, backups should exist that allow the keys/seeds to be recovered in the event the primary keys become inaccessible, and said backups should be stored with at least as much security as the primary keys, if not more.

Level I

- ☐ Are cryptographic keys and/or seeds stored with strong encryption when not in use?
- ☐ Is there a backup in some form (paper, digital, etc.) of the cryptographic key/seed?
- ☐ Is the backup protected against environmental risks like fire, flood, etc.? In general, common methods to achieve this include a water-tight bag for flood protection and a safe or firebox for fire protection.

Level II

- ☐ Does a backup exist for at least as many keys as is required to spend funds? For example, in a 2-of-3 signing setup where any two of three keys are required to spend funds, backups must exist for at least two of these keys.
- ☐ Is the backup key/seed stored in a location that is geographically separate from the usage location of the primary key/seed?
- ☐ Is the backup protected by access controls that prevent unauthorized parties from accessing it, like safes, safe deposit boxes, or locked drawers where only the operator holds the key/combination for the lock?
- ☐ Does the backup employ some form of tamper-evident mechanism that allows an operator to determine when it has been accessed?

Level III

- ☐ Are backups of cryptographic keys and/or seeds stored with the use of strong encryption that is at least equal to the security prescribed for cryptographic keys/seeds above? If backups use a less-secure mechanism than the key/seed itself, the system cannot be certified as Level III.
- ☐ Are backups resistant to electromagnetic pulses that could induce currents in electronics and damage the data stored within?

© Copyright 2019 RedTeam Security Corporation. All rights reserved.

IV. Key Usage

Cryptographic keys and/or seeds should be used in a secure manner that minimizes the risks to the confidentiality of private keys and integrity of funds.

Level I

- ☐ Does access to the primary key/seed require an identifier (i.e. username, email, etc.) and at least two other factors of authentication?
- ☐ Are all keys/seeds used only in trusted environments?
- ☐ Have all key/seed-holders had their references checked prior to being trusted to hold one of these assets on behalf of the organization?
- ☐ Are measures in place to prevent two master keys/seeds of the same multi-signature wallet from being present on the same device?
- ☐ Do digital signatures use a 'k' value that is never repeated?

Learn more about two-factor authentication and other access control policies here.

Level II

- ☐ Have all organizational key/seed-holders undergone identity verification to ensure they are who they say they are?
- ☐ Is verification of fund destinations and amounts performed via an Authenticated Communication Channel prior to key/seed use?

Level III

- ☐ Does access to the key/seed require an identifier (i.e. username, email, etc.) and at least three other factors of authentication?
- ☐ Have all organizational key/seed holders had background checks performed by law enforcement personnel or investigative firms?

© Copyright 2019 RedTeam Security Corporation. All rights reserved.

V. Key Compromise Policy

Every organization dealing in cryptocurrency should have a protocol that dictates the actions that must be taken in the event a cryptographic key/seed or its holder is compromised. Such protocols decrease the risks associated with lost funds and disclosed trade secrets and increase the availability of the information system to its users.

Level I

- ☐ Is there an inventory of all keys/seeds in the organization, with an emphasis on which keys are critical to the successful operation of the information system?

Level II

- ☐ Is there a proper Key Compromise Protocol that outlines each specific class of key used throughout the system along with a detailed plan of dealing with its compromise and the proper use of Authenticated Communication Channels during execution? The plan should identify actors via roles and not names and includes secondary actors in the event any primary actor is unavailable to carry out the KCP.

Level III

- ☐ Are tests of the Key Compromise Protocol executed regularly to confirm the viability of the procedures and to ensure staff remain trained to use them in the case of a compromise? Logs should be kept of executed tests which outline any/all comments and improvements identified.

© Copyright 2019 RedTeam Security Corporation. All rights reserved.

VI. Keyholder Grant/Revoke Policies and Procedures

Staff typically have greater access to an information system with respect to accessing its information, invoking privilege-restricted actions, and representing the organization to the public. This makes the proper onboarding and offboarding of personnel with regards to cryptocurrency of utmost importance.

Level I

- ☐ Is there an organizational awareness of how roles should be managed when onboarding or offboarding staff from keyholder positions?

Learn more about creating strong security policies for departing employees here.

Level II

- ☐ Does the organization maintain checklists that cover all tasks that must be completed when staff vacate or transition into keyholder roles within the organization? These checklists should be reviewed by knowledgeable personnel to ensure "least privilege principles" are applied to the information system.
- ☐ Are all keyholder grant/revoke requests conducted over Authenticated Communication Channels?

Level III

- ☐ Do the organization's checklists include auditing information that records the identity of the staff member that performs the grant/revoke operations?

© Copyright 2019 RedTeam Security Corporation. All rights reserved.

VII. Third-Party Security Audits/Pen Tests

Regardless of the technical skills, knowledge, and experience of staff who build and maintain an information system, it has been proven that third-party reviews very often identify risks and control deficiencies that were either overlooked or underestimated by staff. Different people than those who implement a cryptocurrency system should assess its security.

Level I

- ☐ Has a developer who is knowledgeable about bitcoin security assisted in the design and implementation of the information system?

Level II

- ☐ Has a single audit and/or penetration/vulnerability test been completed by a third-party entity prior to or shortly after launch?

Level III

- ☐ Are security audits and/or penetration/vulnerability tests performed on a defined schedule of at least once per calendar year, with documentation that shows how each of the concerns within the audit were addressed?

RedTeam Security is your trusted partner in cryptocurrency security. We specialize in **application penetration testing**, **network penetration testing**, **social engineering** and **physical security testing** for organizations that store, accept or transact with cryptocurrencies like Bitcoin, Ethereum and Litecoin.

Schedule your free cryptocurrency security consultation with our team today.

© Copyright 2019 RedTeam Security Corporation. All rights reserved.

VIII. Data Sanitization Policy

Data persists on digital media even after it is deleted by the user. Proper sanitization of digital media ensures the proper removal of all keys, eliminating the risk of information leakage from decommissioned devices like servers, hard disk drives, and removable storage.

Level I

- ☐ Is the organization's staff aware of how data persists on digital media after deletion? Staff should have access to tools that perform secure deletion of data and understand when to use such tools to permanently destroy any transient copies of cryptographic keys that may be required during the maintenance of the information system.

Level II

- ☐ Is there a detailed policy outlining the requirements for sanitization of digital media that holds/held cryptocurrency keys, and is it read/understood by all staff who have access to cryptographic keys?

Level III

- ☐ In addition to the above, is an audit trail maintained for every piece of sanitized media?

© Copyright 2019 RedTeam Security Corporation. All rights reserved.

IX. Proof Of Reserve

Operating with a full reserve of user funds ensures the ability of the system to cover simultaneous withdrawals by all users. Establishing regular proofs of reserve provides assurance to the public that all funds are available to the system which eliminates the risks of fund loss.

Level I

- ☐ Has an audit been completed and published online that proves full control of all funds held by the information system? The audit should be signed by an independent party that attests to the accuracy of the audit at the time it was performed, which reduces the risks associated with inaccurate or misleading reports.

Level II

- ☐ Does the organization conduct regularly-scheduled proof of reserve audits that provide proof that the organization continues to operate on a full reserve and that all user funds are accessible at the time each audit is completed?

Level III

- ☐ Is the information system designed in such a way that an independent audit is not necessary to prove complete accessibility of user funds? The information system should make use of public ledgers such as blockchains themselves to make this information available to the public allowing anyone to conduct an audit independently.

© Copyright 2019 RedTeam Security Corporation. All rights reserved.

X. Audit Logs

In the event of unexpected behavior or security incidents, audit logs are an extremely valuable tool that can help investigators understand how the unexpected symptoms occurred and how to resolve the inconsistencies to return the information system to a consistent state.

Level I

- ☐ Do audit trails exist for a subset of actions that are performed within the information system? Examples of this would include recording audit information of all withdrawals and deposits made with the system.

Level II

- ☐ Are all actions by all users logged?

Level III

- ☐ In addition to recording all actions performed within the system, is this audit information regularly backed up to a separate server?

© Copyright 2019 RedTeam Security Corporation. All rights reserved.

About RedTeam Security

RedTeam Security has been a premiere provider of offensive information security services since 2008. In today's marketplace, companies are overwhelmed by security threats from hackers originating from all over the world. Studies show that the number of attacks against companies are increasing and at the same time becoming more complex. As a result of these attacks, the number of data breaches have cost companies tens of millions of dollars as well as grave reputational damage.

The security experts at RedTeam Security have years of experience helping organizations of all sizes identify and mitigate security vulnerabilities. Our highly trained consultants are published authors, hold multiple security certifications and speak at security conferences around the world.

Our portfolio of services includes:

Red Teaming
Network Penetration Testing
Application Penetration Testing
Physical Penetration Testing
Social Engineering
Compliance

It's easy to receive a customized security proposal for your organization. Just **fill out our scoping questionnaire**. You can also **schedule a consultation** with our team of experts or call us at **612-234-7848** for more information.

RedTeam
SECURITY CONSULTING

We educate. We identify. We inform. We reduce your attack surface.