CRYPTOCURRENCY
SECURITY STANDARD

CCSS Version 9.0 Summary of Changes

Document History

Version	Date	Comment
1	12-17-2024	Initial document version.

Introduction

The changes from CCSS version 8.1 to CCSS version 9.0 are significant and include:

1. **Enhancement and clarification of existing requirements wording**, including consolidation of the terminology used, replacement of terms and statements that restrict the use of new technologies, and more clarity on referencing external standards, making CCSS easier to understand and implement.
2. **New requirements addressing emerging security challenges** within decentralized finance (DeFi) and other blockchain-based technical components, such as smart contracts, which introduce more complex key management systems.
3. **New governance requirements include written acknowledgements from executive management and key custodians**, risk management, threat modeling, and service provider management.
4. **Enhancement of the logging aspect** by adding monitoring requirements to ensure log event records are collected and monitored for suspicious activity, and that wallet addresses receive the same scrutiny.
5. **Support for single-signer mechanisms**. Though not considered best practice, single-signer mechanisms are used in many architectures. The latest CCSS update provides detailed considerations when evaluating the use of a single-signer mechanism.
6. **New requirements addressing physical security controls within environments** where key management activities are conducted.
7. **New requirement for training for personnel involved in key management operations** and personnel who could impact the security of the key management system.

Over one thousand documented changes to CCSS from version 8.1 to version 9.0 occurred. Therefore, this document only provides the most critical changes to CCSS. When deemed appropriate for the sake of readability, summaries have been provided instead of recording every single change to CCSS from version 8.1 to version 9.0.

New Aspects and Requirements

Aspect/Requirement	CCSS Level	Comment
1.05.2.2	1	A new requirement to ensure key management processes are isolated from other system processes on the system.
1.05.2.3	3	A new requirement that enhances 1.04.2.2 by requiring that the isolation mechanism requires FIPS 140 or equivalent certification.
1.05.6, 1.05.6.1	1	An aspect and one new requirement that requires all individuals involved in key management activities or can impact the security of key management activities is to have security training related to their role(s).
1.05.7, 1.05.7.1	1	A new aspect and one new requirement for all personnel with key management responsibilities is to acknowledge their responsibilities in writing.
2.05.1.3	2	A new requirement for the key inventory is to be reviewed at least annually to ensure the key inventory is accurate. NOTE: Version 8.1 “Key Compromise Protocol” aspect has been updated in several areas, including the replacement of the current wording with this new requirement and moving this aspect control to the Operations category.

2.01.2, 2.01.2.1, 2.01.2.2, 2.01.2.3	1	A new aspect and three new requirements for addressing smart contract auditing. The three requirements require (1) that all smart contract code is audited before deployment to environments where the entity stakeholders interact with the smart contract, (2) all smart contract code audit reports are accessible to the entity stakeholders and (3) all issues with a severity of medium or higher are remediated before deployment to environments where the entity stakeholders interact with the smart contract.
2.03	N/A	A new aspect introducing governance, risk management, and service provider management to CCSS.
2.03.1, 2.03.1.1	1	A new aspect control and one new requirement. Requirement 2.03.1.1 requires a member of the executive management to acknowledge their responsibilities for information security of the systems in scope for CCSS.
2.03.2, 2.03.2.1, 2.03.2.2	1, 2	A new aspect control and two new requirements. Requirement 2.03.2.1 requires threats to the information system to be identified and a threat model created. Requirement 2.03.2.2 requires that the risk assessment framework uses internationally recognized standards for risk management such as ISO/IEC 27005 and NIST SP 800-37.
2.03.3, 2.03.3.1	1	A new aspect control and one new requirement. Requirement 2.03.3.1 requires a due diligence process for any service provider that can impact the security of the CCSS Trusted Environment.
2.02.3, 2.02.3.1, 2.02.3.2	1, 2	A new aspect control and two new requirements. This aspect control adds log monitoring to CCSS. In CCSS version 8.1, log event records must be stored for a certain period. However, there was no requirement to monitor the log event records for suspicious activity. CCSS version 9.0 adds log monitoring requirements.
2.02.4, 2.02.4.1	3	A new aspect control and one new requirement. This aspect control adds wallet address monitoring to CCSS. Wallet address monitoring has evolved over the years to become a valuable detective control for possible unauthorized access to funds.

Updates to Existing Aspects and Requirements

What Changed for Version 9.0?	CCSS Level	Comment
1.01.3.2, 1.02.1.1, 1.02.2.1, 1.02.4.1, 1.05.9.1	1, 2, 3	CCSS version 9.0 supports single-signer mechanisms. In CCSS version 8.1 the use of a single-signer mechanism was not supported. The CCSS Steering Committee decided to support single-signer mechanisms based on the prevalence of this type of mechanism and stakeholder feedback.
1.01.3.1	3	Version 8.1 of this requirement was too detailed in the technical requirements thus dating CCSS. Version 9.0 of the requirement has been updated to directly reference NIST SP 800-90A for all technical requirements to meet the intent of this requirement.
1.01.3.2	3	The requirement has been updated to provide more detail as to what tasks and actions are required to be addressed in a key generation process.
1.02.1.1	2	Added support for single-signer mechanism for signing transactions. Though single-signer wallets are not as secure as multi-signer wallets, they are used in web3 architectures such as hot wallets. The requirement provides mandatory considerations that must be addressed when considering the use of a single-signer mechanism.
1.02.2.1	2	The requirement has been reworded to support the introduction of the single-signer mechanism.
1.02.3.1	2	The requirement has been reworded to support the introduction of the single-signer mechanism.
1.02.4.1	3	The requirement has been reworded to support the introduction of the single-signer mechanism.
1.03.3.3	N/A	This version 8.1 requirement has been removed. The intent of the requirement was to ensure that electronic backups are resistant to electromagnetic pulses. Instead, in version 9.0, requirement 1.03.3.1 has been updated with “electrical surges” to the wording of the requirement.

1.04.3.1	1	The requirement has been reworded to provide more clarity as to which role(s) are required to have a reference check. The requirement has also been renumbered in version 9.0 to 1.05.3.1.
1.04.4.1	1	The requirement has been reworded to provide more clarity as to which role(s) are required to have an identity verification check. The requirement has also been renumbered in version 9.0 to 1.05.4.1.
1.04.5.1	1	The requirement has been reworded to clarify which role(s) require a background check. This requirement has been amended to include the statement that background checks are to be ongoing during the person's employment. This requirement also considers the different local laws and regulations as to the ability to enforce this requirement. The requirement has also been renumbered in version 9.0 to 1.05.5.1.
1.04.5.1	1	The requirement has been moved from CCSS Level 3 to CCSS Level 1 to align with the other vetting requirements (1.05.4.1 and 1.05.3.1). The requirement has also been renumbered in version 9.0 to 1.05.5.1.
1.04.8.1		This version 8.1 requirement has been updated to remove the term “k” from the wording of the requirement, as this term was deemed confusing by stakeholders. The “k” value has been moved to the requirement’s rationale as an example. The requirement has also been renumbered in version 9.0 to 1.05.10.1.
1.04.9.1	1	The requirement has been reworded to support the introduction of the single-signer mechanism. The requirement has also been renumbered in version 9.0 to 1.05.9.1.

1.05 and all requirements	N/A	This aspect and its requirements have had several changes applied: 1. The aspect control and all requirements have been moved to the Operations category. The aspect and all requirements under the aspect in version 9.0 is 2.04. 2. The aspect title has been renamed from "Key Compromise Policy" to "Key Compromise Documentation." 3. Some requirements in this aspect have been renumbered and moved to different CCSS Levels. 4. Replaced the term “protocol” to focus more on policy, standards and procedures to accommodate other types of documentation required for this aspect. 5. Replaced “KCP Exists” with “Key Compromise Policy Existence” to clarify the type of document required. 6. The testing of the Key Compromise Policy (KCP) has been enhanced to include a breakdown of the individual tasks required. 7. Version 8.1 of this requirement allowed for a process not to be documented but relied on a person’s knowledge. This requirement has been removed from version 9 to ensure all processes are documented in writing.
1.06	N/A	The aspect title has been renamed from "Keyholder Grant/Revoke Policies & Procedures" to "Key Access."
1.06.1.1	N/A	Version 8.1 of this requirement provided an allowance for a process that was not documented but relied on a person’s knowledge. This requirement has been removed from version 9.0 to ensure all processes are documented in writing. NOTE: Version 8.1 requirement 1.06.1.2 is now requirement 1.06.1.1 in version 9.0.
2.01.1.1	1	The requirement has been changed to remove the role “developer” from the wording as it was restricting this requirement to the developer role when, in fact, any person could fulfil it if they had the required expertise.

2.02, 2.02.1, 2.02.2, 2.02.3	N/A	The aspect has been renamed to “Log and Monitor” to reflect the addition of log monitoring requirements. Renamed "Application Audit documentation" to "Application Audit Log". Renamed "Audit documentation backup" to "Audit Log Backup". Renamed "Audit documentation monitoring" to "Audit Log Monitoring". The aspect has been renumbered from 2.03 in version 8.1 to 2.02 in version 9.0.
2.02.1.1	N/A	Version 8.1 of this requirement provided an allowance for a process to not be documented but relied on a person’s knowledge. This requirement has been removed from version 9.0 to ensure all processes are documented in writing. NOTE: Version 8.1 requirement 2.02.1.1 is now requirement 1.07.1.1 in version 9.0.
2.02 and all requirements	N/A	In version 8.1 aspect 2.02 addressed data sanitization requirements and was within the “Operations” category of CCSS. It has been deemed that this aspect and all requirements under the aspect be moved to the “Cryptographic Asset Management” category as data sanitization is part of the key management lifecycle. The aspect and all requirements under the aspect in version 9.0 is 1.07.

In addition to the aspect and requirement changes, grammar and terms have been cleaned up.

1. Removed the terms “must” and “should” from the requirement wording. All CCSS requirements are mandatory for the CCSS Level assigned to them.

2. Replaced “staff” with “personnel” to provide more scope for including other entities such as service providers and contractors.

3. Replaced “organization” with “entity” as an information system could be managed by a group of people not controlled by an organizational structure e.g. a DAO.

4. Several existing aspects and requirements have been moved to other categories and aspects to meet the intent of having key lifecycle management and operations categories within CCSS.

5. Rephrased the statements to denote if there is no requirement for a CCSS Level in an aspect control to reflect that each CCSS Level builds upon the last CCSS Level (1, 2 and 3).

6. Removed the use of “seeds/keys” within the standard, and instead, the correct terms are applied based on the context “seed”, “key”, or “key material” where appropriate.

7. The term “trade secrets” has been removed from the Standard’s requirements.

8. A blanket replacement of the term “creation” to “generation”. In CCSS version 8.1 there was no consistency in whether “creation” or “generation” would be used. It was decided to use “generation” instead of “creation.”

The CCSS is community-driven, industry-focused, and corporate-neutral — putting the needs of the crypto community first. C4 invites the community to submit feedback about V9.0 by March 17th, 2025.