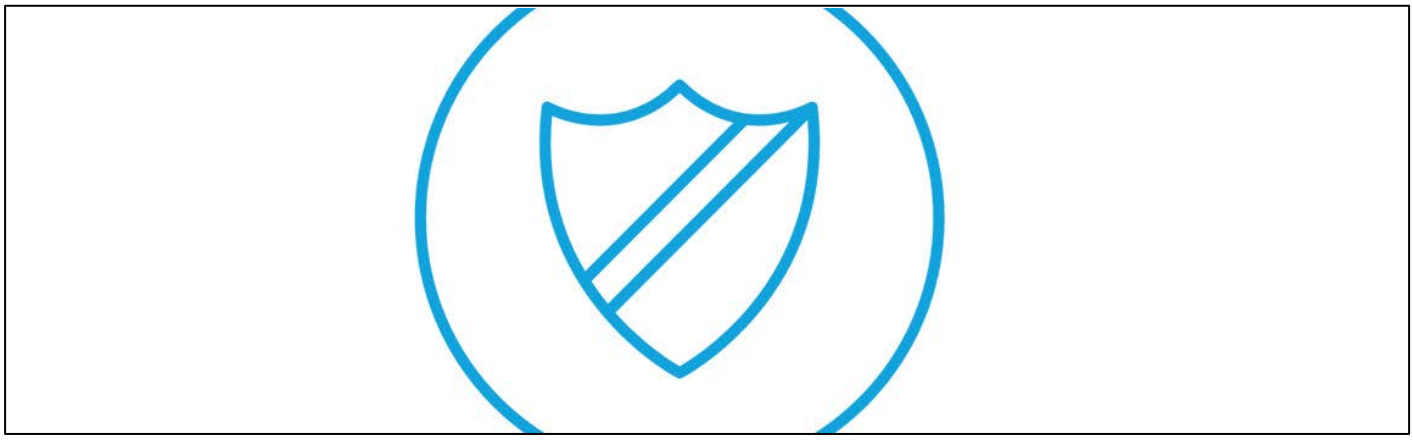


Cryptocurrency Security Standard (CCSS)

By Sandro Psaila

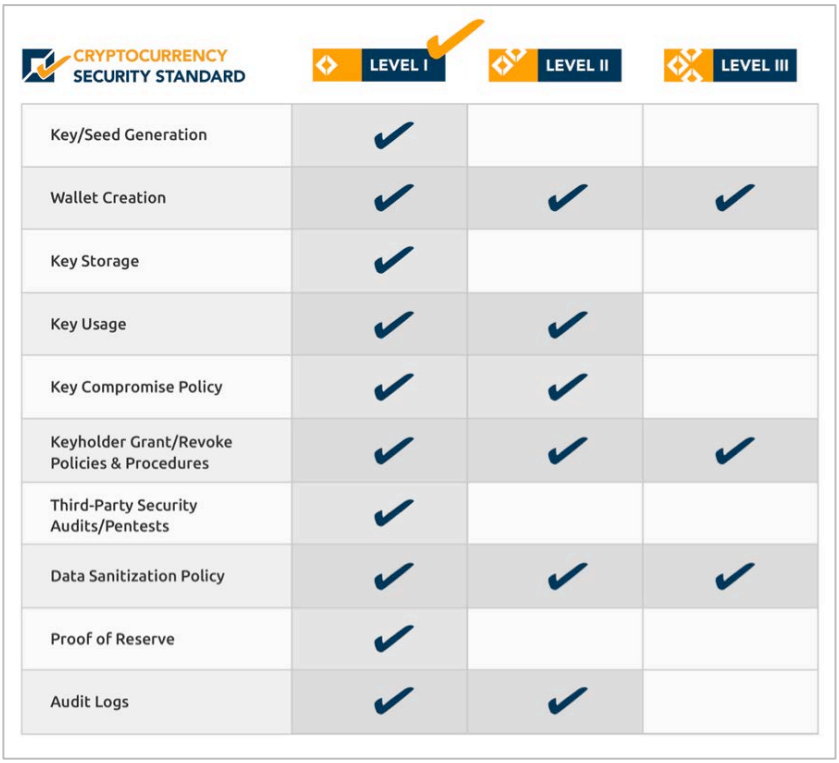
It is now more widely expected that cryptocurrencies (“cryptos”) are here to stay and they will continue to evolve until they become the mainstream currency. Although the global shift to cryptos will not be happening anytime soon, the perspective is that it is only a matter of time WHEN and not IF. Until that day, there will be a lot of “shake out” before cryptos become mainstream.

One of the biggest challenges of cryptos is confidence. People and organisations are concerned about the authentication, authorisation and/or confidentiality limitations of cryptocurrency transactions. Such limitations are currently hindering the adoption rate of cryptos. By standardising the security techniques and methodologies used by crypto systems around the globe, end-users will be able to make educated decisions more easily about which products and services to use and with which companies they wish to align. On the other hand, many cryptos, like Bitcoin, are not governed by a central control point or “authority”; standardising on security will be a challenging process. Standard approaches to a secure environment will come from the cryptos that adopt permissioned-ledger mechanisms such as Ripple XRP. In permissioned-ledger environments, whilst read permissions may be public or restricted to an arbitrary extent, write permissions are kept centralised to one organisation. As such, standardising on security is more achievable.

The success of online payments using traditional or fiat currencies can be partly attributed to the PCI DSS (Payment Card Industry Data Security Standard). This standard was spearheaded by the major payment brands i.e. American Express, Discover Financial Services, JCB International, MasterCard, and Visa Inc. and it has now become the defacto standard for organisations that handle or store credit card details. Non-compliance to this standard means that an organisation will not be able to conduct online payments through the use of credit cards.

A security standard n the crypto space, commonly referred to as CCSS (Cryptocurrency Security Standard), was introduced in 2014 to provide guidance specific to the secure management of cryptos. This standard is currently the go-to standard for any information system that handles and manages crypto wallets as part of its business logic.

The CCSS is an open standard that focuses on the cryptocurrency storage and usage within an organisation[1]. CCSS is designed to augment standard information security practices and to complement existing standards (ISO 27001, PCI, etc.), not replace them. The CCSS standard cannot be compared to PCI DSS as an equivalent standard. Whereas the PCI DSS standard applies to the entire transaction flow (i.e. starting from the technology used to acquire transactions through to how the information in the transaction is treated throughout all steps of processing), the CCSS standard does not provide the same coverage and only focuses on the secure management of the crypto wallets. Additional security measures will be required to secure the environments within which the crypto-security management components operate.



CRYPTOCURRENCY SECURITY STANDARD	LEVEL I	LEVEL II	LEVEL III
Key/Seed Generation	✔		
Wallet Creation	✔	✔	✔
Key Storage	✔		
Key Usage	✔	✔	
Key Compromise Policy	✔	✔	
Keyholder Grant/Revoke Policies & Procedures	✔	✔	✔
Third-Party Security Audits/Pentests	✔		
Data Sanitization Policy	✔	✔	✔
Proof of Reserve	✔		
Audit Logs	✔	✔	

Figure 1: CCSS matrix (credit: https://cryptoconsortium.org/standards/CCSS

CCSS is broken into three levels of increasing security.

- An information system that has achieved Level I security has the ability to protect crypto wallets with strong levels of security.
- A higher level II of CCSS translates into enhanced levels of security with formalised policies and procedures that are enforced at every step within the respective business processes.
- In level III of CCSS, multiple actors are required for the all-critical actions, advanced authentication mechanisms are employed to ensure authenticity of data, and assets are distributed geographically and organisationally.

Put together, these requirements make crypto wallets more resilient against compromise.

In order to ensure the standard remains neutral and up-to-date with industry best practices, the CCSS is maintained by the CCSS Steering Committee, composed of crypto space subject matter experts.

In addition to this committee one also finds the Cryptocurrency Certification Consortium (C4). This group establishes cryptocurrency standards that help ensure a balance of openness and privacy, security and usability, as well as trust and decentralisation. C4 also provides certifications so that professionals can assert their knowledge in cryptocurrencies in the same way they are able to assert other skills. Prior to C4, there was no way for hiring managers and/or placement firms to validate Bitcoin knowledge in their candidates as they could do with other knowledge such as networking, security, and accounting. The next step is to have a more generalised cryptocurrency certification and potentially a certification for CCSS compliance assessors.

Although this standard has been around since 2014 and the number of crypto systems have mushroomed recently, very few organisations are claiming adherence with the CCSS when it comes to the management of crypto wallets. In fact, it is perceived that a considerable number of businesses in this space, mainly start-ups, do not follow security best practices, and their operations do not meet minimal security standards. Typically, start-ups do not invest the proper amount of time and resources into security best practices. They do not have formal security

[1] https://cryptoconsortium.org/standards/CCSS

verification standards in place and they do not exercise regular penetration tests on their systems. Put together, such characteristics make these organisations more attractive and vulnerable to cyber breaches.

While reviewing current breaches, it appears that every system that suffered a high profile cryptocurrency breach was found to be non-compliant with CCSS Level 1. In contrast, systems that are compliant with CCSS Level 2 or higher, are more likely to withstand cyberattacks that gave attackers full access to the crypto-mechanic parts of cryptocurrency. From an IT audit perspective, testing for CCSS compliance will provide a reasonable degree of assurance that the risks related to the management crypto wallets are being minimised and mitigated.

Security is invariably an important consideration, especially when it comes to financial transactions. Money stolen from cryptocurrency wallets is usually unrecoverable. Subsequently, providing the necessary confidence that cryptocurrency wallets are managed by controls that meet industry guidelines becomes a vital issue for anyone who uses any form of cryptocurrency.

About the author

Sandro Psaila is an IT Audit manager in Deloitte Malta Audit & Assurance. For more information, please visit www.deloitte.com/mt

Deloitte
Deloitte Place
Mriehel Bypass
Mriehel BKR 3000
Malta