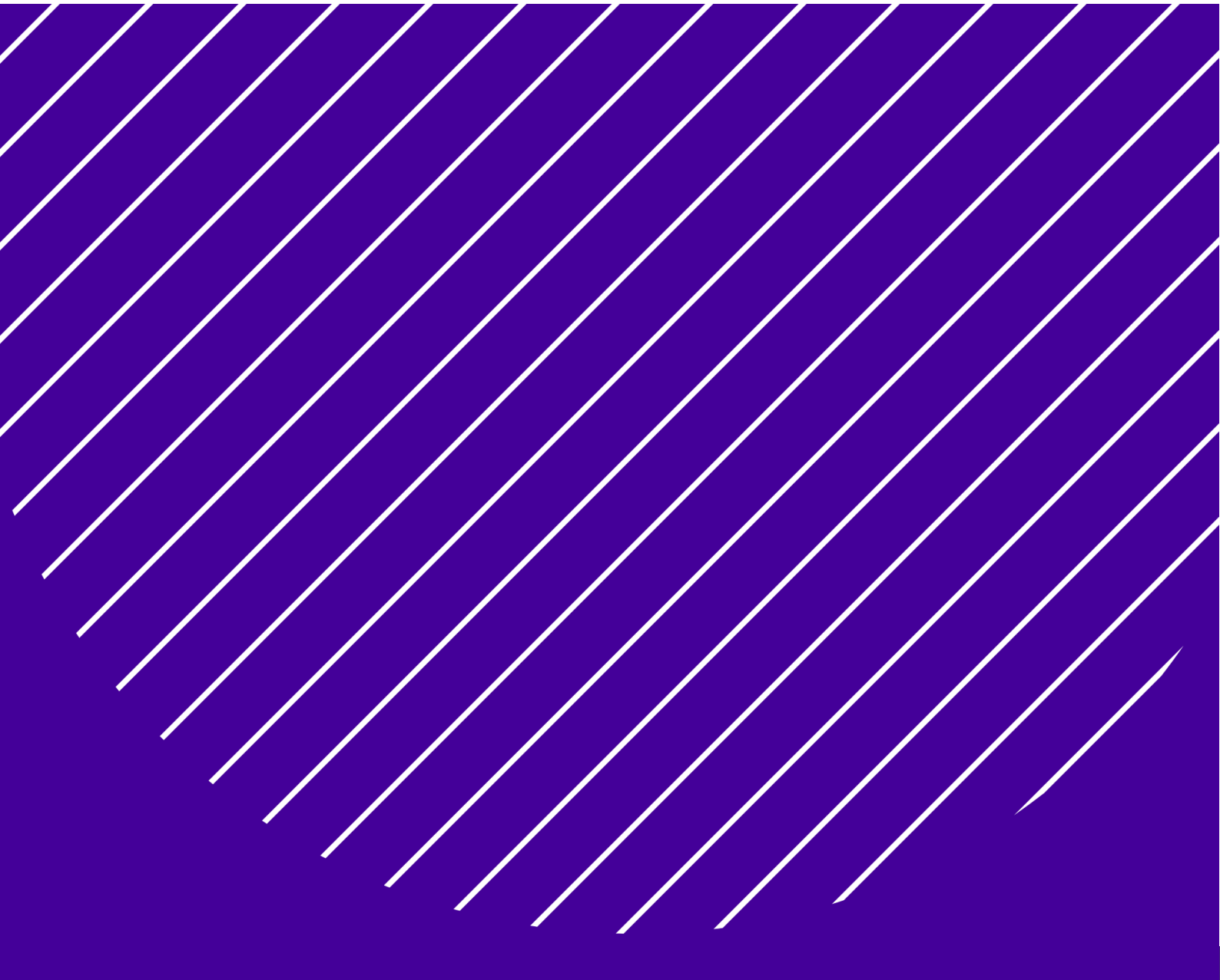
cmta.

Digital Assets Custody Standard

May 2025



Digital Assets Custody Standard

Capital Markets and Technology Association
Route de Chêne 30
1208 Genève

Adopted: October 2020
Updated: March 2023
May 2025

admin@cmta.ch
+41 22 318 73 13

Table of contents

1. INTRODUCTION

§ 1.1 BACKGROUND

The Capital Markets and Technology Association (CMTA) is an independent Swiss association bringing together experts from the financial, technological, audit and legal sectors to promote the use of new technologies in capital markets. The CMTA provides a platform to create open industry standards around issuing, distributing and trading securities and other financial instruments in the form of digital assets using the distributed ledger technology (**DLT**).

This document defines CMTA's Digital Assets Custody Standard (**DACS**), which consists of requirements and recommendations (**RRs**) for technology solutions enabling the custody and management of digital assets.

The DACS aims to contribute to a high level of assurance for digital asset owners, without hampering the custody provider's business nor the usability of the system. There are aspects of digital asset custody that contrast sharply with the operational and security aspects related to the safekeeping of traditional financial assets. These distinctive features present a number of challenges, the most notable being how to generate, operate and secure the private keys (**PKs**) relating to digital assets throughout the lifecycle of the custody services.

The DACS establishes a baseline upon which customers and auditors alike can rely to assess a custody solution or provider. To that aim, the DACS' RRs are defined and formulated to be, as much as possible, verifiable, auditable, as well as agnostic to implementation and the type of asset. By essence, the list of RRs presented in this DACS is not comprehensive.

The guiding principles of the DACS are security, reliability, as well as transparency and control of the custody technology and processes. The RRs were selected through a process involving categorization and prioritization and involved contributors and reviewers from diverse firms that build and use custody technology solutions.

§ 1.2 SCOPE

A digital asset custody solution involves procedures to generate secrets, perform computations using said secrets including the creation of transaction signatures, as well as a number of security controls and procedures to prevent the theft and unrecoverable loss of assets. For example, such controls can include a policy engine enforcing address whitelisting and other transfer restrictions.

In the context of digital assets, the following must be considered as secrets: seeds (or "master keys") and private keys derived from them, as their loss directly implies the loss of the associated assets.

Signature verification keys and addresses tend to not be secret. However, they still require integrity protection, to prevent manipulation and invalid transactions. These values may also be client identifying data (**CID**), thus requiring adequate protection.

A digital asset custody solution system involves both software and hardware computing systems. It is operated via a combination of manual operations and automated actions.

The DACS breaks down the RRs of a custody solution into five sub-categories, grouped in two streams:

A. Operations stream:

    1. choice of custody model; and

2. technical operation of the custody solution.

B. Infrastructure stream:

1. generating secrets;
2. recovering secrets; and
3. development and maintenance.

The operational stream RRs mainly apply to the organization using a digital asset custody solution, as opposed to its vendor. The infrastructure stream RRs, however, apply to a greater extent to the vendor.

The DACS only minimally covers aspects that are not specific to a custody solution, including: physical security concerns, security of the underlying IT and software components (such as workstations, access control mechanisms, IT logs, and so on). The DACS focuses on the components unique to digital asset custody solutions.

The DACS does not address legal and regulatory implications of the choice of custody model or implementation of a particular custody service's offering. In this respect, depending on the implementation and features of the digital asset custody solution, the provider may require a regulatory license, for example if the provider has power of disposal over the digital assets and/or otherwise holds the digital assets for the account of its clients. The DACS does not intend to cover non-custodial solutions.

§ 1.3 DISCLAIMER

Adherence to the DACS requirements may be necessary for a reliable custody solution, but is in no way sufficient. There will inevitably be attack vectors unique to each distinct custody solution and environment. This is because digital asset custody relies on a multitude of technical and procedural components and involves trusting technological components as well as persons involved in their operation. Each institution is therefore responsible for properly integrating the DACS as a component of its risk management process.

§ 1.4 TECHNICAL TERMS | DEFINITIONS

A glossary of technical and capitalized terms used but not otherwise defined in this document is attached as **Appendix A**.

§ 1.5 REVISIONS, ADDITIONS AND UPDATES

The DACS is periodically reviewed and updated by the CMTA.

Any comments or suggestions for future updates may be addressed to the CMTA Secretariat by email to admin@cmta.ch.

2. CUSTODY MODELS

§ 2.1 INTRODUCTION

Financial institutions may custody digital assets through various technical means: either by developing and operating their own custody infrastructure, or by implementing specialized third-party custody technology. The choice of technology implementation is distinct from the custody model itself—an organization either maintains direct custody (self-custody) of assets or delegates this responsibility to another entity (subcustody).

For certain types of financial institutions, particularly those subject to specific regulatory requirements such as collective investment schemes and asset managers, direct custody may not be permissible. These entities may be required by law to engage qualified third-party custodians for client assets.

The following section examines the various models for managing and pooling digital asset ledger accounts (DLAs). These models are technology-agnostic and apply uniformly whether an institution implements proprietary or commercial custody solutions, provided the institution maintains direct custody of the assets.

§ 2.2 CUSTODY MODEL TYPES

Digital assets may be held in custody by an intermediary in accordance with various models, each of which has its own features, parameters and limitations. Most of the available solutions can be classified in one of the model types below.

Model	Description	Allocation	Model
Pooled DLAs	Client only digital assets pooled in one or several DLAs	Pool level allocation - An internal ledger allocates all relevant digital assets to clients at custodian level (but no specific allocation of digital assets is made at the level of each DLA; no allocation on the distributed ledger itself)	1
		DLA level allocation - Internal ledger allocating digital assets held on each DLA to specified clients (multiple clients' ownership of digital assets across multiple DLAs) at custodian level (no allocation on the DL itself)	2
	Proprietary and client digital assets pooled in one or several DLAs	Same allocation options as for models 1 and 2, but with custodian pooling digital assets held for own account with those held for the account of its clients	1P / 2P
Allocated DLAs	One or several DLAs for each client (and no more than one client per DLA)	Internal ledger allocating each DLA to a single client	3
Sub-custody	Digital assets held with a third party sub-custodian	Sub-custody pool allocation at custodian level (internal ledger), and various models possible at sub-custodian level, depending in particular on the jurisdictions involved (see models 1 – 3 above)	4
Private DLAs	One or several DLAs for each client, with PKs controlled by the client exclusively	Non-custodial wallet provider model, no custody services provided	5

The choice of a custody model has legal, technical, and accounting implications as related to the storage and processing of digital assets under custody.

These accounting consequences notably depend on:

A. the legal characterization and types of digital assets concerned (such as cryptocurrencies, claims, securities, and other financial instruments), as well as

B. the type of custodian (such as regulated as a bank or securities firm, or non-regulated custodian).

For custody models 1 to 3, it is assumed here that the PKs for each DLA are controlled exclusively by the custodian (or the sub-custodian), although a shared PK control model is possible and has been observed in practice for custody infrastructure implementations similar to model 3 (*i.e.*, where the client has some, but not a full, degree of control over PKs).

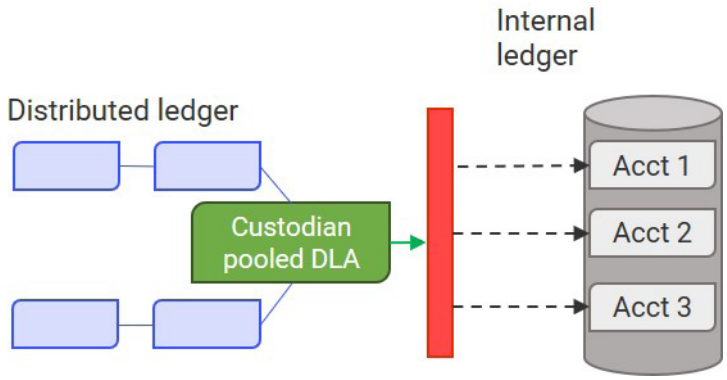
Models 4 and 5 do not involve PK custody operations by the service provider, and model 5 involves no custody at all. These custody models are mentioned for the sake of completeness only and are not discussed in more detail here.

Models 1 – 3 (which involve digital assets custody operations) may be described as follows:

2.2.1 Model 1

In this pooling model, the digital assets are custodied on DLAs created and controlled by the custodian. The PKs corresponding to such DLAs are controlled exclusively by the custodian.

The diagram below illustrates that logic, where the distributed ledger may be a blockchain, the green square is one address controlled by the custodian, and the internal ledger is an off-chain database (the red bar represents the interface between on-chain and off-chain components, typically involving various middleware components).



An internal ledger is maintained by the custodian to track the various DLAs, and match the DLA activity and balance with the financial client accounts. In particular, the internal ledger keeps track of the digital assets held for client accounts in the global pool (pool-level allocation), and of the balance of each client account, which includes the custodian's client accounting infrastructure. Digital assets may in fact be credited by the custodian to the client's "account" within such an internal ledger. However, there is no specific link or allocation of a particular DLA and/or of certain specified digital assets to a particular client. This means that the allocation of digital asset balances to clients exists only on the internal ledger, but not on the custodian's DLAs.

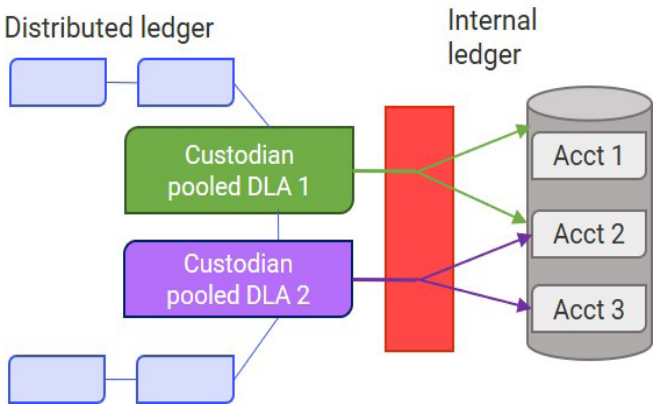
The pool-level allocation may be extended to include digital assets held by the custodian with sub-custodians within the "pool", so that the internal ledger allocation is global across the model 1 pool combined with the sub-custody pool (model 4).

2.2.2 Model 2

In the type 2 pooling model, the digital assets are custodied on DLAs created and controlled by the custodian. The corresponding PKs are controlled exclusively by the custodian. Both model 2 and model 1 contemplate a pooling of assets. The distinctive factor is that, in model 2, the internal ledger allocates the digital assets credited on each DLA to one or several clients (DLA level allocation) and not only a general allocation at pool level as is the case in model 1.

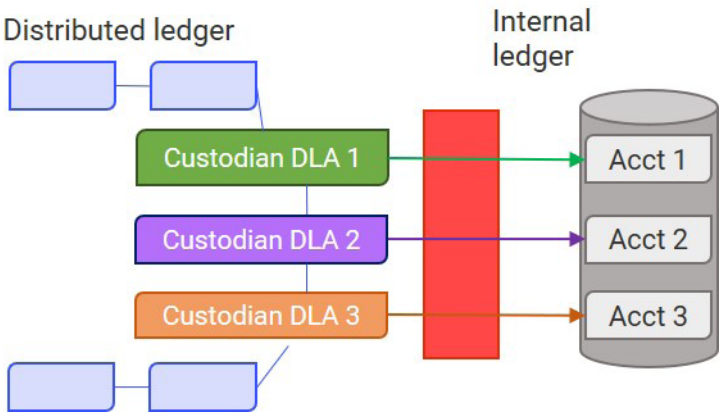
In a situation where a single pooled DLA is maintained by the custodian for a particular type of digital asset, models 1 and 2 are in practice equivalent.

The diagram below illustrates that logic, showing a mapping between the on-chain addresses ("Custodian DLA") and internal accounting ("Acct").



2.2.3 Model 3

In this model, each custodian-controlled DLA is allocated to a single client via an internal ledger maintained by the custodian. There is consequently no pooling of clients' assets, and a direct link can be made between the DLA and the client account. The PKs are either controlled exclusively by the custodian, or control is shared by the custodian and the client. This may be the case when threshold signature schemes or other forms of multi-party computation methods (see § 2.3 below) are used.



§ 2.3 IMPLICATIONS OF THE CHOICE OF A CUSTODY MODEL

The selection of one or more of the custody models outlined above can have legal and regulatory implications, depending on the digital assets concerned and the regulatory regime applicable to the custodian. The DACS does not address those implications. Each custodian should identify their preferred model(s) considering the manner in which they intend to structure their custody service offering and the regulatory regime that applies to them.

Note that models other than the ones described here may be implemented, for example those involving shared control of a DLA or of PKs via methods involving multi-signatures, multi-party signing, aggregate or threshold signature mechanisms and/or other multi-party computation methods (**MPC**). In such situations, it may be the case that no single entity or person has exclusive control over the DLA or the corresponding PKs, and as such is not the "custodian" of the relevant digital assets as per definition of this document. Such models are sometimes referred to as "partial custody".

The DACS is designed to be independent of the custody model.

3. DACS – REQUIREMENTS AND RECOMMENDATIONS

This section lists the DACS requirements and recommendations (RRs). These must be implemented while considering the technology in use in a particular organization, the environment in which the custody services are being provided, and the associated work products and documents. These RRs should be potentially applicable to all viable custody solutions, regardless of their unique internal components. Nonetheless, there might be situations where a given requirement or recommendation might prove non-applicable. The activities described in the RRs must be conducted by parties with adequate expertise and authority.

RRs are split into two streams: operations and infrastructure. The operational stream RRs mainly apply to the organization using a digital asset custody solution, as opposed to its vendor or service provider. The infrastructure stream RRs, however, are relevant to both the user and the provider.

For example, if a financial institution selects a vendor to provide a digital asset custody infrastructure that is to be operated by the financial institution itself, the financial institution will be responsible for ensuring that the operations stream RRs are complied with, while the vendor is expected to provide assurance that the infrastructure solution satisfies the infrastructure stream RRs.

OPERATIONS STREAM

§ 3.1 CHOICE OF CUSTODY MODEL

This section sets out key principles to apply when the operator is determining which type of custody model to adopt. Although this section does not apply to the non-custodial service providers responsible solely for the infrastructure without being involved in its operation, it is expected that vendors are in a position to indicate which custody models and operational restrictions their solution can support.

3.1.1 Requirements

MOD-00: Custody models available for a particular distributed ledger are reviewed according to the strategy and needs of the custody operator. The potential model is assessed and documented by the custodian in terms of business risk, security, and operational fitness. For example, the documentation might demonstrate that the custody model reflects the structure of the custody provider's activities and the nature and expectations of its clientele.

MOD-01: Third-party service providers to which all or part of custody operations are outsourced must not conflict with DACS requirements.

3.1.2 Recommendations

MOD-02: The results of the custody models assessment must be reviewed and updated at least annually and, in any case, before the introduction of new services.

MOD-03: When outsourcing asset custody to a third party, financial institutions must ensure that the infrastructure provider undergoes adequate security and risk assessments, such as technical penetration testing, SOC2 reports, and so on. The resulting reports must be reviewed and evaluated to ensure alignment with the organization's risk controls.

§ 3.2 TECHNICAL OPERATION

This section covers matters related to the operation of the custody solution by its end users. It is not directly relevant to a non-custodial service provider (vendor) providing only the custodial infrastructure without being involved in the operation thereof.

3.2.1 Requirements

OPS-00: A threat model tailored to the organization is created. It documents risks and characterizes with standard metrics such as likelihood and severity of impact. It details mitigation strategies for these risks.

OPS-01: Critical software components and services used during operations are identified, assessed and regularly updated to a recent version. Criticality is assessed and defined in a risk-based manner, in particular with respect to the risk of funds loss and theft.

OPS-02: Critical hardware IT components used during operations are identified, and their software is regularly updated. To the extent possible, external certifications support the security guarantees, for example NIST FIPS 140-3 or Common Criteria evaluations.

OPS-03: Secret values required to perform transaction operations (such as seeds or PKs for signing transactions, or exchanges' API keys), are stored and used in an environment with security controls preventing their unauthorized extraction. A permissible exception is when secret values are distributed through cryptographic means such as threshold signatures or other types of secret sharing.

OPS-03 is typically achieved via physical and logical isolation of these secrets' storage and usage from other less critical operations. Acceptable solutions include (but are not limited to) hardware security module devices, and trusted execution environments of server, desktop, or mobile platforms.

OPS-04: Access to the custody solution's interface requires authentication for each session, without shared accounts. This applies to both graphical user interface and to application programming interfaces (APIs).

Access is periodically reviewed and access rights which are no longer needed are revoked.

OPS-05: Access to administration capabilities of the solution and its components—both of hardware and software —is restricted to a minimal number of parties, and these are regularly reviewed for accuracy and compliance with the organization's risk model. Access rights are revoked if no longer required. Measures are in place to prevent a single person from having administration capabilities over critical software/hardware.

OPS-06: Execution of transactions or operations of a certain criticality level (beyond low-risk transactions or operations that may be automated) requires approval from at least two parties independently of each other. These can include a maker, who initiates the transaction, and an approver, who reviews, verifies, and authorizes the transaction details. Additional levels of authorization can be added where deemed necessary. To prevent unauthorized parties from becoming approvers, onboarding a new approving party requires several parties' review and approval.

OPS-07: All network communications over possibly untrusted networks are cryptographically protected and mutually authenticated, using for example TLS or other technology implementing a secure channel, with adequate configuration. Authentication may be performed via API tokens or cryptographic signatures, for example.

OPS-08: The software or hardware components storing secret values that are sufficient to perform critical operations are not internet-facing, but may be on an internal network where they are only reachable after proper security controls (typically authentication and authorization) have been enforced by another system.

OPS-09: All critical operations must be logged, with the logs retained for a sufficient duration to enable thorough review and detection of suspicious activities.

OPS-10: A process is defined to incontestably prove the control of the stored digital asset, and therefore the possession of the associated private keys. Such a proof of reserve (PoR) may be implemented via microtransactions (so-called "Satoshi test"), via a message signing system (designed in such a way that it cannot be abused to sign transactions), or off-chain legally binding records. See also Appendix A of CMTA's AML Standards for Financial Intermediaries (version September 2024).

OPS-11: Technical security controls are in place to detect technically suspicious activity and prevent abuse, fraud, and the compromise of the solution. Such controls might include whitelisting/blacklisting rules, rate limiting, authorized hours enforcement, auto-lock/reset, and time-lock.

OPS-12: Personnel involved in holding parts of a secret or involved in the operations of a custody service platform are screened regarding their criminal history and do not have relevant entries. They have received training and are fit and knowledgeable to perform their duties.

OPS-13: If secret keys (or shares thereof) are stored in external media storage, there is an inventory list documenting the content and location of the storage media, which is maintained by the custodian of the assets (and thus potentially by a subcustodian). This inventory is kept in a secure location and serves audit purposes.

OPS-14: Custody platform operators are responsible for conducting a due diligence on the clients to be onboarded. If the clients wish to transfer their own digital assets into the operator's ecosystem, a blockchain due diligence must be conducted, consisting of the analysis of the client wallets and last few transactions. This contributes to good standing with respect to Know-Your-Customer and Anti-Money Laundering rules.

OPS-15: The custody solution supplier and user have defined and enforce policies regarding change management, access management, vulnerability management, and patch management, which cover the custody solution and its environment.

OPS-16: Critical software components of the custody solution, as per OPS-01, are assessed at least annually for reliability and security by independent external specialists. These assessments can include source code security reviews, application penetration tests, and certification evaluations.

OPS-17: Critical technology components, as per OPS-02, are regularly updated with the latest available version of associated software (such as operating system, runtime, firmware, and SDK) to the extent possible. Exceptions may be justified for reasons of stability and interoperability if the security risk is properly assessed (notably with respect to security patches).

OPS-18: Any processes regarding digital asset handling are reviewed and approved by management of the party in charge of custody of the client DLA PKs. Any changes go through the standard change management process and require review and approval before being implemented.

3.2.2 Recommendations

OPS-19: It is not possible to access high-privileged capabilities of the custody system without additional security measures such as multi-factor authentication or approval through a quorum. Other appropriate security controls may be acceptable to restrict access to user capabilities. The definition of high-privileged access depends on the custody provider and can be found as “admin” or “super-admin”, for example.

OPS-20: Access to critical information (such as client data) and to critical operations (such as transaction creation) via APIs requires explicit authorization and authentication, as typically enforced via per-account authentication tokens or public keys. Such authorizations are subject to reasonable time limitations, for example via a token’s time-to-live parameter or a certificate’s expiration date.

OPS-21: Credentials required to access or use the custody management application or related components (such as passwords, PINs or PKs) are sufficiently protected from unauthorized access. Controls may include: storage encrypted on a physically separated infrastructure, quorum secret-sharing, multi-factor authentication.

OPS-22: Logs are adequately protected to prevent modification, addition or deletion. Any attempts at tampering should be logged. Logs must not include sensitive information such as passwords or PKs.

OPS-23: Critical security controls (transaction authorization, policy engine) are enforced in a trusted execution environment, such as a secure enclave, a dedicated hardened operating system, or a HSM.

OPS-24: All operations can be temporarily suspended at any time via a dedicated mechanism, for example in case of a suspected security incident.

OPS-25: Validation of transaction data and metadata is performed by different parties on different platforms (such as, different hardware and/or operating system).

OPS-26: Human visual validation of transaction data and metadata relies on a display system hardened to ensure the integrity of the data presented. In other words, controls enforce that the data displayed is the same data processed by the underlying computer program and process. Such technologies may include or be similar to Intel Secure Display or HDCP, and may be bespoke implementations in embedded devices.

INFRASTRUCTURE STREAM

§ 3.3 GENERATING SECRETS

This section covers the security aspects related to the generation of cryptographic secrets, typically seeds or PKs, which are being referred to here as “keys” for simplicity. The primary objective of the custody provider is to ensure a high level of assurance in the following areas: the secrets generation process, maintaining the secrecy of the generated values, and minimizing the risk of permanent loss of these secrets.

The term “key ceremony” refers to the procedure during which secrets are generated and back-ups are created. Different custody solutions might require different types of key ceremonies, but any solution must generate secrets and back-ups thereof.

Systems using multi-party (threshold) signatures must ensure that secrets (and their shares) are generated in a way that minimizes the risk of unauthorized access. Such generation may be centralized or carried out via a distributed key generation protocol (DKG).

3.3.1 Requirements

GEN-00: Secrets are only generated using a cryptographic random or pseudo-random generator whose internal logic (algorithm, entropy sources) is known and documented. Security assurance is provided via third-party security assessments and/or compliance with a reliable standard.

GEN-01: The entropy sources of the pseudo-random generator are identified and there is a way to estimate the minimal entropy of the generator when creating the secrets to ensure that it is high enough.

For example, for generating PKs for Bitcoin or Ethereum, which are 256-bit scalar values that should be uniformly distributed, a minimum of 256 bits of entropy is required in theory.

GEN-02: The key ceremony protocol is documented with sufficient details so that it can be performed by persons familiar with digital assets and related technological tools and possessing the required equipment.

GEN-03: Secrets from which signing keys are derived are only generated during a key ceremony executed as per the approved process.

GEN-04: Critical software components used during a key ceremony are identified, their internal logic is known and documented, and they are used in their latest stable version available, to the extent possible. Critical software may include software components running on an embedded platform, such as a HSM or a mobile phone.

GEN-05: Critical hardware components used during a key ceremony are identified, and hardware dedicated to key ceremonies (such as laptop or printer) are specifically acquired and configured for key ceremonies. The chain of custody is controlled by the party conducting the key ceremony.

GEN-06: During a key ceremony, from the moment that an electronic device interacts with secrets, it is kept disconnected from any system that is not involved in the key ceremony operations and resulting architecture (such as wireless peripherals or online services not required for the ceremony).

GEN-07: Secrets generated during the key ceremony, such as signing keys or seeds, are never visually exposed

to the ceremony participants.

It may be accepted that a share of keys or seeds, as created for multi-party signing or back-up, be visually exposed only to the party controlling that value.

GEN-08: Copies of the keys or related sensitive values (such as shares and back-ups) held temporarily on a device (such as external storage media, or laptop) are securely erased before the end of the ceremony (except for media used for back-up purposes). Measures are taken to prevent extraction from RAM or other temporary system memory.

Secure, permanent erasure depends on the storage technology used.

GEN-09: A report is created after a key ceremony, that includes the identities of the persons involved, their respective roles and responsibilities, a list of the components used (software, hardware, and their version numbers), a list of operations performed, and any deviation from the documented protocol.

3.3.2 Recommendations

GEN-10: The source code of the software used for generating secrets can be inspected and audited.

GEN-11: The wireless receivers of electronic devices used during a key ceremony are physically disabled (for example, removed from their enclosure or unplugged).

§ 3.4 RECOVERING SECRETS

This section covers recovery processes, which are necessary to reconstruct secrets in case of loss, destruction, or unavailability of the main production system.

In the following, a **recovery component** is a physical item such as a storage media, portable computer, or piece of paper, that is used to store secrets or shares thereof. These pieces of data are called **recovery values**.

3.4.1 Requirements

REC-00: Recovery components are created during the key ceremony only.

REC-01: Procedures are defined so that no party or system can single-handedly recover recovery components and reconstruct or use the keys. This may for example be achieved via threshold secret-sharing and distributing shares across segregated sites. Without secret-sharing, additional procedures must be in place to prevent a single party from accessing the recovery value.

REC-02: The validity of recovery components is verified during the key ceremony. When secret-sharing is used, a verification step must validate that any valid combination of shares will yield the expected secret.

REC-03: The recovery process is documented and regularly tested in order to ensure that secrets can be reconstructed efficiently. The documentation is revised according to the test results.

Updating documentation can be crucial for situations in which a secret is reconstructed using a more recent version of a software utility than the version which was used to generate the secret. Using the more recent version of the software may not be compatible with the process initially documented.

REC-04: Dedicated disaster recovery and business continuity plans have been created and documented for the custody solution, and these cover the process for recovering secrets.

3.4.2 Recommendations

REC-05: Recovery components are stored on multiple physical sites distinct from that of the operations site (i.e., the place where the secrets are stored and used). Said sites must have adequate security controls to detect and prevent unauthorized access to the recovery components, physical or logical.

Multiple physical sites should be understood as different buildings, or different cities, rather than different rooms or different safes. In this context, logical access means capability to infer the recovery components, for example using credentials such as a passphrase, certificate, or cryptographic key.

REC-06: Recovery values are computed using a quorum model (such as a threshold secret-sharing, or other equivalent mechanism in terms of access and confidentiality distribution) requiring at least two parties to reconstruct the secret.

REC-07: Recovery values are stored separately (that is, on different recovery components) for different secrets, in such a way that access to a recovery component for one secret does not entail access to that of another secret.

REC-08: Recovery values are stored on at least two types of media, typically, an electronic and non-electronic component, such as flash memory and a sheet of paper. This mitigates the risk of loss related to the physical or electronic nature of the media.

REC-09: Integrity of the recovery components is regularly verified and access is monitored, logged and periodically reviewed. Tamper-evident containers (such as security bags or sealed envelopes) should be used to ensure that recovery values have not been modified.

§ 3.5 DEVELOPMENT AND MAINTENANCE

This section covers matters related to the development and maintenance of the custody solution, to minimize the risk of introducing a security weakness into the system, be it by accident or by malicious intent. This is achieved via preventive and detective measures, by distributing trust, enforcing a high quality level, and by accountability and transparency measures.

3.5.1 Requirements

DEV-00: Permission to modify the source code, configuration, documentation, and other critical components of the solution is granted on a need-to-know basis and is subject to an audit trail.

DEV-01: Access to the source code, configuration, documentation, and other critical components of the solution from the internet requires two-factor authentication.

DEV-02: Accesses are regularly reviewed in order to enforce need-to-know and avoid permission creep, be it for persons or service accounts. These reviews and the ensuing changes are documented.

DEV-03: Each change to a component of the system, in particular to its source code, is logged in a way that records the time of the operation and the person responsible for it. This may be achieved by version control systems such as git.

DEV-04: Third-party open-source components are identified and regularly checked for new known bugs and vulnerabilities.

DEV-05: Critical software components of the solution and related changes are subject to internal and external review and testing before being deployed in production.

DEV-06: Third-party security assessments are performed at least once a year on one or more critical components of the custody solution. Assessment reports include descriptions of any shortcoming identified, and mitigation measures are implemented and documented.

DEV-07: Persons in charge of the development of the solution (such as engineers or managers) do not have permanent access to production systems. This may only be overridden temporarily in emergency situations, and duly authorized, supervised, documented and logged.

3.5.2 Recommendations

DEV-08: Critical software components, such as those interacting with secret values, or those performing security controls, undergo extended security controls compared to the other components (for example via third-party security assessments or formal certifications).

DEV-09: The development team implements a documented secure software development lifecycle and employs at least one employee in charge of security. Said lifecycle may include automated security testing and vulnerability discovery methods.

DEV-10: Security assessments performed as required in DEV-06 include both security assessments of critical components (for example, of proprietary cryptographic code) and “red team” tests covering the whole solution’s attack surface.

APPENDIX A - GLOSSARY

Term	Definition
Administration capabilities	The technical ability to make major changes to a system. Also sometimes referred to as “administrative privileges”.
API	Application programming interface, i.e., computer functionality allowing two systems to communicate.
CMTA	Capital Markets and Technology Association
DACS	CMTA’s Digital Assets Custody Standard
Digital assets	Any type of financial assets, whether natively digital or digitized, issued using DLT such as payment tokens (incl. cryptocurrencies), utility tokens and tokens representing securities.
Distributed ledger (DL)	A database that is consensually shared and synchronized according to a protocol by nodes participating in a peer-to-peer decentralized network. It allows transactions to have public “witnesses” who can access the records shared across the network and can each store an identical copy of it. Any changes or additions made to the ledger are reflected and copied to all nodes. One form of distributed ledger design is the blockchain, which can be either public, permissioned or private.
Distributed ledger technology (DLT)	Technology recording and sharing data across multiple data stores (or ledgers). This technology allows for transactions and data to be recorded, shared, and synchronized across a distributed network of different network participants.
DLA	Distributed ledger account, or address, being a unique identifier on a specified DL that serves as a virtual location for recording incoming and outgoing transactions in one or several digital assets.
Entropy	Computer-collected randomness. The reference to a «collection» process is because computers cannot – strictly speaking – generate random inputs but will use seemingly insignificant data to emulate randomness, e.g. by measuring the timing between mouse movements or system temperature. A secret key generated from a source with entropy of X bits or more means that “guessing” the key would take of the order of 2X operations.
HSM	Hardware security module, a secure crypto processor focused on managing cryptographic keys and which provides additional features such as accelerated cryptographic operations and execution of application-specific code.
Internal ledger	The internal ledger is a private database maintained by the custodian to allocate the balances of each DLA controlled by the custodian to one or many clients or accounts, so that in the books and records of the custodian, either (i) the assets credited on a DLA can be individually allocated to a client or account, or (ii) where the assets on a DLA are allocated to a group of clients or accounts (pool), the share of each client or account in the pool may be clearly determined.
Key ceremony	Procedure whereby secrets are generated in a way that ensures their cryptographic strength and minimizes the risk of leakage or sabotage. A key ceremony typically involves the creation of back-up values.

MPC	Multi-party computation methods, mainly multi-party threshold signatures protocols, in the context of digital assets.
PK	Private key.
PoR	Proof-of-reserve, i.e., proof that the custodian controls the assets that it claims to hold. Such a PoR cannot demonstrate the exclusive control, or the absence of copies of the keys.
Recovery component	Information or value stored on a media, or a (tamper-evident) hardware component that can be used to reconstruct the secret generated during a key ceremony.
RRs	In the context of DACS, requirements and recommendations.
Recovery values	Back-ups of keys, typically as shares stored on physical items such as a storage media, portable computer, piece of paper.
SDK	Software Development Kit.
Seed	The master key, sometimes inadequately called “entropy”, from which signing keys and addresses are derived, typically following an open standard such as BIP32 or SLIP10.
TLS	Transport Layer Security, standard cryptographic protocol for secure communications over computer networks.
Threshold secret-sharing	A method that involves splitting a secret into multiple parts and requiring a designated minimum number of parts for the secret to be unlocked.
Threshold signature	A method that involves splitting a PK into multiple parts and requiring a designated minimum number of parts for a signature to be jointly issued.
Two-factor authentication	A method for confirming a user’s claimed identity or access rights by using a combination of two factors (e.g., a password and a confirmation sent through a mobile device).

APPENDIX B - CHANGES TO THE DACS

Date	Description
May 2025	Review by CMTA's Technical Committee in consultation with CMTA members resulting in the following changes: • addition of paragraphs clarifying the diagrams of custody models 1 and 2; • clarification of language used in the Introduction and numerous RRs; • the content of the following RRs in particular (but not exclusively) has been expanded: OPS-01, OPS-06, OPS-07, OPS-10, OPS-21, OPS-23, GEN-07, REC-03, DEV-02; and • addition of RRs OPS-25 and OPS-26.
March 2023	Review by CMTA stakeholders and update according to new developments in the custody space (especially MPC-based solutions). Moved some controls from recommendations to requirements according to discussions within the group. Improved the wording of requirements to make them more auditable, with respect to the DACS certification. General clean-up and clarification changes to language.
October 2020	Original version of DACS published.