cmta.

Digital Assets Custody Standard

March 2023

Digital Assets Custody Standard

Version: 2.0
Adopted: March 1, 2023

Capital Markets and Technology Association
Route de Chêne 30
1208 Genève

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. In the context of digital assets, the following may be classified as secrets: seeds (or "master keys") from which addresses and key pairs are derived, and direct account PKs. A digital asset custody solution system can involve both software and hardware components, and is operated, at least partially, through manual 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 are relevant for the operator of a digital asset custody solution. An operator is contrasted with a pure infrastructure solution provider, who supplies the infrastructure to custody digital assets, but is not involved in the operation of the solution. The security aspects of the infrastructure stream RRs are relevant for the operator and/or digital asset custody solution provider (if different). The RRs can be technical, procedural, or a combination of both. It is intended that the DACS be updated and supplemented regularly to account for the various alternatives that emerge and are brought to the CMTA's attention.

Among the potentially critical aspects mostly left out of the scope of the DACS are procedural and physical security concerns, security of the underlying IT and software components, security of the hardware components, as well as traceability and accountability concerns. This boundary is set in order to restrict the DACS' scope to the components unique to a digital asset custody solution.

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 CERTIFICATION MARK

The CMTA has created a certification process to offer organizations using a custody solution the opportunity to undergo an audit certifying that they satisfy the DACS requirements. Such audits are performed by recognized auditor firms delivering a formal report. Such audits assess implemented security controls against selected DACS requirements and recommendations.

Documentation about the DACS certification process are available in a separate document.

§ 1.4 DISCLAIMER

Sole adherence to the DACS cannot guarantee the security of a custody solution, let alone that of its operations, for 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. This contrasts with security certifications of hardware components (such as Common Criteria or FIPS 140-2 and 140-3), for which security can be more easily characterized. Each institution is therefore responsible for properly integrating the DACS as a component of its risk management process. Likewise, the DACS does not comprehensively cover all the risk aspects of digital asset custody. For example, blockchain connectivity, "gas" management, and smart contract governance are not covered by the DACS.

§ 1.5 TECHNICAL TERMS | DEFINITIONS

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

§ 1.6 REVISIONS, ADDITIONS AND UPDATES

Although the core of the DACS aims to be technology-neutral to all possible extents, it needs to be practical. The CMTA may therefore periodically proceed to make and publish revisions, additions or updates.

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

Banks and other financial institutions can operate self-custody solutions, whereby a technology solution is developed, built, controlled and operated by the institution in order to manage multiple digital ledger accounts (**DLAs**). The next section describes different DLA management models and their properties.

Not all organizations are in a position to develop, maintain, and operate a self-custody infrastructure for digital assets. Institutional investors such as collective investment schemes or asset managers are generally required by law to work with third party custodians or infrastructure service providers that meet certain requirements when dealing with client assets. As a result, self-custody is often not viable for those financial firms.

Financial institutions need to know the organizations that are safekeeping their clients' digital assets. They must in particular know how the relevant custodians are protecting the secrecy and integrity of cryptographic secrets, such as PKs.

§ 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).

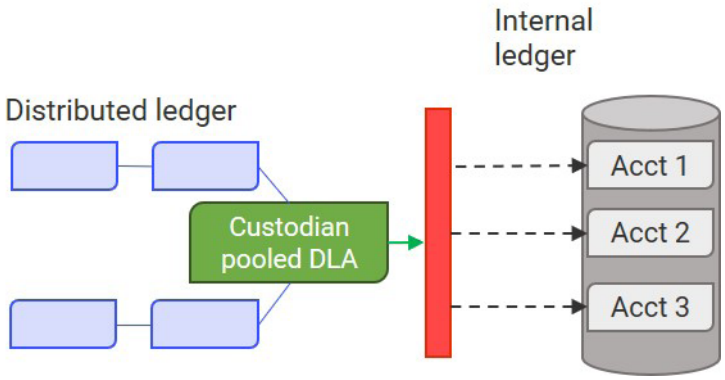
For custody models 1 to 3, it is assumed here that the PKs for each DLA are controlled exclusively by the custodian (or the sub-custodian), although a shared PK control model is possible and has been observed in practice for custody infrastructure implementations similar to model 3 (*i.e.*, where the 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.



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.

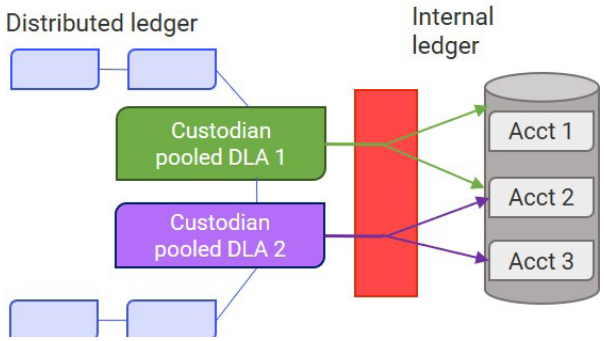
The pool-level allocation may be extended to include digital assets held by the custodian with sub-custodians within the "pool", so that the internal ledger allocation is global across the model 1 pool combined with the sub-custody pool (model 4).

This model is similar to the one adopted by banks and securities firms for holding financial instruments on behalf of clients where multiple sub-custodians (or multiple accounts with a single sub-custodian) are used for the same financial instrument. In practice, for operational reasons, the custody of digital assets is generally rather based on model 2 (see below).

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.

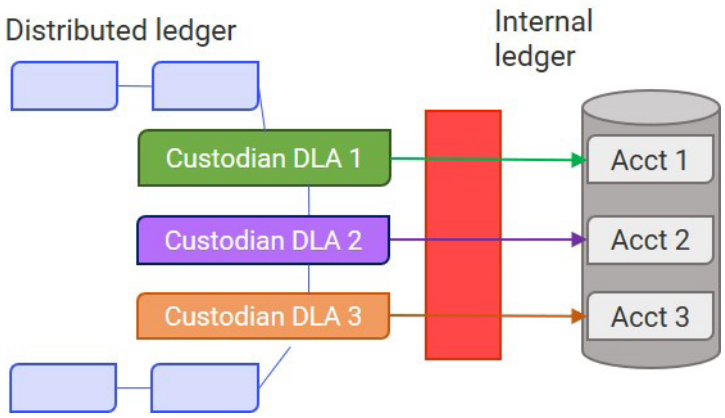
In a situation where a single pooled DLA is maintained by the custodian for a particular type of digital asset, models 1 and 2 are in practice equivalent.



This model is similar to the one used by banks and securities firms for holding financial instruments on behalf of clients in situations where only one single sub-custodian is used for one particular financial instrument (or type of financial instrument) or designated pooled accounts are being used with one particular sub-custodian (*e.g.* pooled accounts held by a Swiss bank or securities firm with a U.S. central custodian).

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, in principle, custody model agnostic, insofar as in its current iteration, it focuses on RRs from a security perspective.

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 operations stream is relevant only for the operator of a custody solution, whereas the infrastructure stream is relevant both for the operator and the non-custodial service provider supplying the infrastructure (if these are different entities). 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 by the organization acting as a custodian in terms of business risk, security, and operational fitness, and this review is documented. 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 delegated must comply with the DACS. Ensuring this compliance is generally the duty of the outsourcing party, unless otherwise specified.

3.1.2 Recommendations

MOD-02: Custody models' assessment results are reviewed and updated at least on an annual basis and in any event prior to the launch of new services.

MOD-03: If outsourcing the custody of assets to a third party, financial institutions ensure that the infrastructure provider undergoes periodic security assessments (*e.g.*, via compliance audits and penetration testing). The audit report is reviewed and evaluated with respect to the risk controls of the organization.

§ 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.

OPS-02: Critical hardware components used during operations are identified and regularly updated. To the extent possible, external certifications are obtained to ensure compliance with standards, for example those set by NIST (FIPS 140-3).

OPS-03: Secret values that are sufficient to perform critical operations (such as seeds or PKs for signing

transactions, or critical authentication tokens), are stored and used in an environment with security controls in place to prevent 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.

Protecting secrets as per OPS-03 is typically achieved by using a component offering the physical and logical isolation of these secrets and of computations involving these. Acceptable solutions include (but are not limited to) hardware security module devices, smart-card-based systems, or trusted execution environments of server, desktop, or mobile platforms.

OPS-04: Access to the custody solution's interface is enabled through individual access control lists and requires authentication for each session. 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 (as opposed to any user), and administration user rights 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 ensure that no single person has control over critical software/hardware functions or components.

OPS-06: Execution of transactions or operations (other than *de minimis* transactions or operations) requires approval from at least two parties independently of each other. These approvers are, whenever possible, in different lines of service. 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.

Note that this OPS-07 may not be feasible at the edge of the system, if transactions are sent to a permissionless network that, by definition, does not require authentication other than the signature of transactions.

OPS-08: The software or hardware components persistently storing secret values that are sufficient to perform critical operations (such as seeds or PKs for signing transactions, or critical authentication tokens) 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 significant operations are logged, and the logs are retained for a sufficient period of time to allow their review for suspicious activities.

OPS-10: A process is defined to create a proof-of-reserve (**PoR**) for all or a subset of the digital assets stored. Such a PoR aims to incontestably prove the existence of funds and establish the ownership of the keys tied to a given digital asset account or group thereof. A PoR may for example be implemented via microtransactions (so-called "Satoshi test"), or via a message signing system (designed in such a way that it cannot be abused to sign transactions).

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, time-lock, and so on.

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. Compliance with OPS-12 needs to be reassessed regularly (in principle annually).

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: Each of the relevant parties has defined and enforces 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 should include source code audits and application penetration tests conducted on the relevant components.

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 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 Application Programming Interfaces (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 not stored in clear (i.e. plaintext and not accessible without high-privilege access rights or further authentication) on the systems accessing the application. Instead, these may be accessed via a separate software vault or hardware token.

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

OPS-23: Critical security controls 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.

INFRASTRUCTURE STREAM

§ 3.3 GENERATING SECRETS

This section covers the security aspects related to the generation of cryptographic secrets, typically seeds or PKs, which we will be referring to as "keys" for simplicity. The overall objective for the custody provider shall be to demonstrate high enough assurance on the process of generating secrets, on the secrecy of the values generated throughout, and on the measures taken to minimize the risk of permanent loss of the secrets.

The following RRs do not aim to cover all security aspects of a key ceremony procedure but instead focus on the secrets' security in terms of confidentiality, integrity, and recoverability.

The term "key ceremony" refers here to the procedure during which secrets are securely generated, in a safe environment, under supervision of trusted parties. Different custody solutions might require different types of key ceremonies, but any solution must inevitably generate secrets, as well as create recovery values and store them on multiple media and/or in multiple locations.

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

3.3.1 Requirements

GEN-00: Secrets are generated using a cryptographic random or pseudo-random generator whose internal logic (algorithm, entropy sources) is known and documented. Security assurance is provided by factors including at least one of the following: external security assessments, compliance with a reliable standard, or other factual evidence that the pseudo-random generator is an established kind that withstood attacks in a real, hostile environment.

GEN-01: The entropy sources of the pseudo-random generator are identified and there is at least a heuristical way to quantify the minimal entropy of the generator when creating the secrets and to ensure that it is high enough to generate secure keys.

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) have been specifically acquired for the purpose of key ceremonies. The chain of custody of the hardware has not been broken and access is continually controlled by the party conducting the key ceremony. Note that hardware components (such as HSMs) may be used in production before and after a 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 playing no role in the ceremony). Authorized connections may include services accessed over internet.

GEN-07: For single-signature schemes (as opposed to multi-signature schemes), secrets and other information pertaining to the secrets generated during the key ceremony, are never visually exposed to the ceremony participants.

It is however tolerated, in order to allow back-ups in different forms, that secret values related to multi-signature or threshold secret-sharing be visually exposed to authorized parties, such as for example a key custodian. This is tolerated as long as no single person has visual access to more key information than they would during normal operation of the system.

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) iare 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 erasure aims to prevent a person or computer program from reconstructing said data after the ceremony, and typically requires techniques erasing the data multiple times and overwriting with unrelated values in order to prevent recovery from memory.

GEN-09: A report is created after a key ceremony, including at least 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. This document is kept safe and serves the purpose of traceability and auditability of the process.

3.3.2 Recommendations

GEN-10: The source code, or at least the binary code, of the random or pseudo-random generator used for generating secrets is available for inspection during security assessments.

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

Processes for recovering secrets must be in place to reconstruct the secrets generated in case of loss, destruction, or unavailability of the medium used for normal operations. As the RRs below emphasize, the mechanism for recovering secrets should be designed in such a way that no single party can recover one or more secrets, and in a way that reduces the risk of permanent loss.

In the following, a **secret-recovery component** (or just recovery component) is a physical item such as a storage media, portable computer or piece of paper which is used to store data that can be used to reconstruct one or more of the secrets generated during a key ceremony. These pieces of data are called recovery values.

3.4.1 Requirements

REC-00: Recovery components are created during the key ceremony only. After the key ceremony, recovery components may only be handled with adequate protection in terms of confidentiality and integrity.

REC-01: Procedures are defined so that no party or system can single-handedly recover the components and reconstruct or use the generated keys following the ceremony. This may for example be achieved via threshold secret-sharing and distributing shares across segregated sites. In cases where no secret sharing is used, and a single recovery component contains one or more keys, additional procedures must be in place to prevent any single person from accessing the recovery components.

REC-02: The validity of all recovery components is verified during the key ceremony in which they are created. In particular, when secret sharing is used, a verification step must ensure that any valid combination of shares will yield the expected secret.

REC-03: The recovery process is documented and accessible to the responsible party. It shall be regularly reviewed and tested in order to ensure that secrets can be reconstructed as needed. The involved individuals receive training on how to proceed in the case of a recovery. The documentation is kept up to date.

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 in order to detect and prevent unauthorized (physical and logical) access to the recovery components.

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.

This implies that a dedicated storage media may be used for each single secret component. In the case that multiple secret components are stored on the same media, different credentials are required to access each individual component. If, for example, ten independent secrets are to be protected with five recovery components each, then fifty storage media units are necessary, which may be inconvenient and error prone.

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 paper. This is to mitigate the risk of loss related to the unique 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, most notably in order to minimize the risk of introducing a security weakness into the system, be it by accident or by malicious intent. This is performed by ensuring that appropriate preventive and detective measures are in place, by distributing trust, ensuring a high level of quality, and by guaranteeing an adequate level of transparency.

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 documented in an audit trail.

If the custody provider's source code is partially open-source (for example in a public GitHub repository), DEV-00 entails specific controls in order to accept changes made or requested by third parties.

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

DEV-02: Access control lists or other permissions are regularly reviewed by responsible persons and adapted in order to minimize permission creep, be it for persons or service accounts. The review of these accounts is adequately documented.

DEV-03: To the extent possible, 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 is typically achieved by modern version control systems such as git.

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

DEV-05: Critical software components of the solution and related changes are subject to internal and/or

external review and testing before being deployed in production. Said reviews (such as source code reviews, or automated testing) are documented.

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, have enhanced security assurance (for example via third-party security assessments or formal certifications), especially if the source code is not available for inspection by their users.

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 focused audits of critical components (for example, of proprietary cryptographic code) and “red team” audits 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 to 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 PK with an entropy of X bits means that the PK is as strong as a string of X bits chosen randomly.
HSM	Hardware security module: a secure crypto processor focused on generating cryptographic keys and which provides accelerated cryptographic operations by means of these keys.
Internal ledger	The internal ledger is in substance 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 includes other operations such as loading software components into trusted hardware.

MPC	Multi-party computation methods, such as multi-signatures, multi-party signing, aggregate or threshold signature mechanisms.
PK	Private key.
PoR	Proof-of-reservce, *i.e.* proof that the custodian holds the assets it claims to hold.
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	DACS' requirements and recommendations.
Recovery values	Physical item such as storage media, portable computer, piece of paper, which is used to store data that can be used to reconstrucut one or more secrets.
SDK	Software Development Kit.
Seed	An input (typically taking the form of text) used to generate a public / private key pair.
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).
User capabilities	The technical ability to use the functions allocated to (a group or all) users.

APPENDIX B - DACS VERSIONS

Version	Date	Description
V2	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.
V1	October 2020	Original version of DACS published.