MACS – Minimum Acceptable Crypto Standard

Core Framework v1.0

Authoritative English Translation

Notice
This English version is an authoritative translation of the German original of the *MACS Core v1.0*.
In case of divergence or ambiguity, the German version shall prevail.

1. Purpose

The **Minimum Acceptable Crypto Standard (MACS)** defines the **minimum organizational, decision-related and documentation requirements** that an organization must fulfill in order for its handling of cryptographically secured digital assets **not to be considered negligent**.

MACS exclusively addresses the **governance and responsibility layer**.
It makes **no statement** regarding the economic attractiveness, technical design or legal permissibility of specific use cases.

MACS presupposes that the handling of cryptographically secured digital assets complies with the **applicable legal and regulatory framework**.

2. Definitions

For the purposes of MACS, **cryptographically secured digital assets** are digital units

- whose disposition, transfer or control is based on cryptographic mechanisms, and
- whose **power of disposal** may lie wholly or partially with the organization itself or with third parties.

The term encompasses all manifestations regardless of technical implementation, form of issuance, degree of centralization or economic classification.

3. Scope of Application

MACS applies to all organizations that, with respect to cryptographically secured digital assets:

- hold, hold in custody, acquire, dispose of,
- transfer, accept, issue,
- lend, pledge, or
- otherwise exercise economic power of disposal over them,

as well as to organizations that deliberately prepare themselves strategically for such use.

The scope of application is independent of:

- whether the technical implementation is carried out internally or by third parties,
- whether transactions actually take place or not,
- whether the assets are recognized on the balance sheet.

A deliberate decision **not** to use such assets is explicitly also within the scope of application.

4. Guiding Principles

The handling of cryptographically secured digital assets is considered acceptable only if **all** of the following principles are met:

1. **Explicit Decision-Making**
   The use or non-use is the result of a deliberate decision and is documented in a verifiable manner.
2. **Clear Allocation of Responsibility**
   Responsibility for decisions and actions is clearly assigned.
3. **Segregation of Critical Functions**
   Decision-making, execution and control functions are organizationally segregated or safeguarded through documented compensating controls.
4. **Avoidance of Single Points of Failure**
   Critical access rights, information or decision-making authority do not depend exclusively on a single individual or **organizational entity**.
5. **Termination and Escalation Capability**
   The organization is at all times capable of terminating the use in an orderly manner.
6. **Management of Uncertainty and Competence Limitations**
   The manner in which knowledge, experience or competence limitations are addressed is defined.
7. **Explainability Towards Third Parties**
   Decisions and structures are explainable in a consistent manner to auditors, supervisory bodies and relevant stakeholders.

5. Core Requirements

An organization fulfills MACS only if **all** of the following requirements are **demonstrably implemented**:

5.1 Definition of the Decision Scope

The following matters are clearly defined and documented:

- whether cryptographically secured digital assets are used or not,
- for which purpose and intended benefit,
- which categories are, in principle, considered,
- which forms of use are excluded,
- which risks and trade-offs are deliberately accepted,
- which measures are implemented to mitigate risks or for which reasons risks are deliberately accepted.

5.2 Decision-Making and Role Model

The following are defined and implemented:

- a decision-making authority,
- an executing function,
- a controlling function,
- a designated substitute for each critical function.

The functions should be organizationally segregated.
Any combination of functions is permissible only if effective control and escalation mechanisms are documented.

5.3 Criticality and Failure Analysis

The organization has identified and assessed:

- critical individuals, access rights and information,
- plausible scenarios of failure, misuse and coercion,
- risks that are accepted,
- risks that are defined as not acceptable,
- dependencies on third parties or central organizational entities that may restrict or withdraw the power of disposal,
- scenarios involving loss of access, permanent unavailability or restrictions of the power of disposal.

The assessment is documented in a manner that is permanently available, comprehensible and reproducible for third parties.

5.4 Termination and Escalation Logic

The following are defined and implemented:

- specific events that trigger a termination,
- the competent decision-making authority in the event of termination,
- the prioritized sequence of actions.

The termination and escalation logic must be appropriate to the current design of use and is subject to ongoing review in the event of material changes.

Termination must not depend exclusively on a single individual.

5.5 Integration into Existing Organizational Processes

The organization has defined and implemented:

- how the handling of cryptographically secured digital assets is integrated into existing accounting, tax and organizational processes,
- how identified risks of unavailability or factual loss are incorporated into such processes,

or for which reasons such integration is currently not performed.

5.6 Documentation and Referencing

The organization is at all times able to consistently demonstrate:

- the internal framework under which it operates,
- the standard to which it refers,
- the version of that standard being applied.

5.7 Custody, Access and Loss Prevention

The organization has defined and demonstrably implemented:

- the form in which cryptographically secured digital assets are held in custody,
- who holds access rights and under which conditions such rights may be exercised,
- how it is ensured that effective and functional access to the assets exists,
- which measures have been implemented to prevent loss, permanent unavailability or unauthorized disposal.

The organization has assessed and documented:

- under which circumstances a factual loss, permanent unavailability or a non-recoverable restriction of the power of disposal may occur,
- how such scenarios are identified, mitigated or deliberately accepted.

The organization has documented:

- whether and to what extent protection against loss risks exists,
- for which reasons such protection exists or does not exist.

Cryptographically secured digital assets for which reliable access does not exist or whose power of disposal is permanently restricted are to be treated as risk-exposed and classified accordingly.

6. Subject Matter of MACS

MACS exclusively addresses:

- decision-making structures,
- responsibilities,
- risk, escalation and termination logic,
- minimum requirements for implementation, demonstrability and explainability

in the handling of cryptographically secured digital assets.

7. Further Development

- The MACS Core is technology- and asset-neutral.
- Specific requirements are addressed exclusively in **Annexes**.
- Amendments are versioned, traceable and transparent.

End of MACS Core v1.0 – Authoritative English Translation