MACS – Minimum Acceptable Crypto Standard

Core Framework v1.0

Deutsche Fassung (Master Version)

1. Zweck

Der **Minimum Acceptable Crypto Standard (MACS)** definiert die **organisatorischen, entscheidungsbezogenen und dokumentarischen Mindestanforderungen**, die eine Organisation erfüllen muss, damit ihr Umgang mit kryptografisch gesicherten digitalen Vermögenswerten **nicht als fahrlässig** einzustufen ist.

MACS adressiert ausschließlich die **Governance- und Verantwortungsebene**.
Er trifft **keine Aussage** zur wirtschaftlichen Attraktivität, zur technischen Ausgestaltung oder zur rechtlichen Zulässigkeit einzelner Anwendungsformen.

MACS setzt voraus, dass der Umgang mit kryptografisch gesicherten digitalen Vermögenswerten im Einklang mit den jeweils **anwendbaren gesetzlichen und regulatorischen Rahmenbedingungen** erfolgt.

2. Begriffsbestimmung

Im Sinne von MACS sind **kryptografisch gesicherte digitale Vermögenswerte** digitale Einheiten,

- deren Verfügung, Übertragung oder Kontrolle auf kryptografischen Verfahren beruht und
- deren Verfügungsmacht ganz oder teilweise bei der Organisation selbst oder bei Dritten liegen kann.

Der Begriff umfasst sämtliche Ausprägungen unabhängig von technischer Implementierung, Emissionsform, Zentralisierungsgrad oder wirtschaftlicher Einordnung.

3. Geltungsbereich

MACS gilt für alle Organisationen, die kryptografisch gesicherte digitale Vermögenswerte:

- halten, verwahren, erwerben, veräußern,
- übertragen, akzeptieren, emittieren,
- überlassen, beleihen oder
- anderweitig wirtschaftlich darüber verfügen,

sowie für Organisationen, die sich bewusst strategisch auf eine solche Nutzung vorbereiten.

Der Geltungsbereich ist unabhängig davon,

- ob die technische Umsetzung intern oder durch Dritte erfolgt,
- ob Transaktionen stattfinden oder nicht,
- ob eine bilanzielle Erfassung erfolgt.

Eine bewusste Nicht-Nutzung fällt ausdrücklich ebenfalls in den Geltungsbereich.

4. Leitprinzipien

Der Umgang mit kryptografisch gesicherten digitalen Vermögenswerten gilt nur dann als akzeptabel, wenn **alle** folgenden Prinzipien erfüllt sind:

1. **Explizite Entscheidung**
   Nutzung oder Nicht-Nutzung ist bewusst entschieden und nachweisbar dokumentiert.
2. **Zuweisung von Verantwortung**
   Verantwortung für Entscheidungen und Handlungen ist eindeutig zugeordnet.
3. **Trennung kritischer Funktionen**
   Entscheidungs-, Ausführungs- und Kontrollfunktionen sind organisatorisch getrennt oder durch dokumentierte Kompensationsmaßnahmen abgesichert.
4. **Vermeidung von Single Points of Failure**
   Kritische Zugriffe, Informationen oder Entscheidungsbefugnisse hängen nicht ausschließlich von einer einzelnen Person oder Stelle ab.
5. **Abbruch- und Eskalationsfähigkeit**
   Die Organisation ist jederzeit in der Lage, die Nutzung geordnet zu beenden.
6. **Umgang mit Unsicherheit und Kompetenzgrenzen**
   Der Umgang mit Wissens-, Erfahrungs- oder Kompetenzdefiziten ist festgelegt.
7. **Erklärbarkeit gegenüber Dritten**
   Entscheidungen und Strukturen sind gegenüber Prüfern, Aufsichtsorganen und relevanten Stakeholdern konsistent erklärbar.

5. Mindestanforderungen (Core Requirements)

Eine Organisation erfüllt MACS nur, wenn **alle** folgenden Anforderungen **nachweisbar umgesetzt** sind:

5.1 Festlegung des Entscheidungsgegenstands

Es ist eindeutig festgelegt und dokumentiert:

- ob kryptografisch gesicherte digitale Vermögenswerte genutzt werden oder nicht,
- zu welchem Zweck und Nutzen,
- welche Kategorien grundsätzlich in Betracht kommen,
- welche Nutzungsformen ausgeschlossen sind,
- welche Risiken und Zielkonflikte bewusst akzeptiert werden,
- welche Maßnahmen zur Risikobegrenzung ergriffen werden oder aus welchen Gründen Risiken bewusst akzeptiert werden.

5.2 Entscheidungs- und Rollenmodell

Es sind definiert und umgesetzt:

- eine entscheidungsbefugte Instanz,
- eine ausführende Funktion,
- eine kontrollierende Funktion,
- eine Stellvertretung für jede kritische Funktion.

Die Funktionen sollen organisatorisch getrennt werden.
Eine Zusammenlegung ist nur zulässig, wenn wirksame Kontroll- und Eskalationsmechanismen dokumentiert sind.

5.3 Kritikalitäts- und Ausfallanalyse

Die Organisation hat identifiziert und bewertet:

- kritische Personen, Zugriffe und Informationen,
- plausible Ausfall-, Missbrauchs- und Zwangsszenarien,
- Risiken, die akzeptiert werden,
- Risiken, die als nicht akzeptabel definiert sind,
- Abhängigkeiten von Dritten oder zentralen Stellen, die die Verfügungsmacht einschränken oder entziehen können,
- Szenarien des Zugriffsverlusts, der dauerhaften Unverfügbarkeit oder der Einschränkung der Verfügungsmacht.

Die Bewertung ist dauerhaft verfügbar, nachvollziehbar und gegenüber Dritten reproduzierbar dokumentiert.

5.4 Abbruch- und Eskalationslogik

Es sind festgelegt und umgesetzt:

- konkrete Ereignisse, die einen Abbruch auslösen,
- die zuständige Entscheidungsinstanz im Abbruchfall,
- die priorisierte Reihenfolge von Maßnahmen.

Die Abbruch- und Eskalationslogik muss der aktuellen Ausgestaltung der Nutzung angemessen sein und ist bei wesentlichen Änderungen fortlaufend zu überprüfen.

Der Abbruch darf nicht ausschließlich von einer Einzelperson abhängen.

5.5 Einordnung in bestehende Unternehmensprozesse

Die Organisation hat festgelegt und umgesetzt,

- wie der Umgang mit kryptografisch gesicherten digitalen Vermögenswerten in bestehende buchhalterische, steuerliche und organisatorische Prozesse eingeordnet ist,
- wie identifizierte Risiken der Unverfügbarkeit oder des faktischen Verlusts in diese Prozesse einbezogen werden,

oder aus welchen Gründen eine solche Einordnung derzeit nicht erfolgt.

5.6 Dokumentation und Referenzierbarkeit

Die Organisation kann jederzeit konsistent nachweisen:

- nach welchem internen Rahmen sie handelt,
- auf welchen Standard sie sich bezieht,
- welche Version dieses Standards angewendet wird.

5.7 Verwahrung, Zugriff und Verlustprävention (Custody)

Die Organisation hat festgelegt und nachweisbar umgesetzt:

- in welcher Form kryptografisch gesicherte digitale Vermögenswerte verwahrt werden,
- wer über Zugriffsrechte verfügt und unter welchen Voraussetzungen diese ausgeübt werden können,
- wie sichergestellt ist, dass ein tatsächlicher und funktionsfähiger Zugriff auf die Vermögenswerte besteht,
- welche Maßnahmen getroffen wurden, um Verlust, dauerhafte Unverfügbarkeit oder unautorisierte Verfügung zu verhindern.

Die Organisation hat bewertet und dokumentiert,

- unter welchen Umständen ein faktischer Verlust, eine dauerhafte Unverfügbarkeit oder eine nicht mehr behebbare Einschränkung der Verfügungsmacht eintreten kann,
- wie solche Szenarien erkannt, vermieden oder bewusst akzeptiert werden.

Die Organisation hat dokumentiert,

- ob und in welchem Umfang eine Absicherung gegen Verlustrisiken besteht,
- aus welchen Gründen eine solche Absicherung besteht oder nicht besteht.

Kryptografisch gesicherte digitale Vermögenswerte, auf die kein verlässlicher Zugriff besteht oder deren Verfügungsmacht dauerhaft eingeschränkt ist, sind als risikobehaftet zu behandeln und entsprechend einzuordnen.

6. Gegenstand von MACS

MACS adressiert ausschließlich:

- Entscheidungsstrukturen,
- Verantwortlichkeiten,
- Risiko-, Eskalations- und Abbruchlogiken,
- Mindestanforderungen an Umsetzung, Nachweisbarkeit und Erklärbarkeit

im Umgang mit kryptografisch gesicherten digitalen Vermögenswerten.

7. Weiterentwicklung

- Der MACS Core ist technologie- und asset-neutral.
- Spezifische Anforderungen werden ausschließlich in **Annexes** geregelt.
- Änderungen erfolgen versioniert, nachvollziehbar und transparent.

Ende MACS Core v1.0 – Deutsche Fassung