BaFin Audited Cardano Smart Contract for compliant Real World Asset Tokenization by NMKR, FluidTokens & IAMX

Date: 24.03.2024, Version: 1.0

Project ID	1100033
Link full project	https://projectcatalyst.io/funds/11/cardano-open-developers/bafin-audited-cardano-smart-contract-for-compliant-real-world-asset-tokenization-by-nmkr-fluidtokens-and-iamx
Challenge	F11: Cardano Open: Developers
Milestone 1	https://milestones.projectcatalyst.io/projects/1100033/milestones/1
Acceptance criteria Re 1 is part of this PDF	1. re legal analysis: a) Documentation of the mandatory information in the Crypto Securities Register eWpG. b) Documentation of the required data when subscribing to a crypto security and initial entry in the crypto securities register. c) Documentation of the required data collection when instructions are issued by authorized persons. Identification data of authorized and acquiring persons. d) In total you can expect about 10 pages in writing. Format: PDF. 2. re analysis current Cardano smart contracts a) What are the specific requirements based on the eWpG that Cardano smart contracts must meet? b) In total you can expect about 3 pages in writing. Format: PDF. 3. re project plan: a) Project plan, including timelines and resources for BaFin compliant Cardano Smart Contract under the Electronic Securities Act (eWpG). b) In total you can expect about 3 pages in writing. Format: PDF.

I. Introduction

A. Coverage Crypto Securities Register eWpG

The Crypto Securities Register under the German Electronic Securities Act (eWpG) is a legal framework established to facilitate the issuance, management, and transfer of electronic securities using distributed ledger technology (DLT) or similar electronic systems. The register is crucial for ensuring the legal recognition and enforceability of electronic securities under German law.

The Crypto Securities Register eWpG covers:
1. Issuance of Electronic Securities, eliminating the need for physical certificates, recording the creation of securities and their initial allocation to investors.
2. Tracking of Transfer of electronic securities between parties and ensuring that each transaction is recorded and ownership is clearly established and updated in real-time.
3. Legal Recognition by Entry in the Crypto Securities Register and therefore providing the same legal status as traditional paper-based securities.
4. Detailed information about the securities, including the issuer's identity, the rights and obligations attached to the securities, and any conditions related to their transfer or redemption.
5. KYC and AML Compliance.
6. Use of DLT or similar technology to ensure that the register is maintained in a transparent, secure, and tamper-proof manner, enhancing the integrity of the securities market.
7. Accessibility to authorized participants, such as investors and regulatory bodies, can access the necessary information in the register, ensuring transparency and facilitating oversight.

B. Temporal scope of Crypto Securities Register eWpG

The eWpG began on June 10, 2021, when the Act on the Introduction of Electronic Securities came into effect. Since then, the rules of the eWpG have been in use. Even though this is the start date, there's a part of the law (section 6, paragraph 3) that also affects securities that were issued before June 10, 2021. This means that securities created before this date can be turned into electronic securities.

C. Territorial scope of Crypto Securities Register eWpG

According to Section 32 (1), the eWpG is generally applicable insofar as the register-keeping entity in whose register the relevant security is entered is under supervision in Germany.
The issuer can be from a different jurisdiction.

D. Material scope Crypto Securities Register eWpG

The Crypto Securities Register eWpG applies to:

1. Bearer bonds [Schuldverschreibungen auf den Inhaber] such as
a) bonds [Anleihen]
b) mortgage bonds [Pfandbriefe]
c) profit participation certificates [Genussscheine]
d) warrants [Optionsscheine]
e) commercial Papers
f) certificates [Zertifikate]

Through a certificate, the investor gets the right to a one-time payment of money or delivery of securities at the end of its term.

The value of the debt represented by the certificate depends on the performance of its underlying asset, such as stocks of a specific company, indices, commodities, or currencies.
g) convertible bonds [Wandelschuldverschreibungen]
h) Investment fund shares [Investmentanteilsscheine] Reference: change to section 95 of the KAGB.
2. registered shares [Aktien, die auf den Namen lauten], and
3. shares made out to bearer if they are entered in a central register [Aktien, die auf den Inhaber lauten, wenn sie in einem zentralen Register eingetragen sind].

E. Transaction protection function and right to inspection
Under Section 10(1) of the eWpG, "participants" in the securities register are allowed to view it. Initially, this includes any holder, person with rights, or affected party (like the issuer) of a listed security. Potential buyers, however, are not automatically granted access. They only gain access by proving a "legitimate material interest" as potential register participants (Section 10(2) eWpG). The government notes that buyers and sellers can demonstrate this legitimate interest.
Access to the register mainly reveals information about the holder's anonymous identifier. According to Section 8(1) No. 2 eWpG, the holder can be a "natural or legal person who holds the electronic security for themselves (individual registration)." However, per Section 17(2) Sentence 2 eWpG, the register uses a pseudonymized identifier instead of specifying the holder as a natural or legal person. Therefore, the identity of the holder and those entitled remains concealed from potential buyers, safeguarding transaction security. One can only verify if the identifier (e.g., public address) given by the seller matches the register's details. But the register does not provide the holder's actual identity (see Section 10(3) eWpG). Only those who "show a special legitimate interest" (Section 10(3) eWpG), such as enforcing rights or claims, can get information on the holder's identity under strict conditions. Merely having an interest in purchasing is not enough to qualify.

F. Raise capital across the EU
The "passport rule" regarding financial prospectuses in the European Union (Prospectus Regulation (EU) 2017/1129) is a regulatory framework that allows a financial prospectus, once approved by the financial regulatory authority in one EU member state, to be recognized across all other EU member states without the need for further approvals. This rule is part of the EU's efforts to harmonize financial services and capital markets across its member states, making it easier for companies to raise capital across the EU. Once the prospectus sheet is approved by the regulatory authority in one EU member state, the company can use this approval to "passport" the prospectus to other EU countries. This means the company can offer the securities in any other EU member state without needing separate approvals from each country's regulators.

II. Documentation of the mandatory information in the Crypto Securities Register eWpG.
[Milestone Acceptance criteria: "1. re legal analysis: a) Documentation of the mandatory information in the Crypto Securities Register eWpG.]

1. Law
Source for the documentation of the mandatory information in the Crypto Securities Register eWpG is Section 17 eWpG: Entries in the Crypto Securities Register.

Section 17: Entries in the Crypto Securities Register
(1) The entity managing the register must ensure that the crypto securities register contains the following information about the registered crypto security:
1. The essential content of the right including a unique identification number and the designation as a security,
2. The volume of issuance,
3. The nominal amount, or for share securities, their number,
4. The issuer,
5. An indication of whether it is an individual or collective entry,
6. The holder,
7. Information on mixed holdings as per Section 9 (3), and
8. For shares, additionally:
a) That they are registered in the name,
b) In the case of shares issued before the full payment of the issue amount, the amount of the partial payment,
c) Whether they were established as nominal value shares or as no-par value shares,
d) The class of shares, if multiple classes exist,
e) In the case of multiple voting rights shares, the number of voting rights attributed to them,
f) Whether they were issued as non-voting shares, and
g) Whether the company's articles of association condition the transfer of ownership on the consent of the company.
(2) In the case of an individual entry, the entity managing the register must ensure that the crypto securities register also contains the following information about the registered security, in addition to the details mentioned in paragraph 1:
1. Restrictions on disposal in favor of a specific person, and
2. Third-party rights.
The designation of the holder mentioned in paragraph 1, number 6, must be done by assigning a unique identifier for an individual entry. The entity managing the register must, upon instruction by a person authorized under Section 18 (1) sentence 1, number 1 or number 2, additionally include information on other restrictions on disposal as well as on the legal capacity of the holder.
(3) The entity managing the register must ensure that the information according to paragraphs 1 and 2, sentence 1, is linked in a way that it can only be retrieved together.

2. Analysis documentation of the mandatory information in the Crypto Securities Register eWpG

2.1 The essential content of the right including a unique identification number and the designation as a security (§ 17 Abs. 1 Nr. 1 eWpG)

a) Creation of the Crypto Security (scriptural process)
Issuing a crypto security involves a documented process that mirrors the procedure for central register securities, structured in three main steps:
1. Entering into the crypto securities register the details mandated by Section 17 of the eWpG, as specified in Section 4(4) eWpG.
2. Submitting the conditions of issuance to the entity managing the register (outlined in Section 5(1) eWpG). This step clarifies the specifics of the electronic security, ensuring its content is clearly defined.
3. Connecting the register entry of the crypto security with its conditions of issuance (detailed in Section 4(4) eWpG). This connection is meant to provide proof of the legal agreement, enabling verification by any party from the register. This link, whether through the security's unique identification number in the register or a direct link to the issuance conditions in the register entry, is maintained by the managing entity and is permanently available for third-party access.
As per Section 13 of the eWpG, similarly to Section 17, including this information in the crypto securities register during issuance is essential for the crypto security's establishment. This requirement is comparable to the traditional method of noting details on a physical certificate.
b) The crypto securities register must include the essential content of the right, such as a unique identification number and designation as a security.
c) For crypto securities, similar to central register securities, the register must clearly indicate the type of security (e.g., bearer bond) and the specific rights it conveys. This may be done by referencing the documented issuance conditions or directly listing essential details in the register. Important information typically includes Duration, Interest rate and calculation method, Payment due dates, Ordinary and extraordinary termination rights, and Subordination agreements.
d) The security must be identifiable by a unique identifier. For central register securities and crypto securities, this is often the International Securities Identification Number (ISIN) and the German securities identification code (WKN). For crypto securities, identification can be through a unique identifier or the security identification number. Identification using a unique number (Section 17 (1) No. 1 eWpG) is sufficient and practical. This could be the unique blockchain address of the smart contract used to create the crypto security. If an ISIN is assigned, it must also be recorded in the register.2.

2.2 The volume of issuance; The nominal amount, or for share securities, their number; The issuer (§ 17 Abs. 1 Nr. 2 – 4 eWpG)

In the crypto securities register, unlike for holders, issuers cannot use pseudonymized entries. The rules, specifically Section 8(2) of the eWpRV, demand that the issuer's identification includes detailed information as described in paragraph 1. For companies, this means providing the name, location, the court where it's registered, and the registration number. An alternative is using a recognized code for companies, known as the Legal Entity Identifier (LEI), which is mentioned in Section 17(1) No. 2 of the eWpG. Using pseudonyms would make it difficult to identify the issuer of the security clearly and accurately.

2.3 Disclosure of the holder (Section 17(1) No. 6 eWpG) and designation by means of a unique identifier (Section 17(2) Sentence 2 eWpG).

a) The crypto securities register, just like the central register, must include the holder's details as required by Section 17(1) No. 6 of the eWpG, identifying the holder by a unique identifier as per Section 17(2) Sentence 2 of the eWpG. When securities are issued, the buyer becomes the holder under the eWpG, gaining ownership of the electronic security. Ownership does not depend on holding the private key.

b) It's important to note the different understandings of possession between the eWpG and traditional blockchain structures: For technical control and authority over a token on a blockchain, holding the private key is essential, whereas for legal ownership of an electronic security (technically, the token), registration as the holder is what counts. However, a holder can't prove their possession to others based solely on the public blockchain entry because it's pseudonymized. To prove ownership, they'd need to present verification or confirmation of ownership from the managing entity of the register.

c) For individual entries of crypto securities, the law mandates pseudonymization of the holder for data protection reasons. Consequently, Section 17(2) Sentence 2 of the eWpG specifies that in the crypto securities register, individual entries must identify the holder using a unique identifier: "The designation of the holder according to paragraph 1 number 6 must be made by assigning a unique identifier for an individual entry." Conversely, this means that for collective entries, the holder must be specifically named, and pseudonymized entries are not allowed.

D) Section 8(1) No. 2 of the eWpRV requires for legal entities (similar to the issuer's identification) the name/company, location, registry court, and registry entry – or alternatively, the Legal Entity Identifier (LEI). In cases of collective entries, it matters whether a central securities depository or a custodian is the holder; hence, their specific identification is necessary (Section 8(1) eWpRV). Whether collective entries become a significant use case in practice remains doubtful. More relevant is the scenario where multiple custodians are individually registered in the crypto securities register for different parts of the issuance they hold in trust for clients or themselves. This allows peer-to-peer settlements between institutional clients on a DLT-based network outside the usual infrastructures.

2.4 Collective and individual registration (Section 17(1) No. 5 eWpG) and mixed holdings (Section 17(1) No. 7 eWpG).

a) Crypto securities, much like traditional central register securities, can be issued in one of three ways: as individual registrations, as collective registrations, or as a mixed holding that combines both for a single issuance, according to Section 9(3) of the eWpG. However, there's a key difference between crypto and central register securities: when issued as a collective registration, crypto securities cannot participate in securities settlement systems, a contrast highlighted in Section 12(3) of the eWpG.

b) In practical terms, it is expected that crypto securities will seldom be issued as collective registrations. This is primarily because their main benefit—being traded within securities settlement systems—is not available to crypto securities. As stated in Section 8(1) No. 1 of the eWpG, in situations of collective registration, only central securities depositories or custodians are eligible to be listed as the holders.

c) The process of pseudonymization, which helps protect holder identities, is only relevant for individual registrations. In cases of collective registration, the law requires that the custodian or central securities depository be explicitly identified in the register, either by their name, as either a natural or legal person, or by their Legal Entity Identifier (LEI).

2.5 Restrictions on disposal in favor of a specific person (Section 17(2) Sentence 1 No. 1 eWpG) and third-party rights (Section 17(2) Sentence 1 No. 2 eWpG)

a) For data protection reasons, the crypto securities register requires that personal information related to the ownership of a crypto security in an individual registration be listed in a pseudonymized manner, utilizing a unique identifier for the holder. This means that the holder's actual name is not recorded in the register.

b) Different requirements exist for recording individuals who have specific rights or are subject to restrictions on disposal. According to Section 8(2), (1) of the eWpRV, for natural persons, details such as the first name, last name, date of birth, and address are necessary. For legal entities, the register must include the entity's name, location, registration number, and court of registration, or, alternatively, the Legal Entity Identifier (LEI).

c) The task of registering any relative restrictions on disposal (which could render transactions relatively invalid) and rights of third parties falls upon the register's managing entity, as mandated by Section 17(2) of the eWpG, which stipulates that the managing entity "must ensure" these details are recorded accurately. It is the responsibility of the managing entity to collect the necessary information or its verification directly from the holder.

2.6 Additional Restrictions on Disposal and Holder's Legal Capacity (Section 17(2) Sentence 3 eWpG)

a) Information regarding further disposal restrictions (like statutory bans and unconditional disposal limitations) and the holder's legal capacity may be recorded in the register, but only if explicitly directed by someone with authority as defined in Section 18(1) Sentence 1 No. 1 or No. 2 eWpG.

b) It's important to note that recording this information isn't compulsory for the entity managing the register; it happens exclusively upon specific instruction from an authorized party (Section 18 eWpG).

2.7 Combining Essential and Supplementary Details, and Ensuring Their Access (Section 17(3) eWpG)

The managing entity of the register is tasked by Section 17(3) eWpG with the responsibility of ensuring that the details outlined in Sections 17(1) and 17(2) Sentence 1 eWpG are interconnected in a manner that allows them to be retrieved only as a complete set. This stipulation specifically targets securities listed through individual entries, as indicated in Section 17(2) Sentence 1 eWpG, which solely pertains to such cases. The method of achieving this technical linkage within the crypto securities register remains a question. While security-related information might be encoded within the metadata of the token’s smart contract, the placement of data regarding disposal limitations and their consistent readability through blockchain explorers poses a challenge. Wallet addresses linked to the token’s contract via transaction histories solidify the connection between holders and their tokens. Fulfillment of Section 17(3) eWpG's requirements is deemed achieved as soon as all limitations, disposal restrictions, and third-party entitlements are accurately listed under the holder’s address.

Table 1: Documentation of the mandatory information in the Crypto Securities Register eWpG
Table 1 for: [Milestone Acceptance criteria: "1. re legal analysis: a) Documentation of the mandatory information in the Crypto Securities Register eWpG.]

No	Mandatory Information	Comment	Reference
1	Essential content of the right	The type of security (e.g., bearer bond) and the specific rights it conveys. This may be done by referencing the documented issuance conditions or directly listing essential details in the register.	§ 17 Abs. 1 Nr. 1 eWpG
2	Unique identification number	International Securities Identification Number (ISIN) and the German securities identification code (WKN).	§ 17 Abs. 1 Nr. 1 eWpG
3	Designation as a security		§ 17 Abs. 1 Nr. 1 eWpG
4	Volume of issuance		§ 17 Abs. 1 Nr. 2 eWpG
5	Nominal amount, or for share securities, their number,		§ 17 Abs. 1 Nr. 3 eWpG
6	Issuer	Unlike for holders, issuers cannot use pseudonymized entries. For companies, this means providing the name, location, the court where it's registered, and the registration number. An alternative is using a recognized code for companies, known as the Legal Entity Identifier (LEI).	§ 17 Abs. 1 Nr. 4 eWpG
7	Indication of whether it is an individual or collective entry		§ 17 Abs. 1 Nr. 5 eWpG
8	Holder	For individual entries of crypto securities, the law mandates pseudonymization of the holder for data protection reasons by a unique identifier. For collective entries, the holder must be specifically named, and pseudonymized entries are not allowed.	§ 17 Abs. 1 Nr. 6 eWpG and § 17 Abs. 2 eWpG
9	Information on mixed holdings as per Section 9 (3)	Crypto securities can be issued in one of three ways: as individual registrations, as collective registrations, or as a mixed holding. When issued as a collective registration, crypto securities cannot participate in securities settlement systems As stated in Section 8(1) No. 1 of the eWpG, in situations of collective registration, only central securities depositories or custodians are eligible to be listed as the holders.	§ 17 Abs. 1 Nr. 7 eWpG

10	For shares, additionally: a) That they are registered in the name,		§ 17 Abs. 1 Nr. 8a eWpG
11	b) In the case of shares issued before the full payment of the issue amount, the amount of the partial payment,		§ 17 Abs. 1 Nr. 8b eWpG
12	c) Whether they were established as nominal value shares or as no-par value shares,		§ 17 Abs. 1 Nr. 8c eWpG
13	d) The class of shares, if multiple classes exist,		§ 17 Abs. 1 Nr. 8d eWpG
14	e) In the case of multiple voting rights shares, the number of voting rights attributed to them,		§ 17 Abs. 1 Nr. 8e eWpG
15	f) Whether they were issued as non-voting shares, and		§ 17 Abs. 1 Nr. 8f eWpG
16	g) Whether the company's articles of association condition the transfer of ownership on the consent of the company.		§ 17 Abs. 1 Nr. 8g eWpG
17	In the case of an individual entry, 1. Restrictions on disposal in favor of a specific person, and 2. Third-party rights.	Different requirements exist for recording individuals who have specific rights or are subject to restrictions on disposal, meaning that pseudonymization by a unique identifier does not apply. According to Section 8(2), (1) of the eWpRV, for natural persons, details such as the first name, last name, date of birth, and address are necessary. For legal entities, the register must include the entity's name, location, registration number, and court of registration, or, alternatively, the Legal Entity Identifier (LEI). The task of registering any relative restrictions on disposal (which could render transactions relatively invalid) and rights of third parties falls upon the register's managing entity, as mandated by Section 17(2) of the eWpG, which stipulates that the managing entity "must ensure" these details are recorded accurately	§ 17 Abs. 2 eWpG

18	Information on other restrictions on disposal as well as on the legal capacity of the holder	Information regarding further disposal restrictions (like statutory bans and unconditional disposal limitations) and the holder's legal capacity may be recorded in the register, but only if explicitly directed by someone with authority as defined in Section 18(1) Sentence 1 No. 1 or No. 2 eWpG. It's important to note that recording this information isn't compulsory for the entity managing the register; it happens exclusively upon specific instruction from an authorized party (Section 18 eWpG).	§ 17 Abs. 2 eWpG

III. Documentation of the mandatory information in the Crypto Securities Register eWpG.
[Milestone Acceptance criteria: "1. re legal analysis: b) Documentation of the required data when subscribing to a crypto security and initial entry in the crypto securities register]

1. The required mandatory data when subscribing to a crypto security

1.1 The Crypto Securities Register eWpG requires the following data when subscribing:

a. Law Crypto Securities Register eWpG § 24 - 27
Unofficial Table of Contents, translated from German to English.
Section 4
Transactions of Electronic Securities in Individual Registration

§ 24 Transaction Transparency
Subject to other legal requirements for their validity, the following transactions require registration or transfer in the electronic securities register:
1. Transactions involving an electronic security,
2. Transactions involving a right from an electronic security or a right to such a right, and
3. Transactions involving a right to an electronic security or a right to such a right.

§ 25 Transfer of Ownership
(1) To transfer ownership of an electronic security, it is necessary for the electronic security to be transferred to the acquirer at the direction of the entitled party, and both parties must agree that the ownership is to be transferred. Until the transfer to the acquirer, the entitled party does not lose ownership.
(2) The right from the security is transferred with the transfer of ownership of the electronic security as per paragraph 1. Section 67(2) sentence 1 of the Stock Corporation Act remains unaffected.
(3) In the case of electronic shares, if the company's bylaws require the company's consent for the transfer of ownership, the register managing entity may only perform the transfer after obtaining the company's consent. Transfer of electronic registered shares by endorsement is not possible.

§ 26 Good Faith Acquisition
In favor of the person who is registered in an electronic securities register based on a legal transaction, the contents of the electronic securities register are considered complete and accurate, and the holder is considered the entitled party unless the acquirer knew or should have known otherwise at the time of their registration due to gross negligence. A restriction on disposal as defined in Section 13(2) sentence 1 No. 1 or Section 17(2) sentence 1 No. 1 is effective against the acquirer only if it is registered in the electronic securities register or known to the acquirer. Sentences 1 and 2 do not apply to information under Section 13(2) sentence 3 and Section 17(2) sentence 3.

§ 27 Presumption of Ownership for the Holder
Unless otherwise provided by this law, it is presumed in favor of the holder of an electronic security that they are the owner of the security for the duration of their registration as the holder.

b. Law Crypto Securities Register eWpG § 18

§ 18 Changes to the Register Content
(1) The register managing entity is only allowed to make changes to the information specified in § 17 paragraphs 1 and 2, as well as to delete the crypto security and its recorded issuance conditions, based on instructions from:
1. The holder, unless the register managing entity is aware that the holder is not authorized, or
2. A person or entity that is authorized to do so:
   a) By law,
   b) Under a law,
   c) Through a legal transaction,
   d) By a court decision, or
   e) By an enforceable administrative act.

In the case of a disposal restriction according to § 17 paragraph 2 sentence 1 number 1, the holder must assure the register managing entity, beyond their instruction, that consent from the individuals benefited by the disposal restrictions for the change exists. In the case of § 17 paragraph 2 sentence 1 number 2, the registered third party takes the place of the holder. The register managing entity timestamps the receipt of instructions. The register managing entity may proceed with an instruction from the holder if the instruction was given using a suitable authentication instrument.
(2) The register managing entity may only make changes to the information specified in § 17 paragraph 1 numbers 1 to 5, 7, and 8, and delete an entry and its recorded issuance conditions with the issuer's consent unless otherwise provided by law. Only the issuer is authorized to instruct the registration of the extinguishment of multiple voting rights registered under § 17 paragraph 1 number 8 letter d.
(3) The register managing entity ensures that changes to the register content, especially regarding the holder, are made only in the order in which the corresponding instructions are received by the register managing entity. The register managing entity timestamps the change of register content.
(4) The register managing entity must ensure that transfers are unique, carried out within a reasonable time, and the transaction cannot be invalidated in the recording system.
(5) If the register managing entity makes a change to the register content without an instruction as per paragraph 1 or without the issuer's consent as per paragraph 2, it must immediately reverse the change. The rights from Regulation (EU) 2016/679, especially its Article 17, remain unaffected.

c. Analysis regarding “The Crypto Securities Register eWpG requires the following data when subscribing”

c1. Data required by the Crypto security register for KYC, AML, KYT to enable subscribing

Clarification: Crypto security register managers (Kryptoregisterführer) according to Section 65(2) of the Banking Act (KWG) with permission for crypto security register management (Section 1(1a) No. 8 KWG), hereinafter referred to as crypto security register.

Clarification: Level of Identification in Germany for eWpG: Video Ident, PostIdent. In other countries: also AutoIdent (example: Level 3 FINMA).

To enable § 25 Transfer of Ownership of Crypto Securities Register eWpG the Crypto security register demands the inclusion of specific attributes to adhere to Know Your Customer (KYC), Anti-Money Laundering (AML), and Know Your Transaction (KYT) regulations, thereby facilitating mutual authentication among participants with the following attributes, derived from a regulatory compliant identification.

Disclosures regarding the specific identity of the holder are provided for under § 10 paragraph 3 of the eWpG. Level of Identification: In Germany: Video Ident, PostIdent. In other countries: AutoIdent.

List 1: Attribute list KYC, AML, KYT with German Crypto security register for natural persons
List for for milestone 1. re legal analysis: b) Documentation of the required data when subscribing to a crypto security
Comment: list is valid for EU, CH.
For a natural person:
1 Wallet Public Key
2 Title
3 First Name(s)
4 Last Name
5 Gender
6 Birthdate
7 BirthPlace
8 BirthCountry
9 US Resident or National?
10 Russian Passport?
11 Sanction list
12 Nationality
13 ID Document Type
14 ID Document Issuing Country
15 ID Document Number
16 ID Document Issuing Body
17 ID Document Issuing Date
18 ID Document Validity End Date
19 Multinational
20 2nd Nationality
21 3rd Nationality
22 Tax residency
23 Street name
24 Street number
25 Sort code
26 City
27 Country
28 Email
29 Tel
30 Mobile
31 PEP-Status (yes/no)
32 Person acts in his/her own name for his/her own account (yes/no)
33 Person identical with Beneficial Owner (yes/no)
34 Special requirements (AML) (yes/no)
35 Origin of the client's assets
36 Requirement according to AML fulfilled? (yes/no)

List 2: Attribute list KYC, AML, KYT with German Crypto security register for companies
List 2 for for milestone 1. re legal analysis: b) Documentation of the required data when subscribing to a crypto security
Comment: list is valid for EU, CH.
For a legal entity or a partnership:

1 Company, name, or designation
2 Legal form
3 Registry number or similar
4 Street name
5 Street name
6 Street number
7 ZIP code
8 City
9 Country
10 Email
11 Tel
12 URL
13 The names of the members of the legal representatives and, if a member of the representative body or the legal representative is a legal entity, from this legal entity the data.
14 Beneficial owner and shareholder 25%+ (other jurisdictions: 10%+): first and last name, date of birth, place of birth, and optional address of the beneficial.
15 Wallet Public Key
16 (LEI optional)

c2. Data required by the issuer, investment brokerage § 1 para. 1a sentence 2 no. 1 KWG, § 2 (2) no. 3 WpIG, investment advice (§ 2 (2) no. 4 WpIG), MiFID II (Markets in Financial Instruments Directive II) to enable subscribing

Information: In Germany, the EU Directive MiFID II (Markets in Financial Instruments Directive II) is primarily implemented through the German Securities Trading Act (Wertpapierhandelsgesetz, WpHG). The WpHG contains the national regulations necessary to comply with the requirements of MiFID II, aimed at increasing transparency, enhancing investor protection, and helping financial markets to be more efficient and resilient.

Law:
Act on the Issuance, Approval, and Publication of the Prospectus to be Published When Securities are Offered to the Public or Admitted to Trading on an Organized Market (Securities Prospectus Act - WpPG).
§ 6 Individual investment thresholds for non-qualified investors
Notwithstanding the provisions in §§ 4 and 5, the exemption from the obligation to publish a prospectus pursuant to § 3 No. 2 is only applicable to an offer of securities if the offered securities are exclusively brokered through investment advice or brokerage by a securities service company that is legally obligated to verify whether the total amount of securities that can be acquired by a non-qualified investor does not exceed the following amounts:
1. 1,000 euros,
2. 10,000 euros, provided that the respective non-qualified investor, according to a self-declaration, has freely available assets in the form of bank deposits and financial instruments of at least 100,000 euros, or

3. Twice the amount of the respective non-qualified investor's average monthly net income according to a self-declaration, but not more than 25,000 euros.
The restrictions according to sentence 1 do not apply to securities offered to shareholders as part of a rights issue.

For this reason, a MiFID II compliant onboarding process is required for the issuer and the liability umbrella, investment brokerage § 1 para. 1a sentence 2 no. 1 KWG, § 2 (2) no. 3 WpIG, investment advice (§ 2 (2) no. 4 WpIG), covering the following areas:

1 Identification: KYC, AML, KYT
2 Client Classification
3 Suitability Assessment for Securities Investments
4 Individual investment thresholds for non-qualified investors

For the distribution of financial instruments (stocks, bonds, certificates, profit participation certificates, etc.), authorization according to § 15 of the WpIG (Securities Institutions Act) is required. Intermediaries of financial investments have the option to use what is known as a liability umbrella. These are securities institutions that manage independent distribution partners as tied agents according to § 3 (2) of the WpIG.

List 3: Attribute list c2 MiFID II
List 3 for milestone "1. re legal analysis: b) Documentation of the required data when subscribing to a crypto security"
Comment: list is valid for EU, CH investment brokerage

1 All attributes from "List 1: Attribute list KYC, AML, KYT with German Crypto security register
2 Financial situation to assess the suitability of the products: Individual investment thresholds for non-qualified investors
3 Knowledge and Experience with different types of financial instruments
4 Investment Objectives and Risk Tolerance: A basic assessment to identify products that are fundamentally unsuitable
5 Wallet Public Key
6 Tax number (withholding tax self custody of wallet)
7 Disclosure to the client of monetary and non-monetary benefits such as sales commissions, placement fees, trailing commissions
8 Client Classification (optional)

2. The required data of initial entry in the crypto securities register
[Milestone Acceptance criteria: "1. re legal analysis: b) Documentation of the required data when of initial entry in the crypto securities register]

2.1 The Crypto Securities Register eWpG requires the following data of initial entry.

Please compare in this document pages 4 – 10:
[II. Documentation of the mandatory information in the Crypto Securities Register eWpG] Section 17 eWpG: Entries in the Crypto Securities Register.
There the documentation of the required data collection can be found:
Table 1: Documentation of the mandatory information in the Crypto Securities Register eWpG

IV. Documentation of the mandatory information in the Crypto Securities Register eWpG.
[Milestone Acceptance criteria: "1. re legal analysis: c) Documentation of the required data collection when instructions are issued by authorized persons. Identification data of authorized and acquiring persons.]

Please compare in this document pages 11 – 15:
[II. Documentation of the mandatory information in the Crypto Securities Register eWpG] Section 17 eWpG: Entries in the Crypto Securities Register.
There the documentation of the required data collection can be found

List 1: Attribute list KYC, AML, KYT with German Crypto security register for natural persons

List 2: Attribute list KYC, AML, KYT with German Crypto security register for companies

List 3: Attribute list c2 MiFID II

Legal Disclaimer: This legal analysis is provided "as is" without any representations or warranties, express or implied. The information contained herein is made available to the recipient solely for informational purposes and is not intended to provide legal advice. While every effort has been made to ensure the accuracy and completeness of this analysis using the best efforts and resources available, no liability is assumed for any errors, omissions, or inaccuracies. Recipients should not rely on this information as a substitute for, nor does it replace, professional legal advice or consultation. No responsibility or liability whatsoever can be accepted by the author(s) or any affiliated persons or entities for any loss or damage, whether direct, indirect, or consequential, that may arise from reliance on this analysis or for the compliance, accuracy, reliability, suitability, or availability of the information.