ANNEX V

CUSTODY POLICY

1. Introduction

1.1 Article 75(3) of Regulation (EU) 2023/1114 on cryptoasset markets (MiCA) establishes the obligation for cryptoasset service providers not considered financial instruments that provide custody and administration services of cryptoassets on behalf of customers to establish a custody policy to ensure the safekeeping or control of such cryptoassets, or of the means of access to such cryptoassets.

These obligations mainly materialize in minimizing the risk of loss of customers' cryptoassets or the rights related to those cryptoassets or the means of access to the cryptoassets due to fraud, cyber threats or negligence.

In addition, Article 70 of MiCA establishes the obligation to implement adequate measures to safeguard customers' property rights and to prevent the use of cryptoassets of a customer for its own account.

In the event of loss of customers' cryptoassets, BBVA will be liable to customers for the loss when such loss is directly caused by an incident that can be attributed to BBVA. For these purposes, the loss of customers' cryptoassets shall not be deemed to have been caused by an incident attributable to BBVA when it has occurred due to an event beyond BBVA's control or BBVA can demonstrate that such loss has occurred independently of the service provided. Notwithstanding the foregoing, when a loss of customer cryptoassets is attributable to BBVA, its liability shall be limited to the market value of the cryptoassets lost at the time the loss occurred. If a Loss Event occurs, BBVA will immediately notify the Customer and inform the Customer of any measures taken to mitigate or reduce the impact of such Loss Event.

1.2. Sections 1.7 and 4.13 of BBVA's General Policy on Customer Conduct and Product Governance establish the general provisions applicable to the custody activity of customer cryptoassets, which establishes the obligation to protect customers' cryptoassets and to adopt the necessary procedures and measures to ensure that such cryptoassets are properly safeguarded and are not used improperly.

1.3. This document is classified internally under the category of Standard, in accordance with the taxonomy of internal regulations set forth in the BBVA Group's Internal Regulatory Framework and the Internal Regulatory Standard that implements it. Therefore, the minimum content and the approval regime applicable to the Group's Standards shall apply to it. However, in accordance with the provisions of Article 2.7. of the Internal Regulation Standard, the nomenclature of the document has been maintained as Policy, in accordance with the requirements imposed by the legislation applicable to this matter.

1.4 A summary of this Policy is available to customers upon request in electronic format.

2. Purpose and scope of application

Purpose

2.1 This Policy establishes the general principles relating to the custody and administration of cryptoassets on behalf of customers, in accordance with the aforementioned regulatory background and its development regulations.

Scope of application

2.2 The Policy is generally applicable to all Customers requesting cryptoasset custody services from BBVA.

3. Policy Principles

3.1 In this context, this Policy establishes the following principles:

- Maintain a system of records and accounts that allows it to distinguish cryptoassets held for one customer from cryptoassets held for another customer and from BBVA's own cryptoassets.
- Have accounting records to verify the accuracy and correspondence of customer accounts with addresses in the Distributed Ledger (DLT) and cryptoassets; record reconciliation systems; and customer identification and authorization systems to ensure that disbursement and transactions on customer cryptoassets are performed by authorized persons.
- Have measures in place to minimize the risk of loss or diminution of customer cryptoassets, or related rights, as a result of misuse, fraud, poor administration, cyber threats, inadequate record keeping or negligence.
- Not use customers' cryptoassets for its own account.
- Have documentary support for customer transactions or contracts.
- Not freeze customers' cryptoassets without a valid justification and associated documentary support.
- Manage the risks inherent to custody by the Cryptoassets Custody Committee.
- Have a procedure establishing how BBVA processes the return of cryptoassets held on behalf of customers.

4. General Provisions

4.1 In accordance with the requirements established in each case by the applicable regulation on this matter, the following provisions are established in the matter of custody of cryptoassets:

01	Segregation of own and customers' cryptoassets	BBVA maintains a 4-level segregation system: accounts, zones, wallets and addresses in the DLT. These 4 levels allow, at any time, without delay and accurately, to distinguish cryptoassets held for one customer from cryptoassets held for another customer and from BBVA's own cryptoassets. BBVA segregates cryptoassets and customer funds, ensuring that they are not used for its own account. This segregation is performed at all 4 levels. By means of a procedure approved for this purpose it is established: i. How BBVA ensures that cryptoassets or customer funds are not used for its own account. ii. That the addresses in the DLT where customers' cryptoassets are registered are different from the addresses in the DLT where BBVA's cryptoassets are registered. iii. Detailed description of the system of approval of cryptographic keys and their safeguarding (e.g., multi-signature virtual wallets); iv. How BBVA segregates customer cryptoassets at the account, zone, wallet and address level in DLT.

02	Reconciliation of balances	The accounts and positions in the DLT are reconciled on a daily basis. If a discrepancy is detected, there is a procedure for handling the discrepancy.
03	Limiting the use of cryptoassets and customer funds	BBVA will not use cryptoassets or customer funds for its own account.
04	Custody of private cryptographic keys	Custody means the storage and safeguarding of private cryptographic keys, in particular: i) the seed that creates it, ii) the algorithm used for its creation and iii) the key itself. Control of this private cryptographic key determines the possession of cryptoassets. BBVA is the holder of the private cryptographic keys. Since BBVA is the owner of the private cryptographic keys, customers will not have access to the private keys of the distributed registry addresses that control and safeguard customers' crypto assets. The private cryptographic key will be used for: • Signing transactions, and making them valid within the blockchain. • Generate public addresses where cryptoassets can be received. The custody of the private cryptographic key is physical, i.e. it is stored in a specific hardware wallet called HSM (Hardware Security Module), which would be equivalent to a safe. HSM devices have the industry certification level (FIPS 140-2 Level 3) that guarantees security and the impossibility of extracting the keys even if there is physical access to the device.

		HSMs are responsible for performing the operations and preventing any operator, administrator or external attacker from accessing the sensitive information. HSMs may be of 3 types: a. Hot: continuously connected to the Internet, it allows 100% automatic transaction initiation. b. Warm: Equivalent to hot but with additional controls to increase security (4-eyes principle, where there is a system of multiple approvals so that several administrators have the power to ratify or deny each operation. c. Cold: not connected to the internet, requires manual processes to initiate a transaction. The Cryptoassets Custody Committee is responsible for establishing the criteria for the distribution of cryptoassets to addresses in the DLT with hot, warm and cold security measures. The creation and use of private cryptographic keys is performed in the HSMs. These keys never leave these devices without being encrypted. Access to these HSM devices is highly restricted, only accessible to certain persons, and with handling procedures that ensure that signing actions are always executed with full security. BBVA has established mechanisms to minimize the risk of loss or diminution of customer cryptoassets, or rights related to such cryptoassets, as a result of misuse, fraud, poor administration, cyber threats, inadequate record keeping or negligence.

05	DLT records, accounts and addresses	At BBVA, a cryptoassets register is kept regarding: i. The individualized position of each customer in each cryptoasset. ii. The means of access to cryptoassets, in the form of private cryptographic keys. iii. The cryptoassets that are available at any given time. iv. Any other data necessary for the purpose of being able to distinguish, at all times and without delay, the crypto-assets of each customer from those of other customers and from its own crypto-assets, as well as to be able to regularly reconcile accounts, addresses in the DLT and internal records. BBVA uses global (omnibus) DLT addresses for the custody of customer cryptoassets, always on behalf of third parties, so that cryptoassets belonging to several customers can be registered under the same DLT address. These accounts will not have BBVA's own positions, with the exception of temporary daily contributions for the payment of gas. If BBVA becomes insolvent, the customer may be temporarily restricted from disposing of its cryptoassets until the ownership of the cryptoassets under custody is determined.
06	Return of cryptoassets to customers	BBVA has a specific procedure for returning cryptoassets to their holders.

5. Governance regime and communication to customers

- Governance regime regarding the custody of customer cryptoassets:

  BBVA has appointed a head of Cryptoassets Safeguarding to ensure, with a global vision, the custody of cryptoassets and customer funds in order to mitigate the risks of a fragmented responsibility among various departments.

  This officer has sufficient skills and authority to perform his or her duties effectively and without hindrance, including the obligation to report to senior management on the effectiveness of senior management's oversight of compliance with customer cryptoasset custody requirements.

  This manager also ensures the application of the criteria agreed in this Policy and prepares the necessary procedures to detail the necessary control processes.
- Customer information:

  i. For the provision of crypto-asset custody and administration services, a Contract for the provision of crypto-asset services is signed with the customers, where the conditions, obligations and rights of the parties are detailed.

     This contract univocally identifies the register of digital asset positions (multi-asset) in which the operations carried out by the holders on the cryptoassets subject to the custody and administration service are recorded.

     Each contract will have an associated cash account, opened at BBVA, in which the credits and debits derived therefrom are recorded.

  ii. A summary of this Policy will be provided to customers upon request in electronic format.

  iii. BBVA does not hold cryptoassets that may be affected by voluntary or mandatory events. In the event that it is considered feasible to custody cryptoassets on which voluntary or mandatory events can be applied, the flows, mechanisms and procedures shall be enabled to allow communicating these events to customers and allowing their exercise.

6. Implementation and follow-up

- Internal frame.

  The implementation of this Policy and its corresponding developments, as well as the control of its degree of compliance, will be carried out in accordance with the BBVA Group's three lines of defense internal control model.

  This Policy and the procedures that will be maintained for its development will be reviewed periodically to ensure its continuous alignment with the applicable regulatory framework.
- External framework.

  - Regulation (EU) 2023/1114 of the European Parliament and of the Council of May 31, 2023 on cryptoasset markets and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937

  - Further developments of the MiCA Regulations are pending approval and publication.

Glossary

Address: address in the Distributed Log (DLT) for a particular blockchain network.

Blockchain Account: component that covers an Address in order to provide an alias, a description and other metadata necessary for the organization of the addresses (e.g. a al i as " Blockchain account 1 " of the address 0x41e42791Dfa7ee586c7d33a414CBC22CF21b1Ea0.

Cryptoasset: a digital representation of a security or right that can be transferred and stored electronically using distributed registration technology or similar technology. Crypto-assets considered as financial instruments are excluded.

Account: account for the custody of crypto-assets that the customer will open in BBVA. This account will be associated with the outflows and inflows of crypto-assets corresponding to the operations carried out by the customer.

Omnibus account: accounting account, owned by BBVA on behalf of third parties, in which customers' cryptoasset transactions and balances are recorded jointly.

Return of cryptoassets: procedure by which BBVA returns cryptoassets held on behalf of its customers.

DLT: Distributed Ledger Technology.

HSM: Hardware Security Module. A hardware-based cryptographic device that generates, stores and protects cryptographic keys.

Financial Instrument: a financial instrument as defined in Article 4(1)(15) of Directive 2014/65 /EU on Markets in Financial Instruments Directive (MiFID II).

Consensus mechanism: The policies and procedures by which agreement is reached on the validation of a transaction between DRT network nodes.

MICA: Regulation (EU) 2023/1114 of May 31, 2023 on cryptoasset markets.

DRT network node: a device or process that is part of a network and that owns a full or partial copy of the records of all operations in a distributed registry.

Distributed log: a repository of information that maintains transaction logs and is shared across a set of DRT network nodes and synchronized among those nodes, using a consensus mechanism.

Wallet: logical segregation that groups Blockchain Accounts (and therefore Addresses) and segregates them according to Blockchain Network (e.g., Bitcoin and Ethereum) and Storage security type (hot, warm and cold).

Zone: logical segregation that groups Wallets to differentiate BBVA's own position from that of customers.

BBVA and the Customer give their consent and approval to the content of this Agreement and its Annexes, formalized in the Agreement for the provision of Cryptoasset services, version 1, consisting of *43* pages, numbered from 1 to *43*, in all of which, in the Model and Version mentioned above, under the terms, conditions and responsibilities set forth therein, are shown in the lower left-hand side, respectively.