CACEIS

Société Anonyme

89, rue Gabriel Péri

92120 MONTROUGE

Report of factual findings resulting from the agreed upon procedures performed on the Smart Contract as Established on April 9, 2026 and May 19, 2026 by CACEIS in the Context of its Public Offering of the Crypto Asset “Euro eXchange Token”

Deloitte.

Deloitte & Associés
6 place de la Pyramide
92908 Paris-La Défense Cedex
France
Téléphone : + 33 (0) 1 40 88 28 00
www.deloitte.fr

Adresse postale :
TSA 20303
92030 La Défense Cedex

CACEIS
Société Anonyme
89, rue Gabriel Péri
92120 MONTROUGE

Report of factual findings resulting from the agreed upon procedures performed on the Smart Contract as Established on April 9, 2026 and May 19, 2026 by CACEIS in the Context of its Public Offering of the Crypto Asset "Euro eXchange Token"

To the Chief Executive Officer,

In response to your request in the context of your white paper (the "White Paper") as notified to the ACPR on April 3, 2026 and relating to the public offering of the crypto asset "Euro eXchange Token", abbreviated "EURXT" (or "electronic money token" or "EMT"), in accordance with the provisions of Article 51 "Content and form of the white paper on crypto assets for electronic money tokens" and Annex III of Regulation (EU) 2023/1114 ("MiCA Regulation"), we have performed the procedures agreed with you on the characteristics of the smart contract (hereafter the "Smart Contract") implemented by CACEIS and used for the issuance, management and redemption of EURXT.

Our findings are based on the versions of the Smart Contract as provided to us on April 9th, 2026 and May 19th, 2026. These findings are valid only under the conditions in which the documents necessary for our review were provided by CACEIS and do not apply to documents or versions subsequent to or different from those analyzed.

This engagement was conducted in accordance with the International Standard on Related Services (ISRS) 4400 "Agreed Upon Procedures Engagements" issued by the International Auditing and Assurance Standards Board (IAASB).

In the absence of a standardized framework to assess the characteristics of the smart contract , we have agreed with you on the procedures to be performed, with reference to various widely recognized market standards, in particular OWASP (Open Web Application Security), CWE (Common Weakness Enumeration), and SWC (Smart Contract Weakness Classification), together with best practices.

It is our responsibility to report to you the factual findings resulting from the performance of these agreed upon procedures, as described in our engagement letter dated May 28, 2026 and summarized below.

Deloitte.

Those procedures were performed solely to assist you in assessing the characteristics of the Smart Contract prepared by CACEIS in the context described above. It is therefore your role to determine the adequacy of the nature and scope of these procedures with respect to your requirements in the aforementioned context.

We note that sections E.9 and E.10 of the White Paper will be drafted as follows:

E.9: The Smart Contract has been subject to an independent report issued by Deloitte, submitted to the ACPR.

E.10: The full report describing the work performed as agreed with the company and the resulting findings is available at [Url link]. This report presents 3 low severity findings that have been mitigated.

The detail of the procedures tested is presented in Appendix 1 of this report.

Our engagement does not constitute either an audit or a limited review performed in accordance with IAASB standards. Had we performed additional procedures or an audit or limited review in accordance with IAASB standards, other matters might have come to our attention that would have been reported herein.

This report was prepared for your attention in the context described above and must not be used, distributed or referred to for any other purpose. It relates only to the information specified above and not to the financial statements of CACEIS taken as a whole.

The work performed for the purposes of this report is not intended to replace the procedures that third parties who may receive this report may need to undertake for their own purposes. In our capacity as chartered accountants, our liability to your company is governed by French law, and we accept no responsibility toward any third party to whom this report may be distributed or into whose hands it may come.

In any event, the liability of Deloitte & Associés in relation to this engagement shall not exceed, on any grounds whatsoever, the total amount of fees actually received by Deloitte & Associés for this engagement.

Paris – La Défense, May 29th, 2026
DELOITTE & ASSOCIES

Anne-Elisabeth Pannier

Anne-Elisabeth Pannier

Deloitte.

Appendix 1 : Detail of the procedures performed

Executive summary:

Upon completion of our work (see detailed procedures performed below), we identified 3 low severity findings, all being mitigated through alternative procedures implemented by CACEIS.

No.	Description of the inspection carried out	Findings/Observation	Status
1	Line-by-line review of the technical specification and the description of the functions. Verification of visibility on each public function/external/internal. Checking consistency with the permissions matrix	No issues identified	Compliant
2	Checking the version of the Solidity compiler used	No issues identified	Compliant
3	Verification of the Solidity pragma declared in the technical specification and on the codebase	No issues identified	Compliant
4	Inspection of the pragma Solidity and that the version is fixed (no caret^ or range)	No issues identified	Compliant
5	Analysis of all external calls in the contract.	No issues identified	Compliant
6	Complete review of the Role x Function matrix (Technical Reference, §5). Checking each onlyRole modifier on mint, burn, pause, blacklist, sixteen, rescue, upgrade. Analysis of last-member protection	No issues identified	Compliant
7	Finding the selfdestruct statement in the design specification and in the codebase	No issues identified	Compliant
8	Analysis of the Check-Effect-Interaction pattern in the mint, burn, seize, rescueERC20 functions. Checking the _seizureInProgress flag and its lifecycle. Finding unprotected external callbacks. The assessement performed has only been made on static code analysis	No issues identified	Compliant
9	Verification of the use of assert() vs require() vs custom errors	No issues identified	Compliant
10	Checking the use of deprecated OZ functions (transfer() vs safeTransfer(), _setupRole() vs _grantRole()). OZ v4.9.x version control for deprecated patterns	No issues identified	Compliant
11	Analysis of all time references in the contract. Checking that block.number or block.timestamp is not used as a reference	No issues identified	Compliant
12	Explicitly check that tx.origin is missing from the contract	No issues identified	Compliant
13	Inheritance tree analysis to identify variables with the same name	No issues identified	Compliant

Deloitte.

14	Searching for any calls to block.difficulty, blockhash(), block.timestamp, or keccack256 used as a source of randomness	No issues identified	Compliant
15	Multiple Inheritance Tree Analysis	No issues identified	Compliant
16	Analysis of functions involving iterations on collections. Checking for no unbounded loop in mint, burn, seize, rescueERC20. Estimating gas costs on main operations	No issues identified	Compliant
17	Transparent Proxy pattern analysis: The proxy delegates only to the implementation address configured by the ProxyAdmin. Verification that the ProxyAdmin is controlled by Taurus Protect with maximum quorum.	**CS-01 No upgrade timelock:** The upgrade (modification of the delegatecall target) does not have a timelock mechanism (on-chain or off-chain). As a result, in the event of a malicious or erroneous upgrade, there is no notice period during which the change can be reverted before it takes effect. The absence of any timelock is the only risk vector identified on the delegatecall	CS-01 **Mitigated**. Every verification will be checked before the upgrade. We were able to confirm that this finding has been mitigated through additional procedure implemented by CACEIS
18	Analysis of blocking scenarios: extended pause, locking of roles, Taurus unavailability	**CS-02 Taurus Protect- single point of failure:** In the event of unavailability (infrastructure failure, cyberattack, bankruptcy of the service provider), no operation (mint, burn, sixteen, upgrade. This scenario represents a total DoS on the token's governance functions	CS-02 **Mitigated**. Risk is covered by Taurus BCP (business continuation plan). We were able to confirm that this finding has been mitigated through additional procedure implemented by CACEIS
19	Analysis of the frontrunning scenario on the seizure procedure (seize) in a paused context. Verification of the sequence unpause -> seize -> documented pause in the governance policy	**CS-03 Non-atomic Seizure:** The required sequence of a pause -> seize -> pause creates an exposure window during which all transfer operations are active.	CS-03 **Mitigated**. The client considers that both functions are required, to be able to blacklist and then (after investigation) to seize. We were able to confirm that this finding has been mitigated by additional procedure implemented by CACEIS.
20	Scan all referenced external addresses: trustedForwarder (immutable), ProxyAdmin (Taurus controlled), token addresses in rescueERC20 (arbitrary)	No issues identified	Compliant
21	Analysis of fund protection mechanisms: blacklist, MAX_SUPPLY, seizureInProgress, multi-group quorums. Checking consistency between mint/burn operations through procedures review (no implementation test performed)	No issues identified	Compliant
22	Analysis of balance manipulation vectors: non-consensual burn, seizure on blacklisted address (legitimate), rescue to unverified address. Verification of protections against BURNER_ROLE or BLACKLIST_ADMIN_ROLE compromise	No issues identified	Compliant

Deloitte.

23	Analysis of the coherence of internal states: _seizureInProgress (atomic set/reset), _blacklisted (simple mapping), paused. Analyzing the consistency between on-chain events and contract status	No issues identified	Compliant
24	Analysis of the dependence on the price or exchange rate oracles of the contract. Verification of the absence of an AMM mechanism or on-chain pricing	No issues identified	Compliant
25	Analysis of mint/burn conditions: on-chain checks, Taurus quorum. Verification of the absence of operational headings in the governance policy (operational thresholds)	No issues identified	Compliant
26	Checking the use of each variable declared in referenced functions	No issues identified	Compliant
27	Verification of compliance with the implemented standards. Checking the semantics of each function against the corresponding EIP specifications	No issues identified	Compliant
28	Verification of compliance with Solidity conventions (Solidity Style Guide, NatSpec, comments). Control of naming consistency, function documentation, event emissions	No issues identified	Compliant
29	Systematic cross-referencing of BES-001 to BEST-035 business needs (Business Spec v1.0) with technical implementations (Technical References V2.1)	No issues identified	Compliant
30	Analysis of oracle usage and the presence of backup processes implemented in case of problems	No issues identified	Compliant
31	Evaluation and completness of unit tests	No issues identified	Compliant
32	External dependency analysis: OpenZeppelin. Checking version fixing (package.json/hardhat.config) and long-term import availability	No issues identified	Compliant
33	Gas cost estimate of the main functions (mint, burn, blacklist, sixteen, pause) based on the specification. Checking the use of custom errors vs string reverts, mappings vs arrays, forwarder immutability	No issues identified	Compliant
34	Analysis of the Governance Policy. Identification of the absence of any documented delay mechanism.	**CS-01 No upgrade time-lock:** Contract upgrades may be executed immediately after quorum is reached. Token holders have no advance notice of business logic changes	CS-01 **Mitigated**. Every verification will be checked before the upgrade. We were able to confirm that this finding has been mitigated through additional procedure implemented by CACEIS

Low severity : no impact on the security of the code
High severity : limited risk on the security of the code either for CACEIS or the token holders
Critical severity : direct or immediate risk on the security of the code either for CACEIS or the token holders