2025

GUIDELINES FOR HANDLING INACCESSIBILITY OF WALLETS AND REISSUANCE OF CERTIFIED CREDITS

Version 1.0

March 15, 2025

INTRODUCTION

Within the aOCP protocol framework and its Web3 operation through the NAT5 infrastructure, certified credits are tokenized and delivered to project developers via decentralized wallets, such as Metamask. This architecture offers security, autonomy, and traceability, but it also introduces new operational challenges—particularly concerning the loss of access to wallets that hold certified assets.

One potential scenario is the loss of the seed phrase, which prevents access to the wallet and, therefore, recovery of the assets by the holder. In such cases, the credit remains technically on the blockchain but becomes inaccessible and practically unusable.

In response to this situation, it is essential to establish a formal, transparent, and secure procedure that allows, in exceptional and duly verified cases, the reissuance of original credits to a new wallet of the holder, ensuring the integrity of the record and preventing duplication or misuse of assets.

I. GUIDING PRINCIPLES

I.1. Immutability of the historical record

Reissuance does not involve the deletion or modification of the blockchain history. The original credit remains recorded as issued but is administratively canceled. The new issuance is documented with a different identifier, keeping the historical trace of all events intact.

I.2. Transparency in traceability

Each step in the process must be fully traceable, documented, and auditable, both internally and externally. This includes technical verification, committee resolutions, reissuance, and the event's publication on the NAT5 ledger.

I.3. No duplication (prevention of double-counting)

It must be ensured that under no circumstances are certified credits counted twice or used simultaneously from two different wallets. Administrative cancellation is a non-negotiable requirement before issuing a new credit.

I.4. Protection of ecological value

Certified credit represents validated environmental impact. Therefore, its integrity and uniqueness are essential to preserve ecological value and avoid distortions in market mechanisms or climate reporting.

I.5. Exceptional nature of the mechanism

This procedure cannot be used as a regular practice. It is reserved for documented and verified cases of access loss and must be approved through a rigorous analysis by the Technical Certification Committee.

II. Criteria for Activating the Reissuance Procedure

- Formal declaration of loss
- Digital signature of the legal representative
- Technical verification of the wallet's status
- Review and approval by the Technical Committee

III. Operational Procedure

III.1. Receipt of formal request and declaration of wallet loss

The credit holder must submit a sworn Declaration of Access Loss (see Annex 1), digitally signed by the legal representative. This declaration must be submitted through a ticket on the official standard platform: https://asessc.inteam.com/servicedesk/new under the topic "*Sworn Declaration of Wallet Access Loss*" for the *Nat5* group.

This request will be sent directly to the Technical Certification Committee for initial analysis.

III.2. Technical verification on blockchain

The technical team will perform verification on NAT5 to confirm:

- The existence and status of the reported wallet;
- That the certified credits remain intact with no recent transactions;
- That no transfers have been made to third parties.

III.3. Evaluation and resolution by the Technical Committee

The Technical Committee will assess:

- The accuracy and consistency of the documentation;
- The results of the technical blockchain analysis, and issue a resolution, which may be:
  - Approval of reissuance, or
  - Justified rejection of the procedure.

III.4. Administrative cancellation of the original credit

If reissuance is approved:

- Administrative cancellation of the original credit will be recorded in the Internal Registry (see Annex 2).
- This action is carried out only with explicit authorization from the Technical Committee.

III.5. Reissuance of credit with new ID

A new token will be issued with a new identifier (ID) and transferred to a wallet validated by the developer. The new wallet must be verified.

III.6. Notification and confirmation signature

The user will receive official notification of the reissuance and must sign the corresponding confirmation form (see Annex 3) to close the procedure.

IV. Governance of the Procedure

IV.1. Technical Certification Committee

Responsible body for:

- Evaluating each reissuance request;
- Verifying compliance with technical and documentary criteria;
- Issuing founded resolutions (approval or rejection);
- Signing the official records related to cancellation and reissuance.

IV.2. Registry of Exceptional Events

All approved cases must be documented in an Internal Registry of Exceptional Events, including:

- Case details
- Submitted documents
- Committee resolution
- Key process dates
- Identifiers of original and reissued credits

This registry may be consulted by authorized actors of the NAT5 ecosystem, promoting transparency and traceability.

IV.3. External supervision (optional)

To reinforce the legitimacy of the procedure, an external auditor or observer (independent) may be invited to periodically review recorded events and compliance with the protocol.

V. ANNEXES

- Annex 1 – Sworn Declaration Format for Wallet Access Loss
- Annex 2 – Administrative Cancellation and Reissuance Record
- Annex 3 – Confirmation Form

Annex 1. Sworn Declaration Format for Wallet Access Loss

I, *[Full name of the legal representative*], acting as [*position*], SOLEMNLY DECLARE that we have lost access to the wallet [*public address*], which contained the certified credits under the Ases On-Chain Protocol and issued in the Nat5 registry.

I state that this loss is irreversible, that all recovery avenues have been exhausted, and that the wallet's contents have not been transferred or modified since the credits were issued.

Attached to this declaration:

1. Copy of the signatory's identification document.
2. Address of the new verified wallet: [*new address*].

Signature: _____

Date: _____

Annex 2. Administrative Cancellation and Reissuance Record

****Exceptional Event Record – Reissuance of Certified Credits****

Original Credit ID: [ID]

Original Wallet Address: [address]

Original Issue Date: [date]

Administrative Cancellation Date: [date]

Technical Committee Resolution: [approved/rejected]

Remarks: [relevant details]

****Reissued Credit****

New ID: [new ID]

Receiving Wallet: [new address]

Reissuance Date: [date]

Signed by:

- NAT5 platform administrative officer: _____
- Technical Committee representative: _____

Annex 3. Confirmation Form

I, [*name of the legal representative*], express my agreement with the reissuance procedure of certified credits carried out according to the NAT5 protocol guidelines.

I declare that the new wallet [*address*] will be used for storing the reissued assets, and I commit to reporting any event affecting its accessibility.

Signature: _____

Date: _____

DOCUMENT HISTORY		
Version	**Date**	**Comments**
V1.0	15/03/2025	• Initial version published for review by the aOCP Steering Committee under aOCP Version 1.