MarketBorn

MARKETBORN DOCUMENTATION / 04

The Born Standard

Draft v0.1 | October 9, 2026

The Born Standard describes the address rule used by MarketBorn's official Solana creation flow and how to interpret the resulting origin signal. It gives participants a recognizable starting point while keeping full-address verification essential.

This prelaunch edition explains the implemented suffix gate and the verification principles for release. It does not certify any particular token or announce public mainnet availability. A recognizable address ending is a clue to investigate, not a guarantee of authenticity or quality.

IN THIS DOCUMENT

01 The exact address rule

02 Where the rule is enforced

03 Preparation before reveal

04 Checking an origin claim

05 What the signal does not establish

06 Handling an uncertain creation outcome

01

The exact address rule

The official creation flow requires the token's mint address, written in Solana's base58 format, to end with the four lowercase characters born. The match is exact and case-sensitive. An ending such as Born or borN does not satisfy the rule.

The rule applies to the mint address, not the token name, ticker, image, project URL, or a creator's wallet address. Matching a displayed name is not a substitute for comparing the complete mint address.

02

Where the rule is enforced

MarketBorn's official reveal gate checks the prepared address before asking the creator's wallet to approve creation. It derives the address and compares it with the address independently produced by the transaction builder. Both must agree and end in born; otherwise the gate refuses to proceed.

This is an official application and SDK flow rule, not a protocol-wide suffix restriction. The underlying program can accept a valid creation instruction built outside that flow without this suffix gate. It would therefore be inaccurate to label every token created through that program as an official born-flow token.

03

Preparation before reveal

The preparation engine searches on the creator's device for a value that produces a qualifying future address. Search time varies; a successful preparation does not mean a token has been created. Before reveal, the public preparation view does not expose the future mint address.

Prepared data is device-local where supported, with a tab-memory fallback that has weaker persistence. It is not token custody or escrow, and it is not a cross-device backup. Losing the preparation can require starting again. At reveal, the expected mint becomes available for transaction review before creator approval.

04

Checking an origin claim

Start from the official MarketBorn website and the relevant project record. Compare the entire mint address with the address shown in your wallet or block explorer, and confirm the network. A matching suffix alone is insufficient: another address can end with the same four characters.

A completed origin check should also connect that address to the relevant creation record and transaction. If the address, network, or record cannot be reconciled, treat the origin as unverified. Do not rely on a screenshot, an abbreviated address, or a social post as the only evidence. The launch guide will identify the released verification surfaces.

05

What the signal does not establish

A verified creation origin does not establish a creator's legal identity, prove the accuracy of project claims, or guarantee responsible conduct. It does not demonstrate an audit, sufficient liquidity, an available trading route, or an investment result. Those are separate questions requiring separate evidence.

External tokens remain external tokens even when MarketBorn displays their information or supports trading them. Neither marketplace inclusion nor a coincidentally matching suffix converts an external token into one created through MarketBorn's official flow.

06

Handling an uncertain creation outcome

If a submitted creation has an unknown outcome, the current flow keeps it tied to the original attempt rather than starting a second creation. An exposed preparation followed by a definitive failure enters a recovery-required state; the engine does not automatically create a replacement token.

These safeguards address duplicate creation and uncertain transaction status. They do not eliminate network, software, or wallet risk. Follow the released recovery instructions and establish the original transaction's outcome before attempting another creation. Future editions will identify any changes to the rule or its verification process.