Best Practices for Regulated Tokens in a BRC-100 Ecosystem

Preventing Identity Spillover and Cross-Activity Correlation

Purpose of This Paper

BRC-100 applications may eventually support ordinary BSV, tokens, identity certificates, social activity, AI-agent payments and regulated financial assets inside one interoperable wallet environment.

That versatility creates a problem developers may overlook: an application can cautiously avoid requesting a user's root identity key or identity certificates for ordinary activity, but later introduce a regulated token requiring identity verification. If both activities are handled inside the same BRC-100 wallet, does the identified token relationship expose or contaminate the user's otherwise pseudonymous activity?

The answer is:

> **Not automatically—but the risk becomes substantial unless the regulated activity is placed behind a genuine wallet and data firewall.**
>
> **A separate basket inside the same BRC-100 wallet is organizational separation. It is not strong identity separation.**

This paper applies to any asset or service that requires identity verification, not only stablecoins.

The Regulated-Token Scenario

MNEE provides a useful current example, although this paper does not claim that MNEE presently requires BRC-100 identity keys or BRC-52 certificates.

MNEE is a regulated stablecoin operating through 1Sat Ordinals. Its terms distinguish verified MNEE Customers, who may obtain direct issuance and redemption services, from unverified Non-Customers, who may still hold and use MNEE. Direct customers are subject to identity verification, transaction recordkeeping and compliance monitoring. MNEE also describes responding to lawful requests for customer identity, activity records and address freezes.

MNEE can already coexist with BRC-100 functionality in the same consumer wallet. Yours Wallet, for example, describes itself as a BRC-100 wallet supporting BSV, 1Sat Ordinals, tokens and MNEE while tracking keys and transaction history and optionally synchronizing wallet data through remote storage.

This creates the foreseeable architectural question:

> **What happens when one wallet contains both identified regulated-token activity and activity intended to remain pseudonymous?**

Does Identity “Poison” the Entire Wallet?

Not at the cryptographic level.

Identity attached to one regulated-token account or transaction does not automatically reveal every BRC-42-derived key or every BSV output controlled by the same BRC-100 wallet. Outside observers cannot derive the wallet’s complete transaction graph merely from its identity public key.

However, cryptographic non-linkability is only one layer of privacy.

A single BRC-100 wallet may also maintain:

- transaction and output histories;
- output baskets, labels and tags;
- application-origin records;
- derivation and counterparty information;
- identity keys and certificates;
- token instructions and provenance;
- local or remotely synchronized storage; and
- optional key-linkage capabilities.

BRC-100 expressly combines identity management, certificates, output baskets, transaction metadata and key-linkage revelation within the standard wallet interface.

If regulated and pseudonymous activities share the same wallet database, device profile, application account or storage provider, an application operator, wallet provider, forensic examiner or compelled party may be able to correlate them without defeating BRC-42 cryptography.

> **The risk is therefore not automatic public exposure. It is identity spillover through shared metadata and infrastructure.**

Why a Separate Basket Is Not a Firewall

BRC-100 baskets group and track particular outputs and restrict which applications may access them. That is useful permission separation.

But two baskets inside one BRC-100 wallet may still share:

- the same master key environment;
- the same wallet history;
- the same storage database;
- the same remote synchronization provider;
- the same user account or device;
- the same permission manager; and
- the same recovery package.

A “MNEE basket” and a “private BSV basket” may prevent one application from casually listing the other’s outputs. They do not guarantee that the wallet implementation, storage provider or anyone obtaining the complete wallet records cannot see both.

> **For meaningful separation, regulated-token activity should use a separate wallet boundary—not merely a different folder inside the same wallet.**

Recommended Architecture

1. Create a Separate Regulated-Token Wallet

Regulated tokens should be held in a distinct BRC-100 wallet instance using:

- a separate master key and identity key;
- a separate wallet database;
- separate storage and backups;
- separate permissions;
- a separate application account or session where practical; and
- no automatic access to the user’s primary BSV wallet.

A second basket or application profile within the same wallet should not be represented to users as equivalent separation.

2. Keep Ordinary BSV and Unregulated Assets Outside It

The regulated-token wallet should contain only:

- the regulated token;
- the minimum BSV or supporting outputs required for its operation;
- credentials specifically required for that regulated activity; and
- transaction records necessary to use and recover those assets.

Ordinary savings, pseudonymous payments, social activity, collectibles and unrelated tokens should remain in a separate wallet.

3. Do Not Reuse the Human’s General Identity

Where identity verification is required, use a credential or identity dedicated to the regulated service.

The application should not request the user’s root identity key merely because it is available. It should not make the regulated identity the identifier for unrelated wallet activity, and it should not require the same certificate for payments, social accounts or unregulated tokens.

Certificate disclosure should be limited to the exact fields required. Verified eligibility should be preferred over disclosure of underlying personal data wherever possible.

4. Disable Cross-Wallet Linkage

The regulated-token application should not receive:

- BRC-69 linkage information concerning unrelated counterparties;
- permission to inspect other wallet instances;
- broad transaction-history access;
- access to unrelated baskets; or
- authority to export or correlate the user’s general identity.

Any linkage revelation should require a fresh, narrowly described human approval. It should never be bundled into routine token onboarding.

5. Separate Storage and Authentication

Using separate keys while retaining both wallets in one shared remote database weakens the firewall.

Regulated and pseudonymous wallets should not depend upon the same storage account where separation can reasonably be maintained. Applications should also minimize shared login identifiers, analytics identifiers and device fingerprints.

This will not make correlation impossible. The same IP address, device, timing patterns or direct transfers may still provide clues. The purpose is to remove unnecessary architectural linkage.

6. Avoid Mixing Inputs and Directly Linking Activity

Identified and pseudonymous funds should not be combined as inputs in the same transaction.

Developers should also warn users that transferring funds directly between their regulated and pseudonymous wallets may create an observable relationship. Amounts, timing, counterparties and change patterns can reconnect activities even where the underlying keys are cryptographically separate.

A wallet firewall limits internal metadata spillover. It cannot erase links users create on-chain.

7. Preserve Independent Recovery and Exit

The regulated-token wallet should have its own complete backup and recovery procedure. Restoring it should not require importing the user’s primary BSV wallet or exposing unrelated keys and history.

Developers should test whether:

- the regulated token can be recovered independently;
- ordinary BSV can be withdrawn to a conventional address;
- the token can move to another compatible wallet;
- identity credentials can be removed when no longer needed; and
- closure of the regulated account leaves the unrelated wallet unaffected.

What Wallet Separation Cannot Prevent

A strong wallet firewall reduces cross-activity exposure. It cannot remove the controls that are inherent to the regulated asset itself.

A regulated issuer may still retain customer identification and transaction records, monitor activity, comply with subpoenas or freeze identified addresses according to its legal authority and terms. MNEE's published terms expressly contemplate identity verification, transaction reconstruction, monitoring, information requests and address-freeze requests.

MNEE also advertises an enterprise program in which partner-originated tokens may carry invisible metadata linking them to the originating partner, visible to MNEE and participating partners.

Therefore:

> **Wallet separation can prevent a regulated-token relationship from unnecessarily exposing unrelated BSV activity. It cannot make the regulated token itself pseudonymous or remove issuer-level visibility and control. This paper does not argue against regulated tokens; it argues against unnecessarily mixing them with activity intended to remain pseudonymous.**

Minimum Best-Practices Checklist

Before adding a regulated token to a BRC-100 application, developers should be able to answer **yes** to the following:

- Does the regulated token use a separate wallet key root?
- Is its wallet database separate from ordinary BSV activity?
- Are remote storage and backups separated?
- Are identity credentials limited to the regulated function?
- Is the root identity key avoided?
- Are unrelated baskets and histories inaccessible?
- Are BRC-69 linkage functions disabled by default?
- Are identified and pseudonymous inputs prevented from being combined?
- Are users warned that direct transfers may create on-chain linkage?
- Can the regulated wallet be recovered and closed independently?
- Can ordinary BSV exit to a conventional address?
- Are issuer monitoring, freezing and recordkeeping powers clearly disclosed?

If the answer to these questions is no, the application should disclose that introducing the regulated token may increase the correlation risk of all activity held within that wallet environment.

Conclusion

Adding one regulated token does not automatically reveal every key or transaction inside a BRC-100 wallet.

But placing identified regulated activity and pseudonymous activity inside the same wallet, storage system and application account creates an unnecessary concentration of information. The separation then depends upon permissions and promises rather than a genuine technical boundary.

The safest principle is simple:

Regulated assets belong in a separate wallet—not merely a separate basket.

Developers building the BRC-100 ecosystem now have an opportunity to establish that boundary before combined identity, token and wallet implementations become the default. Once users have accumulated funds, credentials, transaction histories and application relationships inside a common wallet architecture, correcting the design will be far more difficult.