# **PIN Transaction**

# **1 Basics**

A table with an overview of the support status and applicability.

|  |  |
| --- | --- |
| Status: | **Supported** |
| Architecture(s): |  |
| Component(s): |  |
| Hardware: | *n/a* |

# **2 Overview**

As an additional security measure, the user can require a 4-digit PIN code to be entered to submit a transaction to the blockchain.

# **3 User details**

Enabled by default and setup upon wallet creation. This feature can be modified and turned off completely from the settings panel in the user’s console or smart wallet application. If the PIN is attempted more than (X) times, the account will lock until the user can recover with a mnemonic phase.

# **4 Technical details**

This 4-digit PIN will not be recoverable as it will be encrypted on the back end and not stored in a central server. It can, however, be reset if the previous PIN or mnemonic backup phrase is known by the user.

Simple backend password encryption should be implemented to mask the PIN from any unauthorized users.

# **5 Limitations**

# **6 Testing**

This feature will fall under the umbrella of security testing, which should be a rigorous process done by a third party. For this feature specifically, testing will include attempts at decryption by an outside party.

# **7 Areas for improvement**

Additional recovery methods could be added to build more confidence in the user.

# **8 Known issues**

List of known issues or bugs. For tech preview or experimental features, this section must contain the list of items needing fixing for its status to be upgraded.

# **9 References**