ARCULUS

Arculus™ – How It Works

What Is Arculus?

Arculus is a cryptocurrency cold storage hardware wallet that protects your crypto and secures your private keys with 3-factor authentication. Arculus was created by **CompoSecure** (NASDAQ: CMPO), a trusted fintech leader with over 20 years of experience developing innovative security, payment, and digital storage solutions worldwide. Arculus is composed of two components:

- **Hardware: a physical Arculus Key™ Card**
- **Software: the Arculus Wallet™ App available for iOS and Android.**

The Arculus Key Card is a sleek, metal card with leading-edge embedded security technology including a CC EAL6+ Secure Element Hardware Classification to securely generate and store your private keys.

Working together, the **Arculus Key Card** and **Arculus Wallet App** use 3-factor authentication requiring:

1

Something you are

A biometric such as Face ID or a fingerprint

2

Something you know

A custom 6-digit pin code

3

Something you have

The Arculus Key Card that must be tapped to the back of your mobile device to sign transactions via secure NFC

How It Works

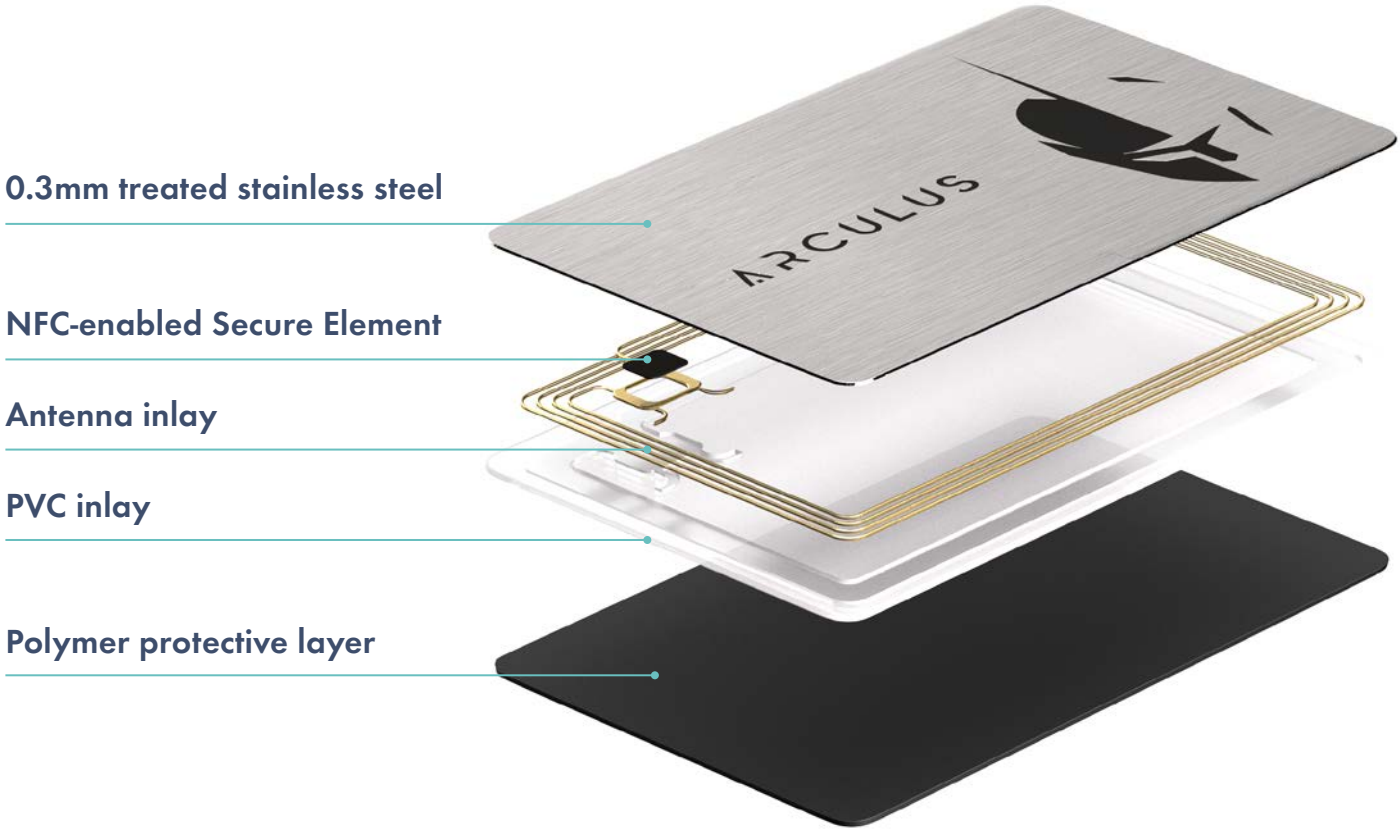

Figure 1: Components of the Arculus Key Card

Your private keys are generated, encrypted, and stored in the Secure Element on the Arculus Key Card. The Arculus Key Card doesn't use any cables or USB connections and never runs out of power. Unlike other devices, the Arculus Key Card is shipped locked, meaning the code on the card can't be updated so it isn't possible for hacked or infected code to be introduced. The Arculus Key Card communicates with the Arculus Wallet App via secure NFC which for security purposes has a range of only a few centimeters unlike Bluetooth which has a range of 10 meters. Your private keys never leave the Secure Element on the Arculus Key Card, and the card is necessary for signing all transactions.

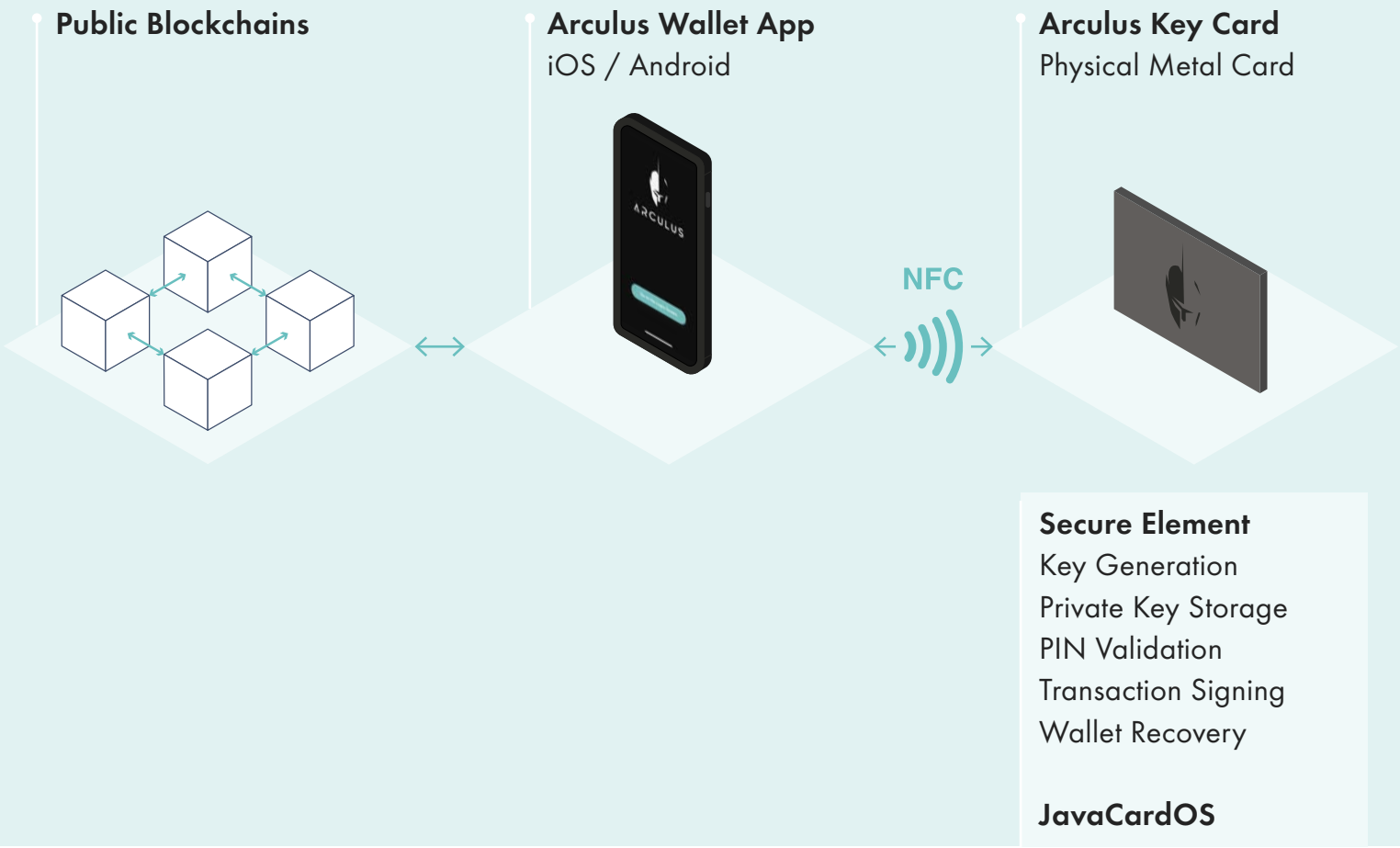

Figure 2: Arculus Key Card communicates with Arculus Wallet App

The wallet architecture is based on a "split knowledge" principle. By separating execution logic between the secure application processor and the Secure Element which provides security without the possibility to remove or read the private key from the Arculus Card.

Wallet Creation/Restoration

When you create a new wallet or restore an existing wallet, the Arculus Wallet App first prompts you to create a six-digit PIN. This PIN is distinct from your phone PIN and specific to your Arculus Wallet App. This PIN is stored only on the card and is an important part of Arculus' 3-factor authentication. PIN verification attempts are tracked on the card and after 3 failed PIN attempts, the card is reset and the keys on the card are wiped. You have to restore your wallet using your 12-word recovery phrase.

Key Generation

When generating a private key, the Secure Element on the Arculus Key Card uses a True Random Number Generator (TRNG) as opposed to a Pseudo-Random Number Generator (PRNG). Keys are generated using the EIP2333 standard and the 12-word recovery phrase (the BIP39 Mnemonic) is generated using the BIP39 standard.

After the private keys are generated, the recovery phrase is shown in the app one time so that you can write it down and secure it. Then in the immediate next step, you must re-enter the 12-word recovery phrase in the app to verify that you have accurately captured the recovery phrase. Note that the recovery phrase is not stored on the card or the phone. If you are restoring a wallet using an existing 12-word recovery phrase, you must enter the phrase (in the original order) in the mobile app so that it can be transmitted to the card. The Arculus Wallet can restore using any 12-word recovery phrase that was generated using the BIP39 standard. Once you have done that, the app will never show your recovery phrase again. It is recommended that when creating a new wallet or restoring an existing wallet, you do it in a safe, quiet, and secure location.

User Authentication And Transactions

The Arculus Wallet App can use either biometrics or the Key Card to authenticate the user before giving access to balances. All transactions require you to enter your PIN and tap your card to authenticate. The app verifies that the card's GGUID (Globally unique identifier) and Account public keys match its stored information. The mobile application has access to the account public keys, but not the Account private keys.