

ZTPASS

Key Manager — User Guide

VERSION 1.0

Last Updated: June 8, 2026 • ZTPASS Inc. • connect@ztpass.com

The ZTPASS logo is displayed in white text on a black square background.

Secure management of FIDO2 and PIV credentials
on hardware security keys via USB and NFC.

iOS NFC Support	Android NFC & USB	FIDO2 Passkey Mgmt	PIV Certificate Mgmt	Zero Cloud All Local
---------------------------	-----------------------------	------------------------------	--------------------------------	--------------------------------

All cryptographic operations occur locally. No user authentication data is transmitted to ZTPASS servers.

Table of Contents

- 1 Overview**
- 2 Platform & Connectivity Support**
- 3 System Requirements**
- 4 Getting Started**
- 5 Adding a Device**
- 6 Device Management**
- 7 FIDO2 Management**
- 8 PIV Management (USB Only)**
- 9 PIN & PUK Policy**
- 10 Security Architecture**
- 11 Troubleshooting**
- 12 Support & Contact**

1 Overview

ZTPASS Key Manager is a secure mobile application that enables management of **FIDO2** and **PIV** functionality on compatible hardware security keys and smart cards using USB and NFC on supported iOS and Android devices.

The app provides essential tools to configure authentication credentials and manage device security in a controlled, fully local environment.

✓ All cryptographic operations occur locally. No user authentication data is ever transmitted to ZTPASS servers.

2 Platform & Connectivity Support

Feature	iOS NFC	iOS USB	Android NFC	Android USB
Device Detection	✓	✗	✓	✓
FIDO2 Management	✓	✗	✓	✓
PIV Management	✗	✓	✗	✓

✗ = Not supported on this platform/connection combination.

3 System Requirements

iOS	Android
• iPhone with NFC capability • iOS 16 or later • NFC-enabled ZTPASS security key (FIDO2) • USB adapter required for PIV operations	• Android 10 or later • NFC capability OR USB-C support • OTG enabled for USB usage • Compatible ZTPASS security key

4 Getting Started

4.1 Launching the App

Open **ZTPASS Key Manager** from your device. Upon launch, the Home Screen displays all previously registered devices. If no devices are registered, follow the instructions in Section 5 to connect a compatible hardware security key.

4.2 Device Detection Behaviour by Platform

■ iOS — NFC Only (manual scan)

1. Open the app
2. Pull down on the Home Screen to start scanning
3. Hold the NFC-enabled key near the top front of the iPhone
4. Wait for detection confirmation
5. Device appears on the Home Screen

■ Android — NFC & USB (automatic)

1. Open the app — scanning begins automatically
2. NFC: tap the key to the back of the phone
3. USB: connect via USB-C and accept the permission dialog
4. Device registers automatically
5. No manual scan action required

■ iOS supports NFC for FIDO2 operations only. A USB adapter is required for PIV operations on iOS.

5 Adding a Device

5.1 iOS — NFC (FIDO2 Only)

1. Open the app
2. Pull down on the Home Screen to initiate scanning
3. Hold the security key near the **top front** of the iPhone
4. Wait for detection confirmation
5. The device will appear on the Home Screen

5.2 Android — NFC

1. Open the app
2. Tap the security key to the **back of the phone**
3. Wait for automatic detection and registration

5.3 Android — USB

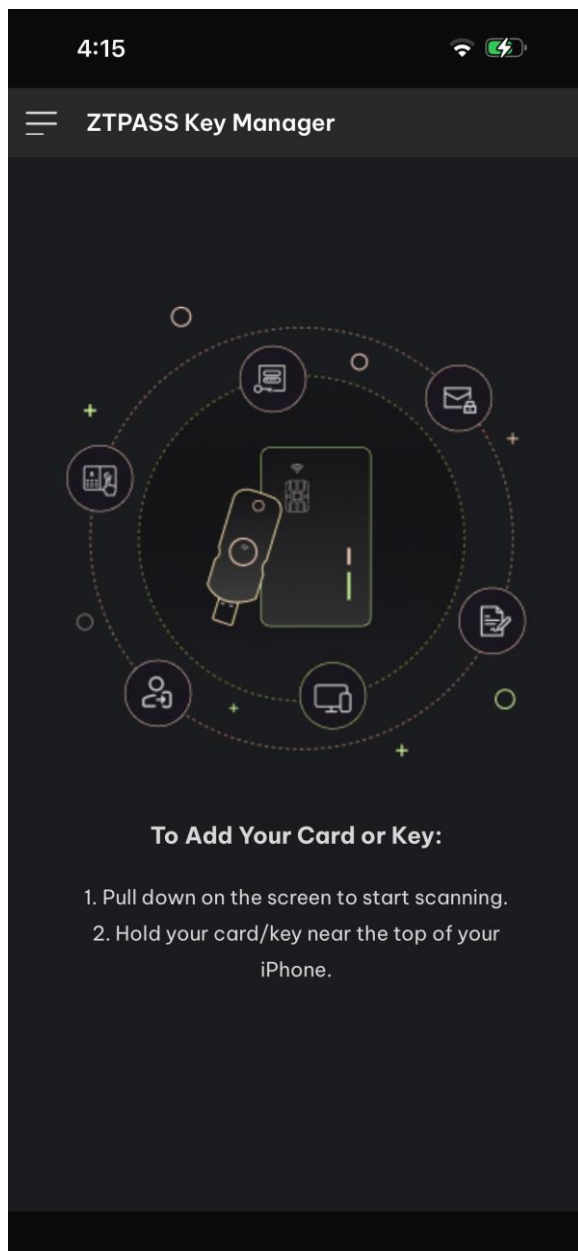
1. Connect the security key via USB-C
2. If prompted, tap **Allow** to grant USB permission
3. The device will automatically register in the app

6 Device Management

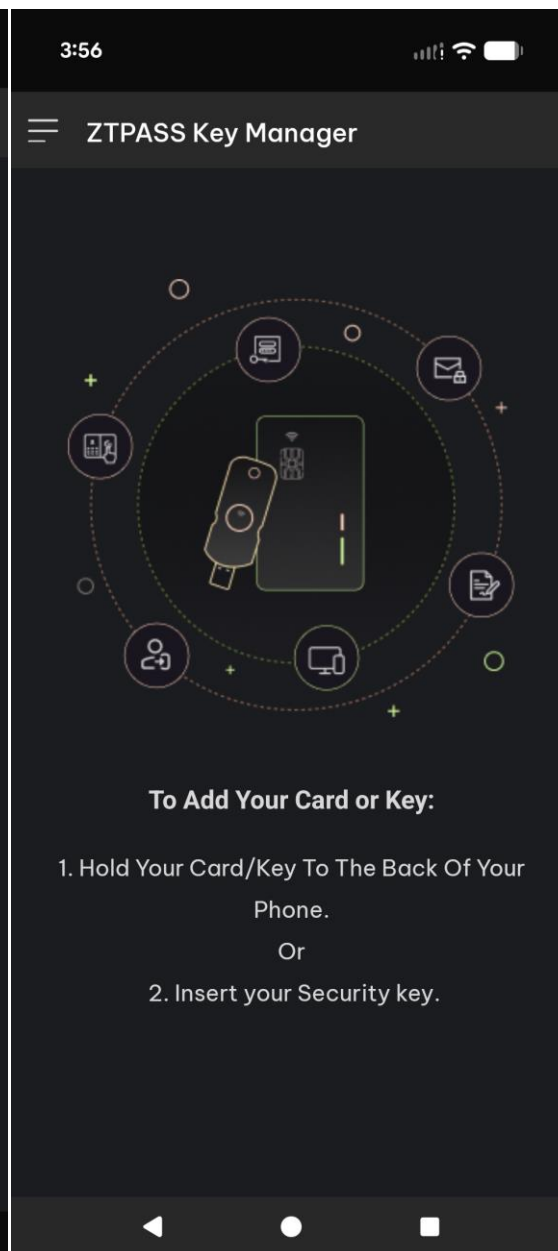
From the Home Screen you can:

- Add multiple hardware security devices
- Remove a device from the app

✓ Removing a device from the app does NOT erase data from the hardware key. Your credentials remain intact.



iOS



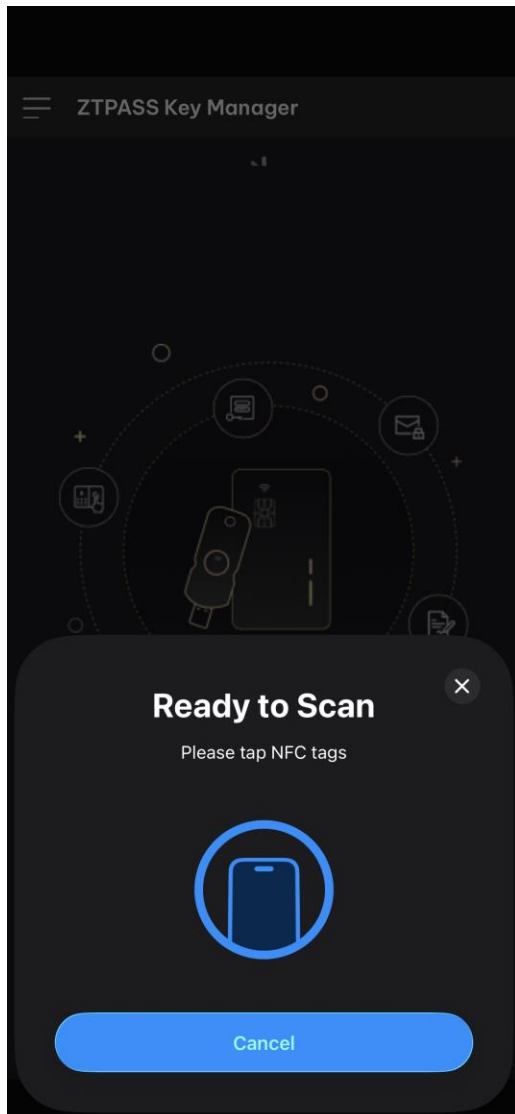
Android

5. Adding a Device

5.1 iOS – NFC (FIDO2 Only)

1. Open the app
2. Pull down to initiate scanning

3. Hold your security key near the top of the iPhone
4. Wait for detection confirmation
5. Device will appear on the Home Screen

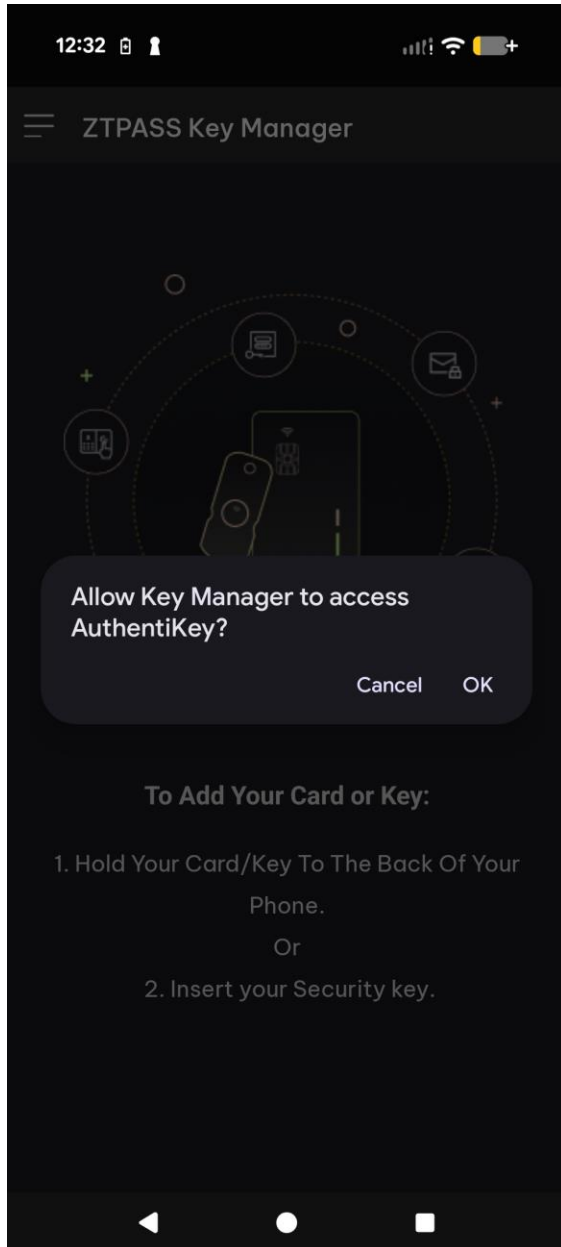


5.2 Android – NFC

1. Open the app
2. Tap the key to the back of the phone
3. Wait for automatic detection

5.3 USB Mode (Android)

1. Connect the security key via USB-C
2. If prompted, tap **Allow** to grant USB permission
3. The device will automatically register in the app



7 FIDO2 Management

FIDO2 management is available on **iOS (NFC)** and **Android (NFC & USB)**.

7.1 Available FIDO2 Features

- Set PIN (first-time setup)
- Change PIN
- Reset FIDO authenticator
- View stored passkeys
- Edit passkey display name / username
- Delete passkeys

7.2 Set FIDO PIN — First-Time Setup

If no PIN has been configured on the security key:

1. Open the device from the Home Screen
2. Navigate to the **FIDO** section
3. Select **Set PIN**
4. Enter a new **6–8 digit** PIN
5. Confirm the PIN
6. Wait for confirmation — the PIN is stored securely on the hardware key

7.3 Change FIDO PIN

1. Open the device and navigate to **FIDO**
2. Select **Change PIN**
3. Enter the current PIN
4. Enter and confirm the new PIN

■ Entering the current PIN incorrectly multiple times may lock the key.

7.4 View Stored Passkeys

Access to stored passkeys requires successful PIN verification.

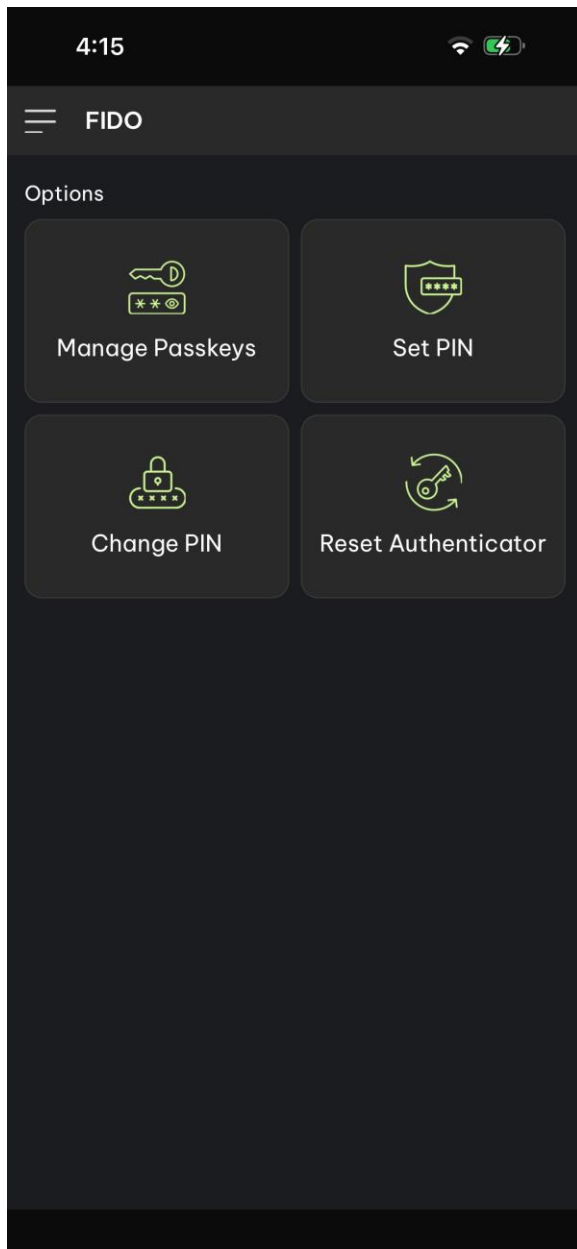
1. Open the device and navigate to **FIDO**
2. Select **View Passkeys**
3. Enter your PIN in the text box
4. Upon successful verification, stored passkeys are displayed

Each passkey shows its ID, display name, domain, and username.

7.5 Manage Passkeys (Edit or Delete)

After passkeys are listed:

1. Tap **Manage** at the top of the screen



7.2 Set FIDO PIN (First-Time Setup)

If a PIN has not been configured on the security key:

Steps:

1. Open the device from the Home Screen
2. Navigate to the **FIDO** section
3. Select **Set PIN**

4. Enter a new 6–8 digit PIN
5. Confirm the PIN
6. Wait for confirmation

The PIN is stored securely on the hardware key.

4:16

← Set PIN

Set PIN

A PIN provides strong, additional security. PIN should be between 6 and 8 digits.

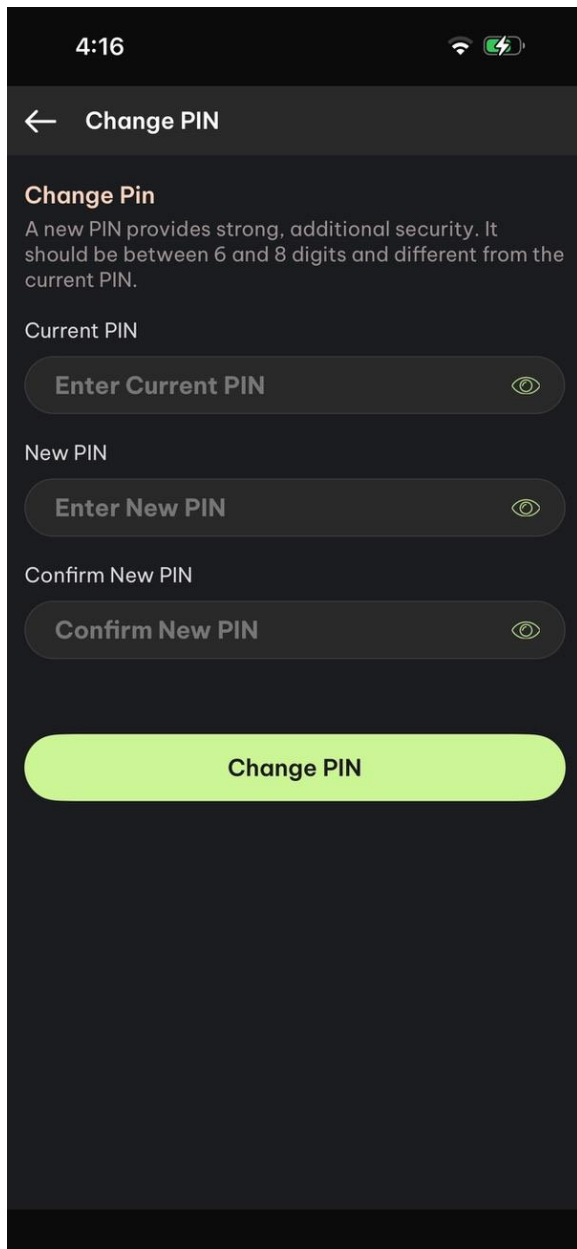
New PIN

Enter New PIN

Confirm New PIN

Confirm New PIN

Set PIN



7.4 View Stored Passkeys

Access to stored passkeys requires successful PIN verification.

Steps:

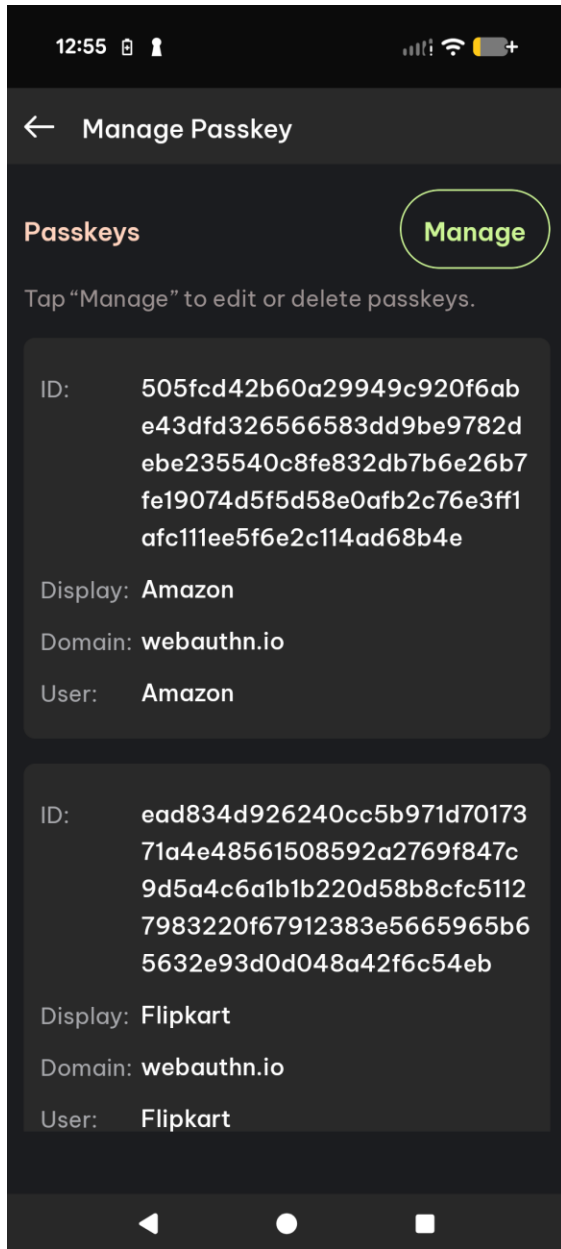
1. Open device
2. Navigate to **FIDO**

3. Select **View Passkeys**

4. Enter PIN in the textbox

5. Upon successful verification, the stored passkeys will be displayed

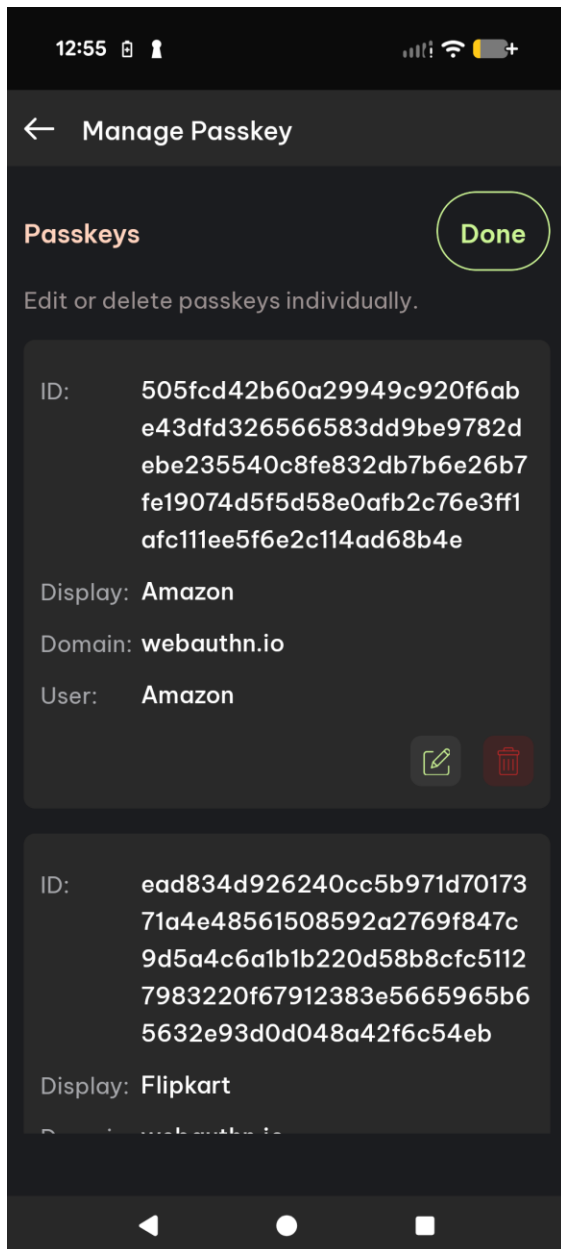
If PIN verification fails, access will be denied and remaining attempt count may decrease.

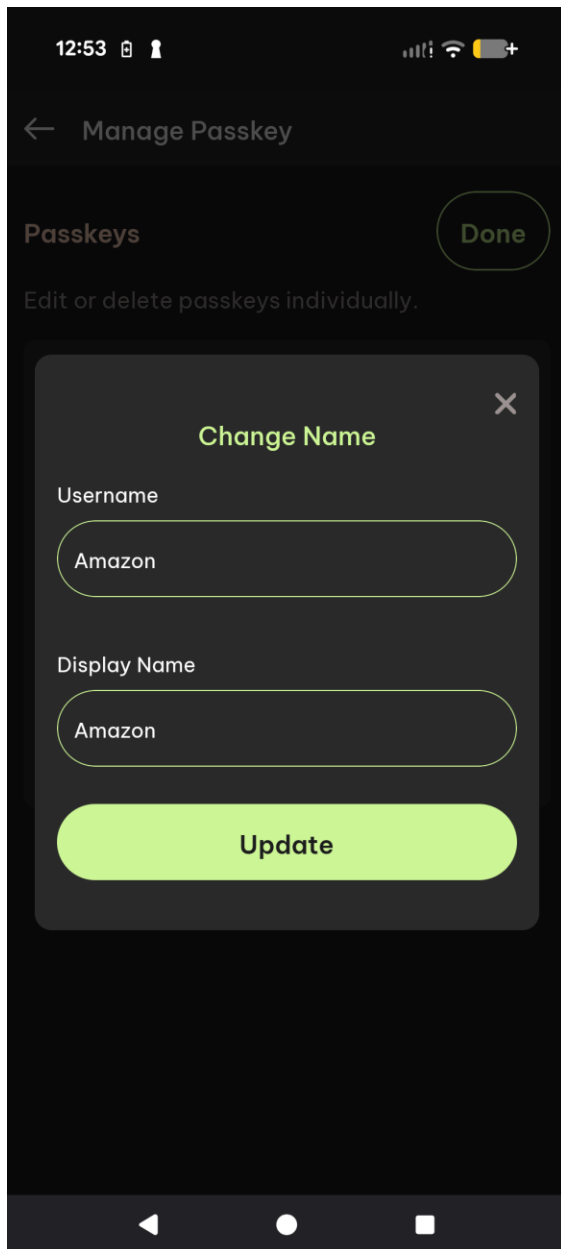


7.5 Manage Passkeys (Edit or Delete)

To modify or remove a passkey:

1. After passkeys are listed, tap **Manage** (top of the screen)
2. Edit and Delete options will appear for each passkey





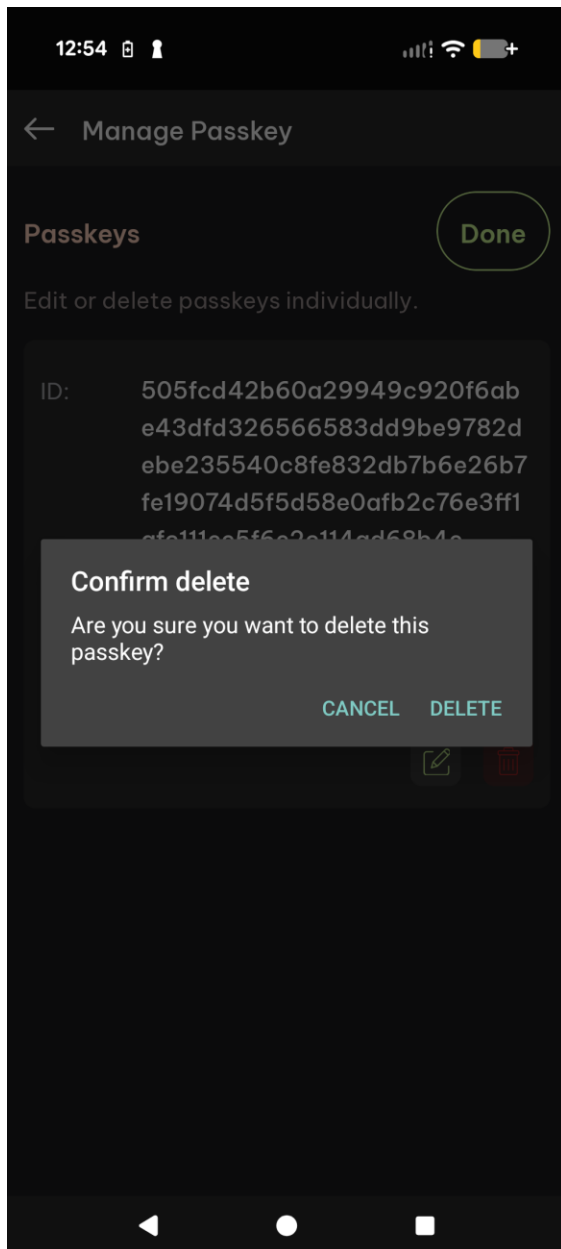
Delete Passkey

⚠ Deleting a passkey permanently removes that credential from the hardware key. This action cannot be undone.

Steps:

1. Tap **Delete** next to the desired passkey

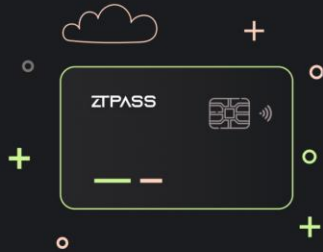
2. A confirmation dialog will appear
3. Confirm deletion
4. Perform hardware confirmation:
 - a. **iOS:** Tap the security key
 - b. **Android:** Tap (NFC) or reinsert device (USB)
5. Wait for confirmation



4:17



← Reset Authenticator



Are you sure you want to reset your authenticator?

This will delete all credentials and remove the PIN.
This action cannot be undone.

Reset Authenticator

2. Edit or Delete options appear for each passkey

- **Edit:** Updates display name or username only. The underlying cryptographic credential is NOT altered.
- **Delete:** Permanently removes the credential from the hardware key. This action cannot be undone.

For both actions, hardware confirmation is required:

- **iOS:** Tap the security key (NFC)
- **Android NFC:** Tap the key to the back of the phone
- **Android USB:** Reinsert the device when prompted

7.6 Reset FIDO Authenticator

■ Resetting FIDO permanently deletes ALL FIDO credentials stored on the key. This cannot be undone.

1. Open the device and navigate to **FIDO**
2. Select **Reset Authenticator**
3. Confirm the action in the dialog
4. Perform hardware confirmation (tap / reinsert as prompted by your platform)
5. Wait for the confirmation message

The reset completes only after successful hardware confirmation.

8 PIV Management (USB Only)

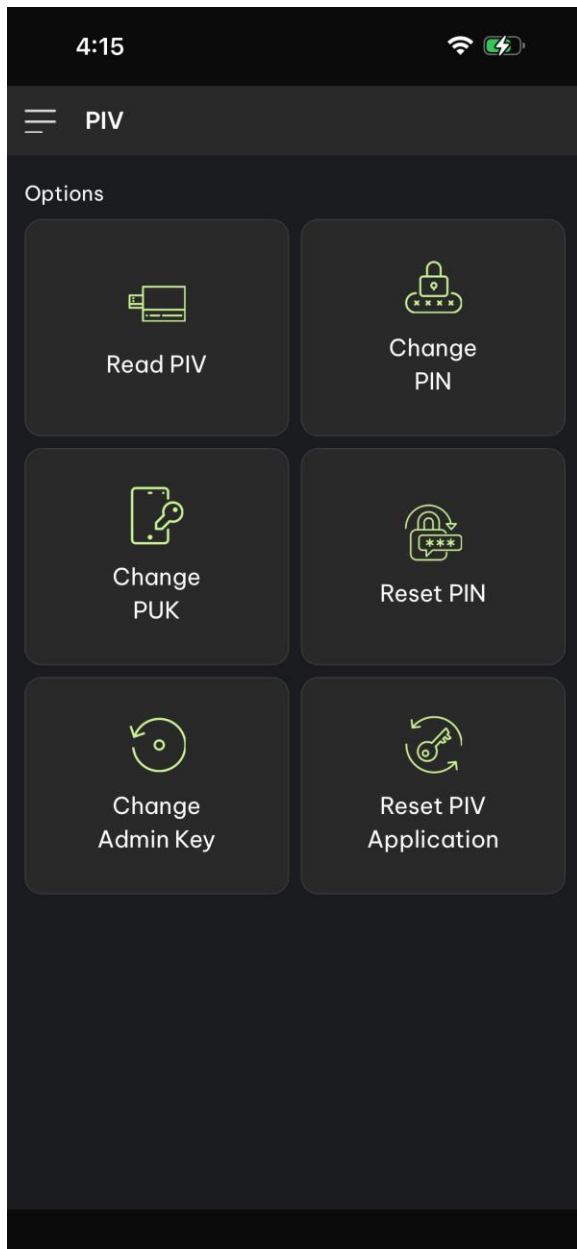
PIV functionality is supported **only in USB (contact) mode** on both iOS and Android. NFC is not supported for PIV operations.

8.1 Available PIV Features

PIV Feature	Description
Reset PIV Application	Wipes all PIV credentials and restores factory defaults
Change Admin Key	Updates the management key used for privileged operations
Reset PIN using PUK	Recovers access when PIN is blocked
Change PIN	Updates the current PIV PIN (6–8 digits)
Change PUK	Updates the Personal Unlocking Key (exactly 8 digits)
View Certificates	Read-only display of X.509 certificates in each slot

8.2 Change PIV PIN

1. Navigate to **PIV** → **Change PIN**
2. Enter the current PIN
3. Enter and confirm the new PIN
4. Insert the device if not already connected



8.2 Change PIV PIN

Steps:

1. Navigate to **PIV → Change PIN**
2. Enter current PIN
3. Enter new PIN

4. Confirm
5. Insert device (if not already connected)
6. Wait for confirmation

4:16

← Change PIN

Change Pin

A new PIN provides strong, additional security. It should be between 6 and 8 digits and different from the current PIN.

Current PIN

Enter Current PIN

New PIN

Enter New PIN

Confirm New PIN

Confirm New PIN

Change PIN

8.3 Reset PIN Using PUK

If the PIN is blocked:

Steps:

1. Navigate to **PIV → Reset PIN (Using PUK)**
2. Enter PUK
3. Enter new PIN
4. Confirm
5. Insert device (if not already connected)
6. Wait for confirmation

⚠ Multiple incorrect PUK attempts may permanently lock the PIV application.

3:58

← Reset PIN

Reset PIN

Insert your Security Key via USB and reset the PIN using the PUK.

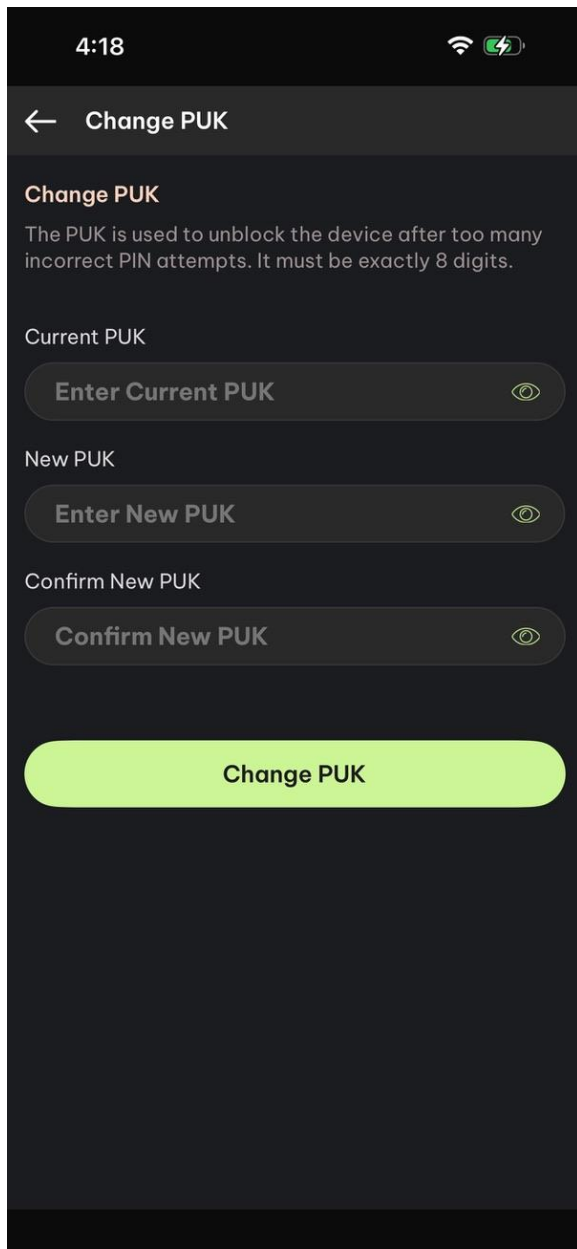
PUK [Use default PUK](#)

Enter PUK

New PIN

Enter New PIN

Reset PIN



8.5 Change PIV Admin Key

The PIV Admin (Management) Key controls privileged administrative operations within the PIV application.

⚠ After changing the Admin Key, it must be securely stored.
The previous key will no longer work.

4:18

← Change PIV Admin Key

Change PIV Management Key

Enter the current PIV Management Key or select "Use Default." Then, enter a new key and select the appropriate algorithm.

Current Key (Hex) [Use Default Key](#)

Enter Current Admin Key

New Key (Hex)

Enter New Admin Key

Generate Copy

Tip: After changing the key, you must use this new key for future admin operations. Copy and store it safely.

Select New Algorithm

AES-192

New key must be 48 hex characters for the selected algorithm.

Change PIV Management Key

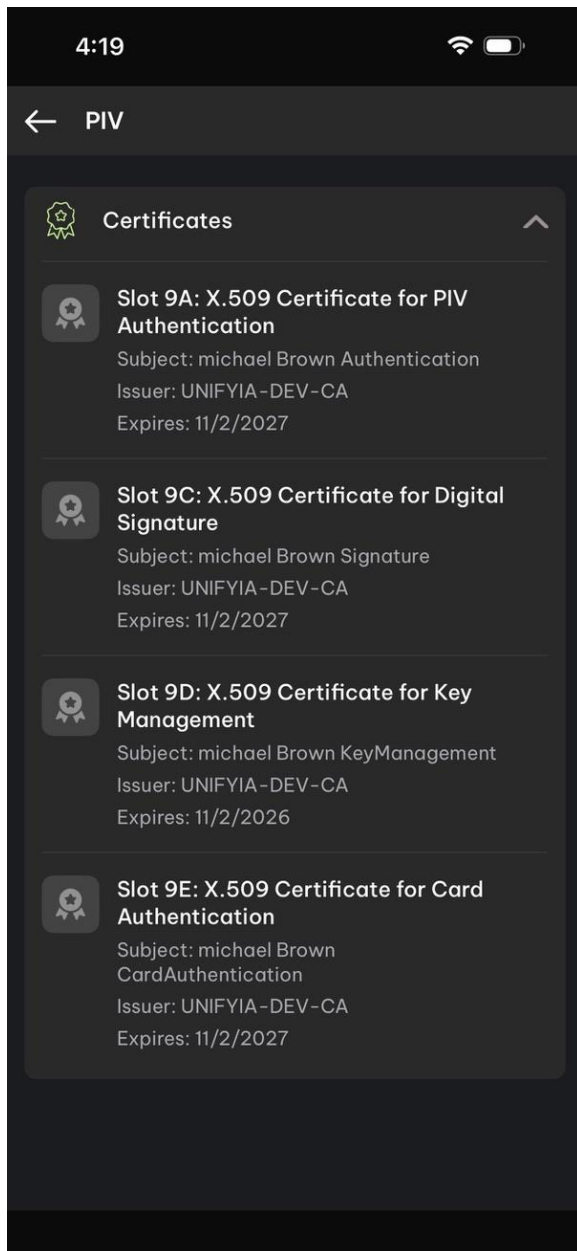
8.6 View PIV Certificates

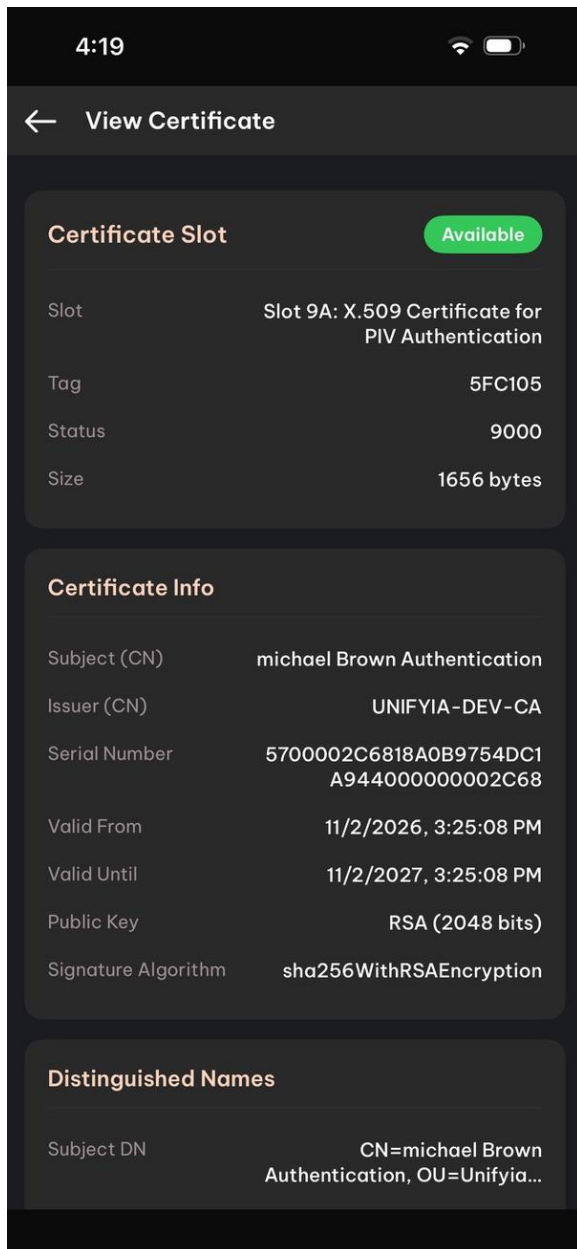
Access to PIV certificates requires successful PIN verification and hardware interaction.

PIV operations are supported in **USB (contact) mode only**.

Steps to View Certificates

1. Open the device
2. Navigate to the **PIV** section
3. Enter the **PIN** when prompted
4. If the device is not already connected, insert the security key via USB when prompted
5. Upon successful verification, the list of available certificate slots will be displayed



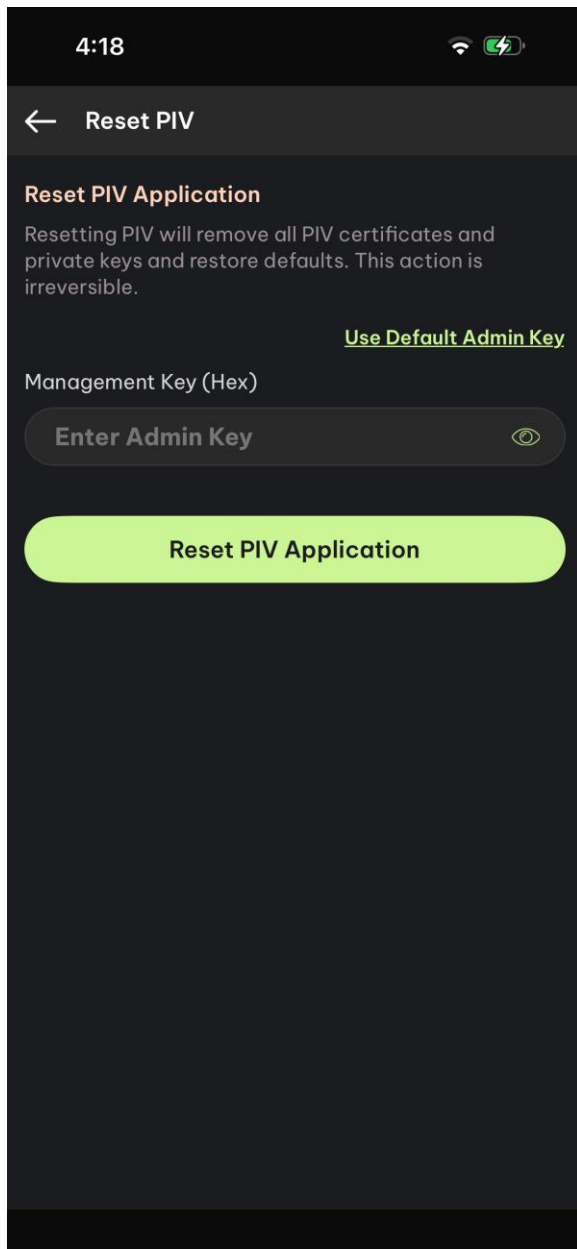


8.7 Reset PIV Application

⚠ Warning:

Resetting the PIV application will:

- Remove all PIV certificates
- Delete associated private keys
- Restore default configuration



9. PIN & PUK Policy

- PIN must be 6–8 digits
- PUK must be 8 digits
- Multiple incorrect PIN attempts may lock the key
- PUK is required to unlock a blocked PIN

5. Wait for confirmation

8.3 Reset PIN Using PUK

Use this if the PIN has been blocked by too many incorrect attempts.

1. Navigate to **PIV** → **Reset PIN (Using PUK)**
2. Enter the PUK
3. Enter and confirm the new PIN
4. Insert the device if not already connected
5. Wait for confirmation

■ Multiple incorrect PUK entries may permanently lock the PIV application.

8.4 Change PUK

The PUK (Personal Unlocking Key) is used to recover a blocked PIN. It must be **exactly 8 digits**.

1. Navigate to **PIV** → **Change PUK**
2. Enter the current PUK
3. Enter and confirm the new PUK (8 digits)
4. Tap **Change PUK**
5. Insert the device if not already connected
6. Wait for confirmation

After a successful update, use the new PUK for all future PIN recovery operations.

8.5 Change PIV Admin Key

The PIV Admin (Management) Key controls privileged administrative operations within the PIV application.

1. Navigate to **PIV** → **Change Admin Key**
2. Enter the current Admin Key (Hex) — or select **Use Default Key** if applicable
3. Enter the new Admin Key (Hex); use **Generate** to create a random key
4. Select the algorithm: **AES-128**, **AES-192**, or **AES-256**
5. Tap **Change PIV Management Key**
6. Insert the device if not already connected
7. Wait for confirmation

■ Store the new Admin Key securely. The previous key will no longer work.

8.6 View PIV Certificates

Access to PIV certificates requires successful PIN verification and USB connection.

1. Open the device and navigate to **PIV**
2. Enter the PIN when prompted
3. Insert the security key via USB if not already connected

4. Upon successful verification, available certificate slots are displayed
5. Tap a certificate slot to view full details

✓ Certificate data is read-only. Private keys remain on the hardware device and are never exposed to the app.

8.7 Reset PIV Application

■ **IRREVERSIBLE:** Resets all PIV certificates, deletes private keys, and restores factory defaults.

1. Navigate to **PIV** → **Reset PIV Application**
2. Enter the Admin Key (Hex) — or select **Use Default Admin Key**
3. Tap **Reset PIV Application**
4. Insert the device if not already connected
5. Wait for confirmation

After reset, all PIV credentials must be re-provisioned.

9 PIN & PUK Policy

Rule	Detail
PIN length	6 to 8 digits
PUK length	Exactly 8 digits
Incorrect PIN attempts	Multiple failures may lock the key; use PUK to unlock
Incorrect PUK attempts	Multiple failures may permanently lock the PIV application
Forget PIN	Use PUK to reset (PIV) or reset authenticator (FIDO2)

10 Security Architecture

ZTPASS Key Manager is built with a **security-first, zero-trust** design. Sensitive data never leaves the hardware device.

Security Feature	Details
No Account Required	Use immediately — no sign-up or cloud account needed
No Cloud Sync	All data stays on your hardware key
No Analytics / Tracking	Zero telemetry transmitted to ZTPASS servers
Screenshot Protection	App prevents screenshots of sensitive screens

Security Feature	Details
Screen Recording Block	Recording is blocked within the application
Hardware PIN Enforcement	PIN is stored and verified by the hardware key
Encrypted Communication	FIDO2/CTAP encrypted channel between app and key
Private Key Isolation	Private keys never leave the hardware device

11 Troubleshooting

Issue	Possible Cause	Resolution
NFC not working	NFC disabled, thick case, key position	Enable NFC, remove bulky cases, hold key near the NFC zone
USB not detected	OTG disabled, permission denied, wrong cable	Enable OTG (Android), use compatible cable, accept USB permission dialog
Incorrect PIN	Wrong PIN entered; remaining attempts decreasing	Check remaining attempts; use PUK to reset if blocked; contact admin if Admin Key needed
Key locked after resets	Exhausted PUK or PIN attempts	Reset FIDO (FIDO2) or Reset PIV Application (PIV) — all data will be lost
PIV options missing	Connected via NFC instead of USB	Switch to USB connection — PIV is USB-only

12 Support & Contact

ZTPASS Inc.

11710 Plaza America Dr, Suite 2000
Reston, VA 20190, United States

Email: connect@ztpass.com

Website: <https://ztpass.com>

ZTPASS Key Manager v1.0 — User Guide • February 2026
Copyright © 2026 ZTPASS Inc. All rights reserved.