

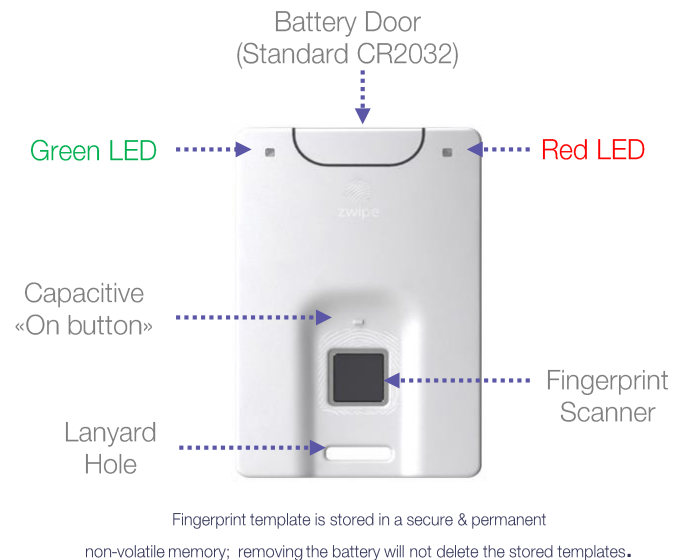
Zwipe Access – User Guide

Quick Start Guide

- 1) Remove Battery Door
- 2) Insert CR2032 Coin Cell Battery (+ side up)
- 3) Close Battery Door

The Card will start up immediately, and you will see **Green & Red** LED blinking 3 times for 0,5 Seconds

This means the card is ready for Fingerprint Enrollment, card registration and application/sector programming.



System Registration & adding Applications (13.56MHz)

Before a fingerprint is enrolled, the Zwipe Access card is unlocked and works like a regular contactless credential allowing the Card Serial Number (CSN) or Facility Code & Badge number to be freely read. Additionally, this is best time to add additional organizational specific applications/sectors to the card (13.56MHz cards only).

- Step 1) Turn on card either by entering it into an 13,56 MHz read/write unit or by touching Capacitive “On button”

.....▶ *Touching the fingerprint sensor during registration process initiates enrollment phase. Simply remove the card from the reader, let the card cycle off (up to 20 sec.) and start again.*

- Step 2) Registration: The reader will read the CSN or FC/Badge # and automatically enter it into your PAC system, or it will display that information for you to enter it into your PAC system. – card is active for 20 sec.

Application programming: Follow standard card programming process and tools (use your existing software and read/write unit). The card programmable for 20 sec. before it turns off.

- Step 3) After the card is registered in your PAC system, and/or programmed, proceed to the fingerprint enrollment phase by following the Enrollment Steps in this Guide.



Zwipe Access – User Guide

Enrollment Before You Begin

1. Watch the Zwipe Access Enrollment Video:

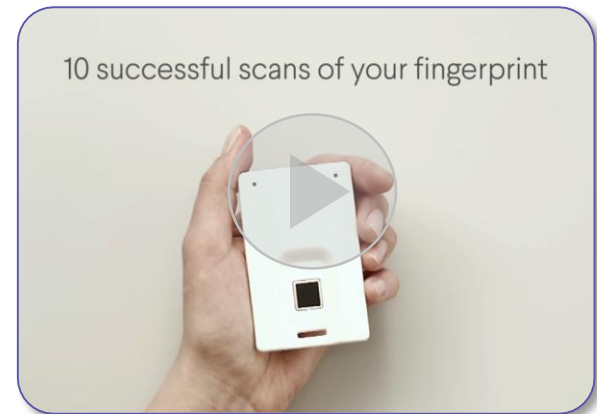
2. Wash your hands, for better captures

(As all future captures are matched with these initial captures, let's make the captures good).



3. Practice makes perfect

If you have a Zwipe Access demo card, use the demo card to practice best finger placements & become comfortable with the card, before enrolling on the normal mode cards.



Watch our Fingerprint Enrollment Video:

[\(Above image contains a link to video on PDF\)](#)

Enrollment & Usage - Finger Positioning Checklist

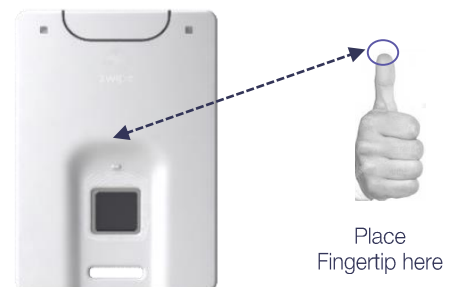
✓ Put center of your fingerprint flat on the scanner

Look at your thumb fingerprint, try to capture the center or "whorl" – this part of your finger contains the most useful data.



✓ Avoid using the fingertip

Generally the tip of people's fingers contain very little unique properties which can be used for matching.



✓ Aim the tip for the top of the groove

If the thumb fingerprint tip is placed at the top of the groove, then the center of the finger should be well placed on the scanner.

✓ Use moderate finger pressure

If you touch the scanner very weakly, then only a faint picture will be captured, if you press very hard, the image will be very dark, and the details may be distorted – moderate pressure is optimal.

Zwipe Access – User Guide

Fingerprint Enrollment Process

.....➔ A High Quality Enrollment of Fingerprint = Better User Experience with Card

- 1) Turn the card on by touching the capacitive “On button”,
The Green & Red LED will blink together 3 times for 0,5 seconds,
followed by a Green blinking LED indicating the card is ready for enrollment.



Put your thumb on the fingerprint scanner until you see a:

- Green flashing followed by 1 Sec. solid **Green LED** = Good Capture
- Green flashing followed by 1 Sec. solid **RED LED** = Bad Capture, try again

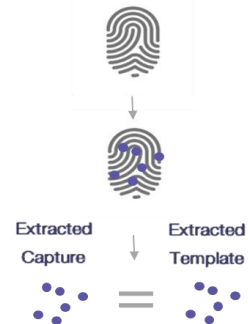
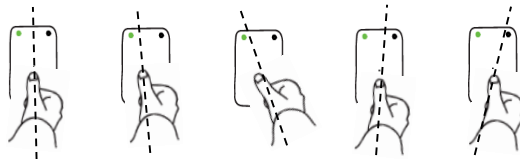
- 2) Once the Green or Red LED times out, remove your finger from the scanner, until you again see a green blinking light.

Interrupted During Enrollment?

If you are interrupted during enrollment or want to start over before enrollment was completed, simply allow the card to cycle off (up to 20 sec.) and restart the process – No fingerprint templates are stored before enrollment is successfully completed.

- 3) Repeat steps 1) – 2) until you have 10 good captures

.....➔ Position your finger slightly differently on each try & try to center finger on fingerprint scanner for better results in enrollment.



- 4) Once you have 10 good captures, the **Green** LED will light for 5 seconds to indicate the enrollment was successful, and after this the card will turn off – On next card start, the card is enrolled & ready to use.



Secure

Fast

Easy

Zwipe Access – User Guide

Daily Use

Touch the “Capacitive On” button to activate the card – you will see a Green blinking LED indicating that the card is ready for the finger (after 20 sec. the card will turn off). Place the enrolled finger on the sensor.

Green: If the Green LED turns solid, authentication has been granted allowing the card to communicate with the reader for 5 seconds. Hold the card to the RF reader.
After 5 seconds the card automatically turns off.

Red: If the Red LED flashes, remove finger from sensor and try again when the Green LED starts blinking. After 3 consecutive failures, the card will power down for 3 seconds.
After 3 seconds, just touch the “On” button to start over.

Zwipe Access LED Signals Overview

LEDs	Pattern	Meaning
Green & Red	3 * 0,5 sec.	Enrollment / Programming
Green	0,5 sec. blinks	Ready for Finger
Green	10/sec. flashing	Card processing
Green	Solid 1 sec	Good Capture
Red	Solid 1 sec	Bad Capture, try again
Green	Solid 5 sec	Enrollment Complete/ Authentication Complete ready for transaction
No LED	N/A	Lift Finger
Red then Green	4 * 0,5 sec alternating	Battery Low Power Indicator





Secure

Fast

Easy

Zwipe Access - User Guide - FAQ

How is the fingerprint data stored on the card?

- a. During enrollment, the fingerprint scanner captures a 3D representation of the finger and sends this to the patent pending algorithm which extracts the unique information used for matching and stores this as a data template **no full fingerprint is stored**. More precisely, a hash cryptogram is made of the template, and this is permanently saved within the processor's non-volatile memory. The processor is hereafter locked down to ensure confidentiality of the firmware and fingerprint templates.
- b. The Zwipe hash of a fingerprint, has no value in any other fingerprint based system.

How does the Zwipe card prevent RF (Radio Frequency) communications?

- a. RF communications between the transponder and reader is locked down until proper authentication is granted by the "fingerprint system" on the card. Once authentication is granted the card allows full two-way read & write communication between the transponders and RF reader for five (5) second before terminating the session.

Does the Zwipe processor communicate with the RF transponder?

- a. Biometric enrollment and authentication is **100% independent** of the embedded RF transponder (i.e., Prox or Mifare chip) so that there is no communication link between the two – and there is thereby no way to interact with the fingerprint data over the RF transponder (i.e. Prox or Mifare), once the fingerprint is stored in the card.

Can I read/write to the RF transponder after the card owner's finger has been enrolled?

- a. Yes, after authentication has been granted by the card, a standard RF communication session is established between the transponder and reader. During this session the card's data file or files can be updated on the card for 13.56MHz based transponders. A new application/segment can be loaded (i.e., Mifare vending application) or an existing segment/data file can be updated.

What is the Battery life?

- a. Zwipe credentials use a standard replaceable #2032 coin cell battery readily available at any retail outlet. The battery supports up to 4,000 authentications, which can range from 1 to 2 years depending on daily use. We recommend changing the battery once a year.
- b. If the battery is low, the LED will blink Green-Red-Green-Red four (4) times after authentication. While the cards still works, please replace the battery. If the battery is completely drained, no lights will appear. If this occurs simply replaced the #2032 cell battery.

Do I need any external fingerprint programming tools or API?

- a. No, the entire fingerprint enrollment process is conducted directly and entirely on the card. The card cannot communicate any biometric information to any external device.

How long does it take to authenticate a finger?

- a. Less than 1 second.

Do the cards come with any external identification number?

- a. Zwipe cards comes with an external, generic, serial number, it is not the CSN or FC/Badge#.



www.zwipe.com

ZAC20160722

ZWIPE EUROPE: +47 98 07 60 64
ZWIPE NORTH AMERICA: +1 331 472 3140



Secure

Fast

Easy

Zwipe Access - User Guide - FAQ

How do I program the card into my Access Control software?

- a. Prior to fingerprint enrollment, the embedded RF Transponder's CSN/UID or Facility Code/Badge number are freely read as the card is unlocked – just as a regular mifare or prox card - and can be easily read by your existing badge enrollment reader and entered into your PAC (Physical Access Control) or LAC (Logical Access Control) system.
- b. After the card is programmed into your PAC and/or LAC system, the employee should then enroll their fingerprint directly on the card which "locks" it to the user, so only they are able to use the card after enrollment.
- c. Optionally, have the card owner first enroll their finger directly on the card to establish card ownership. Then have the employee authenticate on the card and then hold the card to the PACS reader to associate the card to the PAC database – there will be a 5 second programming window after each verified authentication.

What happens if I remove the battery?

- a. Because the fingerprint template is stored in non-volatile memory, removing the battery does not erase or delete the stored templates.

Is the card tamper resistant

- a. The Zwipe credential is tamper resistant/evident using a combination of a special liner for water resistance and internal locking posts. Attempts to open the card would cause physical damage to the internal posts indicating the card has been tampered with.

Does the card lock out after a certain number of authentication failures?

- a. The credential allows 3 failed authorization attempts then powers down. The authentication process can immediately start again by powering up the credential. Zwipe has not incorporated a permanent lock out feature.

How durable is the card?

- a. Treat your Zwipe credential like your cell phone (or better), for years of use. The credentials hold up well being exposed to dirt, grease, moisture, and the occasional drop. The cards are water resistant, not water proof, and operate best between -20° to 40° C. The fingerprint sensor is tested to 10 million scans and has a protective scratch resistant material over the sensor's surface.

Can I personalize the card for an employee?

- a. Yes, the back side of the card accepts most standard clamshell badge ID labels, with or without, a slot opening. Such badge labels can be printed in most standard CR80 / ISO7810 compatible credential printers.

What is the warranty?

- a. All Products sold are warranted against defects in workmanship and material under normal use for a period of twelve (12) months. Products which have been subjected to unusual physical, environmental or electrical stress might not be covered under warranty.

Can I reissue a Zwipe Access card?

- a. For security purposes, only Zwipe or an authorized channel partner has the tools to delete stored templates so that a card can be reissued. Deleting the fingerprint templates does not impact the transponder or any application stored on the transponder.

How long does it take to enroll a finger?

- a. Less than 60 seconds.



www.zwipe.com

ZAC20160722

ZWIPE EUROPE: +47 98 07 60 64
ZWIPE NORTH AMERICA: +1 331 472 3140