What is Zwipe Access?

Zwipe Access is a card-based fingerprint access control solution. Fingerprint capture, extraction, and comparison are performed completely within the Zwipe Access card. This means that the cardholder's biometric data never leaves the card, providing increased data privacy to the cardholder.

Zwipe Access enables two-factor authentication using biometrics without the need of an additional fingerprint reader. The card verifies the enrolled cardholder's identity and the access control system then verifies the card's authenticity and integrity.

Zwipe Access uses a Java Card infrastructure that allows Java Card-based applications (applets) to be run securely within the platform. With Zwipe Access, HID® Seos® and LEGIC advant applications such as access control, time and attendance, network login and secure printing can be virtualized and combined with strong fingerprint authentication. Customers may also run their own Java Card applications, such as FIDO, PKI, Crypto wallets, secure storage, or any other custom applications on the Zwipe Access platform.

Zwipe Access shares its platform with our payment product, called Zwipe Pay, which has undergone the security and durability testing mandated by payment schemes (like Visa & Mastercard) for the daily usage of payment cards. Zwipe Access has also undergone testing performed by both HID® and LEGIC following their standard procedures.

Zwipe Access is designed as a "Biometric System-on-Card" for organizations of any type or size to quickly and securely add instant authentication to their existing access control system, without the need to upgrade to expensive software or install biometric readers throughout their facility.

In review, Zwipe Access:

- Is card-based fingerprint access control
- Enables two-factor authentication
- Uses Java Card infrastructure
- Works with HID® Seos® and LEGIC advant
- Has undergone strict durability testing
- Is a "Biometric System-on-Card"

How Zwipe Access Works

Zwipe Access uses a batteryless, passive inlay to capture and securely transfer the cardholder's fingerprint data to the Idemia Secure Element on the card. The secure storage of that fingerprint data, which the enrollment process converts into a biometric template, means that there is no external storage of the cardholder's biometric data and therefore a much-reduced risk of identity theft or infringement of government privacy laws.

The Secure Element's hardware and software tamper-proof mechanisms make it virtually impossible for an attacker to access the smart card's memory. Moreover, it is not possible to convert a biometric template back into the fingerprint from which it was computed. Simply put, a live scan of the cardholder's finger is matched against the stored biometric template to accurately verify that the one presenting the card to a reader is indeed the enrolled user of that card. When the card is presented, the RF field of the reader empowers the card and only the access control data is gleaned to verify the user's access rights.

Once enrolled there is only one user of the card, as anyone else will not get a biometric match when placing a finger over the sensor. The card will also not work for the enrolled cardholder unless they correctly place an enrolled finger over the sensor when presenting it to a reader. If there is no match, the card will not release the access control information. Zwipe Access is true multifactor authentication in a secure, handheld biometric system.

Before enrollment, Zwipe Access cards can be personalized on any thermal dye sublimation, retransfer or inkjet (drop-on-demand) ID card printer, as long as there is no printing directly over the smart chip or fingerprint sensor. You can personalize them just as you would any other ID or access card.

Zwipe Access biometric enrollment is also fast and easy, and can be done with an approved card reader in less than 30 seconds.

- Biometric Template
- Batteryless Inlay
- Tamper-proof Security
- RFID Reader Powered
- Privacy Compliant
- True Authentication
- Printer Compatible
- Easy Enrollment

Where Zwipe Access Works

Zwipe Access can work anywhere you are using an HID® Seos® or LEGIC advant reader. And it works for any application that you would regularly use access control. Opening doors or parking gates or asset lockers or any other physical access control application is no problem at all.

Zwipe Access also works for any logical security application you might already use as well, such as logging into your office computer, network access for remote workers or any other cybersecurity application you need.

Zwipe Access simply gives you the ability to quickly and easily add true multifactor biometric authentication to your existing access control infrastructure.

And it works for any organization of any type or size. Whether you need to enhance your access control solution for thousands of employees across a global enterprise, or just increase security for a handful of authorized personnel in a single location, Zwipe Access is the most cost-effective way to add biometric authentication to scale.

Airports, seaports, data centers, public utilities, hospitals, research laboratories and critical infrastructure facilities are just a handful of locations where increased security through biometric authentication has become essential. Zwipe Access is a perfect fit for them all.

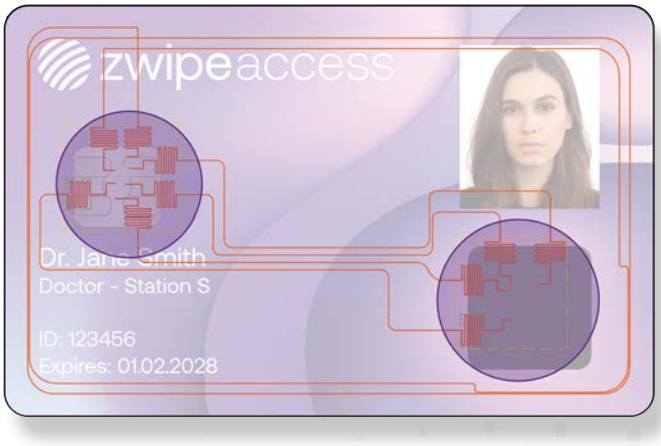
Zwipe Access not only works for physical and logical access control, but also allows organizations to include their own Java Card-based applets for additional functionality. This increases the value of Zwipe Access by letting you customize where it can be used within your facility, on your campus or across your fleet.

Also, in light of recent pandemics, Zwipe Access is a frictionless solution, as the enrolled user touches only the sensor on their card and not a shared biometric reader.

- Airports & Airlines
- Seaports & Maritime
- Healthcare Facilities
- Data Centers
- Public Utilities
- Research Labs
- Critical Infrastructure
- Corporations

Technical Specifications

Zwipe Access is currently available in two formats: HID® Seos® and LEGIC advant. Apart from the application specs for those access technologies, below are some of the key technical details on the physical makeup, chipset and certifications of Zwipe Access cards. For more information on the HID® Seos® or LEGIC advant applications, please refer to their individual product data sheets.



BIOMETRIC SECURE ELEMENT

Secure Element	Idemia Starchip® SCR496U
Architecture	CORTUS® APS3cd 32-bit core with RISC
Interfaces	ISO/IEC 7816-3, Class A&B, ISO/IEC 14443, Type A

FINGERPRINT SENSOR

Fingerprint Sensor	IDEX Biometrics IDX3405
Fingerprint Sensing Technology	Off-chip capacitive
Fingerprint Active Sensing Area	9.5 mm x 9.5 mm

FUNCTIONAL

Operating Frequency	13.56 MHz with ISO/IEC 14443 Type A
Communication	ISO/IEC 7816-3, ISO/IEC 14443 Type A
Communication speed	848 kb/s (ISO/IEC 14443 Type A)
Typical Maximum Read Range	2-5 cm (depending on the reader used)
NVM Memory Type	FLASH
Write Endurance / Data Retention	Min 500,000 cycles / 10 years
Platform	Oracle Java Card Platform, Classic Edition 3.0.4 and Global Platform Card Specification, v2.3 with Global Platform Financial Configuration, v1.0.2
Security Certification	EMVCo certified Hardware platform
Durability Certification	Mastercard CQM & Visa Biometric Card Body Innovation Testing
Multi-application Support	Yes
Available Platform Memory	200 kBytes

PHYSICAL & OPERATIONAL

Dimensions	ISO/IEC 7810 ID1 size - 85.6 × 53.98 × 0.68 mm3
Material Composition	5-layer symmetrical laminated PVC with embedded copper wire inlay
Operating Temperature	0 °C - 45 °C
Operating Humidity	20% - 80% RH, non-condensing
Operating Lifetime	5 years (normal use conditions)
Printable	Yes, on front avoiding fingerprint & contact chip area & all of back, using dye sublimation, inkjet/drop-on-demand & thermal retransfer printing technologies
Slot Punch	Not available

Zwipe.com/Access
sales@zwipe.com
US: 954-649-6222

Zwipe AS
Henrik Ibsens gate 90
N-0255 OSLO, Norway