e-data.com | 866.807.3549

Biometric Access Control | Retail Applications

Benefits of e-DATA Access Control with Fingerprint Key biometric reader

The proper access control equipment can be the most cost effective measure to deter theft at any retail store. With the increasing affordability of fingerprint biometrics, access control systems now offer a greater level of ease and security by eliminating keys and cards. Yet despite an industry wide trend toward greater sophistication, nearly all access control systems still rely on legacy platforms that require a dedicated computer or server in each store. Based on a software embedded platform, e-DATA stands apart in developing next generation technology that eliminates the brass key without introducing the access card or fob.

With e-DATA, access control works with any IT infrastructure, or stands alone in the WAN. No longer requiring external servers or software, users can manage their stores' access system from anywhere in the world with the internet. And with the Fingerprint Key, e-DATA has made biometrics as simple to install and use as a standard card reader while eliminating the hassle and security-risk of cards.

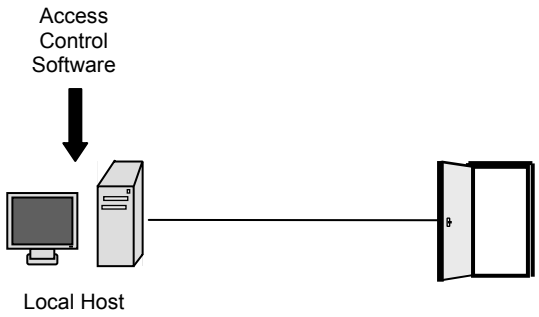
The Fingerprint Key combined with e-DATA's access control system, creates an unmatched offering that should usher in widespread use of biometrics and internet-based access control.

Traditional Retail Access Control

Legacy access control platforms force users to use a dedicated server or computer to run a locally managed access control system. Users must install access control software to a computer or server and access the software locally to make access right modifications. For example, if a user wanted to give someone nighttime access, they would have to go to the host computer and make changes to the software application locally. In these systems the host server or computer must run constantly in order to support any and all actions, from changing access rights to verifying a proximity card for entry.

Exhibit 1

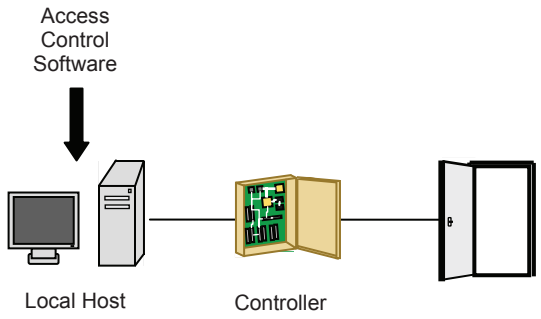
Traditional Centralized Access Control



In other systems, access control is run on a distributed system, but e-DATA Access Control offers a new level of distribution that eclipses the distributed architecture.

Access control systems that run on the distributed architecture rely on a local host for any access control change to the system. For example, if an administrator wants to change access rights for a particular room, he must access the computer that houses the application to change the criteria for access. The controller then houses the changes in access rights to be used the next time the person tries to gain entry. Access control information is distributed between the host computer and controller, and the controller carries out these access rights settings to open a door when appropriate (see Exhibit 2).

Exhibit 2
Traditional Distributed Access Control

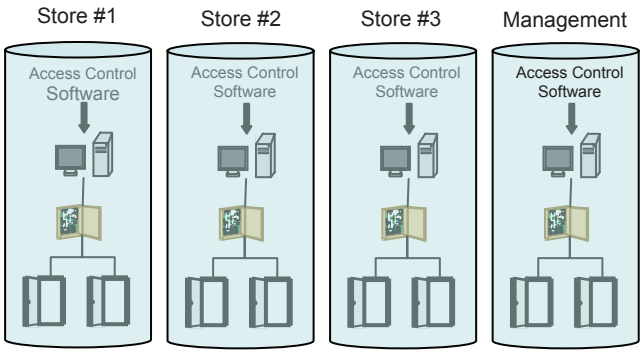


Limitation #1: Dedicated Server Required
With traditional access control modeled in Exhibit 1 and Exhibit 2, users must allocate a dedicated computer or server to run the software. This creates complications installing and maintaining software and configuring a server to act as an access control host. With these systems, access control becomes another program that the IT department or store manager has to maintain along with other programs vying for time and hard drive space.

Limitation #2: Local Software=Local Administration
Because software is hosted on a local server and controllers and readers are connected directly to the host, administration of software must be managed locally. In order to make changes to the access control system, you must access the host and make changes to the installed software.

Limitation #3: No Enterprise Solution
Unlike e-DATA's products, traditional access control hardware is not designed as a network application. With dedicated hardware hosting software that is administered locally, traditional access control makes it difficult to manage multiple stores. In order to make these systems work, each store must download software to local computers or servers. Because these servers or computers were not designed to communicate as a network access control system, each store becomes isolated by the limitations of a dedicated server that cannot communicate without extensive software and hardware peripherals. Each store is an access control silo (see Exhibit 3) instead of a branch in an access control network (see Exhibit 4)

Exhibit 3
Traditional Access Control with Multiple Stores



Traditional Biometrics
When you combine traditional biometrics with the current access control systems, the complexity is compounded, creating a complicated jumble of hardware and software that is difficult to install and almost impossible to manage.

With traditional biometrics you encounter many of the same problems found in traditional access control systems.

Limitation #1: Dedicated Server Required
Just like access control, traditional biometrics readers require dedicated hardware to host biometrics software that stores templates.

Limitation #2: Local Software=Local Administration
With software hosted locally, users administer biometric templates through a local host.

Limitation #3: No Enterprise Solution
Because all software requires local hosting and administration, systems are constrained by the limitations of local hardware. If a user wants to register a fingerprint, he must register locally and store the template on local hardware.

e-DATA Biometric Access Control
e-DATA Biometrics eliminates many of the limitations that have plagued systems designed on legacy platforms. Its flexible design makes it ideal for various applications, particularly those involving a mobile or floating workforce interacting over multiple sites.

e-DATA Access Control is entirely web based. All Master Unit hardware is IP configurable, so each intelligent piece belongs to a network. This connectivity makes the entire system expandable. So if you want to manage a single store or multiple stores around the world, you can, with an integrated network managed over the web.

e-DATA Access Control offers many advantages over the traditional access control system. The advantages combine to create an unparalleled product for retail installations.

Advantage #1: Embedded Software
e-DATA's access control products come with software embedded directly on the hardware. With embedded software, you will never have to install or maintain access control software again. The access control software sits outside of IT systems and is open source and Linux based.

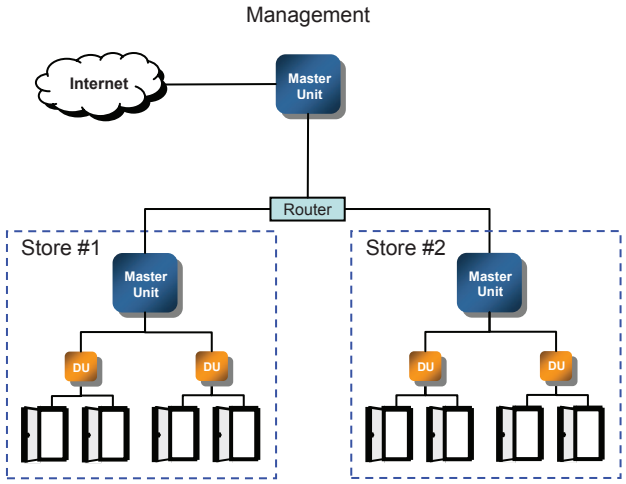
Advantage #2: Internet Based=Global Administration
With embedded software and web connectivity, all e-DATA Access Control products can be managed over the internet from any location in the world. Instead of managing software from a single location, users can modify the access control software from anywhere.

The embedded, internet based application is not a feature that requires extra hardware peripherals but is standard on the e-DATA Access Control. With no modifications, e-DATA products can be accessed over the internet from anywhere in the world with any browser-enabled device.

Advantage #3: Infinite Enterprise Solution
e-DATA Access Control is scalable to meet the needs of any size solution. In order to increase the size of an access control system, users simply add additional Master Units. These Master Units then support local door controllers and readers. The Master Units are easily managed at the local site or at any site in the world. This flexible framework allows for simple and quick expansion. If you need to manage more stores or more areas within a store just add another branch to the tree with a Master Unit or Door Unit (see Exhibit 4). This eliminates the silos of traditional access control systems and allows management to maintain and grow its access control network without dedicated local computers and without installing any software.

Advantage #4: Reduces Total Cost of Ownership
Clients run and update any operating system without worrying about reinstalling access control software or about the interoperability of the new operating system with the access control software. The only time users need to update their access control software is when they want to download the latest features and version. Unlike other access control systems, they are not forced into cost extensive updates caused by changes in server databases and operating systems.

Exhibit 4
e-DATA Access Control with Multiple Stores



The Fingerprint Key Biometrics
Unlike traditional biometrics, The Fingerprint Key is as easy to install and manage as any card reader. Your finger is the only key you'll need, and it can't be lost, stolen or borrowed.

The Fingerprint Key requires no additional hardware or software to manage templates. Like traditional card readers, The Fingerprint Key can be added to any Door Unit (DU, door controller) in e-DATA Access Control.

The Fingerprint Key achieves simplicity of installation and use by being built on the same software-embedded platform as the access control system. Like the Master Unit and Door Unit, The Fingerprint Key comes with software embedded on the hardware. This design brings the ease of e-DATA Access Control to biometrics.

Advantage #1: Embedded Software
Like the e-DATA Access Control, The Fingerprint Key's embedded software eliminates the need for extra hardware or external servers or host computers. Templates are managed in The Fingerprint Key allowing the entire access control process with biometrics to occur without the need for any additional hardware or software.

Advantage #2: Manage and Transfer Fingerprints Globally
Another key feature that distinguishes The Fingerprint Key from other biometric readers is the ability to transfer fingerprint templates anywhere in a network. This allows administrators to register employees only once and then transfer templates to any other Fingerprint Key readers on the network.

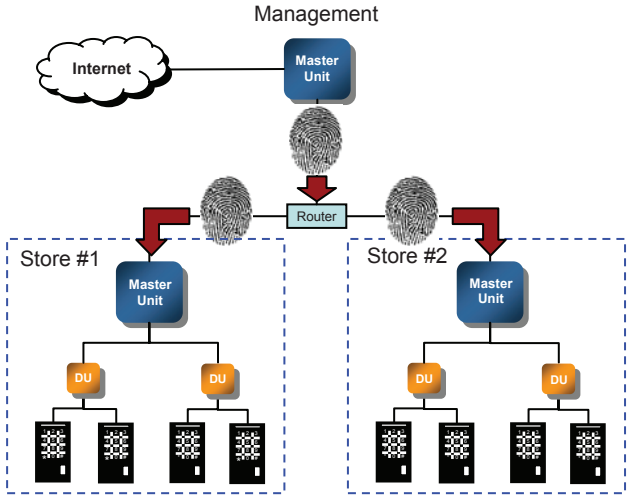
For example, a pharmacist originally registered at a store in Chicago needs to cover a weekend shift in Evanston. Instead of having to register at the location in Evanston, the access control administrator can send the individual's fingerprint template to The Fingerprint Keys in Evanston by logging on to the e-DATA Access Control application over the internet (see Exhibit 5). The administrator changes the pharmacist's access rights for the Evanston store for that day and when the pharmacist arrives on the property in Evanston, she will have all the access rights she needs to enter the store and open secure areas and cabinets.

The propagation of the pharmacist's template to the Evanston location occurred with the click of a button over the internet when the administrator granted the pharmacist access rights for the day. This same scenario can be duplicated an unlimited number of times at locations across the country all over the internet in a matter of seconds. The Fingerprint Key eliminates the need to register at multiple facilities, simply register once and propagate when needed.

Exhibit 5
Fingerprint Propagation: Register Once, Send Anywhere

Advantage #3: Infinite Fingerprint Keys on Access Control Network
With the e-DATA Access Control, each Fingerprint Key can be addressed over the Web. This allows administrators to manage individual readers from anywhere in the world over the internet. Each Fingerprint Key acts as a part within a larger access control network. This system allows for the management of specific readers regardless of the network's size. So whether you are managing one reader or a thousand readers you can make changes to any individual reader on the network. This allows for intelligent expansion to potentially infinite scale.

Exhibit 6
The Fingerprint Key Network



Advantage #4: Eliminate Keys, Lock Changes and Cards
All e-DATA products were created to support biometric credentials without any software or hardware. This allows retail store owners to eliminate the use of keys and cards, increasing the level of security and saving time and money related to card procurement, theft and turnover.

Without keys, stores never have to worry about the cost of lost keys or the cost of changing locks. Employees cannot lose their fingerprint, ensuring that secure areas are truly secure. Along with the savings related to reduced shrinkage, biometrically secured access control eliminates the cost of purchasing and replacing cards and locks. And with biometrics, businesses are not substituting the expense of keys with the expense of cards; they are eliminating the problem at its source.
By building systems built around biometric technology, e-DATA makes the most secure access control systems that happen to be the most economical.

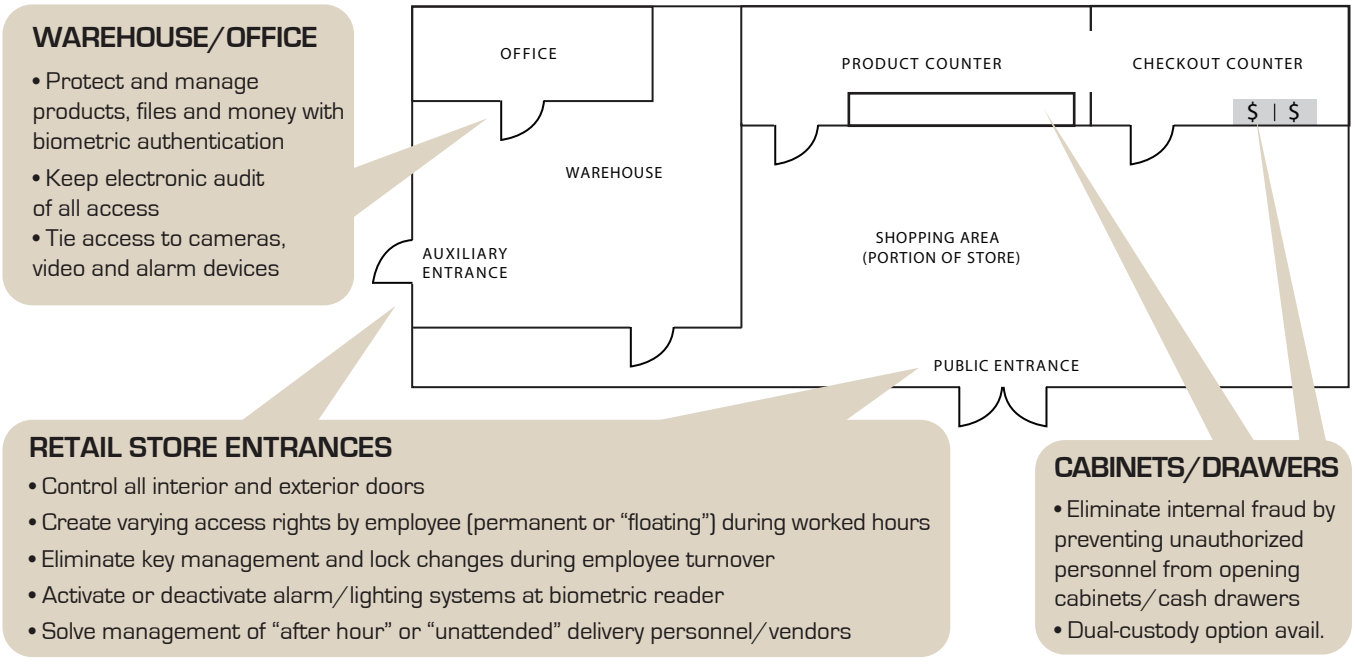
Advantage #5: Track Access Events
Each time an employee gains access using The Fingerprint Key, the embedded access control software creates a time stamp of that event. This allows businesses to review reports if an incident occurs, easily track code compliance and have a more detailed record of all access related store activity.

Advantage #6: 3-in-1 Solution
A keypad comes standard on all Fingerprint Keys giving corporations the option and flexibility to use biometrics alone, biometrics plus keypad or keypad only. Also, e-DATA offers a model of The Fingerprint Key that comes with an embedded iClass reader providing the flexibility of three credentials (keypad, biometrics and smart card) in one unit. These credentials can be used in any combination or independently, giving users every reader option. Also, because e-DATA's readers can be managed through e-DATA's embedded access control software, businesses can utilize different credential types at different stores or different areas in a store with all various credentials interacting over the same network.

Advantage #7: Eliminate False Alarms
Authenticate the users of your intrusion system through e-DATA Biometric Alarm Interface Control: Eliminate PIN confusion that leads to false alarms and PIN recoding for new users/PIN removal for old users -- without replacing your current alarm system. This is especially effective for after-hour/night vendors and deliveries. Alarm and access can also be tied to cameras and video monitoring.

e-DATA's Alarm Interface allows users to merge e-DATA Biometric Access Control with standard burglary systems. By presenting their authenticated finger right at the Fingerprint Key, users can disarm and arm an alarm. Combining these systems fosters greater ease of use and eliminates false alarms. Only those who are authorized to turn on/off the alarm can enter a building.

Conclusions
With embedded software, a Web-based design, fingerprint propagation and alarm interface, e-DATA offers an unmatched suite of features for retail store access control. The robust offerings are combined with systems designed for quick and easy installation, dramatically cutting down the time for setup, whether at one store or thousands. And whether its for one door or 96 doors.



About e-DATA

e-DATA is a leading manufacturer of Web-based appliances used for biometric access control and biometric time & attendance. Our offices are located in Coppell, Texas (Dallas), and Leonberg, Germany (Stuttgart).

In 1999, e-DATA developed the first network-ready, Web-enabled data collection terminal using Java on a Linux OS. For more than 15 years, e-DATA has developed and deployed enterprise-level access control systems that are used by major banks, retailers and pharmacies. Building on that foundation, e-DATA has developed a full line of feature-rich access control and time & attendance products with the software application embedded in the hardware, eliminating the need for servers and software.

The company was founded by Dietrich Titze more than 20 years ago near Stuttgart, Germany, under the name Titze Datentechnik GmbH. Today, e-DATA is led by Chairman George K. Broady and President John Carter.