Access control and Identification : what it is and what it means

Many users often speak about electronic access control systems and identification without really knowing in detail what they are talking about. However they base their decision in which system is the best for their needs on the little knowledge they have. Often this results in an oversized system with the wrong ID technology.
Each technology, starting from the simplest keypad up to the complex read/write system has its own application domain.
Therefore we feel that some explanations in this field will be very welcome.

A word about identification

All electronic access control systems have 1 main function : identifying a person before deciding to unlock the door or activate a device. The identification method used can be divided into three categories.

1) PIN-only systems

These are the least secure. And even here, a subdivision can be made.
Systems with a single common code – where everyone uses the same number – are the cheapest and least secure.
Slightly better are unique PIN systems, where each person has a different number Here at least you can sometimes delete a single user code if it has become “unreliable”. But still the risk remains that a code is passed on, deliberate or accidental, and little way of retrieving what happened.

2) Token-based systems

This type is the most popular. Token-based systems use cards, tags etc. and offer much better security. Each token is usually unique and if you want even to increase security (so that stolen tokens can not be used anymore), you can add an extra PIN number (just like a cash machine).

The choice of card technology can be very confusing at first, but each technology has its own characteristics and pricing and therefore its own applications. Basically, there are two types : swipe cards that need to be inserted or swiped through the reader, and those where the card is read at a distance. This second type is mostly short range (i.e. proximity) working from 10 cm up to 60 cm.

3) Biometric systems

Biometric systems are only at this moment, after being available already for several years, starting to find some minimum acceptance in the security market. The most popular in terms of cost, accuracy and acceptability seems to be fingerprint recognition. But also facial recognition and iris recognition are available on the market. Quite often these systems are not as rapid in terms of identifying the user and offer a poor price/performance ratio. As a result, this type of systems is only finding its applications in the high security domain.

Components of token-based systems

1) Card or tag

This is the identifier of the person. It usually is credit-card-sized or shaped like a key fob. Sometimes, it can be shaped as a bracelet or inserted in a watch or ring. Depending on the technology, it has to be “swiped” through the reader or just presented within a few centimetres (“proximity”) of the reader. Some even don’t need to be removed from the pocket (“hands-free”).

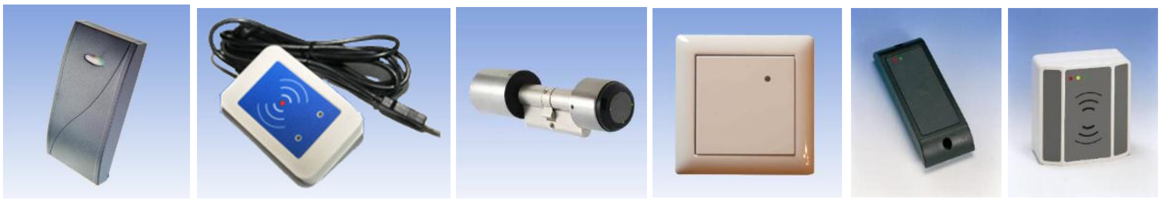
The choice of technology will be based on cost of readers and cards, the level of security needed and the personal preference. Sometimes there is a pre-existing reason for choosing (e.g. if time and attendance cards have to be used also for access control). An overview of the different technologies with their costs is shown below :

Technology	**Reader cost**	**Card Cost**	**Security**	**Other remarks**
Magstripe	Low	Low	Low	Cards are easily damaged. High risk of copying cards. Readers are usually not weatherproof.
Bar code	Low	Low	Low	Cards can very easily be copied. Very low security level.
Proximity	Medium	Medium	Medium	Easy to use. “Passive” cards (i.e. without a battery) offer unlimited lifetime. These are the standard tags for many applications.
Hands-free	High	High	Medium	Limited lifetime of cards due to integrated battery. Risk of unwanted readings when passing to close to a reader.
Smart Card (e.g. Mifare, Legic, …)	Medium	Medium	High	Offers possibility to integrate several different systems on a single card without data being merged.

2) Reader

This device is what identifies the person at the door by reading the card and sending its unique code to a control panel.

Some readers are less vandal-proof than others, but mostly the reader does not carry any intelligence or door opening devices. Attacks on a reader will therefore very rarely result in unauthorised access, but only in a damaging of the reader. Proximity readers offer the option that they can be installed hidden behind panels so that there is no way to get hands on them.



Some examples of ProxTech readers : from left to right : Premium, DESK, PT-Lock, NOVA, Mini and MCR

If there is a need to control both entrance and exit, two readers are required, one on each side of the door. This offers the possibility of knowing everyone's whereabouts at all times, but then you will have to keep in mind that every employee will have to pass his card each times he passes a door, even when this door is kept open by a colleague…

Readers can be found in a wide variety of shapes and designs. Most know are the mullion or wall mount readers, which are located normally next to the door. Sometimes the reader can be integrated into a special housing, such as a switchbox for perfect blending with a building's architecture.

And sometimes, it can even be integrated into the door lock cylinder to avoid all cabling.

3) Controller

Controllers receive the data sent by the reader and usually decide on whether the door is to be opened or not. There are types with a built-in reader or others using remote readers. Controllers may control one or several doors.

For networkable systems, the different controllers can be linked into a network. Connection between the controllers and between controllers and the host PC is usually done via a bus. Although a bus structure such as RS485 is still very commonly used, modern controllers offer also the option of TCP/IP interfaces. With this type, you can connect your controller via a standard Ethernet bus.

4) Software

In some more complex installations (when several doors have to be controlled), software makes it easier to program cards and define the access rules for the system. This information is usually then sent to the controllers. That way it is the controller that makes the final decisions.

Software will also be very useful for monitoring and recording events (e.g. who has passed where and when), saving the information and creating reports.

5) Lock

Locks are available in a wide range of types. The choice of lock mainly depends on the door type and on the required resistance to attack.

All types have their advantages and disadvantages. In most cases it is best to consult a specialist to get the needed advice.

6) Door sensor

The door sensor is an optional component, used to detect the opening state of the door. The control panel can receive the information on whether a door is closed or opened and decide to sound an alarm if the detected opening is “unauthorised” or when the door is not closed again within a set period after an authorised opening.

7) Egress button

Again, an optional component to allows people to pass a door without the use of a card or PIN through a door. Of course this is only acceptable when passing from a secure area to a less secure area. Pushing the button causes the lock to be released, just as if a card had been entered.

A commonly used application for this is a button at the receptionist to let visitors enter a building

8) Door Ajar Sounder

Even the most advanced access control system is useless if the door is propped open. If a door sensor is fitted, this situation can be detected and an alert can be sound.

Different types of System

A quick word on the most commonly used types of systems on the market :

1) Stand-alone single door systems

The simplest system is a combined reader/controller, providing a convenient all-in-one package. This is used to control access at a single door and can easily and quickly be installed. These systems sometimes don’t offer the options of a door sensor. Programming is very simple and done directly on the unit mostly with master cards and a keypad. A fine example here is the PL1000 of ProxTech.

Figure : ProxTech’s PL1000 system

The highest risk with this kind of products is that the intelligence, i.e. the place where the decision is taken and the door opener is activated from, is on the insecure side of the door, and therefore liable to attack. Some better systems, e.g. ProxTech's PL3000, offer the possibility of fitting a non-intelligent slave reader on the insecure side and the controller unit on the secure side of the door.

2) Stand-alone multiple door systems

When multiple doors have to be controlled, a suitable controller for this number of doors has to be installed. Controllers can be found for 2, 4, 8, 16, … doors. This can have a positive influence on the cost since there is only 1 controller, but it will also result in a higher cost of cabling. It is needed here that all pros and contras are carefully reviewed.

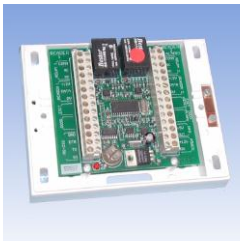


Figure : ProxTech's PL962 2-door stand-alone access controller

3) Networked systems

Above stand-alone systems don't need a computer and software for the installation. However for multiple door situations, it will very soon prove to be more advantageous to use software based systems with a network of separate controllers, each controlling a part of the doors.

Figure : ProxTech's AccessPLUS networkable access control system

Conclusion

As you can see for yourself, for every single application, a solid study is needed to come to the appropriate system. And then we even didn't mention the special situations, such as car parks or elevators that need to be controlled, or systems needing to make a different identification of both visitors and employees.

At ProxTech we have decided to make this decision a little bit easier. As in most cases people first select the type of system and the controller and then are bound to take up the card technology that is supported by that system, this often results in the wrong card

technology being used in that specific application. ProxTech’s entire RFID reader range of card readers is however available with a wide variety of interfaces, so they can be connected to almost every controller. Now you can freely make your choice of card technology (or use the same cards as you’re already using for e.g. time and attendance) regardless of the rest of the system.
Of course, sometimes this will require some investigation, especially when the data format on the controller is not known. But then our engineers will be at your service to assist you in a very efficient way.

Contact Details:

bvba ProxTech International
Zakstraat 104
9112 Sinaai (Belgium)
Tel : + 32 (0)3 722 91 60
Fax : + 32 (0)3 722 91 66
E-mail : luc@proxtech.com
Web site : www.proxtech.com