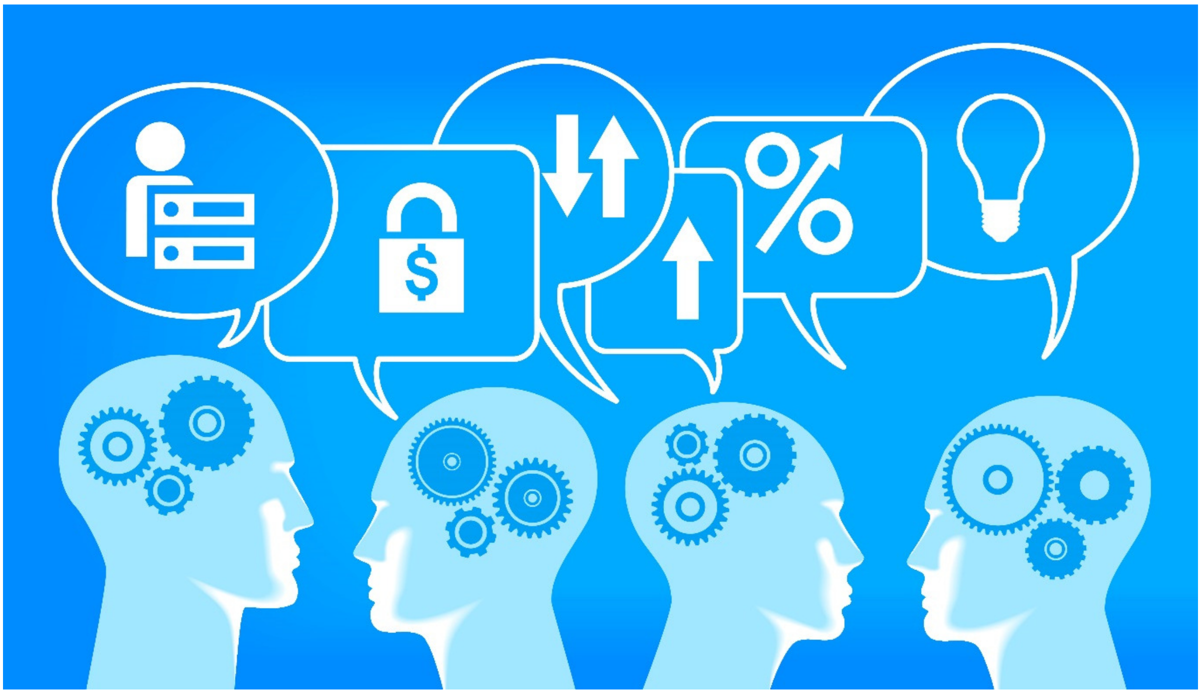
Factors to consider for

Choosing the right RFID reader



Version	Date	Author	Description
1.00	20.9.2017	AR-P	First version
1.01	19.12.2018	KMa	VM Pin's and VS Pin's IK class added, mobile identification added
1.02	28.12.2020	KMa	Information about mobile identification updated
1.03	8.2.2023	KMa	Information about mobile identification updated

1. Introduction

Radio Frequency Identification (RFID) is an accurate, cost-effective and secure identification technology that needs neither contact nor even line of sight between an identified object and a reader. Because of this, RFID allows accurate tracking of moving people, vehicles, commodities and components, profoundly reducing required resources in comparison to manual tracking.

At its most basic, an RFID system consists of a transponder containing data, and a reader to query its data when the transponder comes close enough. They are usually paired with a database, most often in a nearby controller or system PC that the reader can interface with. RFID comes in a great many different technologies and device types. Together, they offer wide differences in reading distance, data capacity, security, interfaces, durability and other characteristics. Your site's unique requirements and environment will significantly limit which technologies, devices you should consider deploying.

We've created this help guide to help you navigate through the different factors that will ultimately narrow your options when choosing an RFID technology and devices. We will begin with considering two basic questions to help plan an RFID reader purchase: what task will your reader be performing in your system? In what kind of an environment will you install that reader?

We'll finish with a summary of the primary features of Idesco readers that reveal why they could be the best choice for your system.

RFID reader and transponders

2. Challenges of site environment

RFID installations can vary widely, from comfort-regulated indoor office environments to the harshest industrial or outdoor settings, where readers and transponders are exposed to extremes of heat, cold, sun, moisture, dirt and reactive chemicals. This range of conditions correspondingly place widely different demands on readers.

2.1. Temperature

Most RFID reader manufacturers guarantee basic storage and operational temperature ranges for their readers. However, if your site will be exposed to temperature extremes, it's essential you check a reader's rating before making a purchase. Most Idesco readers withstand temperatures from -40...+65 °C as documented from rigorous testing.

2.2. Shock, vandalism and wear

Some sites often find themselves more prone to vandalism. Or you might need to install a reader in a position where it is could sustain other kinds of impact. It's always wise to plan for such possibilities when choosing a reader for potentially exposed locations.

Idesco's Basic housing enjoy the highest durability class IK-10 of the SFS-EN 62262 standard, proven to withstand impacts of 20 joules. Idesco's Slim, Sim Pin, VS Pin, VM Pin and Quattro N housings belong to the next highest durability class, IK-09, withstanding impacts of up to 10 joules. Such toughness is achievable because all Idesco reader electronics are cast in epoxy inside their housings, making them uncommonly resistant to shock impacts, while also making them nearly impenetrable to liquids. Note that a plastic cover filled with tough, hardened epoxy will prove more resistant to impact than even hollow metal housings.

Epoxy filling inside the reader

2.2.1. Durable keypads enhance reliability

Keypad without moving parts

If you must deploy a pin pad reader, remember that many use moving keypads that can easily collect dirt, dust, or form ice between keys, eventually preventing them to function. Some moving keys often prove easy to damage or vandalize. It's wise to choose a pin pad reader carefully if it will be exposed to weather, potential damage or even vandalism.

This is why Idesco makes pin pads without moving keys, using key pressure-detecting electronics beneath protective covers instead.

2.2.2. Tamper alarms

Tamper alarms in readers can be an essential security feature. They are embedded to activate and send an alarm to your system when someone tries to pry a reader away from its surface. This often happens if someone seeks to access a reader's inner electronics or its controller cabling. So, tamper alarms provide your site and system with an additional level of protection. Idesco readers use optical instead of mechanical tampers. Optical tampers offer greater reliability since the sensitivity of mechanical tampers to temperature change leaves them prone to false alarms. In turn, false alarms inevitably require costly maintenance visits. It's another reason we employ optical tampers: to help keep your costs down.

Idesco embeds tamper alarms in all its most popular access control readers.

2.3. Moisture, dust and chemicals

In general, RFID readers and transponders can be designed to work reliably in harsh conditions and industrial settings. However, a reader's IP-rating is the best indicator of whether it is suitable for outdoor conditions with moisture or dust. (Most Idesco readers possess IP67 protection classification, meaning they are suitable for all environments and can even be sunk in water.

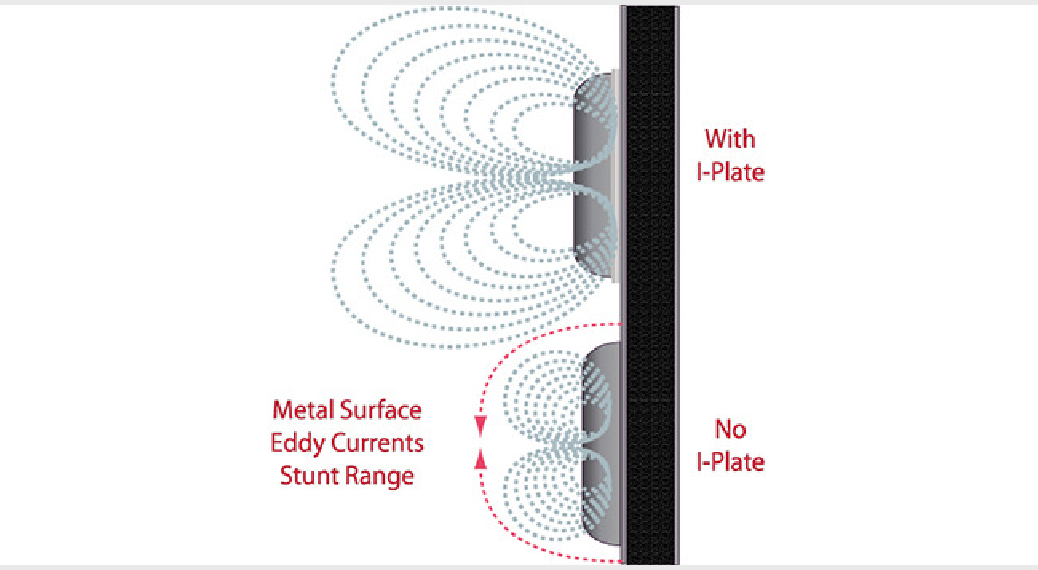
Manufacturers usually guarantee minimum IP ratings, temperature ranges and durability classes for their devices. These tell you in what conditions you can reliably deploy their readers.

2.4. Metal surfaces

Installing over metal surfaces frequently will disturb an RFID reader's performance. Unfortunately, not all manufacturers appear comfortable revealing or explaining this to their customers. The issue with metal surfaces arises because metal's conductivity combines with the energy a device emits, creating electromagnetic eddy currents beneath the device, often significantly shortening its reading zone (see illustration, next page). For example, while all Idesco's smart card readers can be installed over metal surfaces, their specified interrogation distance will be measurably shorter on them than over non-conducting surfaces.

Years ago, Idesco developed installation plates for its readers specifically to address this problem. These plates lift Idesco readers just high enough above a metal surface, significantly minimizing the eddy currents that degrade read distances on such metal surfaces.

Idesco subsequently developed metallic shield plates to leverage a major advantage of metal surfaces: they thoroughly shield readers from each other that are installed back-to-back on opposite sides of a wall. Readers installed so closely without shielding will similarly degrade each other's reading zone*)*



Eddy currents (red arrows)

2.5. Install-ability

Planning a reader’s location (to address factors like user convenience) will occasionally limit the reader dimensions you can reliably accommodate there. You may find it wiser to shop manufacturers able to offer you a wide variety of housing sizes, accommodating different settings, such as narrow doorframes, electrical sockets, vending machines, etc. Of even greater potential advantage to you will be a manufacturer able to identify ways to lower your own installation costs or accommodate customized deployment inside other devices like vehicles or vending machines.

Idesco makes Slim readers explicitly for installation on narrow doorframes, whereas Quattro housings fit over and replace standard electrical sockets. Indeed, when you install Quattro readers over sockets, you can freely use existing electrical socket holes to thread your cable. Lastly, when replacing Legacy readers with Idesco readers, the abovementioned installation plates prove doubly useful by covering the old readers’ screw holes, making installation faster and more convenient.

Idesco also provides an integrated RFID module for embedding in other devices like autos, vending, machinery, etc., letting you collect data, control access or identify users in a variety of settings.

Installation and shield plates

2.6. Deploying readers securely - without cables

It is possible to ensure secure data transfer between your RFID readers and their controllers wirelessly. Using wireless technology to secure readers' data transfer opens up a new world of RFID solutions. That's because wireless data transfer lets you deploy readers in settings where data cabling would be too time-consuming, costly, or simply impossible. Furthermore, such wireless RFID solutions almost always install much more quickly, yielding significant cost savings. Even existing systems can quickly integrate wirelessly-managed readers, again to significant savings.

More interestingly, wireless data transfer cost-effectively permits solutions for temporary, even moveable access control zones. Truly remote areas can be controlled by readers mediating data transfer via GPRS frequencies (available practically everywhere).

Idesco's readers supporting data transmission over mobile network permit some remote modification of settings via SMS.

2.7. Readers' appearance and design

In particularly distinguished buildings an access control reader is often seen as part of structure's aesthetic. In such settings, it can be important to choose a manufacturer whose array of housings gives your customer options for meeting any aesthetic concerns they have.

Idesco designs all its access control readers to be both elegant while still robustly reliable in outdoor settings that experience hostile, inclement conditions. However, we have also designed and offer refined smooth, quality stone housings and finely-crafted wood housings specifically designed for refined indoor settings [only IP60 protection class*]*.

3. Technical requirements of your setting

A reader's technical features determines its suitability to your planned deployment. You must understand clearly everything your planned system is expected to do – today as well as in the future. How will your reader interface with the system? Wiegand, RS232, RS-485, etc.? At what distance will end-users be expected to present their transponders? What security requirements does your planned system place on the reader? Will transponders and credentials need to be encrypted, or not? If not encrypted today, are you certain that could never change in the future?

All these factors (and more, see below) determine whether a particular reader's technical features and capabilities make it suitable for your planned system. So, careful consideration and determination of all these factors will ensure your system's reader choice is a wise one.

3.1. Reading distance – what do you plan to identify?

RFID readers operating at frequencies of 125 kHz and 13,56 MHz offer read distances that are usually a couple or a few centimeters. By contrast, UHF (Ultra High Frequency) readers permit transactions at much greater distances, even out to tens of meters depending whether you choose an active or passive UHF technology. However, because UHF technologies are more expensive and not well-suited for short-range applications they are usually chosen only for deployments where such distance capability is necessary. A good example is vehicle identification (VID), for toll booths and parking entrances, or logistics, for example. Let's begin by looking first at shorter range access control.

3.1.1. Access control

Access control, for identifying persons, almost always deploys either 125 kHz and 13,56 MHz frequency readers. The major difference between these two frequencies is the amount of data that can be transferred during an interrogation. Since the data transmission speed of 125 kHz is essentially 100 times slower than 13,56 MHz, its transponders rarely contain more than a short unique serial number for identifying the user.

Access control

In recent years, the relative ease of cloning 125 kHz transponders has triggered a noticeable shift away from 125 kHz technologies in access control. By contrast, the wide array of security features available to the most secure 13,56 MHz technologies' (because of 1000x greater data capacity) has effectively make transponder cloning impossible. These features are discussed in more depth below.

A specialized niche of UHF (Ultra High Frequency) readers has begun seeing deployment for personal ID in certain access control settings. Since UHF readers at distance can interrogate transponders affixed to clothing, it frees users from the necessity to approach and closely present a badge to a reader. Such 'hands-free' solutions are being selected whenever fast, convenient access by badged personnel through dense traffic points is preferred, or when users' hands are burdened by either packages or control of vehicles or machinery.

UHF readers normally tend to be larger in size (and more expensive) which has limited their deployment in access control settings. However, the 'hands-free' UHF access control readers are intentionally designed smaller. While this tends to shorten their effective reading distances somewhat, it still makes them a viable solution in settings requiring their read-at-distance capability.

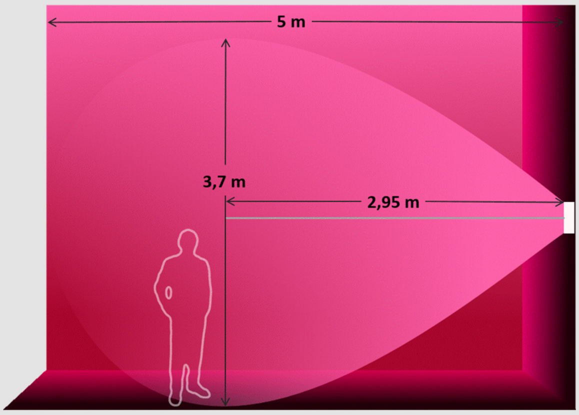
Idesco's EPC Compact 2.0 is one such doorframe profile reader, with a reading distance out to 4 meters.

However, by far, the vast majority of access control readers sold today use either 125 kHz or 13,56 MHz frequencies. As mentioned above, the access control industry recently began shifting noticeably away from 125 kHz (also called low frequency or LF) technologies. This is because LF doesn't have the bandwidth to transmit much data during the interval of a transponder interrogation; usually no more than a factory-coded identifier which can be as short as four digits. That means LF transponders are increasingly vulnerable to cloning – no small risk to a security manager.

By contrast, the 1000x greater bandwidth of 13,56 MHz permits it to transmit that much more data, permitting it to host security protocols for defeating cloning attempts. Admittedly, not all 13,56 MHz technologies are equally secure. So, identifying what level of security (see Security, section 3.8) your customer's site needs will help you identify the right technology to meet their needs, while still keeping their costs to a minimum.

3.1.2. Vehicle identification and logistics

By their nature, vehicle identification and logistics settings frequently require the longer identification distances that Ultra High Frequency (UHF) readers are able to provide. Occasionally, one might encounter 126 kHz and 13,56 MHz technologies being used for asset marking and similar logistics tasks requiring only the shortest interrogation distances. If you need to identify a moving object (e.g. vehicle), or simultaneously discriminate and identify vehicles transiting through opposed lanes, both tasks are prime examples of deployments that UHF readers excel at solving and to which they are frequently assigned.



Representative cone of EPC reader emission

Not surprisingly, the siting of readers and the approaching angle of tags play a major role in determining how successful a UHF deployment will be. The 'emission cone' of UHF readers must be carefully aimed toward where transponders are expected to transit. Approaching transponders themselves should be optimally-oriented toward the reader as they pass through its 'emission cone' (see figure, left). Testing and satisfactorily addressing both conditions is required to ensure reliable interrogations.

Additionally, UHF tags only perform well when installed specifically on the surface they were designed for. Different dedicated tags exist for metal and glass surfaces, for example. Each also has their own level of responsiveness to interrogation. This means a metal surface tag, for example, might have a greater responsive range than a glass surface tag.

3.1.2.1. Unique UHF reader features

Anti-collision is an RFID reader ability to interrogate multiple tags within its range simultaneously. Such a feature can be particularly valuable when a UHF reader is tasked to monitoring a site where dense traffic regularly transits an access control point, or wherever there is a need to monitor a zone with a finite population of tagged items or individuals (zone control).

Consider a need to determine the direction of a moving tag transiting an access point you monitor. If you could connect a second, auxiliary external antenna to your reader it would prove much less expensive than purchasing and adding a 2nd, additional reader to your deployment. Such a 2nd external antenna would let you monitor traffic on both opposed lanes simultaneously just as effectively as two purchased readers would.

An ability to adjust the transmission power (amplitude) of an UHF reader can be another valuable feature. Adjusting its amplitude is a clever way to filter out replies from more distant tags (e.g. more distant vehicles in neighboring lanes) that you don't want your system to capture.

Lastly, it is also possible to integrate access control, vehicle identification and payment into single transponders. One transponder, interrogated by different readers assigned different roles, can mediate parking access, office access, and store tokens to pay for meals in an office cafeteria.

Idesco's EPC 2.0 readers support all these features, in addition to being designed with the tough, rugged reliability for outdoor settings that their wide operating temperature range and IP67 protection class provides them. They read encrypted EPC Gen2v2 transponders.

Vehicle identification deployment

3.1.2.2. Active vs. passive technology

Longer UHF reading distances become achievable when you choose active instead of a passive UHF technology. For example, if a deployment requires consistent, reliable interrogations beyond 15 meters, active UHF technology becomes a more viable solution. The caveat with choosing active transponders is they are also dependent on an internal power source (a battery) to boost the amplitude of their reply to a reader. That 'active boost' is what extends the range at which their reader will detect their reply.

Conversely, passive UHF technology transponders don't need batteries to function, relying entirely on the energy of the reader's transmission to power their reply. Whereas the finite, depletable power source that active transponders require makes them much more expensive to purchase and to service regularly by replacing or replenishing their batteries. Furthermore, providing easy access to an active transponder's battery tends to lower their protection rating, making them more vulnerable to harsh, inclement conditions than passive transponders. Therefore, if a detection range of 10 to 15 meters is sufficient for your planned deployment, passive UHF technology will prove both more cost-effective and reliable over the long term.

3.2. Access Control Identification protocols

There are three most common protocols used for identification at RFID access points. The first and simplest is identification managed entirely by a user's transponder. The second protocol is users enter a pin code into a keypad; their pin code can be either universally-held or a unique pin code issued to each user that also identifies them. The last and most secure method combines transponder interrogation with pin code.

Biometric protocols like fingerprint or facial recognition are considered a more expensive, problematic variant of unique user pin codes. Even indoor fixed biometric readers can't yet guarantee the 100% reliability of RFID so their deployment in outdoor settings is now commonly avoided. Nevertheless, the access control industry has begun closely monitoring how and where mobile device-hosted biometrics will make its first, major, profitable entrance. This is because of a growing suspicion that mobile platforms may ultimately supplant fixed readers.

It is not uncommon to schedule periods for two or more of these methods at a site. For example, on certain days or during certain times in the day, only users' transponders would be needed to gain access (during work hours), whereas at all other times users' would also be required to provide their pin code to authenticate their identification and gain access.

Transponder Identification with reader able to accept pin codes.

3.3. Mobile identification

Idesco's 8 CD 2.0 MI reader supports mobile device transactions. In addition to reading conventional transponders, it reads access credentials you can store in your smartphone, then forwards them to the reader host for authentication. It supports BLE and NFC transactions. Bluetooth settings of this reader can be conveniently configured with Mobile Coder mobile application installed in a smartphone.

8 CD 2.0 MI works together with Idesco ID mobile access app. You can download Idesco ID mobile access app from Google Play or AppStore. Downloading the app creates a unique device ID that serves as your phone's mobile credential. This UID is enrolled to your access control system using

Enrollment Station. Combined with 8 CD 2.0 MI readers and our free Idesco ID mobile access app, Enrollment Station gives you a cost-effective pathway to offer mobile access to your organization.

By contrast, organisations that frequently need new mobile credentials and/or with larger user populations, find Idesco ID service greatly beneficial. Simply, Idesco ID service lets you distribute mobile credentials to phones from your own access control system. With Idesco ID, both mobile access for users and the management of their credentials becomes faster, easier, simpler.

Idesco's 8 CD 2.0 MI readers let you assign different security levels for every door they are deployed at, while giving you three authentication options. For convenient (and hygienic) hands-free access, authentication occurs when the phone is in the users' pocket, at a reading distance you choose out to ten meters. For the most secure settings, unlocking your phone's own security lock (e.g. pin code or fingerprint) may be required. This provides a much simpler way to biometrically authenticate users.

Lastly, mobile access security is as high as any found in conventional access control. Data transmitted between phones and readers is protected by effectively unbreakable 128-bit encryption.

Mobile identification

3.4. Interfaces

RFID systems always have specific requirements determining how readers must connect and interact with them. So, it's not just important to choose a reader able to interface with your system's cabling, inputs and outputs. It must also readily accommodate the precise communication protocols and parameters your system needs to reliably and consistently interact with it. For example, certain Wiegand-interfaced system's parameters might require not only parity bits, but even specific bit timings to ensure a reliable 'handshake' between the system and its readers.

All these reasons are why most Idesco readers support a range of interfaces such as Wiegand, RS232, RS485, C&D, OSDP vers. 1 & 2, etc. More importantly, we also provide user-friendly software that simplifies and speeds the configuration of readers. We do this to ensure our readers can always precisely meet your system's specific requirements quickly and efficiently – to save you money.

3.5. Users' interaction with readers

RFID readers usually offer some type of programming options for configuring the behavior and color of their LED indicator lights, and the behavior of a beeper. When these options are included they let you provide users a visual, aural, or both visual and aural indicator when a reader is powered and usable, and to notify them after interrogation if access was either granted or denied. Of course, the greater the programmability of these options, the more customizable a reader is and thereby able to satisfy concerns about certain (or even sensitive) access points.

Idesco's reader configuration software offers the widest range of configurability in programming LEDs, including pin LEDs, and beeper response. If you anticipate needing to accommodate a much wider range of user interactivity, Idesco also offers a reader that integrates two additional LEDs and a detailed LCD display [shown below] to provide users more detailed information, and with function keys above its pin pad, to widen the range of users' response during transactions.

Display reader with expanded LEDs, LCD display, pin pad + function keys for enhanced user interactivity.

3.5.1. Convenience and usability

An RFID reader can be designed with special features to enhance their usability in different, unique settings. For example, a keypad backlight can make the reader's keypad easier to use in the dark. Or it might let you program keypad backlighting to activate automatically when an authorized tag is shown to the reader, or when a key is pressed. Of course, most such backlit pin pad readers should also be expected to support programming of backlights to be powered continuously, or to follow a time schedule provided by its host.

All of these features and more are supported by Idesco's most popular pin pad readers. For example, to further improve usability, Idesco also offers pin pad housings with slightly-raised, depressable keys and a raised pip 5 key for the visually-impaired, wherever haptic feedback or key orientation is required.

Idesco also provides angled installation plates in different sizes and angles. These installation plates enable installing readers in lower heights and improve their usability e.g from wheelchairs.

Haptic keypad with raised keys. Inclined installation plate optimizes reader angle for convenient use when installed at lower elevation.

8 CD 2.0 VM Pin ja 8 CD 2.0 VS Pin readers provide users tactile feedback when they press a key

3.5.2. Readers for settings with tags triggering applications

Note that you can assign users' transponders other tasks besides opening doors or vehicle gates. With the right reader installed, transponders can trigger PC applications to initialize, activate machinery and even start vehicles. In many such cases, housing the reader inside a card holder is preferable. For example, such a card-holder reader can be installed in hotel rooms to activate additional lighting when guests insert their keycard. Or they can be installed to trigger the activation of vehicles or machinery when an authorized card is inserted.

Card-holder desktop reader.

3.6. Identification without system connections

It's also possible to assign an RFID reader to control a door, for example, without connecting it to a hosting system. Such readers (known as 'Standalone Readers' in the industry), function by embedding a single activating credential in any transponders from the larger surrounding system you wish to authorize. Usually, only a single shared credential is permitted because standalone readers can't access authenticating databases of different credentials like normal system readers can. Nevertheless, standalone readers can be made very secure if their interrogation protocol is encrypted, like DESFire interrogations are. In addition to controlling door locks, standalone readers are also often ideal for securing diggers, tractors or other large machinery by controlling ignition. Standalone identification can be mediated by transponder only, transponder and pin code, or pin code only. This is because keypads without an RFID reader can also control doors using only a pin code.

3.7. Write-able transponder data

If you anticipate your deployment may require changes to a transponder's data during an interrogation, you will need to deploy read/write (R/W) readers. R/W readers are often used in payment or vending applications. For example, a certain value stored in the transponder will be programmed to represent how many times its user will be entitled to access a certain place, or the number of tokens remaining they can spend on a vending machine's stored product or products. After the R/W reader determines the current value in the transponder, it will overwrite it with a new, lower value. This method can also be used to limit users access to a controlled area to a finite amount of access events, for example, boarding a mass transit bus using a token-storing transit card.

3.8. Combining Time & Attendance with Access Control

Time and attendance is the collection of employee work time data for use by payroll and personnel administration. A growing trend in workplaces is to provide a graphical user interface where employees can timestamp their entrances and departures with a transponder. Such RFID touchscreens also let them review past work hours and independently document planned or previous absences, lunch breaks, overtime, etc., with considerable payroll administration cost savings.

Equally important, an organization's population of access control transponders can usually be assigned to interface with a planned Time and Attendance console, as long its RFID reader is compatible with (can read) the technology of the access control transponders. Such RFID touch screen devices are also often deployed in cafeterias as payment terminals, letting employees select and even pay for their meals with their access control transponder.

Idesco's RFID touch screen terminal, Access Touch 4.0 supports numerous technologies, compatible with a wide and diverse range of transponders from 125 kHz HID Prox to 13,56 MHz MIFARE® DESFire

Idesco Access Touch 4.0 time and attendance terminal

3.9. Security

Nowadays, RFID reader technologies differ widely regarding security. Recall that technologies used in access control are usually divided into low frequency (or LF) 125 kHz and higher frequency, 13,56 MHz (or Smart Card) technologies (see above, 3.1.1).

Low frequency technologies rely almost entirely on reading nothing more than a transponder's factory-coded unique serial number (SN or UID). (The simplicity of this technology is why, today, it is increasingly considered a very vulnerable, insecure access control technology.)

By contrast, the much greater data capacity of Smart Card technologies lets an order of magnitude more data to be transmitted during interrogations. That allows, at the highest end, truly robust encryption to protect interrogation transactions. For example, most MIFARE® DESFire readers today can provide one of the industry's most secure encryption protocols: the 128-bit AES cipher. This cipher is what is used to give users' credentials essentially unbreakable protection.

In addition to a range of secure technologies, including MIFARE's Classic and DESFire, Idesco also offers its award-winning AESCO solution for encrypting reader-host communication. AESCO easily embeds in your current controller, so your credential database and system will remain unchanged. Secure data transfer protocols, like OSDP v2 take care of data security also inside the system.

3.9.1. Powerful security enhancement: Pin Codes

Personal user pin codes are an inexpensive way to powerfully enhance the security of an RFID access control system's security. This can be especially important in systems most vulnerable to cloning (only UID credentials, no interrogation encryption). Such unprotected systems benefit the most in security when they integrate pin codes in their identification protocol. Additionally, as mentioned in chapter 3.2, pin codes can be flexibly deployed whenever users raise concerns over convenience. A system can require them only on certain days or after hours on workdays, for example. Be sure, however to choose a reader configurable to the pin code length (number of digits) that your system and security manager require. Because, once again, not all reader brands are alike. Some readers will either not be configurable at all for pin length, or will only support a couple of pin length choices.

Adding pin codes can be a powerful way to bolster access control security

3.10. Configurability and system evolution

Certain reader technologies, particularly the newest generation of MIFARE® DESFire readers, offer greater flexibility and freedom to configure and even update readers. This is particularly important if you want to offer your customers a system able to adapt to changing system requirements. For starters, many of the newest generation readers are designed to be backwards-compatible with older, legacy technologies so you can deploy them to read an older system's tag population. Then, when the need to update your customer's system arrives, you simply re-configure (or migrate) their readers to the more modern, more secure technology. Such updatable readers support a system's evolution without themselves ever needing replacement.

Besides being able to support such important technology updates, a reader's ease of configuring other parameters can be vitally important (pin code length, tamper alarm, LED, buzzer, etc.). That is because, in addition to ensuring the reader's best performance fit within a planned system, such parameters will also determine how adaptable you can be to your customer's change requests.

Idesco's newest generation access control readers let you configure a nearly-unmatched variety of parameters, in addition to being able to update them to a new technology. Best of all, this is done by merely exposing them to a configuration card, without ever uninstalling or even powering them down.

Migrate installed readers to more secure technology using configuration card

3.10.1. Disadvantages of closed reader technologies (vs. open technologies)

Proprietary or closed technologies are technologies that bind you to a single manufacturing source. Their technology is structured in a way that forces you to purchase additional readers (and sometimes also transponders) only from them. In this manner, you let yourself be bound to a sole source, leaving you vulnerable to their pricing, to supply shortages and lack of access to support.

By contrast, open technologies (e.g. MIFARE®, EPC) are supported by consortia of manufacturers around a commonly-accepted standard. A common standard ensures when you choose readers and transponders, from among a variety of different manufacturers and suppliers - you can rest confident they will be fully compatible. It ensures you won't be at the mercy of a sole source's pricing, availability or experience constrained access to support if your customer's system needs expansion, enhancement or reader unit replacement.

All Idesco's current range of readers use MIFARE®, EPC and Legic open technologies, ensuring their compatibility with systems currently using or migrating to them.

3.11. RFID reader safety standards

For some time, the manufacturing and operation of RFID devices has been regulated by international standards. In Europe, RFID products are required to comply with standards set by the European Telecommunications Standards Institute (ETSI). ETSI's standards ensure that compliant devices will be both safe and won't interfere with other radio communication, e.g. broadcasting or emergency services. Some countries also established their own national regulations based on ETSI standards.

3.11.1. Health and RFID interference with medical devices

Stringent regulations and standards limit RFID devices' power levels and frequency ranges. Correspondingly, the regulations and standards set for limiting the power of RFID devices establishes limits well below any that could cause interference with devices (e.g. pacemakers).

The power levels and frequencies at which Idesco's RFID readers operate are far below limits established by even the most conservative European health regulating agencies and research institutes. Consequently, Idesco's products have been approved for use without individual site licenses. Lastly, independent, third-party testing has confirmed Idesco products' compliance with these standards.