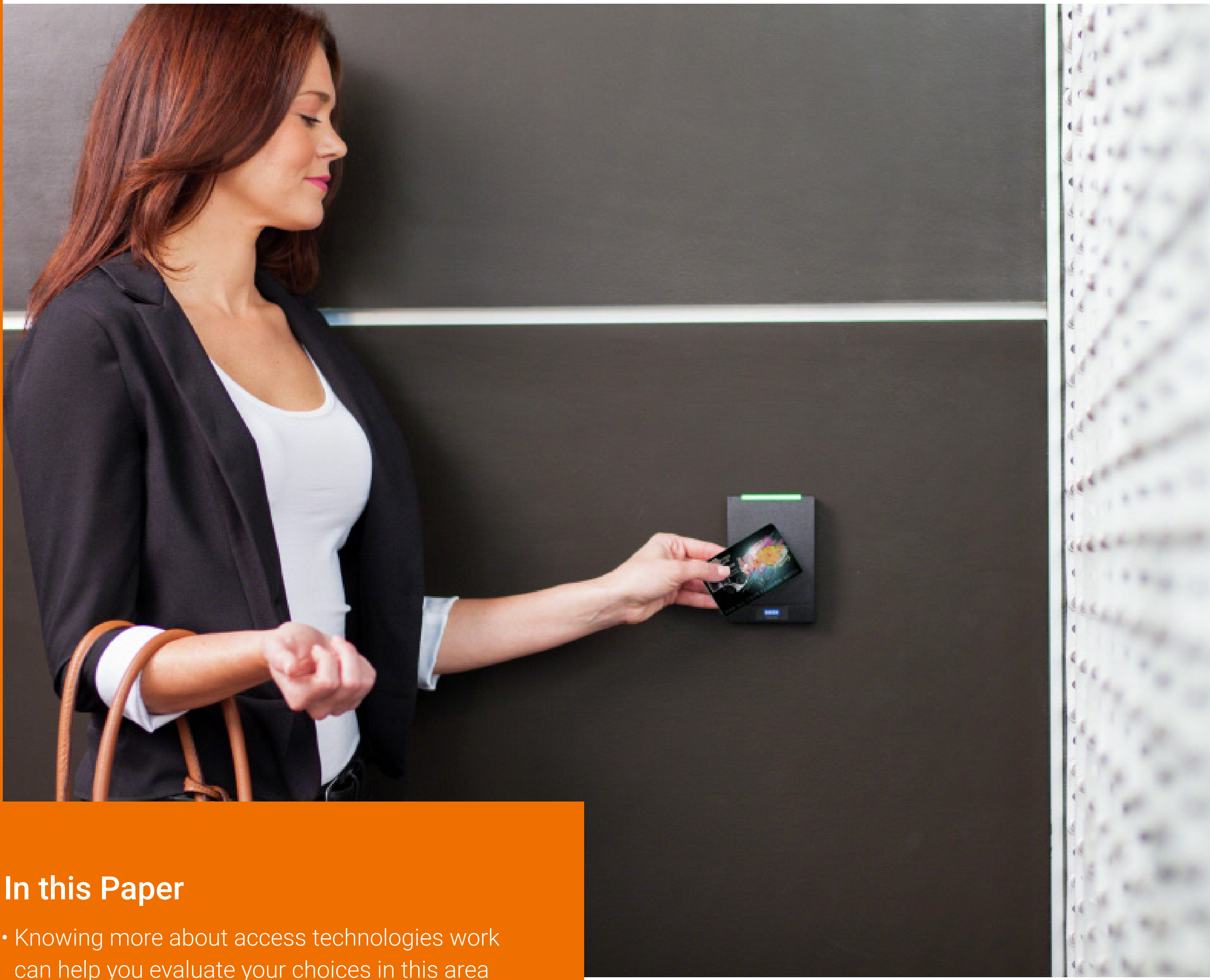
TECHNOLOGY SOLUTIONS BRIEF

Sponsored by

HID

How a Credential is ‘Read’



In this Paper

- Knowing more about access technologies work can help you evaluate your choices in this area
- Learn to better understand how the process of mutual authentication works
- Explore the four common elements of an access control solution and how they interact

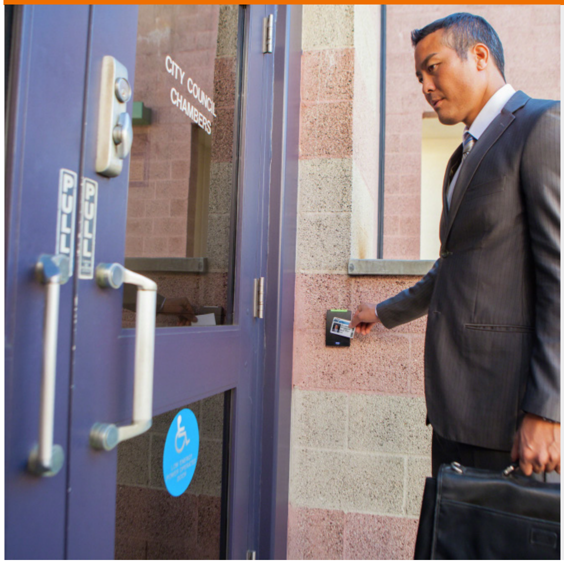
A QuinStreet TECHNOLOGY SOLUTIONS BRIEF © 2018

Most of us use some type of contact or contactless technology for access every day, perhaps even multiple times a day. Have you ever stopped to think about what happens in that split second at the door, gate or network application?

Security professionals and facility managers within the organization are no longer the only decision-makers weighing in on security investments. A growing number of organizations are adopting credential technology that can be used for multiple purposes, including the combination of physical and network access. Today's more mobile workforce requires a greater choice in supported devices.

In order to take advantage of the benefits offered by today's current technology standard, moving away from legacy systems is necessary. Knowing more about how access technologies work can better enable you to evaluate the choices put before you. This Technology Basics Brief will explain the nature of the transaction at the door or other access point in technical terms that a layman can understand. It is important to be familiar with which data is encoded on the credential and how it relates to other parts of the system to properly evaluate access control suggestions and proposals.

How a Credential is 'Read'

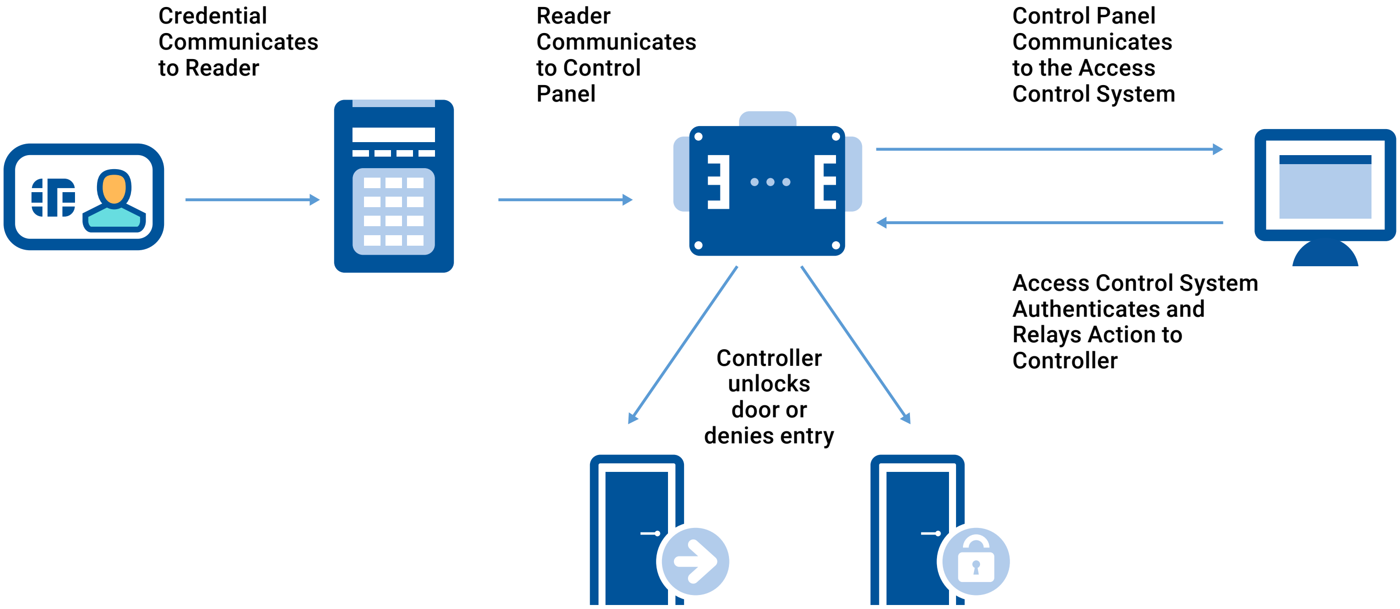


The Four Elements of a Physical Access Control System

Most physical access control systems consist of four basic elements. Depending on the size and purpose of the system, there may be additional devices, but generally, the four basic elements are:

1. Credentials
2. Readers
3. Controllers
4. Host

Typical Communications Process for Smart Card Door Access


Credential Communicates to Reader
Reader Communicates to Control Panel
Control Panel Communicates to the Access Control System
Access Control System Authenticates and Relays Action to Controller
Controller unlocks door or denies entry

The Credential

Almost all physical access credentials carry a number, or set of numbers that are used to identify the holder. This most often takes the form of a simple string of binary numbers (ones and zeros) often referred to as the "payload." Manufacturers will program and personalize credentials capable of carrying this kind of binary data onto a form factor (e.g., Smart Card, fob, mobile device, etc.).

The way data is conveyed to the reader varies according to the technology involved. In every case, however, the "payload" is a string of binary numbers of some fixed configuration and length. The way this data is configured is called the **format**. The credential itself has no awareness of the makeup of its format, nor is it aware of any access privileges for the cardholder. That information exists only at the panel and host software.

Common Credential Technologies Found in Access Control Applications

The technologies commonly found in access control credentials deployed today include:

- Magnetic Stripe (Legacy Technology)
- Low Frequency 125 kHz (Legacy Technology)
- High Frequency 13.56MHz (Current standard)
- Ultra High Frequency

Occasionally, two or more of the above technologies are combined on a single form factor. The combination of outdated legacy technologies and the current industry standard of 13.56 MHz should only be employed as a short-term strategy for gradual upgrade, not as a permanent solution. Decreased risk can only be assured by full adoption of the high frequency standard.

> "Almost all physical access credentials carry a number, or set of numbers that are used to identify the holder."

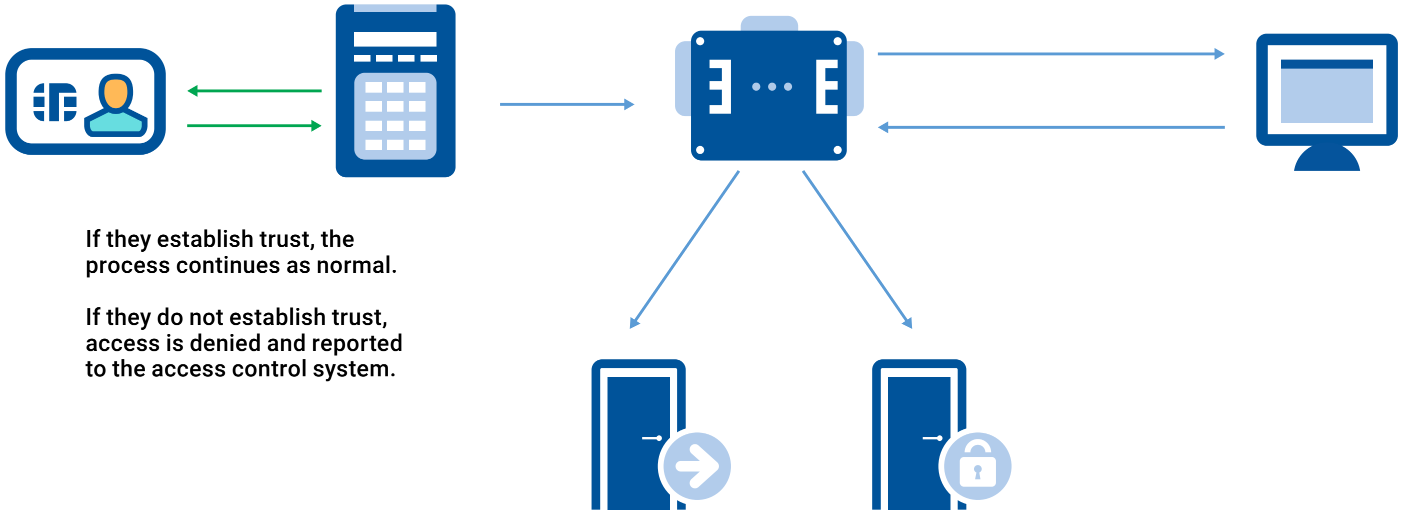
How a Credential is 'Read'

Credential & Reader Mutual Authentication

To protect against common vulnerabilities, including forgery, cloning, and spoofing, some contactless smartcards and mobile credentials have an additional security step called "mutual authentication" that is completed before the binary data can be extracted from the credential.

For this more secure method, both the credential and reader contain a set of cryptographic keys (like a password or a shared secret handshake). When the credential is first presented to the reader, the two use a complex mathematic process to compare keys. If it is determined that the keys match, the credential shares the binary data with the reader and the reader accepts it as genuine. However, if the keys do not match, the credential will keep the binary data private and the transaction will be terminated with generally no reaction from the reader.

Smart Card Door Access Employing Mutual Authentication



Credential and reader establish they are part of a trusted population (not forged, cloned, or spoofed)

If they establish trust, the process continues as normal.

If they do not establish trust, access is denied and reported to the access control system.

There are two things to understand about effective mutual authentication:

1. **The Technology Matters** | Best practice today recommends that the underlying credential technology should leverage the latest security standards. Most legacy credentials have vulnerabilities that have been exposed by researchers in published documents. Such vulnerabilities make it possible for hackers to easily forge/clone/spoof a credential. Next-generation credential technology is based on the latest security standards, built to provide the highest levels of security and privacy protection available.

> “Cryptographic keys must be unique to the organization and treated as highly confidential information.”

2. **The Key is Key** | Cryptographic keys must be unique to the organization and treated as highly confidential information. Best practice is to have the key values automatically generated by machines and never seen or accessed by people. Further, all devices containing keys (credentials, readers, encoders) should store and execute cryptographic operations on a secure hardware platform/chip or secure element. Lastly, all devices should have chain-of-custody control and tracking so that they are only accessible by trusted parties.

The Reader

Readers can be configured to read only the credentials in the respective cardholder population. Some are designed to support just one technology, but some support a vast array of multi-technology configurations.

A **configuration** is a set of physical reader attributes and capabilities combined with programming options to suit the reader application.

Typical reader configuration options include

- What credential types can be read

- Type of encryption used
- LED and beeper behavior
- Whether there is a keypad
- When a credential is read
- When the optical tamper switch is enabled

Some configuration options can be updated in the field (e.g., change the LED color, add an encryption key or enable/disable a credential type). In some cases, configuration options are tied to the hardware (a keypad or magstripe reader sidecar).

A reader reads the binary data from the card and transmits that data to the controller. Most commonly, readers transmit this data to the controller. The most common protocol is "Wiegand." Wiegand is transmit-only; meaning that data is only sent one way, from the reader to the controller. Wiegand is limited to 500 feet and cannot be encrypted. The Open Supervised Device Protocol (OSDP) standard, however, is a bi-directional protocol that can be encrypted. OSDP is the clear choice for new installations as it is more secure.

The reader itself has no awareness of the makeup of the card data format, nor is it aware of any access privileges for the cardholder. That information exists only at the controller and host software.

The Controller

When the controller receives the data from the reader, its embedded firmware begins the process of deciding whether or not to grant access. This is usually done in the following sequence of stages:

1. **Length of data format** | Does the length of the binary data match a format length the controller is expecting? Some controllers are programmed to only accept a certain length of data (e.g., 34 bits). If the data from the card is too long or too short, the controller will either ignore it completely or send an "access deny" message for a non-matching format length.

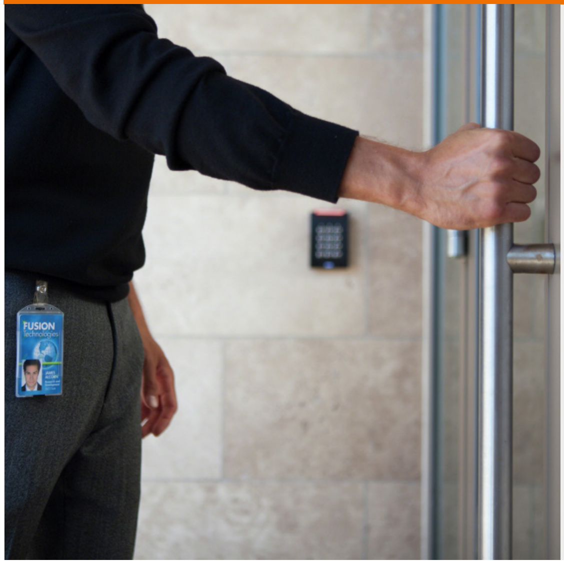
2. **Evaluation of format structure** | If the length is acceptable, the controller then breaks the binary string down into its component parts as defined by the "card format." These commonly include the following components:

   a. **Parity Bits** | Do the Parity Bits suggest the data transmission was received from the reader without error? Parity bits are the simplest form of error-detecting code and are commonly used in card formats. If the card format specifies parity bits, the controller will perform a simple calculation to better ensure that no error was made in the encoding, reading, or transmission of the binary data. If that simple calculation indicates error, the controller will send an "access deny" message for incorrect parity.

   b. **Facility & Site Codes** | Does the Facility Code match an authorized value? The controller will examine the data to determine if the Facility Code portion of the format matches a value that has been programmed into the controller. Most controllers can support many different Facility Codes and even multiple formats simultaneously. If the Facility Code does not match, the controller will send an "access deny" message for invalid facility code. If the format contains a Site Code or other secondary identifier, it will be handled just like the Facility Code.

   c. **Credential Number** | Is the credential number in memory? The controller will examine the data to determine if the credential number portion of the format matches one of its stored values. Most

How a Credential is 'Read'



controllers can store tens or hundreds of thousands of credential numbers locally. If the Credential number does not match any stored value in memory, the controller will send an "access deny" message for invalid credential number.

d. Access Rights Evaluated | Is the credential number authorized for this reader at this date and time? The controller will reference the stored authorized time/ date conditions of the credential number at the reader where it was presented. If access under current conditions is not authorized, the controller will send an "access deny" message for invalid time schedule. If access under the current conditions is authorized, the controller will send an "access grant" message, trigger relay to unlock the door, and temporarily suppress the door position sensor alarm.

The controller is the only device in the system where the binary credential data format can be decoded and acted upon. Only the controller (and possibly the host) is aware of the makeup of the format and whether the received data makes sense. Different brands of controllers react in different ways to unsupported card data formats. They can:

- Completely ignore an incompatible format and give no reaction at all
- Have a unique descriptive log message for every conceivable type of "access deny" event
- Have only one generic log

Understanding specific controller capabilities is required to fully evaluate or debug issues with credential/reader performance.

The Host

Every access control system has some form of user interface, usually a discrete PC application or web-based interface for operators to interact with the system. They will use it to:

- Add and delete cardholders
- Assign, modify or delete access privileges
- Create and modify time schedules, holiday lists, etc.
- Configure system hardware for doors, alarm points, etc.
- Monitor system events in real time
- • Generate historical reports on all types of system activity

In most cases the access system is fully automated and the access rights data is distributed to all connected controllers. This allows systems to perform efficiently, while protecting against disruption to network connectivity. Most controllers connect to the reader and door hardware via dedicated wiring and have their own back-up power source.

Summary

This brief explored the four common elements of an access control system and how they interact within the system. Here are some important points to take away:

- Adopting current industry standard over legacy technology is beneficial and reduces risk

- Solutions offering mutual authentication between reader and credential offer additional protection against cloning, spoofing and forgery, particularly for multi-purpose credentials

- In most cases, the controller is the only device in the system where the binary card data format can be decoded and acted upon. Understanding controller capabilities will give you greater insight into how your system will perform with any given credential technology

- The host system is where access control rights are managed and maintained

For a closer look at HID Global access control solutions, visit our website: www.hidglobal.com.

Readers: www.hidglobal.com/products/readers

Credentials: www.hidglobal.com/product-display/ cards-and-credentials

Controllers: www.hidglobal.com/products/controllers.