Choosing the right card technology

nedap

www.nedapsecurity.com

It’s crucial that physical access control systems identify people reliably. This whitepaper highlights the most common ways in which people can be identified using ID cards. Many different types of ID cards are available, from simple, printed barcode cards to microprocessor-based RF cards. Before discussing the various card technologies, we look at the criteria you should consider to select the most appropriate technology for your organisation, including security, convenience and durability.

Card technology characteristics

Different card technologies have several specific characteristics. Taking these characteristics into account allows you to determine the most suitable technology for your organisation. The most important characteristics are outlined below.

Data size

To select the right card technology you need to decide how many services you want to implement. For access control, for example, only a few bytes of data (4-10) are needed for encoding a unique ID number. When other services such as cashless vending or follow-me printing are being used, or where other data such as biometric templates and authorisation data need to be stored, more storage space is needed on the card.

Security

The major threats that need to be taken into account are cloning and replay of cards. Replay is when data sent between the card and the reader is stored, for example on a laptop. When this data is replayed and sent to the reader, the card can be simulated. Cloning and replay can be prevented by using an appropriate level of encryption. The card and reader then check if they are allowed to exchange data by using secret keys in the authentication process. Hands-free and other systems are also making it harder to snatch cards virtually, as they can stay invisible in bags or clothes.

Convenience

Convenience is an important factor in increasing usability and uptake of your chosen card technology. Convenience refers to the handling of the card at the reader, and the speed of the transaction.

Standardisation

Using standardised technology gives you independence from suppliers. Having the option to use various suppliers for the products in your access control system allows you to make replacements more easily. An example of standardised card technology is the ISO 14443A standard. Thanks to ISO standardisation, cards and card readers from different manufacturers are interchangeable as far as the communication between the card and reader is concerned.

Durability

Many access control cards are used intensively, so wear is a factor to consider. Common proximity and hands-free systems require no physical contact between card and reader, so wear is low. In outdoor use, it's important to remember that RFID antennas are much more weather resistant than swipe readers.

The history of card technologies

Organisations have been using a range of card technologies for access control. Some of those, however, have been (partially) replaced by newer technologies. This paragraph briefly describes the older types of card technologies to give you an insight into how the card technology industry has evolved over the last decade.

Magnetic stripe technology requires the user to swipe the card into a reader, so physical contact between the card and reader is essential. As well as being inconvenient, the interaction causes wear to both the reader and the card; increasing maintenance and replacement costs. And, because it's relatively easy to copy these types of cards, this technology is no longer applied in access control solutions.

Wiegand cards were the first cards not to require direct contact between card and reader. But they do need a similar reader to a mag stripe card, so convenience is only slightly improved. They were difficult to duplicate, making them tamper proof, but the introduction of low-cost RFID cards made the Wiegand card obsolete and it's not used in modern access control systems anymore.

Barcode technology provides an optical way to present and read data. Barcode cards are particularly convenient for visitor management as printing them is easy and the cost is low. These cards can, therefore, be authorised for limited time periods and don't need to be returned after use. Barcodes are very easy to duplicate, however, making them less suitable for security applications.

We all know **contact smartcards** as they're the type of cards that carry a chip and are issued by banks. As these cards have to be inserted into a slot, which limits user convenience, contact cards are not ideal for use in physical access control. Contact-based smartcards are, however, commonly used for accessing IT devices such as laptops, which is why the technology still appears in modern RFID cards when physical access and IT access are combined on one card.

Modern card technologies for access control

Newer card technologies commonly applied in physical access control are described in more depth below with an explanation of their pros and cons.

RFID

Contactless technology or Radio Frequency Identification (RFID) was developed in the late 1970s. The RFID technology most commonly used for access control is that seen in wired logic cards such as MiFare and Legic. Wired Logic cards contain a chip and coil that's activated to transfer the card number to a reader. More sophisticated types of these cards are able to run general or custommade applications. Adding applications onto the card allows staff to use one card for several functions, such as cashless payment and logging onto the IT network. Typically, most access control systems use RFID cards to identify people. We talk about cards exclusively here, but these concepts could equally apply to RFID-based fobs or tokens. Contactless technology requires no direct contact between the card and reader. So it is particularly attractive for securing physical access control when the ID card and reader need to operate in harsh conditions, or where a high degree of user-convenience is needed.

Low frequency RFID technology refers to 125 or 120 kHz read-only technology. It is used frequently in today's RFID access control systems and is based on de facto industry standards rather than international standards. This means that cards and readers from different manufacturers don't necessarily work together. Most of these types of cards hold a fixed serial number (for example those by HID, Deister and Nedap). While some have a read/write memory for storing variable information, such as programming a monetary value for use with a cashless vending system or parking application, and authentication functionality (for example those by Hitag, NeXS and Nedap). Low-frequency products have proven to be very reliable and have a comfortable reading range of up to one metre, depending on the type of card and reader. Data transmission at this frequency isn't easily influenced by moisture and dirt, for example. The newer types of cards have extra encryption built-in to prevent the data being 'sniffed' between card and reader. Low-frequency technology, however, has a low data rate so only small amounts of data can be transmitted. Levels of security are high, on the other hand, as the information on some technologies is less widely available to the general public.

High frequency RFID technology refers to 13.56 MHz technology. High-frequency cards are commonly used in the access control industry and meet the various ISO standards for proximity cards. They have an operating range of no more than 10cm and memory sizes range from 64 bytes to several kilobytes.
One of the best-known commercial products using the 13.56 MHz frequency is Mifare. For new applications, DESFire is recommended as this provides a higher level of data encryption using triple DES or AES encryption standards. From Legic, Advant cards are available, which are also equipped with triple DES encryption. All these cards are now widely used in access control systems, particularly as they have a large memory size so more data can be stored on the card.

Ultra high-frequency RFID technology (UHF tags) operate in the 858 to 930 MHz frequency band. They have a versatile reading range from a few centimetres to several metres without needing a battery. This makes the technology suitable for various applications, such as supply-chain and inventory tracking, anti-counterfeit and identification. The read range, however, can be strongly affected by moisture and metal. A card may contain both UHF and high-frequency technology. This could, for example, enable one card to provide long-range access control for vehicles as well as short-range access control for a building.

Microwave RFID technology functions at a standardised frequency of 2.45 GHz. Detection distances of up to 10m are possible, depending on the antenna and tag dimensions. This allows the technology to be used in access control applications that require a large identification distance, for example vehicle access control applications. This type of Microwave technology uses a narrow beam to read the tag from the reader, which means it can be used where there are multiple vehicle lanes without them interfering with one another. While this type of technology requires a battery in the tag, modern batteries can last for many years, removing the inconvenience of regularly replacing batteries or tags.

NFC technology

NFC refers to 13.56 MHz technology rather than RFID high-frequency technology. NFC can be used in cards, but has more practical value in mobile phones. However, although using NFC technology in mobile phones is possible from a tech-

nological perspective, it’s not yet mature from a commercial point of view. NFC is very much comparable to RFID, but specific characteristics such as convenience, reading distance and durability depend on the way NFC is implemented in the access control system.
When using NFC technology in mobile phones for access control, the mobile phone communicates with NFC-compatible external readers, much like a traditional contactless smartcard. Programming a unique ID number in a mobile phone can be done in several ways, using either a secure element or through host card emulation:

- **In the secure element in the phone**
  NFC technology can be applied to the secure element of a phone’s hardware. The difficulty is that this requires co-operation with phone manufacturers; they must be willing to provide access to the secure element of the phone to program the solution.

- **In the secure element of the SIM card**
  The number of SIM cards with a secure element is growing, enabling NFC to be implemented securely on them. The difficulty here is implementing the technology on specific SIM cards, as there are many different mobile network operators (MNOs) in different countries. Agreements need to be made with MNOs to access the secure element and apply the technology. The number of trusted service managers is growing, however, increasing the ease of implementing NFC on SIM cards. These intermediary companies control the secure element of the phone enabling service providers to manage the application of NFC technology on the secure element remotely.

- **In the secure element of the microSD card**
  A designated microSD card allows for secure storage of data by specific manufacturers of access control systems. As the manufacturer can manage the secure element, this is also a secure way of using NFC technology to grant access. Moreover, it is easy to apply NFC as manufacturers can program designated microSD cards, which are stored in the user’s phone. MicroSD cards are, however, rather expensive, making this solution less attractive.

- **Using host card emulation**
  Replacing the need for a secure element, host card emulation provides a virtual representation of the smartcard in the phone. As this solution is based on software, it enables NFC technology to be used easily for different purposes. Data, on the other hand, cannot be stored as securely as when using a secure element. This can be improved when offering host card emulation in combination with a secure element in the cloud. Another downside of host card emulation is the fact that users must run an application on their phone and the phone needs to be on when trying to get access, making it less convenient.

Using NFC technology for access control can make RFID cards obsolete and can increase levels of flexibility. However, secure use of NFC technology in access control is currently very complex, despite the technology being mature enough. NFC technology needs to grow from a commercial point of view before it is attractive enough to replace current access cards.

Card technology characteristics at a glance

	Mag-strip	Wiegand	Barcode	Smart-card	RFID LF	RFID HF	RFID UHF	RFID Micro wave
Data size	✗	✗	●	✓✓	●	✓	●	●
Security	✗	✓	✗	✓✓	●	✓✓	✓	✓
Convenience	●	●	●	●	✓✓	✓	✓	✓
Standardisation	✓	✓	●	●	✗	✓	●	●
Reading distance	✗	✗	●	✗	✓✓	✓	✓	✓✓
Durability	✗	✓	✗	●	✓✓	✓✓	✓✓	✓✓

Key	Significance
✓✓	Excellent
✓	Good
●	Sufficient
✗	Not recommended
✗✗	Insufficient

Want to know more?

Just get in touch with us.

Nedap Head Quarters
Parallelweg 2
7141 DC Groenlo
The Netherlands
+31 (0)544 471 111
info@nedapsecurity.com