WHITE PAPER

Best Practices in Access Control

Table of Contents

Introduction 1

Choosing the Right Reader and Card Technology 2
- Relative Security of Commonly Used Card Technologies 2

Use Proper Key Management 3

Protect the Communications 4

Use Security Screws 5

Prevention Using Antipassback 5

Use Additional Factors of Authentication 5

Mind the Cards 6

Protect the Cards 6

Detection – The Second Line of Defense 7
- Protect and study the Security Logs 7
- System Upgrades and Migration Strategies 8

Conclusion 8

Appendix A: The Dangers of Using CSN-only Smart Card Readers 9
- Introduction 9
- Why Use Contactless Smart Cards? 9
- A False Sense of Security 9
- How is a CSN Used for Access Control? 10
- The Most Commonly Used Card Format Intensifies the Problem 10
- Using the CSN Sacrifices Security for Interoperability 11
- Using the CSN is Inconvenient and May Add Hardware Costs 12
- Using the CSN Can Decrease Privacy 12
- CSN Emulation 12
- U.S. Government and International Organizations Recommendations 12
- Cryptographers and Industry Expert Opinions 13
- Refuting Commonly Held CSN Beliefs 13
  - What About Encrypted CSNs? 13
  - Chips with Programmable CSNs 13
- When Should a CSN Reader Be Used? 13
- Conclusion 14

Introduction

To insure that the ever-changing security requirements of a facility are met, a periodic review of a site's access control system and its associated policies is a necessity. In fact, conducting an annual access control system review is the first step in establishing a systematic process for assessing the security of your organization; it is the principle best practice that provides the framework for all the other guidelines.

Once a yearly review process is in place, the fundamental best practices concept is that an effective security system uses a layered approach to security. A good analogy of this concept would be one where a home protected by a burglar alarm might use both glass break detectors and motion sensors to detect when an intruder enters the house.

This white paper contains important guidelines for all of the stakeholders in an access control installation including the facility owner, the system specifier, the installer, and the end user.

Choosing the Right Reader and Card Technology

Contactless smart cards are fast becoming the technology of choice for access control applications. Security, convenience, and interoperability are the three major reasons for this growth. Since there are a wide variety of reader technologies being offered by today's manufacturers, it is important to make sure that the correct technology is chosen to match the desired level of security. Using a good, better, best grading system will help make the correct choice easier.

Recognizing that there are many legacy card technologies still in use and that replacing them with the latest contactless smart card technology may be expensive or logistically difficult, implementing the recommendations included in this paper will raise the level of security of an installation and should be done regardless of the card technology employed.

Relative Security of Commonly Used Card Technologies

Figure 1 illustrates and ranks the relative strength of commonly used card technologies based on how much publicly available information there is about the technical details of the card technology and the degree of difficulty required to illegally read or copy from the technology. The higher the number, the more secure the technology:

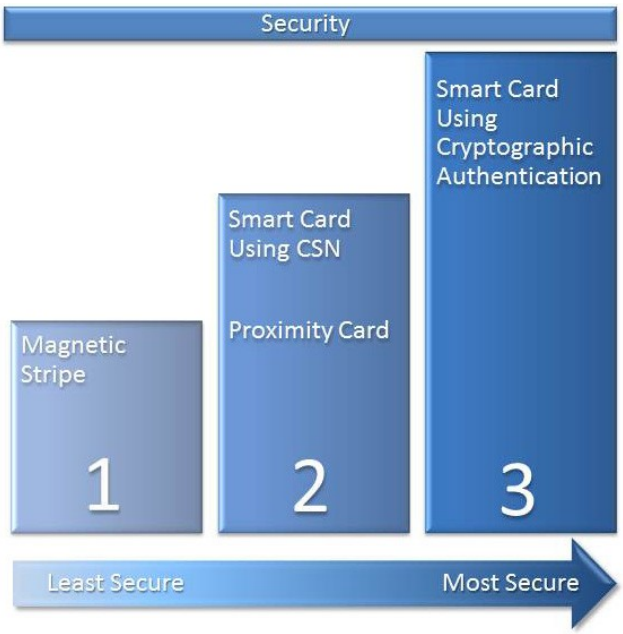


Figure 1: Relative Security Levels of Commonly Used Card Technologies (lowest to highest)

Magnetic stripe (magstripe) has the lowest security with its technical details being well documented by ISO standards. This technology typically uses little or no security protections. Additionally, off-the-shelf devices are widely available to encode magstripe cards. Although there are some techniques that can make magstripe more secure, widespread adoption of these techniques in the access control industry have not occurred due to the convenience, security, and increased memory available in contactless smart cards.

125 kHz proximity (Prox) card technology and the use of the Card Serial Number (CSN) of a contactless smart card are better than magnetic stripe but are not as secure as contactless smart cards. Prox card devices that can copy and emulate (mimic) Prox cards have been demonstrated. Similarly, because there is no secure authentication of the CSN and the knowledge of the CSN workings are published as part of the ISO standards, CSN emulation is also easily accomplished. (For more details on the dangers of using CSN readers, see the Appendix that describes these dangers in greater detail.)

Contactless smart cards, when properly implemented and deployed, offer the highest level of security and interoperability. These cards use mutual authentication and employ cryptographic protection mechanisms with secret keys. They may also employ special construction and electrical methods to protect against external attacks.

Use Proper Key Management

Key management deals with the secure generation, distribution, storage, and lifecycle management of cryptographic keys. This important subject deserves an entire white paper by itself, but here are a few of the essential key management best practices.

Whenever there is a choice, choose a manufacturer that allows you to utilize your own cryptographic authentication key that is different that its other customers so you have a unique key for your facility or organization. Although it may be easier not to have the responsibility of managing and safeguarding your own keys, utilizing your own authentication keys will protect your organization from a key compromise that occurs in someone else's readers purchased from the same manufacturer.

Do not choose a manufacturer that stores the same key in all of its credentials. Extraction of the key from a single card compromises all of the cards in use. Use a manufacturer that uses diversified keys, which means that each card uses a different key that is cryptographically derived from a master key. Ideally this diversification would use a public scrutinized algorithm such as DES or AES.

If offered a choice, use readers that protect their master key from being easily extracted from the reader. Reader manufactures that use a secure element such as a Trusted Platform Module (TPM), Secure Access Module (SAM), or other equivalent device to store cryptographic keys. Some manufacturers even go one step further and actually do all of the cryptographic operations inside the secure element making it even more difficult to compromise the integrity of the key or data.

Be prepared to act quickly in case a key compromise does occur and know how to use the manufacturer's procedures to roll or change the keys in both the readers and cards. Some manufacturers have the capability to move cryptographic data, such as keys as well as reader firmware upgrades, securely from a secure 'vault' on their premise directly into the secure element inside the reader using end-to-end security among trusted devices.

Protect the Communications

The individual components of an access control system need to communicate with each other. Typical data includes card read messages, door unlock messages, audit trail data, cardholder privilege changes, and much more. Consequently, it is critical to protect this information exchange on the communications media on two levels. The actual communications medium, be it hard-wired or wireless, as well as the data content must be protected.

When the communication takes place using wires, there are many different methods, interfaces and protocols to choose from. The most popular and de-facto industry standard is the Wiegand Protocol. This protocol became very popular because it is universally supported by almost all reader and panel manufacturers. More modern communication methods such as RS485 and TCP/IP offer more security and are therefore more desirable.

If a perpetrator can get access to the wires used for communications between the reader and the upstream device, it may be possible to intercept messages; this could result in a loss of privacy as well as the possibility of replaying a previously captured message and unlocking the door. It may also be possible to simply send an 'unlock' message as well. That is why a secure protocol is important, ideally employing 1) mutual authentication to ensure that each device trusts the other device, 2) encryption, and 3) message replay protection.

An additional reason to protect the wiring is to prevent a 'denial of service' attack in which the wires are cut or shorted together to interrupt communications. Another vulnerability due to unencumbered access to the wires can be initiated by the use of command cards used by some manufacturers to program the operating characteristics of readers. Typically, command cards are only accepted for a short time after power has been interrupted and then restored to prevent them from being used at any time. If the power wires to a reader are accessible, then a perpetrator would be able to interrupt the power to the reader so that command cards could be read in an attempt to put the reader in a state where cards are no longer read, creating a denial of service attack. An even more destructive denial of service attack can be launched in which the communication wires are connected to a high power source in an attempt to destroy the reader and/or the upstream device.

To minimize these risks, installing the security systems wiring in conduit makes it more difficult to access the wires without being noticed due to the difficulty of identifying the correct conduit, not to mention the additional time required to compromise the wiring in the conduit. Even if the entire wire run is not fully enclosed in conduit, just using conduit in the most vulnerable publicly accessible areas is desirable. Additionally, bundling several wire runs together (ideally in conduit) to make it more difficult to identify the correct set of wires is also desirable. (Follow the manufacturer's recommended installations. Some wiring, such as power wiring, may not be recommended to be in the same conduit as data communications wires.) It is particularly important to protect the wiring of outside readers that are located at the entrance to a premise.

Additionally, avoid the use of readers with built-in connectors that make it easier to quickly swap out a reader and avoid the use of wire-nut connectors to connect the reader wire pigtails to the panel wiring. Instead, connect the wires in a more secure and permanent fashion, such as soldering with shrink-wrap tubing to cover the connections.

Use Security Screws

Always utilize security screws that require special tools to remove a reader and other security components. If the correct tool is not available, then it makes it nearly impossible to remove the reader without causing damage to the screws. This damage may be noticed alerting security of a potential intrusion attempt – especially if policy dictates that readers be physically examined on a periodic basis. (Physical examination of readers should be included on guard tours.) It also has the effect of making the removal process more difficult, and slowing down the removal increases the possibility that the perpetrator will be noticed.

Prevention Using Antipassback

Another best practice that may be feasible is to program the access control host software to refuse granting access to a cardholder that is already inside the facility, which will prevent a duplicate card from entering the facility. This mechanism, referred to as antipassback, is available in many access control systems. Note that this feature requires two readers at the door – an 'in' reader and an 'out' reader. One additional benefit of using antipassback is that it prevents a user from using their card with others following through an open door (tailgating).

Use Additional Factors of Authentication

It is generally accepted that multiple factors of authentication consisting of something you have (e.g., a card), something you know (e.g., a password), and something you are (e.g., a biometric) increases the probability that the person presenting his card at a reader is the same person that was initially issued the card. Ideally the use of all three factors is best but just adding one additional factor can be effective. A relatively inexpensive, easy-to-use second factor is a password, which can be achieved with the use of card readers with built-in keypads. Keypad readers are ideal solutions for environments where additional layers of security are required – such as in a lab or corporate research environment and the perimeter entrances to a facility.

Readers with a built-in keypad minimize the likelihood that a lost card can be picked up and simply used to enter a facility. It also minimizes the threat of card cloning. Ideally, the password should be changed periodically, or if a common password is utilized, change it every day to increase the effectiveness. Note that some systems store the actual password inside the card itself. Although this is generally effective if the card technology is secure, it is better to have the password stored on the host.

The use of biometric readers to insure that the person presenting the card is actually the same person that was issued the card can be used in environments where an even higher level of security is required. A similar solution is to use hand-held biometric fobs that only emit RFID card data after a biometric authentication has occurred. These types of devices actually help to increase privacy and cannot be surreptitiously read without the user's permission since the access control credential cannot be read until the biometric authentication process has taken place.

If the use of multiple factors presents throughput or convenience obstacles, consider only requiring multiple factors of authentication outside of normal business hours where the risk of unauthorized entries are highest or automatically turned on when there is an elevated 'threat level'.

Mind the Cards

A perpetrator may use surreptitiously obtained cards for nefarious purposes. One way to do this is to claim that a card was lost when it really wasn't. Make sure that lost cards are voided immediately. Another way for a perpetrator to fraudulently obtain cards is through gray market sources such as eBay or even legitimate card resellers. There are several best practices to prevent this. First, make sure that only issued cards are valid; don't have spare cards pre-validated and ready to hand out.

Some access control systems can also generate a different message than just denied in the case of presented card in an ID number range that haven't been entered in the system. When an illegally obtained card is used, if the message generated by the access control system was 'Card out of range' instead of simply 'Denied', it should signal more urgency to be investigated. Similarly, cards using a different data format that are reported as 'Unrecognized', as well as cards with the wrong facility code are also indications that illegally obtained cards are being presented to the system. Therefore, any messages reported by the host access control system with wrong formats, wrong site codes, or out of range should be immediately investigated.

Don't succumb to the argument made by alternate card suppliers that proprietary card formats are more expensive and are an attempt by manufacturers to keep you from buying cards from open sources. The use of proprietary formats offered by an OEM or one that is exclusive to a particular site is a desirable best practice.

Cards with proprietary formats are much more difficult to fraudulently obtain as compared to the industry-standard open-format 26-bit Wiegand format and proprietary cards typically provide provisions for non-duplication of card numbers. Some manufacturers' readers can even be set to ignore 'foreign' cards completely, which will also present an obstacle to using cards obtained on the open market.

As described earlier, never use contactless smart card readers that solely rely on the card serial number such as CSN readers. It doesn't make sense to use a contactless smart card with increased security over legacy card technologies and ignore the security capabilities built-into the card. Some companies advocate these types of readers because they do not require implementation of security mechanisms which may not be available for license to that reader manufacturer and typically add additional costs which makes the readers more expensive. Using CSN readers is analogous to using a high security reader on a glass door.

Protect the Cards

Cardholders should be instructed not to wear their badges in prominent view when outside the premises and be aware of people approaching them attempting to perform a 'bump and clone' in which an attempt is made to try and surreptitiously read their card using an electronic skimming device. For contactless smart cards operating at 13.56 MHz, there are many companies that sell RFID shielding devices that are packaged into a card holder that are very convenient to use that prevents these kinds of attacks.

Another best practice is to avoid putting any identifying data on the card that gives an indication as to the location or address of the facility to make it harder to identify where a lost card can be used. Of course, many companies put their company logo on their cards but organizations should balance this requirement with the disadvantage of including artwork that reveals the company's location.

For companies with multiple facilities at different physical locations, do not use the same facility code (also known as site code) data in all of the cards so that a lost card can be used at any of the locations.

Another best practice is to have a policy that lost cards need to be reported as soon as possible. And make it a policy that when a card is reported lost, it is immediately removed from the system. As an alternative, consider making the cost for a replacement card high enough so that a cardholder will think twice about being careless. Of course, this policy may actually discourage a cardholder from immediately reporting a lost card in the hope that it might be found.

Detection – The Second Line of Defense

Buy readers with a tamper detect mechanism that provides a signal when the reader has been removed from the wall. Almost every panel manufacturer provides the ability to monitor this alarm signal and report when a reader is tampered with. If the panel supports 'supervision', another method that can be used by installers is to include an additional pair of wires that are connected together through a resistor at the reader. This loop can be monitored by the panel using a technique called 'supervision' that can detect when the wires are cut, shortened, or other changes in the electrical characteristics of the wires are made. Of course the panel must support this capability.

Immediately investigate tamper alarms even if they are momentary and return to normal. You might actually detect the perpetrator in action or find that a foreign device has been installed in an attempt to monitor and/or modify the communications between a reader and the upstream device. If the reader is controlling a sensitive location, such as a perimeter door, have it and the door monitored by CCTV. Some access control systems can automatically switch the viewing monitor to the door with the tamper alarm as well as tag the video history log with the event for later review. And, if you are using your own company-specific cryptographic keys that are stored in a reader, realize that a reader that has been removed from the wall might have had the cryptographic keys extracted from the reader, which compromises the entire security of your installation.

Many reader manufacturers also have the capability of sending 'health' messages (also referred to as 'heartbeat' or 'I am Alive' messages) on a periodic basis to the upstream device.

This functionality can also be used to detect when the wires are cut and does not require any additional wires to get this protection. If these periodic messages are set to occur faster than it would take to install a rogue listening device, then the panel would notice and report the interruption. Ideally these messages would be set to occur as fast as every second. Monitoring health messages also provides additional benefits since they will detect reader malfunctions. It is better to know when a reader is not working before somebody complains (usually in the middle of the night when they cannot get in the door).

For converged physical and logical access control systems, geographic monitoring is available. For example, if a person has just come in through a door at a site in Buffalo but is trying to log into his computer in Denver, then obviously there is a problem. Another benefit in converged systems is to not allow a person to log onto his computer if he hasn't used his card at a perimeter reader. This simple concept will get people to change their behavior and not tailgate when they are denied access during the computer log-on process.

Protect and Study the Security Logs

The audit trail of the transactions (i.e., security logs) should be protected as it contains very sensitive data, such as who is going through what doors at what times, card numbers, and much more. If audit trails are electronically stored, keep them encrypted and secure. If they are printed out, shred them when done. (If any of this data is available from a remote site over the network, or for that matter, if the server is accessible or uses the public Internet, make sure that a proper penetration [PEN] test is performed by a reliable third-party.)

The security logs are invaluable after a security-related event has occurred because they might provide clues as to who the perpetrator was. But that is not the only time to study the logs. Periodically look at the logs in an attempt to see patterns of events that don't make sense. Even better yet, use computer software to analyze the logs for suspicious behavior patterns. For example, a cardholder requires a finite amount of time to travel between entry points and if the same card is used at two different locations in a very short time, this could indicate that a cloned card is being used.

System Upgrades and Migration Strategies

Choose a manufacturer who has a strong portfolio of migration products and strategies including multi-technology cards in which both the legacy credential and the new credential technology can co-exist on the same card. Similarly, multi-technology readers capable of reading both the legacy credential and the new replacement higher security credential are useful in a migration strategy. And often a combination of these products may be necessary to effectively migrate in the shortest, most convenient, and cost effective manner.

Conclusion

Following as many of these best practices as feasible, with attention to appropriate levels of security, will result in a system that better fulfills its intended function with less possibility of being compromised. And these are just a few best practices to look for. There are many additional best practices that have not been discussed in this paper, such as the use of security mechanisms on the card (like holograms) and other tamper evident technologies and much more. This paper will be continually expanded to include additional best practices for organizations to effectively balance cost, convenience and security when deploying an access control system. Please set a book mark where you downloaded this document check back for later versions.

Appendix A: The Dangers of Using CSN-only Smart Card Readers

Introduction

Some manufacturers, in an attempt to sell a 'universal' reader capable of reading almost any contactless smart card technology, actually disable all of the built-in security mechanisms in order to achieve their goal. Reading only the CSN of a contactless smart card actually provides a false sense of security analogous to installing a high security door without any locking mechanism.

These readers, referred to as 'CSN readers', only read the card's serial number which, as per ISO standards, must NOT be protected by any security since they are needed by the reader to be able to detect when more than one card is presented to a reader at the same time. This process, referred to as anticollision, takes place before the card and reader mutually authenticate each other. Because the ISO specifications are a publicly available document, details of how this anticollision process works can be used by a perpetrator to build a device to clone (simulate) the CSN of a contactless smart card.

Understanding this misuse of the CSN is critical for users of the technology to ensure that access control security is maximized. If implemented and deployed properly, contactless smart cards represent one of the most secure identification technologies available today.

Why Use Contactless Smart Cards?

The most modern contactless smart cards incorporate advanced state-of-the-art security mechanisms. Before a reader can begin a dialogue with a card, it uses mutual authentication to ensure that both the reader and card can 'trust' each other. Only after this process occurs is the reader allowed to access the data stored inside the card. This data is protected by cryptographic algorithms and secret keys so that if the data were somehow extracted or even spied on, it can be very difficult to decipher and utilize.

As with 125 kHz Prox technology, contactless smart cards are convenient for users who merely present their cards near a reader. In addition, users do not have to carefully insert the card into a slot or worry about proper orientation. This also minimizes the physical wear-and-tear on both the card and the reader, the potential for vandalism, and environmental elements.

Amplifying the convenience of contactless smart cards is their capability to support more than one application at a time. For example, a single card can be used for the dual purposes of opening a door and logging on to a computer.

Contactless smart cards also provide greater and ever-increasing amounts of memory, enhancing the sophistication of applications. Enough memory is available to store biometric templates and even photos, enabling additional factors for user authentication. Such authentication of both the card and user increases the security and likelihood that the person using the card is indeed the authorized user of that card.

A False Sense of Security

To understand why using the serial number of contactless smart cards provides a false sense of security, it is first important to understand some basic definitions and contactless smart card mechanisms.

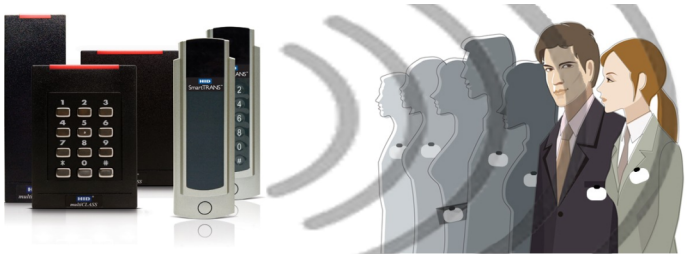
CSN: CSN refers to the unique card serial number of a contactless smart card. All contactless smart cards contain a CSN as required by the ISO specifications 14443and 15693. CSNs are typically 32 to 64 bits long.

The CSN goes by many other names including UID (Unique ID), CUID (Card Unique ID), and of course CSN (Card Serial Number). It is important to note that the CSN can always be read without any security or authentication as per the ISO requirements.

Think of the CSN using the analogy of the identifying number on a house. It is important for everyone to be able to read the house number to find it. Similarly, the CSN is used to uniquely identify a card when more than one card is presented at a reader at the same time. Moreover, nobody can get in to your house or get in to a smart card without using the correct key.

Anticollision: Anticollision is part of the communications protocol used by contactless smart cards to uniquely identify a card when more than one card is presented at a reader at the same time. It provides the ability to communicate with several contactless smart cards simultaneously. This is especially important in long-range readers, as illustrated by Figure 2: Anticollision.

Figure 2: Anticollision



The ISO standards require that every contactless smart card have a unique CSN and these standards describe several methods to implement anticollision. It must be pointed out that the CSN was never intended by ISO to be used for any purpose other than anticollision.

How is a CSN Used for Access Control?

CSN readers are readers that use the CSN of a contactless smart card instead of the credential data stored in the secure area of the card. When a card is presented to the reader, it reads the CSN and typically extracts a subset of the CSN, converts it to a 26-bit Wiegand or other output format, and then outputs this data to an upstream device such as a panel or host computer.

The Most Commonly Used CARD Format Intensifies the Problem

There are many card formats available and formats are comprised of multiple fields. The most commonly used format contains a total of 26-bits and includes a site code field (8-bits), a card number field (16-bits), and two parity bits.

The site code field (also called a facility code) is usually the same for all cards at a given site and is used to ensure that cards from different facilities in the same geographic area can be distinguished from each other. Without this field, cardholders with the same card number might be able to access facilities for which they do not have authorization. The card number field uniquely identifies each cardholder and the parity bits are used to detect data communication errors.

If the 26-bit Wiegand protocol is being used, the 16-bit card number field is extracted from the CSN and the site code field is usually created from a pre-programmed number stored in the reader. Because the smart card manufacturer preprograms the CSN, using only a small portion of the CSN is utilized. This introduces the likelihood that there will be duplicate card numbers. Statistically, out of every 65,535 cards, there will be at least one duplicate.

This is why it is desirable to use a card format with more bits in the card number field. Some manufacturers offer a card format that uses both a larger card number field and includes an additional OEM field together with the site code field.

Keep in mind that the issue of duplicate card numbers is not limited to the Wiegand protocol. It occurs in *any* protocol that uses a reduced number of bits derived from the CSN to represent a card number.

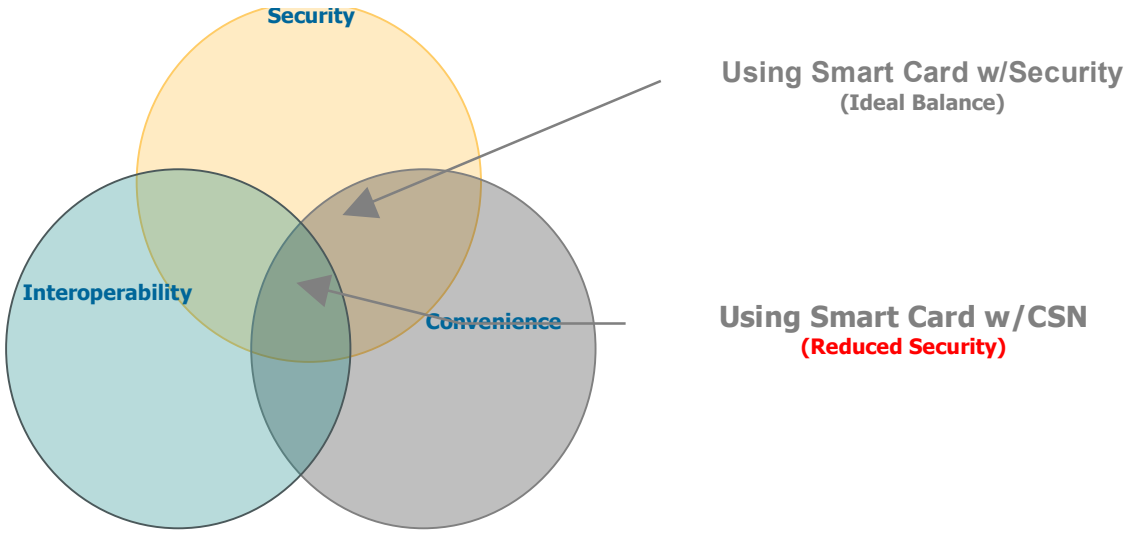
Using the CSN Sacrifices Security for Interoperability

To create a low-cost, universal reader capable of reading any manufacturer's contactless smart card, reading the CSN is the easiest and sometimes the only way to achieve interoperability. One or more of the following reasons are at the heart of the problem:

1. The inclusion of the hardware chip containing the security algorithms adds cost.
2. The reader manufacturer may have to pay a license fee for the security algorithms or the reader manufacturer may not even be able obtain a license.
3. The security keys to the contactless smart cards are not available.

Using a low-cost, universal reader that does not avail itself of the security features that contactless smart cards offer will compromise the security of the facility or area where it is used. As noted earlier, the three major reasons to use contactless smart cards are security, convenience, and interoperability. Figure 3 illustrates how using the CSN compromises these three key reasons.

Figure 3: Using Smart Card with CSN Reduces Security



Using the CSN is Inconvenient and May Add Hardware Costs

CSNs are non-consecutive numbers that are in a random order. Therefore, referring to a cardholder by its CSN makes it impossible to group employees by card number ranges such as 1 – 100. Furthermore, as discussed above, it is desirable to use all of the bits required to represent the entire CSN. A 32-bit CSN would be represented as a number with as many as 10 digits and a 64-bit CSN requires as many as 20 digits. Even using the hexadecimal notation to enter, CSNs still require a person to type up to 16 characters to add or change a card.

With an enrollment reader, the process of adding cards to a system can be simplified since the CSN of a card can be automatically read instead of being typed. However, this introduces more complexity to the system, requiring additional access control software and hardware enrollment readers. Moreover, if a cardholder's privileges have to be changed, an enrollment reader is of no use when the card is not available.

Using the CSN Can Decrease Privacy

Because reading only the CSN of a contactless smart card requires less power, read distances are often greater. This is because the power-hungry cryptography circuitry inside the contactless smart card is not used. Greater read distances, coupled with no authentication or security, make the cards far less secure from illegal activities at even greater distances.

In addition, using the CSN gives the false impression that a particular reader's performance is greater than it actually is. This may be doubly misleading for users because the CSN reader may be less expensive and offer better read distances than a reader that fully implements the security protections available with contactless smart card technology.

CSN Emulation

An earlier section identified additional security threats based upon the availability of information required to illegally read or copy a card technology. It concluded that using the CSN of a contactless smart card is low security because it is well documented by ISO standards and no security is used to authenticate a CSN. Many smart card development tools such as protocol analyzers can emulate an ISO 14443 or 15693 CSN. Furthermore, universities are also teaching the ISO protocols and students are writing firmware to emulate CSNs. What better way to prove that a student correctly understands the ISO protocol than to actually create firmware to emulate a CSN and fool a reader to prove that the firmware actually works?

U.S. Government and International Organizations Recommendations

A US Government report recommends not using the CSN for identification purposes since "… using the CSN as a unique identifier works only for 14443A, and for 14443B it [may] be a random number that changes every time and will be discussed in a future version of the specification."

The International Civil Aviation Organization also warns, "There is no protection in use of a CSN because this is often set in software by chip manufacturers and can be changed."

Cryptographers and Industry Expert Opinions

Both cryptographers and industry experts also warn of the dangers of using the CSN to identify a cardholder. David Engberg of Corestreet Ltd. said, “The serial number has no cryptographic or protocol-level protections to prevent an attacker from asserting the same serial number as any real card. By implementing ISO 14443 directly, an attacker can imitate any desired CSN.”

Bruno Charrat, CTO of Inside Contactless, concurs with David Engberg, adding, “As soon as there is no security in the communications, you can clone a card and then enter anywhere you want! It is as simple as that.”

In an article from Security Technology & Design, Greg Young, Technical Sales Manager for RFI Communications & Security Systems, warns against the assumption that contactless smart cards offer more secure transmission than 125 kHz Prox cards. “They can be more secure, but they’re not necessarily more secure,” he said. “Many manufacturers are touting readers that read multiple types of smart card technology —MIFARE, iCLASS—when really all they’re reading is the serial number sent unencrypted from the card, in the same way Prox is. Unless you make sure that what you’re reading is from a secure sector on the card that can be truly encrypted, and there is a handshake procedure between the reader and the card before transmission, what you’re getting is no more secure than proximity technology.”

Refuting Commonly Held CSN Beliefs

What About Encrypted CSNs?

Encrypted CSNs offer no real protection from cloning and replay attacks.

Chips with Programmable CSNs

The statement – ‘The CSN is a unique serial number permanently written into the device’s nonvolatile memory at the factory; it cannot be modified and is guaranteed to be unique for all devices.’ – is not always true.

Some contactless smart cards have programmable CSN. For example, one vendor’s contactless smart card chip data sheet states: “The CSN is written at time of manufacture, but part of it can be customer-accessible and customer-writable, on special request.”

Similarly, another manufacturer’s data sheet states: “The CSN is defined by the customer during personalization … it is usually unique… may be set to any value.”

Clearly, we see that there is no guarantee of the authenticity of a CSN and CSN reader’s compromise security.

When Should a CSN Reader Be Used?

CSN readers are very useful as a temporary solution to migrate from one smart card manufacturer to another. A single reader can be used to read both the existing cards using its CSN and the new replacement cards using full security and authentication. This provides a window of time to replace the cards. When all of the existing cards have been replaced, the reader can then be instructed to turn off its CSN reading capability. For maximum security, it is best to keep the replacement time period as short as possible.

Conclusion

Using the CSN for anything other than its intended use severely reduces the security of a contactless smart card. In other words, CSN is really an acronym for Compromizable Serial Number. When implementing and deploying contactless smart card technology, always consider the following:

1. Contactless smart cards are secure when used properly.
2. Using the CSN of a contactless smart card bypasses the security built into smart cards.

Understanding the security risks associated with using the CSN instead of reading the data protected by security mechanisms will help ensure that the proper protections are in place for both personnel and property.

Revision 1.1