11.7. Card Access Control Systems

Objective

11.7.1. To ensure Access Control Systems incorporating contactless RFID or smart cards are used safely and securely in order to protect privacy, prevent unauthorised access and to prevent the compromise of secure spaces.

Context

Scope

11.7.2. This section provides information relating to the risks, security and secure use of RFID or smart cards in access control systems. This section does not discuss biometric access control systems.

11.7.3. The previous section (11.6. Radio Frequency Identification Devices) provides background information and technical detail of the RFID aspects and should be read in conjunction with this section.

Background

11.7.4. Contactless access control systems based on RFID (Radio Frequency Identification) has largely replaced earlier technologies such as magnetic swipe cards in almost all security-critical applications. Two generations of RFID access cards exist:

- an earlier generation of cards, which use only basic proprietary security mechanisms; and
- a more recent generation that incorporates advances in CMOS and smart card technology to implement cryptography and other protective measures.

11.7.5. Older access control systems often incorporated a magnetic strip and were easily cloned. More recent systems support the use of PINs in addition to RFID. Unfortunately PINs are also sometimes stored on the cards, often unencrypted and unprotected, and thus facilitating attacks on both the card and the PIN.

11.7.6. Access control systems typically comprise four components:

- A reader that programmes the access cards for particular employees and their permitted access to parts of the site, building to secure areas.
- A transceiver at each control point to communicate with cards.
- A controller to control the locks of access points (doors).
- The backend system that hosts all permissions and authorised data and interfaces with the reader, transceiver and controllers.

11.7.7. Traditionally access control systems were hosted by stand-alone equipment. Modern access control system may be hosted on standard computer equipment and hosted in the organisation's datacentre. It is possible that a system intrusion can target access control systems, making the switches, gates and locks remotely accessible.

11.7.8. Low frequency RFID badge systems use 125KHz, (ISO 11784/5 and ISO 14223). Newer high frequency RFID cards use 13.56MHz (ISO 15693, ISO 14443 and ISO 18000-3).

11.7.9. Some cards also operate at UHF frequencies of 850-960Mhz (ISO 18000-6). Some cards are designed to operate at low and high frequencies by embedding multiple antennae in the cards.

11.7.10. The ISO/IEC 14443 standard for contactless smart card communications defines two types of contactless cards ("A" and "B") and allows for communications at distances up to 10 cm operating at 13.56 MHz.

11.7.11. The alternative ISO/IEC 15693 standard allows communications at distances up to 50 cm. The ISO/IEC 7816 standard (in 15 parts) defines the physical, electrical interface and operating characteristics of these cards.

11.7.12. UHF cards follow the EPC Global Gen2 standard and the ISO 18000-6 standards and are designed to operate at distances of up to 10 metres.

Smart Cards

11.7.13. Smart cards typically incorporate an embedded integrated circuit typically incorporating a microchip with internal memory, a read-only CSN (Card Serial Number) or a UID (User Identification). The card connects to a reader with direct physical contact or a contactless radio frequency (RFID) interface. With an embedded microchip, smart cards can store large amounts of data, carry out on-card functions (such as encryption and authentication) and interact intelligently with a smart card reader. Smart card technology can be found in a variety of form factors, including plastic cards, key fobs, watches, subscriber identification modules used in mobile phones, and USB-based tokens. Smart cards are widely used in payment card (debit and credit cards and electronic wallets) and access control systems.

11.7.14. In common with other RFID devices, smart cards incorporate an antenna embedded in the body of the card (or key fob, watch or token). When the card is brought within range of the reader, the chip in the card is powered on. Once powered on, an RF communication protocol is initiated and communication established between the card and the reader for data transfer.

11.7.15. Smart cards typically incorporate protective mechanisms including authentication, secure data storage, encryption, tamper-resistance and secure communication. Support for biometric authentication may also be incorporated.

Near Field Communication (NFC)

11.7.16. NFC is an RFID technology that enables two electronic devices to establish communication by bringing them within 4 cm of each other. As with other "proximity" technologies, NFC employs electromagnetic induction between two loop antennae when NFC devices exchange information. NFC operates in the globally available unlicensed radio frequency band of 13.56 MHz conforming to the ISO/IEC 18000-3 standard. In access control applications these devices are sometimes known as “prox cards”.

Attacks

11.7.17. In addition to attacks on RFID components described in the previous section, access control cards can be susceptible to relay and chip hacking attacks.

11.7.18. Relay attacks rely on rogue readers to activate the tag even when not in proximity to a legitimate reader. The card holder will be unaware that such an attack is underway. An effective defence is to incorporate distance-to-reader verification although few RFID systems incorporate this mechanism.

11.7.19. Signals between cards and a legitimate reader can be intercepted at distances of up to a metre. Greater distances are possible with higher powered equipment, special antennae and in low interference environments. The signals and data, including card credentials, are captured off-line and used to clone access cards. Again the card holder will be unaware that such an attack is underway.

11.7.20. Chip hacking is facilitated by physical access to the card but can be mitigated by second factor authentication, encryption of data on the card and card tamper detection.

11.7.21. Threats, vulnerabilities and mitigations of RFID access control systems are summarised in the table below:

Threat/Vulnerability	Mitigation
Interception of the RFID signals	Encryption of RF links Harden RFID elements
Implants	Physical security CCTV Tamper resistant readers
Cryptographic attacks	Use of approved cryptographic algorithms and protocols Strong key management Incident detection and management Use of evaluated products
Replay Authentications	Robust Random Number Generation on readers
Key extraction reader attacks through side channel analysis or fault injection	Use of evaluated products with SAM chips Incident detection and management
Attack on authentication keys on the card	Key diversification Strong key management Incident detection and management
Chip Hacking	Use of approved cryptographic algorithms and protocols on the card Tamper protection Incident detection and management
Malware	Update and patching for all system components Incident detection and management
Backend systems	System hardening Update and patching for all system components Intrusion detection Incident detection and management

Product Selection

11.7.22. A number of protection profiles related to smartcards and related devices and systems are provided on the Common Criteria website. Refer also to Chapter 12 – Product Security.

Secure Access Module

11.7.23. A Secure Access Module (or Secure Application Module - SAM) is used to enhance the security and cryptographic performance of devices. SAMs are commonly found in devices needing to perform secure transactions, such as payment terminals. It can be used for cryptographic computation and secure authentication against smart cards or contactless payment cards.

11.7.24. Physically a SAM card can either be a separate component and plugged into a device when required or incorporated into an integrated circuit. A typically use is for the secure storage of cryptographic keys or other sensitive data. SAM hardware and software are designed to prevent information leakage and incorporates countermeasures against electromagnetic radiation, timing measurements, and other side channel attacks. These properties mean that SAMs offer a much higher level of protection than the terminals and readers, which often utilise general-purpose computers.

11.7.25. SAM's typically support 3DES and AES cryptographic algorithms and SHA hashing algorithms in their hardware cryptographic co-processor implementations. Refer to Chapter 17 for information on approved cryptographic algorithms and protocols. It is important to note that 3DES is approved for use on legacy systems only and SHA-1 is not an approved hashing algorithm.

Card Protection

11.7.26. RFID blocking wallets and RFID card sleeves are available to block RFID frequencies. These are typically used for the protection of credit and other payment, access, transit cards and e-passports as a countermeasure for skimming attacks.

References - Guidance

11.7.27. Further references on Guidance can be found at:

Reference	Title	Publisher	Source
	Common Criteria Protection Profiles	Common Criteria	https://www.commoncriteriaportal.org/pps/
SP 800-82	**NIST Special Publication 800-82 rev.2 Guide to Industrial Control Systems (ICS) Security, May 2015**	NIST	Guide to Industrial Control Systems (ICS) Security (nist.gov)

References - Standards

11.7.28. Further references on standards can be found at:

Reference	Title	Publisher	Source
ISO/IEC 7816-1:2011	Identification cards -- Integrated circuit cards -- Part 1: Cards with contacts -- Physical characteristics	ISO	https://www.iso.org/standard/54089.html
ISO/IEC 7816-2:2007	Identification cards -- Integrated circuit cards -- Part 2: Cards with contacts -- Dimensions and location of the contacts	ISO	https://www.iso.org/standard/45989.html
ISO/IEC 7816-3:2006	Identification cards -- Integrated circuit cards -- Part 3: Cards with contacts -- Electrical interface and transmission protocols	ISO	https://www.iso.org/standard/38770.html
ISO/IEC 7816-4:2013	Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange	ISO	https://www.iso.org/standard/54550.html
ISO/IEC 7816-5:2004	Identification cards -- Integrated circuit cards -- Part 5: Registration of application providers	ISO	https://www.iso.org/standard/34259.html
ISO/IEC 7816-6:2004	Identification cards -- Integrated circuit cards -- Part 6: Interindustry data elements for interchange	ISO	https://www.iso.org/standard/38780.html
ISO/IEC 7816-7:1999	Identification cards -- Integrated circuit(s) cards with contacts -- Part 7: Interindustry commands for Structured Card Query Language (SCQL)	ISO	https://www.iso.org/standard/28869.html
ISO/IEC 7816-8:2019	Identification cards -- Integrated circuit cards -- Part 8: Commands and mechanisms for security operations	ISO	https://www.iso.org/standard/75844.html
ISO/IEC 7816-9:2017	Identification cards -- Integrated circuit cards -- Part 9: Commands for card management	ISO	https://www.iso.org/standard/67802.html
ISO/IEC 7816-10:1999	Identification cards -- Integrated circuit(s) cards with contacts -- Part 10: Electronic signals and answer to reset for synchronous cards	ISO	https://www.iso.org/standard/30558.html
ISO/IEC 7816-11:2017	Identification cards -- Integrated circuit cards -- Part 11: Personal verification through biometric methods	ISO	https://www.iso.org/standard/67799.html
ISO/IEC 7816-12:2005	Identification cards - Integrated circuit cards -- Part 12: Cards with contacts -- USB electrical interface and operating procedures	ISO	https://www.iso.org/standard/40604.html
ISO/IEC 7816-13:2007	Identification cards -- Integrated circuit cards -- Part 13: Commands for application management in a multi-application environment	ISO	https://www.iso.org/standard/40605.html
ISO/IEC 7816-15:2016	Identification cards -- Integrated circuit cards -- Part 15: Cryptographic information application	ISO	https://www.iso.org/standard/65250.html
ISO/IEC 10373-7:2019	Identification cards -- Test methods -- Part 7: Vicinity cards	ISO	https://www.iso.org/standard/74958.html
ISO 11784:1996 Amdt 2:2010	Radio frequency identification of animals — Code structure — Amendment 2: Indication of an advanced transponder	ISO	https://www.iso.org/standard/45365.html
ISO 14223-1:2011	Radiofrequency identification of animals — Advanced transponders — Part 1: Air interface	ISO	https://www.iso.org/standard/50979.html
ISO 14223-2:2010	Radiofrequency identification of animals -- Advanced transponders -- Part 2: Code and command structure	ISO	https://www.iso.org/standard/45364.html
ISO 14443-1:2008	Identification cards – Contactless integrated circuit cards – Proximity cards – Part 1: Physical characteristics	ISO	https://www.iso.org/standard/39693.html

ISO/IEC 14443-2:2010	**Identification cards – Contactless integrated circuit cards – Proximity cards – Part 2: Radio frequency power and signal interface**	ISO	https://www.iso.org/standard/50941.html
ISO/IEC 14443-3:2011	**Identification cards – Contactless integrated circuit cards – Proximity cards – Part 3: Initialization and anticollision**	ISO	https://www.iso.org/standard/50942.html
ISO/IEC 14443-4:2008	**Identification cards – Contactless integrated circuit cards – Proximity cards – Part 4: Transmission protocol**	ISO	https://www.iso.org/standard/50648.html
ISO/IEC 18000-3:2010	**Information technology -- Radio frequency identification for item management -- Part 3: Parameters for air interface communications at 13,56 MHz**	ISO	https://www.iso.org/standard/53424.html
ISO/IEC 18000-6:2013	**Information technology -- Radio frequency identification for item management -- Part 6: Parameters for air interface communications at 860 MHz to 960 MHz General**	ISO	https://www.iso.org/standard/59644.html
ISO/IEC TR 29123:2007	**Identification Cards – Proximity Cards – Requirements for the enhancement of interoperability**	ISO	https://www.iso.org/standard/45146.html
ISO/IEC 15693-1:2010	**Identification cards -- Contactless integrated circuit cards -- Vicinity cards -- Part 1: Physical characteristics**	ISO	https://www.iso.org/standard/39694.html
ISO/IEC 15693-2:2006	**Identification cards -- Contactless integrated circuit cards -- Vicinity cards -- Part 2: Air interface and initialization**	ISO	https://www.iso.org/standard/39695.html
ISO/IEC 15693-3:2019	**Identification cards -- Contactless integrated circuit cards -- Vicinity cards -- Part 3: Anticollision and transmission protocol**	ISO	https://www.iso.org/standard/73602.html

Rationale and Controls

Risk Assessment

11.7.29.R.01. **Rationale**

As with many technologies, adoption of RFID access cards has the potential to introduce a wide range of risks in addition to the risks that already exist for agency systems. This may compromise the cards and enable unauthorised access, in addition to RFID risks discussed in the previous section. A risk assessment is an essential tool in determining and assessing the range and extent of risk and threat in the use of RFID access cards.

11.7.29.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3130]

Agencies MUST conduct and document a risk assessment before implementing or adopting an RFID access card system.

11.7.29.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3131]

This risk assessment MUST be the basis of a security architecture design.

Security Architecture

11.7.30.R.01. **Rationale**

The foundation of strong security architecture in RFID follows these important principles:

1. **Physical Security** - over readers, secure areas, issued and unissued access cards;
2. **Controlled access to the data** – only authorised entities (people, systems, devices) can read and write information to the cards, card databases and backend systems;
3. **Control over access to the system** – only authorised entities can configure or add devices to the system, and all devices on the system are authentic and trustworthy;
4. **Confidence and trust** – back-end systems are designed and implemented in accordance with the current version of the NZISM. This includes intrusion detection and incident management mechanisms and procedures.

11.7.30.R.02. **Rationale**

Some access systems may cover several organisations or sites. In such cases, multiple organisations or sites may require access to databases that

contain personnel identifiers, passwords and access permissions. The security architecture should incorporate strong security controls including the authentication of external entities, incident management, audit logging and other essential security controls.

11.7.30.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3138]

Agencies MUST develop a strong security architecture to protect access to databases and systems.

11.7.30.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3139]

Agencies SHOULD apply the NZISM access controls (Chapter 11) and cryptographic controls (Chapter 17) to access card systems.

11.7.30.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3141]

Agencies SHOULD consider the application of the following design elements:

- Implement a Demilitarized Zone (DMZ) to isolate card systems from other parts of the organisation's network and from high-risk Internet Protocol (IP) network connections;
- Secure or remove connections between the Internet and card system network segments;
- Secure or remove vulnerable dialup modem links;
- Secure or remove vulnerable wireless radio links and network access points; and
- Network activity monitoring for unusual or anomalous access activity and well as intrusion detection.

Policy

11.7.31.R.01. **Rationale**

An Access Card Usage Policy is an essential component addressing topics such as how personal information is stored and shared, card holder responsibilities and procedures to manage card loss or damage. Refer also to Chapter 20 – Data Management.

11.7.31.R.02. **Rationale**

Any access card implementation should also be incorporated into the agency's security policies. Refer also to Chapter 5 – Information Security Documentation.

11.7.31.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3156]

Agencies SHOULD develop, implement and maintain an Access Card Usage Policy.

11.7.31.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3157]

Agencies SHOULD incorporate access cards into the agency's security policies and information security documentation.

Physical Security

11.7.32.R.01. **Rationale**

Physical security over readers, door controls, cables and control systems, as well as the cards themselves is fundamental to the operation of a secure system.

11.7.32.R.02. **Rationale**

In order to minimise unnecessary electromagnetic radiation readers and control equipment should be carefully positioned. Care should be taken with the use of card readers in proximity to:

- Fuel, ordnance, and other hazardous materials,
- Metal and reflective objects that can modify and amplify signals in unintended and potentially harmful ways, and
- Legitimate radio systems to avoid interference.

11.7.32.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3162]

Agencies SHOULD select systems that provide resistance to physical or electronic tampering.

11.7.32.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3163]

Agencies SHOULD implement systems to minimise the risk of physical or electronic tampering.

11.7.32.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3165]

Agencies SHOULD consider placement of tags and location of readers to avoid unnecessary electromagnetic radiation.

11.7.32.C.04.

Control System Classifications(s): All Classifications; Compliance: Should [CID:3166]

Agencies SHOULD consider and select other physical controls in accordance with the PSR.

Card Data Protection

11.7.33.R.01. **Rationale**

Cards are invariably retained by the card holder and subject to loss, theft or being misplaced. Cards are also not always within the control of the card holder outside of normal office hours. Measures to protect cards in these situations are fundamental to the maintenance of the integrity and security of the access control system.

11.7.33.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3171]

Agencies MUST follow the requirements of the NZISM in the selection and implementation of cryptographic protocols and algorithms, and in key management, detailed in Chapter 17 - Cryptography.

11.7.33.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3173]

Agencies SHOULD encrypt data before it is written to cards.

11.7.33.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3175]

Agencies SHOULD consider the use of cards systems incorporating Secure Access Modules (SAMs).

Incident Management

11.7.34.R.01. **Rationale**

Incident management and audit procedures, logging and time stamps help detect and manage security breaches. These are important tools in protecting systems and managing security breaches.

11.7.34.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3180]

Agencies MUST develop and implement incident identification and management processes in accordance with this manual (See Chapter 5 – Information Security Documentation, Chapter 6 – Information Security Monitoring, Chapter 7 – Information Security Incidents, Chapter 9 – Personnel Security and Chapter 16 – Access control and passwords).

Disposal

11.7.35.R.01. **Rationale**

Card disposal and recycling procedures that permanently disable or destroy sensitive data reduces the possibility that they could be used later for tracking or targeting, and prevents access to sensitive data stored on cards. In addition the continued operating presence of a card after it has performed its intended function can pose an unauthorised access, business intelligence or privacy risk, including tracking and targeting of personnel or access to sensitive data on the access card.

11.7.35.R.02. **Rationale**

Disposal may be undertaken by electronically by using a card's wipe feature or using a strong electromagnetic field to permanently deactivate a tag's circuitry. Alternatively physical destruction can be achieved by tearing or shredding. Where a tag supports an electronic deactivation mechanism, tags should be electronically deactivated before physical destruction.

11.7.35.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3189]

Agencies SHOULD consider secure disposal procedures and incorporate these into the Access Card Usage Policy. Refer also to Media and IT equipment management, decommissioning and disposal.