# 11.6. Radio Frequency Identification Devices

## Objective

11.6.1. To ensure Radio Frequency Identification (RFID) devices are used safely and securely in order to protect privacy, prevent unauthorised access and to prevent the compromise of secure spaces.

## Context

### Scope

11.6.2. This section provides information relating to the risks, security and secure use of RFID devices. Card access control systems incorporating RFID or smart cards are discussed in more detail in Section 11.7 - Card Access Control Systems.

### Background

11.6.3. This section contains a short description of the history, formats, operating frequencies, risks, controls and countermeasures related to the use of RFID.

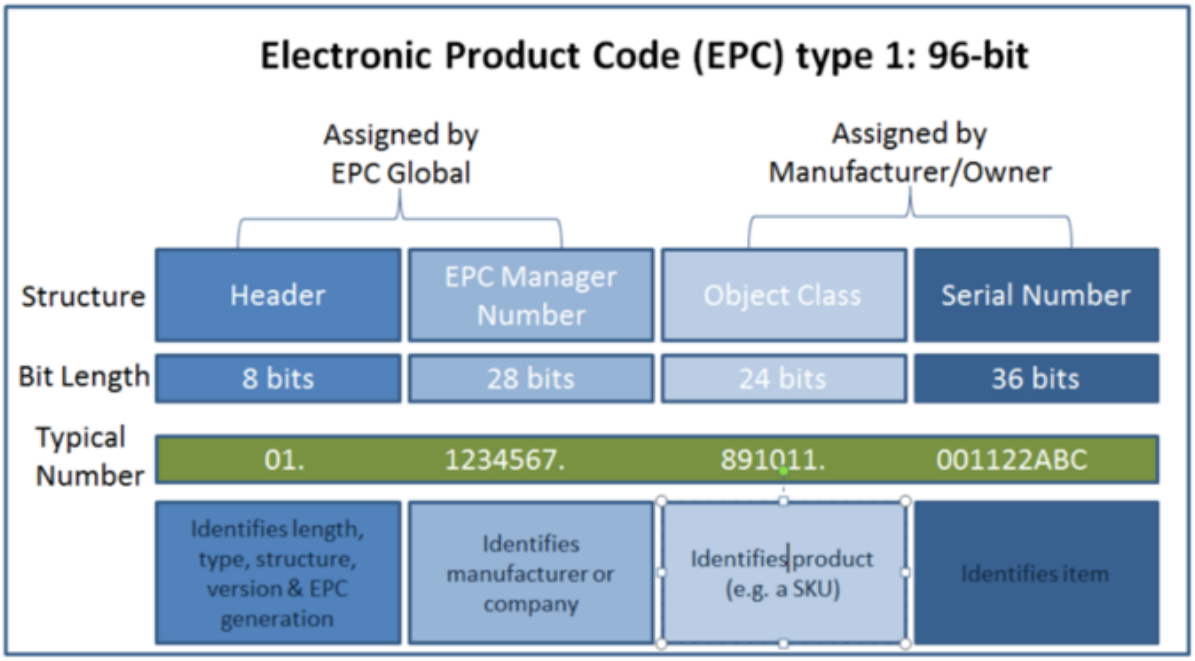
11.6.4. In practical use since the 1970's, RFID is now widely used for product identification, stock control, as anti-theft in manufacturing and retail organisations, payment cards (smart ATM and paywave cards) and access control systems. They are useful tools in improving logistics, profoundly changing cost structures for business, and improving levels of safety and authenticity in a wide range of applications such as access control, passports, payment cards, vehicle immobilisers, toll roads, pharmaceuticals tracking, management of high value items and weapons control. RFID tags are now produced in a wide variety of types and sizes, from the size of a grain of rice or printed on paper to much larger devices incorporating a battery or other power supply.

11.6.5. Unlike bar coding systems, RFID devices can communicate without requiring line of sight and over distances ranging from a few centimetres to kilometres. They can be equipped with sensors to collect data on temperature changes, sudden shocks, humidity or other factors affecting product safety and quality.

11.6.6. RFID devices typically use radio signals to transmit identifying information such as product or serial numbers, manufacture date, origin and batch number. This identifying information is invariably in the form of an Electronic Product Code (EPC) following the standards and conventions published by GS1. GS1 is a global group that also develops standards for other identifiers such as barcodes. The GS1 standards and conventions are now incorporated into ISO standards, see references table at 11.6.57.

### Basic Formats

11.6.7. The basic format of an Electronic Product Code (EPC) is illustrated below:




11.6.8. RFID devices are often referred to as "tags". Passive tags are unpowered and harvest power from the RFID reader. Active tags incorporate a power supply, usually a battery. Tags are produced in Classes 0 to 5 and are now generally produced to Generation 2 specifications. The EPCGen2 standard for Class 1 tags focuses on reliability and efficiency but supports only very basic security. Features of the Gen 2 specification include:

- **a 96 bit EPC number** with read/write capability and can be designated used for other data ;
- **a 32/64 bit tag identifier** (TID) – identifies the manufacturer of the tag, also with read/write capabilities;
- **32 bit kill password** to permanently disable the tag;
- **32 bit access password** to lock the read/write characteristics of the tag and also set the tag for disabling ;
- **User memory** – dependant on the manufacturer and can be as little as 0 bits to 2048 bits. Larger user memory is in development.

11.6.9. The distance from which a tag can be read is termed the read range. A read range will depend on a number of factors, including the radio frequency used for reader/tag/reader communication, the size and orientation of the antennae, the power output of the reader, and whether the tags have a battery or other power supply. Battery-powered tags typically have a read range of 100 meters (approximately 300 feet) although this can extend to kilometres under favourable conditions. It is possible that powered RFID tags, typically used on cargo containers, railway wagons, vehicles and other large assets, could be read from a satellite if there is little background "noise" and the broadcast signal is sufficiently powerful.

11.6.10. RFID tags are divided into classes 0 to 5:

| Class | Description |
|---|---|
| **0** | Read only, passive tags |
| **1** | Write once passive tags. 128-bit memory. |
| **2** | Read/Write with up to 65Kb read/write memory and authenticated access control. Can monitor temperature, pressure, vibration. |
| **3** | Semi-Passive. Own power source but cannot initiate communication. Remains passive until activated by a reader. Up to 65 Kb read/write memory and integrated sensor circuitry. |
| **4** | Active tags (own power source) with integrated transmitter. Can communicate with readers and other tags operating in the same RF band. Rewritable memory and ad hoc networking capability. Read range >100 metres (approx. 300'). |
| **5** | Reader tags, can power class 1 to 3 tags and communicate with all classes. Includes all the capabilities of class 4 tags. |

## Operating Frequencies

11.6.11. RFID operates in several parts of the Radio Spectrum. Not all frequencies are authorised for use in all countries and will depend on the radio spectrum allocation authority in each country. It is important to note, however, that some RFID tags designed to operate at frequencies not used in the importing country may be attached to imported goods. This can represent a risk from scanning at frequencies not authorised or normally monitored in the importing country.

11.6.12. Depending on the design and intended application, RFID tag can operate at different frequencies. It is important to note that longer range RFID tags operate at frequencies close to or within allocated Wi-Fi frequencies. Allocated frequencies are:

| Band | Frequency | Typical Range |
|---|---|---|
| **LF** | 125-134.2 kHz and 140-148.5 kHz | Up to 1/2 metre |
| **HF** | 13.553 - 13.567 MHz and 26.957 - 27.283 MHz | Up to 1 metre |
| **UHF** | 433 MHz, 858 - 930 MHz, 2.400 - 2.483 GHz, 2.446 - 2.454GHz | 1 to 10 metres |
| **SHF** | 5.725 - 5.875 GHz | > 100 metres |

11.6.13. As RFID devices are deployed in more sophisticated applications such as matching hospital patients with laboratory test results or tracking systems for dangerous materials, concerns have been raised about protecting such systems against eavesdropping, unauthorised uses and privacy breaches.

### Smart Cards

11.6.14. Smart cards typically comprise an embedded integrated circuit 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.

11.6.15. 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. 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.

11.6.16. 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.

11.6.17. 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.

## Threats and Vulnerabilities

11.6.18 Some important characteristics of RFID, inherent in the design and properties of the technology are:

- RFID tags are powered by the field emitted by an RFID reader, so whenever a tag is placed in a reader field it is activated and available. In general terms, class 0 and class 1 tags cannot be powered off, only permanently deactivated;
- RFID tags automatically respond to reader interactions without explicit control of the tag owner, so RFID tags can be operated without their owner's consent;
- It is trivial to establish a communication with an RFID tag and there is no visual confirmation of a tag/reader interaction (i.e., no physical connection or manual operation is required), so it is possible to interact with an RFID tag without being detected.

11.6.19 Specific threats and vulnerabilities in the use of RFID technologies include:

- **Legitimate data-mining**: This risk predates the use of RFID technology, but the volume of data provided by RFID tags, loyalty cards, Near Field Communication (NFC) for bank cards and for electronic wallets increases the risk. Some data collection methods keep to ethical use of data-mining techniques to discover the characteristics and habits of an individual or an organisation. This can pose a business intelligence risk. At times, however, this may challenge the bounds of privacy and data ownership. For example, customer loyalty card data used to discover medical information about an individual or RFID tags to track shipments or deliveries to an organisation by a competitor.
- **Eavesdropping and Data theft**: This risk is similar to the data-mining risk but employs unethical and possibly illegal methods of data collection or obtaining data for nefarious or malicious purposes. RFID tags are designed to broadcast information and data theft by easily concealable RFID scanners is technically trivial. Data theft can pose a risk to business processes.
- **Skimming**: Occurs when an unauthorised reader gains access to data stored on a token. This type of attack is particularly dangerous where contactless access or payment cards are used.
- **Relay Attacks**: Relay attacks use eavesdropping to intercept legitimate tag/reader transmissions and relay these to a device at some distance from the legitimate tag. The device can then behave as the genuine tag. Again this type of attack is particularly dangerous where contactless access or payment cards are used.
- **Insert Attacks**: Insert attacks insert system commands where normal data is expected and relies on a lack of data validation. It is possible that a tag can have legitimate data replaced by a malicious command.
- **Tag Cloning**: Clones replicate the functionality of legitimate tags and can be used to access controlled areas, abuse private data, or make an unauthorised electronic transaction. Tag authentication using a challenge-response protocol is a defence against cloning as the information that attackers can obtain through the air interface (such as by eavesdropping) is insufficient to provide a legitimate response. The design of the tag can also incorporate measures at the circuit manufacturing stage to protect tags from duplication by reverse engineering.
- **Data corruption**: Most RFID tags are rewritable by design. This feature may be locked (turning the tag into a write-once, read-many device) or left active, depending on application and security sensitivity. For example, in libraries, the RFID tags are frequently left unlocked for the

convenience of librarians in reusing the tags on different books or to track check-ins and check-outs. If tags are not protected, it creates an opportunity for malicious users to overwrite data, typically in the theft of high-value goods by marking them as low-value items or in the case of weapons monitoring, changing the weapon identification.

- **Shipment or People tracking**: While RFID tags are designed to assist in stock control and supply chain management, unauthorised tracking of shipments or of people is undesirable and may even be dangerous. It is possible to follow individuals carrying tags using several techniques, including placing fake readers at building access points, deploying unauthorised readers near legitimate readers and creating relay points along expected routes.
- **Tag Blocking**: This is a form of denial of service by introducing a blocker tag which is designed to simulate all possible tags in an allocated range. This causes readers to continually perform multiple reads on non-existent and non-responsive tags. Blocker tags are sometimes used where privacy or confidentiality are required.
- **Denial of Service (DOS)**: Also known as flooding attacks where a signal is flooded with more data than it is designed to handle. Similar in many respects to RF Jamming.

## Attack Vectors

11.6.20. Attack vectors for RFID devices include:

- interception of legitimate transmissions;
- interception of authorised reader data by an unauthorised device;
- unauthorised access to tags and readers;
- rogue/cloned tags;
- rogue and unauthorised RFID readers;
- side-channel attacks (timing measurements, electromagnetic radiations etc.);
- attacks on back-end systems;
- jamming of legitimate signals.

11.6.21. Because RFID devices incorporate antennas, there is a possibility of radiation hazards from high –powered devices, particularly active tags and readers. It is important to note however that these cases are rare, occur in high powered devices only and that the vast majority of RFID devices do not pose radiation hazards. Related hazards include electromagnetic radiation hazards to personnel (HERP), fuel (HERF) and ordnance (HERO).

11.6.22. Threats and Vulnerabilities of RFID systems are summarised in the table below:

| Threat/Vulnerability | Tag | RF | Reader | Network | Back-End | People |
|---|---|---|---|---|---|---|
| Eavesdropping | ● | ● | | ● | ● | |
| Relay Attack | | ● | | | | |
| Unauthorised Tag Reading (skimming) | ● | ● | ● | | | |
| People Tracking | ● | ● | | | | ● |
| Shipment Tracking | ● | ● | | | | |
| Tag Cloning | ● | ● | | | | |
| Replay Attack | ● | ● | | | | |
| Insert Attack | ● | | ● | ● | ● | |
| Tag Content Modification | ● | | | | | |
| Malware | ● | | ● | ● | ● | |
| RFID System Failure | | | ● | ● | ● | ● |
| Tag Destruction | ● | | | | | |
| Tag Blocking | ● | ● | | | | |
| Denial of Service (DoS) | ● | | ● | ● | | |
| RF Jamming | ● | ● | | | | ● |
| Back-End Attacks | | | | ● | ● | |
| Radiation Hazard | ● | ● | ● | | | ● |

11.6.23. It is important to note that attacks are often used in combination creating blended attacks. Blended attacks may be a combination of attack types, use of multiple attack vectors, the targeting of individual sub-systems or combinations of all three elements.

## Good Practices and Countermeasures

11.6.24 Good practice for ensuring the security and privacy of RFID systems includes:

- a risk assessment to determine the nature and extent of risk and threat in the proposed use of RFID;

- strong security architecture to protect RFID databases and communication systems;
- authentication of approved users of RFID systems;
- encryption of radio signals when feasible;
- temporarily or permanently disabling tags when not required;
- shielding RFID tags and tag reading areas to prevent unauthorised access or modification;
- incident management, audit procedures, logging and time stamping to help detect and manage security breaches; and
- tag disposal and recycling procedures that permanently disable or destroy sensitive data.

### Authentication

11.6.25. By design and usage, RFID technologies are item, product or shipment identification **but** not authentication technologies. Authentication of a reader or tag requires a common secret (key) shared when establishing communication, and before data is exchanged. Currently, only RFID tags with microprocessors have sufficient computation resources to use authentication techniques. These can be found in such applications as e-passports, or payment or ticketing applications (public transport, for example).

11.6.26. With a challenge/response authentication mechanism the reader issues an enquiry to the tag which results in a response. The secret tag information is computed information from internal cryptographic algorithms by both the tag and reader and the results are sent. Correct responses are required for a successful information exchange. The system is essentially the same as encrypting data over a standard radio link.

11.6.27. The ISO/JTC1/SC31 committee is in the process of establishing new standards to support the use of simple RFID authentication and encryption protocols.

### Keyed-Hash Message Authentication Code (HMAC)

11.6.28. HMAC is a protocol where both an RFID reader and RFID tag share a common secret key that can be used in combination with a hash algorithm to provide one-way or mutual authentication between tag and reader. When HMAC is applied to messages, it also assures the integrity of data in the messages.

11.6.29. HMAC is not specified in any RFID standard, but the capability is generally available in vendor products. HMAC is often used where the risk of eavesdropping is high and passwords alone are considered to offer an inadequate authentication mechanism. This will be determined by the risk assessment. HMAC is also used where applications require evidence of a tag's authenticity.

### Digital Signatures

11.6.30. Digital signatures are compatible with existing RFID tag standards. In authenticated RFID systems, tags can receive, store, and transmit digital signatures with existing read and write commands because the complexity is managed by readers or back-end systems. However, the use of digital signatures to support authentication of readers to tags would require tags to support relatively complex cryptographic functions, beyond the capacity of common tag designs.

11.6.31. In addition, digital signatures that are not generated by the tag itself are subject to replay attacks. An adversary could query a tag to obtain its evidence of authenticity (i.e., the digital signature created by a previous reader) and then replicate that data on a cloned tag. Consequently, password or symmetric key authentication systems likely will support tag access control, as opposed to tag authenticity verification, for the immediate future.

### Encryption

11.6.32. Data stored in the memory of an RFID tag is intended to be freely shared with the various tag users (manufacturers, stock controllers, shipping agents, etc.). Only an RFID reader is required to access the data which raises the question of data security. Memory and computational power of an RFID tag is limited, but data elements can be password-protected or reserved for nominated usage. Several levels of authorisation (read-only, read and write, delete, etc.) can be determined. It is also advisable to encrypt the data entered onto the tag, the encryption/decryption taking place at the RFID reader or back-end system.

### Cover-Coding

11.6.33. Cover-coding is a method of hiding information from eavesdroppers. In the EPCglobal Class-1 Generation-2 standard, cover-coding is used to obscure passwords and information written to a tag using the write command. Some proprietary technologies also support similar features. Cover-coding is an example of minimalist cryptography because it operates within the challenging power and memory constraints of passive RFID tags.

11.6.34. Cover-coding is a useful mitigation where eavesdropping is a risk, but adversaries are expected to be at a greater distance from the tags than readers. Cover-coding helps prevent the execution of unauthorised commands that could disable a tag or modify the tag's data. Cover-coding mitigates business process, business intelligence, and privacy risks.

### Rolling Code

11.6.35. A rolling code approach is a scheme where the identifier given by the RFID tag changes after each read action. It requires the RFID reader and RFID tag to use identical algorithms. If multiple readers are used, they must be linked so that tracking of code changes can be monitored. This scheme

reduces the usefulness of any responses that may be observed unless the pattern of change can be detected or deduced.

## Other Defensive Measures

11.6.36 Other defensive measures, sometimes described as palliative techniques, include shielding, blocker tags, tag "kill" commands, tamper resistance and temporary deactivation. It is important to note these techniques do not use encryption.

### Shielding

11.6.37. RF shielding is designed to limit the propagation of RF signals outside of the shielded area. Shielding helps to prevent unauthorised reading, access to or modification of the RFID tag data or interfering with RFID readers. Shielding can be applied to small, individual items, such as passports and credit cards or to large elements such as shipping containers.

11.6.38. Shielding is also important where interference is present or detected. This may be caused by environmental conditions, such as operating in a port area, or by deliberate attempts to access readers or tags.

11.6.39. Engineering assessments will determine the requirement for shielding from adverse environmental conditions and the risk assessment will determine the likelihood and threat from unauthorised and deliberate attempts to access readers, tags and data.

11.6.40. RFID blocking wallets and **RFID card sleeves** are available to block RFID frequencies. These are typically used for credit and other payment, access and transit cards and e-passports, as a countermeasure for skimming attacks or unauthorised tracking.

### Blocker Tags

11.6.41. A special tag, called a "blocker" tag, blocks an RFID reader by simultaneously answering with 0 and 1 to every reader's request during the identification protocol. The reader is then incapable of distinguishing individual tags. The blocker tag may block a reader universally or within ranges.

11.6.42. This furnishes privacy by shielding consumers from the unwanted scanning of RFID tags that they may carry or wear. It also protects against unauthorised readers and eavesdroppers. The blocker tag is an alternative to more simple solutions such as the kill command, shielding and active jamming. It is important to note that active jamming may be illegal (see 11.6.53).

11.6.43. Blocker tags can also implement one or more privacy policies and multiple blocker tags may cover multiple zones. The blocker tag has a very low-cost of implementation and standard tags need no modification and little support for password-protected bit flipping. A threat is that blocker tags can be used to mount DoS attacks in which a malicious blocker tag universally blocks readers.

### Tag "Kill" Command

11.6.44. The "kill" command is a password-protected command specified in the EPC Gen-1 and EPC Gen-2 standards intended to make a tag non-operational. A typical application is anti-theft where the kill command is activated at a point-of-sale terminal, after goods have been paid for. Kill commands can be password protected.

11.6.45. Kill commands function by fusing a ROM component or antenna connection by applying a large amount of power to the tag at the point of sale reader/terminal. It is important to note that the antenna deactivation method does not completely kill the tag but rather disable its RF interface. Once in the disabled state, the tag still retains data and can still function.

11.6.46. The kill feature can represent a threat to an RFID system if the password is compromised. This risk is particularly apparent where the same password is used for multiple tags. If a weak (e.g., short or easily guessed) password is assigned to the kill command, tags can be disabled at will. Also important is the longer a tag uses the same password, the more likely it is that the password will be compromised.

11.6.47. Data stored on the tag is still present in the tag's memory after it is disabled (although it can no longer be accessed wirelessly), and, therefore, still may be accessible with physical access to the tag.

### Tamper Resistance

11.6.48. Some RFID tags are designed with tamper resistant or tamper-evident features to help prevent unauthorised alteration of removal of tags from the objects to which they are attached. A simple type of tamper resistance is the use of a frangible, or easily broken, antenna. If this tag is removed, the connection with the antenna is severed, rendering the tag inoperable. Other, more complex types of RFID systems monitor the integrity of objects associated with the tags to ensure that the objects have not been compromised, altered, or subjected to extreme conditions.

11.6.49. Simple forms of tamper resistance may leave data intact and subject to the same threats described above. In addition it is possible to circumvent tamper resistance mechanisms by repairing a frangible antenna. It is important to note that tamper-resistance and tamper-evidence technologies do not prevent the theft or destruction of the tag or its associated items.

### Temporary Deactivation

11.6.50. Some tags allow the RF interface to be temporarily deactivated. Methods vary amongst manufacturers with some methods requiring physical intervention. Typically tags would be activated inside a designated area and deactivated when shipped, preventing eavesdropping or other unauthorised transactions during shipment. When the tags arrive at their destination, they can be reactivated, for example for inventory management. Conversely, tags can be used for tracking during shipment and may be deactivated on delivery.

## RFID Risks and Controls Summary

11.6.51. A summary of RFID Risks and Controls is presented in the Table below:

| Risk Control | Business Process | Business Intelligence | Privacy | Electro-Magnetic Radiation | Back-End System Attack |
|---|---|---|---|---|---|
| Tag Access Controls | ● | ● | ● | | ● |
| Password Authentication | ● | ● | ● | | ● |
| HMAC | ● | ● | ● | | ● |
| Digital Signature | ● | ● | | | ● |
| Cover-Coding | | ● | | | ● |
| Encryption – Data in Transit | | ● | ● | | |
| Encryption – Data at Rest | | ● | | | ● |
| Encryption – Data on Tag | ● | ● | ● | | |
| Shielding | ● | ● | ● | ● | |
| Blocker Tags | | ● | ● | | |
| Tag Kill Feature | | ● | ● | | |
| Tamper Resistance | ● | ● | | | |
| Temporary Deactivation | ● | ● | ● | | |
| RF Engineering and Frequency Selection | ● | ● | ● | ● | |

## Relevant Legislation

11.6.52 In New Zealand, operation of radio and other equipment in the RF spectrum is controlled Radiocommunications Act 1989, Reprint as at 5 December 2013 and administered by the Ministry of Business Innovation and Employment.

### RF Jammers

11.6.53. It is illegal to import, manufacture, sell or use a radio jammer in New Zealand except with a licence issued by the Radio Spectrum Management unit of the Ministry of Business, Innovation and Employment. The use and management of RF jammers is governed by the Radiocommunications Regulations (Prohibited Equipment – Radio Jammer Equipment) Notice 2011 under the Regulation 32(1)(i) [a notice in the Gazette] of the Radiocommunications Regulations 2001.

### Secure Spaces

11.6.54. The use of RFID technology in secure areas must be carefully considered, recognising that an RFID tag or system incorporates antennae and transmitting capabilities which may compromise the security of such areas. Passive tags (classes 0 and 1) pose little risk in themselves as they require a reader to activate and have little on-board capability. Read/write tags (class 2) pose a higher risk as they have the capability to store data. Other tags (classes 3 to 5) can pose a significant risk to secure spaces.

## PSR references

11.6.55. The relevant PSR Mandatory Requirements are:

| References | Title | Source |
|---|---|---|
| **PSR Mandatory Requirements** | GOV2, INFOSEC1, INFOSEC2, INFOSEC3, INFOSEC4, PHYSEC1 and PHYSEC2 | Home \| Protective Security Requirements<br>Security governance (GOV) \| Protective Security Requirements<br>Information security (INFOSEC) \| Protective Security Requirements<br>Physical security (PHYSEC) \| Protective Security Requirements |

## References - Guidance

11.6.56. Further references on Guidance can be found at:

| Reference | Title | Publisher | Source |
|---|---|---|---|
| SP 800-98 | Guidelines for Securing Radio Frequency Identification (RFID) Systems | NIST | https://www.nist.gov/publications/guidelines-securing-radio-frequency-identification-rfid-systems |
| FIPS PUB 198-1 | The Keyed-Hash Message Authentication Code (HMAC), July 2008 | NIST | https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.198-1.pdf (PDF, 136 KB) |
| FIPS PUB 180-4 | Secure Hash Standard (SHS) | NIST | https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf (PDF, 814 KB) |
| EPC/RFID | Implementation Guide for the use of GS1 EPCglobal Standards in the Consumer Electronics Supply Chain | GS1/EPCglobal | https://www.gs1.org/standards/epcrfid |
| | Smart Border Alliance RFID Feasibility Study Final Report Attachment D – RFID Technology Overview | US Department of Homeland Security | https://www.dhs.gov/sites/default/files/publications/privacy/privacy_rfid_attachmentD.pdf (PDF, 1.49 MB) |
| | Smart Border Alliance RFID Feasibility Study Final Report Attachment E – RFID Security And Privacy White Paper | US Department of Homeland Security | https://www.dhs.gov/sites/default/files/publications/privacy/privacy_rfid_attachmentE.pdf (PDF, 1.8 MB) |
| | Test Operations Procedure (TOP) 03-2-614A Electromagnetic Radiation Hazards Testing For Non-Ionizing Radio Frequency Transmitting Equipment | US Defense Technical Information Center (DTIC), | |
| | Electromagnetic Environmental Effects Requirements for Systems - MIL-STD-461C | US Department of Defense Interface Standard | https://quicksearch.dla.mil/qsDocDetails.aspx?ident_number=STD-461C_26512 |
| | OECD Policy Guidance – A Focus on Information Security and Privacy Applications, Impacts and Country Initiatives. | OECD Directorate for Science, Technology and Industry | http://www.oecd.org/sti/ieconomy/40892347.pdf (PDF, 1.79 MB) |
| TR-03126-5 | Technical Guidelines for the Secure Use of RFID (TG RFID) Subdocument 5: Application area "Electronic Employee ID Card" Version 1.0 | BSI - The German Federal Office for Information Security | https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG03126/TG_03126_5_Application_area_Electronic_Employee_ID_Card.pdf?__blob=publicationFile |

## References - Standards

11.6.57. Further references on standards can be found at:

| Reference | Title | Publisher | Source |
|---|---|---|---|
| | **EPC Tag Data Standard Version 1.9, Ratified, Nov-2014** | GS1/EPCglobal | http://www.gs1.org/epcrfid-epcis-id-keys/epc-rfid-tds/1-9 |
| | **EPC™ Radio-Frequency Identity Protocols Generation-2 UHF RFID Specification for RFID Air Interface Protocol for Communications at 860 MHz – 960 MHz Version 2.0.1** | GS1/EPCglobal | https://www.icao.int/publications/pages/publication.aspx?docnum=9303 |
| **ICAO Doc 9303** | **Machine Readable Travel Documents Parts 1-12** | International Civil Aviation Organization (ICAO) | https://www.icao.int/publications/Documents/9303_p3_cons_en.pdf [PDF, 2.24 MB] |
| **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 7816-4:2020** | **Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange** | ISO | https://www.iso.org/standard/77180.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 7816-6:2016** | **Identification cards -- Integrated circuit cards -- Part 6: Interindustry data elements for interchange** | ISO | https://www.iso.org/standard/64598.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 7816-8:2004** | **Identification cards -- Integrated circuit cards -- Part 8: Commands for security operations** | ISO | https://www.iso.org/standard/37989.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 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 15961-1:2013** | **Information technology -- Radio frequency identification (RFID) for item management: Data protocol -- Part 1: Application interface** | ISO | https://www.iso.org/home.html |
| **ISO/IEC 15963:2009** | **Information technology – Radio frequency identification for item management – Unique identification for RF tags** | ISO | https://www.iso.org/home.html |
| **ISO/IEC 18000-1:2008** | **Information technology -- Radio frequency identification for item management -- Part 1: Reference architecture and definition of parameters to be standardized** | ISO | https://www.iso.org/home.html |
| **ISO/IEC 18000-2:2009** | **Information technology -- Radio frequency identification for item management -- Part 2: Parameters for air interface communications below 135 kHz** | ISO | https://www.iso.org/home.html |

## Legislation and Regulation

11.6.58. Further references on Legislation and Regulation can be found at:

| References | Title | Publisher | Source |
|---|---|---|---|
| | **Radiocommunications Act 1989** | Parliamentary Counsel Office | https://legislation.govt.nz |
| **SR 2001/240** | **Radiocommunications Regulations 2001, Reprint as at 1 February 2015** | Parliamentary Counsel Office | https://legislation.govt.nz |
| | **Radiocommunications Regulations (Prohibited Equipment - Radio Jammer Equipment) Notice 2011** | New Zealand Gazette Office, Government Information Services, Department of Internal Affairs | https://gazette.govt.nz/notice/id/2011-go4051 |
| | **Radio Spectrum Management** | Ministry of Business, Innovation and Employment | https://rsm.govt.nz/ |

## Rationale & Controls

### Risk Assessment

11.6.59.R.01. **Rationale**

As with many technologies, adoption of RFID has the potential to introduce a wide range of risks in addition to the risks that already exist for agency systems. This may include privacy risks, depending on the use, information held and implementation of the RFID system. A risk assessment is an essential tool in determining and assessing the range and extent of risk and threat in the use of RFID devices.

11.6.59.R.02. **Rationale**

Risks to RFID system vary according to the technology used, system engineering, the systems architecture, application, context and deployment scenario. A holistic approach to risk at each stage of the system life cycle and each for system component is essential if a robust security strategy is to be developed.

11.6.59.R.03. **Rationale**

The identification of classes of tags is fundamental to managing the risks of RFID devices in secure spaces. Classes 0 and 1 pose little risk. Other classes of tag (2 to 5), however, have limited data storage capability and active tags include transmitter functionality which introduces higher levels of risk. RFID readers are, by definition, transmitters and are not permitted in secure spaces.

11.6.59.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:2956]

Agencies MUST conduct and document a risk assessment *before* implementing or adopting an RFID solution.

11.6.59.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:2957]

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

## Security Architecture

11.6.60.R.01. **Rationale**

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

- **Controlled access to the data** – only authorised entities (people, systems, devices) can read and write information to and from the RFID tags (EPC number, tag identifier, kill password, access password and user memory) and RFID databases;
- **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;
- **Confidence and trust** – back-end systems are designed and implemented in accordance with the current version of the NZISM.

11.6.60.R.02. **Rationale**

Sensitive data should be held in a secure RFID Enterprise Subsystem and retrieved using the tag's unique identifier with only an identifier stored on the tag itself. The Enterprise RFID subsystem should be established as a separate domain where data can be more adequately protected. This structure makes it more difficult for adversaries to obtain information from the tag through scanning or eavesdropping. Data encryption and access control is often more cost-effectively performed in the enterprise subsystem than in the RF subsystem.

11.6.60.R.03. **Rationale**

Some RFID systems may cover several organisations, for example in supply chains. In such cases, multiple organisations may require access to databases that contain tag identifiers and passwords. The security architecture should incorporate strong security controls including the authentication of external entities, incident management, audit logging and other essential security controls.

11.6.60.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:2962]

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

11.6.60.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:2963]

Agencies MUST minimise the information stored on RFID tags and in the RFID subsystem.

11.6.60.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2964]

Agencies SHOULD disable any rewrite functions on RFID devices.

11.6.60.C.04. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2965]

Agencies SHOULD apply the access control requirements of the NZISM (Chapter 11 - Communications Systems and Devices) to RFID systems.

## Policy

11.6.61.R.01. **Rationale**

An RFID Usage Policy is an essential component of an agency's privacy policy, addressing topics such as how personal information is stored and shared. The RFID usage policy should also address privacy issues associated with the tag identifier formats and the potential disclosure of information based solely on the tag identifier format selected. Agencies MAY be required to ensure that devices that collect and store data comply with relevant regulation and guidance, such as the Privacy Act. Refer also to Chapter 20 – Data Management.

11.6.61.R.02. **Rationale**

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

11.6.61.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2969]

Agencies SHOULD develop, implement and maintain an RFID Usage Policy.

11.6.61.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2970]

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

## Inspections

11.6.62.R.01. **Rationale**

Many system component manufacturers use RFID tags to track shipments. RFID tags may be embedded in the packaging, printed on the reverse of labels, attached to or embedded in the device itself. The ability to identify and track devices may pose a security concern for secure areas or equipment deployed in high security applications.

11.6.62.C.01. **Control System Classifications(s): Secret, Confidential, Top Secret; Compliance: Must** [CID:2973]

Agencies MUST conduct visual and technical inspections of packaging and devices to determine if RFID devices have been attached and either permanently disable or remove such devices.

11.6.62.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2974]

Agencies SHOULD conduct visual inspections of packaging and devices to determine if RFID devices have been attached and if these RFID devices pose a security concern.

11.6.62.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2975]

Agencies SHOULD conduct visual inspections of packaging and devices to determine if RFID devices or labelling have been tampered with and whether this is a security concern.

## Shielding

11.6.63.R.01. **Rationale**

RF shielding is designed to limit the propagation of RF signals outside of the shielded area. Shielding helps to prevent unauthorised reading, access to or modification of the RFID tag data or interfering with RFID readers. Shielding can be applied to small, individual items, such as passports and credit cards or to large elements such as shipping containers. The requirement for shielding is determined by the risk assessment and an engineering assessment.

11.6.63.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2978]

Agencies SHOULD consider undertaking an RF engineering assessment where security concerns exist or where the RFID systems are to be used in areas with high levels of RF activity.

11.6.63.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2979]

Shielding SHOULD be considered where eavesdropping or RF radiation is a concern, as determined by the risk assessment.

## Positioning of Tags and Readers

11.6.64.R.01. **Rationale**

In order to minimise unnecessary electromagnetic radiation tags and readers should be carefully positioned. Care should be taken in use of RFID readers in proximity to:

- Fuel, ordnance, and other hazardous materials,
- Humans and sensitive products (e.g., blood, medicine) that may be harmed by sustained exposure to RF radiation,
- Metal and reflective objects that can modify and amplify signals in unintended and potentially harmful ways, and
- Legitimate radio and Wi-Fi systems to avoid interference.

11.6.64.R.02. **Rationale**

Tag location cannot always be controlled, such as when tags are used to track mobile items or goods in transit. Other difficulties occur with persistent radio interference. In these situations, relocation of readers and tags may provide a solution. Consideration should be given to alternative but cost-effective RF protection measures, such as grounded wire fencing. The engineering assessment undertaken to determine the shielding requirements will assist in determining such measures.

11.6.64.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2983]

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

## Encoding and Encryption

11.6.65.R.01. **Rationale**

If an adversary reads an identifier that is encoded with a published format, such as in the EPC standard, an adversary may be able to obtain useful information such as the manufacturer or issuer of the item, as well as the type of item. Because RFID tags hold limited information and identifier formats are published in standards, it may be important to use identifier formats that do not reveal any information about tagged items or the agency using the RFID system. This will be determined in the risk assessment. Encoding schemes to limit information revealed from unauthorised scanning may include serially or randomly assigning identifiers.

11.6.65.R.02. **Rationale**

Adversaries can often obtain valuable information from the identifier alone. For example, knowledge of the EPC manager ID and object class bits may reveal the make and model of tagged objects in a container. If individual items or boxes of items are tagged, the quantities may also be discernible. An adversary might target containers based on their contents.

11.6.65.R.03. **Rationale**

The smallest tags generally used for consumer items, such as clothing, do not have enough computing power to support data encryption. At best these tags can cater for PIN-style or password-based protection. Data can, however, be encrypted before it is stored on a tag. In these designs, encryption is undertaken by the RFID subsystem or the RFID reader. This is an effective means of protecting the data on a tag. Refer also to Chapter 17 – Cryptography.

11.6.65.R.04. **Rationale**

The current Gen 2 standard provides for an on-chip 16-bit Pseudo-Random Number Generator (RNG) and a 16-bit Cyclic Redundancy Code (CRC-16) to protect tag/reader channels. Neither of these encryption methods is strong because of the short bit length in the RNG and because CRCs are not suitable for protection against malicious alteration of data.

11.6.65.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:2989]

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.

11.6.65.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2990]

Agencies SHOULD encrypt data before it is written to RFID tags.

11.6.65.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2991]

Agencies SHOULD assign RFID identifiers using formats that limit information about tagged items or about the agency operating the RFID system.

## Authentication

11.6.66.R.01. **Rationale**

Both an RFID reader and RFID tag share a common secret key that can be used in combination with a hash algorithm to provide one-way or mutual authentication between tag and reader. This is known as a **Keyed-Hash Message Authentication Code (HMAC)**. When HMAC is applied to messages, it also assures the integrity of data in the messages. HMAC is not specified in any RFID standard, but the capability is generally available in vendor products. HMAC is often used where the risk of eavesdropping is high and passwords alone are considered to offer an inadequate authentication mechanism. This will be determined by the risk assessment. HMAC is also used where applications require evidence of a tag's authenticity.

11.6.66.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2994]

Agencies SHOULD consider the use of HMAC when tag authenticity is required.

## Password Management

11.6.67.R.01. **Rationale**

RFID tags generally require passwords before execution of commands such as reading and writing of tag data, memory access control, and the tag kill feature. Passwords are an important control in maintaining the security and integrity of the RFID system. Refer also to Chapter 16 – Access Control and passwords.

11.6.67.R.02. **Rationale**

Tags should not share passwords, although this may not be practical in all cases. In applications such as supply chains, multiple organisations may require access to databases that contain tag identifiers and passwords. In such cases external entities must be authenticated and incident management, audit logging and other security controls are essential. While in traditional IT systems, passwords are often changed on a periodic basis, in RFID systems, such changes may be impractical, especially if the tags are not always accessible to the agency assigning the passwords.

11.6.67.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:2998]

Agencies MUST assign passwords for critical RFID functions.

11.6.67.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2999]

Agencies SHOULD follow the guidance for passwords management in the NZISM (Chapter 16 – Access control and passwords).

### Temporary Deactivation of Tags

11.6.68.R.01. **Rationale**

The RF interface on some tags can be temporarily deactivated. In a supply chain application, for example, tags may be turned off to prevent unauthorised access to the tags during shipment. This feature is useful when communication between readers and a tag is infrequent allowing the tag to be activated when required but limiting vulnerability to rogue transactions if left operational for extended periods with no authorised activity. Temporary deactivation can also extend battery life in powered tags.

11.6.68.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3002]

Agencies SHOULD consider temporary deactivation of RFID tags where the tag is likely to be inactive for extended periods.

### Incident Management

11.6.69.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.

11.6.69.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3006]

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

11.6.70.R.01. **Rationale**

Tag 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 tags. In addition the continued operating presence of a tag after it has performed its intended function can pose a business intelligence or privacy risk, including tracking, targeting or access to sensitive data on the tag.

11.6.70.R.02. **Rationale**

Disposal may be undertaken electronically by using a tag's "kill" 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.

11.6.70.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3010]

Agencies SHOULD consider secure disposal procedures and incorporate these into the RFID Usage Policy. Refer also to Chapter 13 – Media and IT equipment management, decommissioning and disposal.

### Operator Training and User Awareness

11.6.71.R.01. **Rationale**

Operator training can help ensure that personnel using the RFID system have the necessary skills and knowledge follow appropriate guidelines and policies. If HERF/HERO/HERP risks are present, appropriate security training covers mitigation techniques, such as safe handling distances.

11.6.71.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3047]

Agencies MUST develop and implement user awareness and training programmes to support and enable safe use of RFID services (See Section 9.1 – Information Security Awareness and Training).

## Abbreviations

11.6.72.

| Term | Meaning |
|---|---|
| **EMV** | Europay, MasterCard, and Visa technical standard |
| **EPC** | Electronic Product Code |
| **HERF** | Hazards of Electromagnetic Radiation to Fuel |
| **HERO** | Hazards of Electromagnetic Radiation to Ordnance |
| **HERP** | Hazards of Electromagnetic Radiation to Personnel |
| **HMAC** | Keyed-Hash Message Authentication Code |
| **RFID** | Radio Frequency Identification |
| **SAM** | Secure Access Module/ Secure Application Module |

## Terms

11.6.73.

| Term | Meaning |
|---|---|
| **EMV** | Europay, MasterCard, and Visa technical standard for payment cards, payment terminals and automated teller machines (ATMs) |
| **EPC** | An Electronic Product Code (EPC) is a universal identifier that gives a unique identity to a specific physical object. In most instances, EPCs are encoded on RFID tags attached to the object and used for stock tracking and management purposes. Many types of assets can be tagged including fixed assets, documents, transport containers and clothing items. |
| **Radio Frequency Identification (RFID)** | RFID is technology utilising electromagnetic or electrostatic coupling in the radio frequency (RF) portion of the electromagnetic spectrum to uniquely identify an object, item, animal, or person. RFID is increasingly used as replacement for bar codes. An RFID system consists of three components: an antenna, transceiver (usually the RFID reader) and a transponder (also known as a tag). |
| **Secure Access Module** | A **Secure Access Module** (or Secure Application Module) 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 EMV cards.<br>Physically a SAM card can either be a separate component and plugged into a device when required or incorporated into an integrated circuit. |
| **Tag** | The transponder in an RFID system, frequently found attached to an item or object to provide electronic identification. |