CHARTERED PROFESSIONAL ACCOUNTANTS CANADA

Radio Frequency Identification and Near-field Communications

TECHNOLOGY SPOTLIGHT

Radio frequency identification (RFID) is a wireless, noncontact system that uses radio-frequency electromagnetic fields to transfer data from a tag attached to an object to a scanner, for the purposes of automatic identification and tracking.

Some tags do not require a battery and are powered by the electromagnetic fields used to read them. Others use a local power source and emit radio frequencies. The RFID tag contains electronically stored information that can be read from several metres away. Unlike bar or quick response (a two-dimensional bar code) codes, the tag does not need to be within the line of sight of the reader and may be embedded in the tracked object. RFID tags are used in the retail, automotive and pharmaceutical sectors, as well as with livestock and pets where the tags, about twice the size of a grain of rice, may be injected. Uses range from point-of-sale terminals to tracking progress and location.

Near-field communications (NFC) is a set of standards for smartphones and similar devices to establish radio communication between devices by placing them in close proximity, usually no more than a few centimetres apart. Present and anticipated applications include contactless payment systems, similar to those used in some credit cards, electronic smartcards and bank client cards, data exchange, ticketing systems for public transport and simplified setup of more complex communications such as Wi-Fi. NFC-enabled devices can also act as electronic identity documents and keycards. Because NFC has a short range and supports encryption, it may be more suitable for business applications than less-private RFID systems.

This publication was originally published by The Canadian Institute of Chartered Accountants in 2012.
It has been reissued by Chartered Professional Accountants of Canada.

But there are risks to using RFID and NFC. Although the communication range of NFC is limited to a few centimetres, the signal for the wireless data transfer can be picked up with antennas. While it is difficult to modify the data and still have it meaningful, it is relatively easy to destroy data with an RFID jammer. A lost NFC card or a mobile phone can give the finder access, particularly if the card is acting as a single-factor authenticating device. Mobile phones may be protected by a PIN code. Protecting against use after loss or theft requires an extended security concept that includes more than one physically independent authentication factor.

While applications may use higher-layer encryption such as SSL to establish a secure channel, ensuring security for NFC data requires the cooperation of device providers, businesses and customers.

From a business perspective a secure environment needs to be created, one in which customers can protect their RFID-enabled devices and data using a combination of techniques such as passwords, tokens, keypad locks and encryption, as well as antivirus software and other solutions to prevent spyware and malware from infecting transacting parties.

Description

The use of RFID (radio frequency identification) to provide a range of identification, tracking and transaction execution functions, including Near Field Communications (NFC).

Importance

The business advantages of being able to locate and track inventory, tools, technology and equipment can provide benefits in inventory control, theft prevention and misuse of company assets.

The use of NFC can improve throughput and record information efficiently and effectively.

Business Benefits

Business benefits from adopting RFID and NFC include:

- Quicker data capture and faster processing of transactions;
- Less shrinkage of inventory, small tools or other similar small but valuable products and devices;
- Ability to capture information without having to have line-of-sight communication;
- Reduced investment in tools as their location can be easily tracked and determined;
- Provide improved technology to support workers;
- Ability to store over-stock items in available space and locate them easily and quickly using RFID, thereby reducing unnecessary increases in inventory.

Issues and Risks	Possible Mitigation
Lost or stolen NFC cards may enable unauthorized access. **The impact of misuse of an NFC card may not be easily identifiable.**	Develop and implement policies and procedures to ensure that lost or stolen NFC cards are reported immediately. Establish technology processes to deactivate lost or stolen cards.
Lost or damaged tags will make it difficult to determine the exact location of inventory if products are not stored in predetermined areas.	To the extent practicable store products and like products in the same general area, allowing for search of similar products to narrow down the physical search area. Implement systems to identify and replace missing or damaged tags.
Concerns over loss of information or loss of privacy by card users.	When not used store/carry cards in copper-lined sleeves, similar to the ones provided with Nexus cards.
Walk-off: the possible compromise between a user leaving the site and a NFC transaction timing out.	Limit the ability to eavesdrop.
Removal/switching of RFID tags.	For high-priced merchandise and tools use secure tags and implement a program to ensure all items are tagged.