Basic Working Principal -

**# RFID** is the process by which items are uniquely identified using radio waves, and **NFC** is a specialized subset within the family of **RFID** technology. Specifically, **NFC** is a branch of High-Frequency (HF) **RFID**, and both operate at the **13.56 MHz** frequency.

# the range at which a card can be read is very short and, even if the criminal is close enough to grab data and do a transaction, he cannot create a copy of the card. This is not true of magnetic strip cards.

# RFID has a data rate of 106 to 848 kbit/s

# NFC Payment cards falls under the ISO/IEC 14443

**ISO/IEC 14443-3:2011 describes:**

* polling for proximity cards or objects (PICCs) entering the field of a proximity coupling device (PCD);
* the byte format, the frames and timing used during the initial phase of communication between PCDs and PICCs;
* the initial Request and Answer to Request command content;
* methods to detect and communicate with one PICC among several PICCs (anticollision);
* other parameters required to initialize communications between a PICC and PCD;
* optional means to ease and speed up the selection of one PICC among several PICCs based on application criteria.

Protocol and commands used by higher layers and by applications and which are used after the initial phase are described in ISO/IEC 14443-4.

ISO/IEC 14443-3:2011 is applicable to PICCs of Type A and of Type B (as described in ISO/IEC 14443-2).

ISO/IEC 14443 implementations -

* [MIFARE](https://en.wikipedia.org/wiki/MIFARE) cards (partial or full implementation, depending on product)
* [Biometric passports](https://en.wikipedia.org/wiki/Biometric_passports)
* [EMV](https://en.wikipedia.org/wiki/EMV) payment cards
* [National identity cards in the European Economic Area](https://en.wikipedia.org/wiki/National_identity_cards_in_the_European_Economic_Area)
* [Near Field Communication](https://en.wikipedia.org/wiki/Near_Field_Communication) is based on in part, and is compatible with, ISO/IEC 14443
* [Calypso](https://en.wikipedia.org/wiki/Calypso_(electronic_ticketing_system)), open security standard for transit fare collection systems
* [CIPURSE](https://en.wikipedia.org/wiki/CIPURSE), open security standard for transit fare collection systems

EMV payment cards defined in 3 Technology -

[PayPass](https://en.wikipedia.org/wiki/PayPass)

[Visa payWave](https://en.wikipedia.org/wiki/Visa_payWave) (Visa Contactless)

[ExpressPay](https://en.wikipedia.org/wiki/ExpressPay)

**analysis Hardware Tools -**

# ACR1252U NFC Forum Certified NFC Reader



Source : [Amazon.in](https://www.amazon.in/ACR1252U-USB-NFC-Reader-III/dp/B01KIKBYAG/ref=pd_sim_147_11?_encoding=UTF8&pd_rd_i=B01KIKBYAG&pd_rd_r=4a0243af-a153-11e8-b694-39dbcfa8fb4b&pd_rd_w=f9SUO&pd_rd_wg=D9jFO&pf_rd_i=desktop-dp-sims&pf_rd_m=A1VBAL9TL5WCBF&pf_rd_p=f8891fd1-e867-4fdb-9599-be53438ba393&pf_rd_r=3JA9W0PETP2WCRYVGZGX&pf_rd_s=desktop-dp-sims&pf_rd_t=40701&psc=1&refRID=3JA9W0PETP2WCRYVGZGX) (Rs 4,703)

Supports ISO 14443 Type A and B cards, MIFARE, FeliCa, and all 4 types of NFC (ISO/IEC 18092) tags

* Supports MIFARE 7-byte UID, MIFARE Plus and MIFARE DESfire
* Built-in anti-collision feature (only 1 tag is accessed at any time)
* NFC Support: NFC Reader/Writer Mode, Peer-to-Peer Mode, Card Emulation Mode

Attack vectors implies -

**card Emulation**

**by a special purpose app -**

**Preplay Attack -** pre computing the random number generation of a pos terminal and generating a set of transation validating codes and preplays them on the duplicate card.

**\* Requires a special type of NFC tags that comes with interchangable UID**

# **LINQS - Smartrac Circus NTAG213 NFC Tag (Micro Pack - Set of 4) | Small size, great performance!**

[LINK](https://www.amazon.in/LINQS-Smartrac-Circus-NTAG213-performance/dp/B01AG1FXCM?tag=googinhydr18418-21&tag=googinkenshoo-21&ascsubtag=a8e1194f-b52f-4894-8569-daf7a4460cc6)

**Smartrac Circus is the industry's best known all-purpose NFC tag. It is compatible with all NFC phones/tablets/readers.**

* This tag is characterized by superior performance - compared to other tags of the same size. The tag's diameter is just 22mm making it ideal for applications where small size & great readability is a must.
* The tag comes with the new NXP NTAG213 chip equipped with 144 bytes user memory with password protection. It also offers UID mirroring & interaction counter that makes it simple to uniquely identify a tag & # of times it was used.
* All tags come with 100% Quality Assurance & are Performance Tested.
* The tags are paper thin with strong adhesive on back & water resistant white PET film on front.