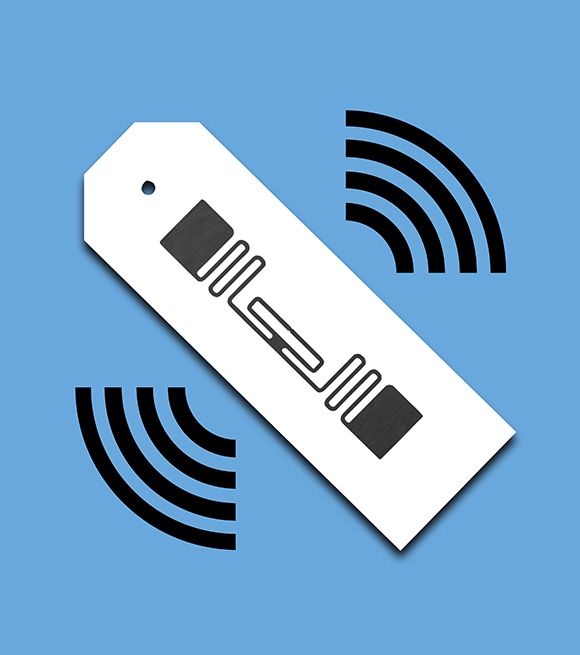
**Introduction to RFID**



**Overview**  
Radio Frequency Identification (RFID) is the most popular short-range radio solution. It is commonly used to store and transmit information that identifies an entity. RFID systems consist of tags and readers that communicate using radio waves. RFID tags can be either passive or active. Passive tags rely on power from the reading antenna, while active tags have their own power source, such as an embedded battery.

**Classes of RFID Tags**

  
EPCglobal divides RFID tags into six categories, with each category adding capabilities on top of the previous one, ensuring backward compatibility.

1. Class 0: Passive tags operating in UHF bands, preprogrammed by the vendor, with unchangeable memory.  
2. Class 1: Can operate in HF bands, written only once post-production, and often include CRC checks for error detection.  
3. Class 2: Rewritable multiple times.  
4. Class 3: Semi-passive with embedded sensors for recording environmental parameters, but cannot initiate communication.  
5. Class 4: Active tags capable of initiating communication with other Class 4 tags.  
6. Class 5: Can provide power to other tags and communicate with all previous classes, functioning as RFID readers.

**Information Stored in RFID Tags**

An RFID tag's memory typically stores:  
- Identification Data: Identifies the entity to which the tag is attached, including user-defined fields such as bank accounts.  
- Supplementary Data: Provides additional details about the entity.  
- Control Data: Used for the tag's internal configuration.  
- Manufacturer Data: Contains a Unique Identifier (UID) and production details.

The ISO standard specifies the Application Family Identifier (AFI) and Data Storage Format Identifier (DSFID), which indicate the kind of object the tag belongs to and the logical organization of user data, respectively. Security controls restrict read/write operations on memory blocks using lock mechanisms that often come with vendor-configured default passwords, which can be customized by tag owners.

**Comparison of Low & High Frequency RFID Tags**

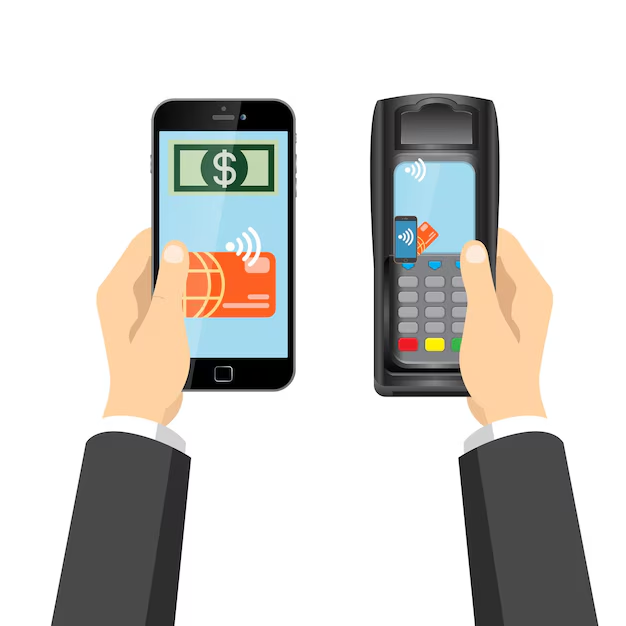
**Low-Frequency RFID Tags (125 kHz)**  
- Used in systems that do not require high security (e.g., building access, gym membership cards).  
- Operate within 30 kHz to 300 kHz, typically 125 kHz to 134 kHz.  
- Features include long range, primitive protocol, and low security.  
- Common protocols: EM-Marin, HID Prox II, Indala.

**High-Frequency RFID Tags (13.56 MHz)**  
- Used for more complex interactions requiring cryptography and authentication (e.g., bank cards, public transport).  
- Operate at 13.56 MHz and follow protocols like ISO 14443, commonly referred to as NFC.  
- Features include short range, advanced protocols, and high security.  
- Support cryptographic algorithms like AES and asymmetric cryptography.

**CTF Challenge: Bypassing RFID Security**

**Tools and Requirements**  
- Basic knowledge of RFID technology  
- Access to online resources for learning about RFID (e.g., [HackTricks - Pentesting RFID](https://book.hacktricks.xyz/todo/radio-hacking/pentesting-rfid))  
- Optional: RFID reader/writer for practical exploration

**Scenario**

  
As a cybersecurity beginner, your task is to answer questions related to RFID technology and common methods used to bypass RFID security. This will help you understand the basic concepts and potential vulnerabilities of RFID systems.

**Questions**

Flag 1: What does RFID stand for?  
Answer: Radio Frequency Identification  
Flag Captured

Flag 2: What are the two main components of an RFID system?  
Answer: RFID reader and RFID tag  
Flag Captured

Flag 3: Which frequency range is commonly used for RFID systems in access control applications?  
Answer: 13.56 MHz  
Flag Captured

**Hint**  
Use reliable web resources to look up definitions and examples of RFID technology and its applications. Focus on understanding the key components and security concerns of RFID systems.