u3a Computing Group

Alan Hopwood, 2 May 2024

Presentation

Near Field Communications

(and RFID)

(and BLE is mentioned)

Agenda

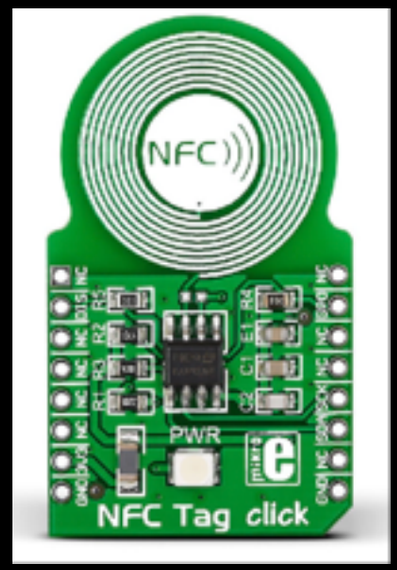
Near Field Communications

- What is NFC
- What is Radio Frequency Identification (RFID)
- RFID technology
- History and development of RFID
- Development of NFC
- NFC technology
- Applications of NFC
- Demonstration

Near Field Communications

NFC

- NFC is an offshoot of RFID (Radio Frequency Identification) technology
- It provides contactless communications between devices held in close proximity.
- One of the devices can be passive - i.e. not have its own power but be powered from the radio waves emanating from the other device.
- A specific version of NFC is used for contactless card payment



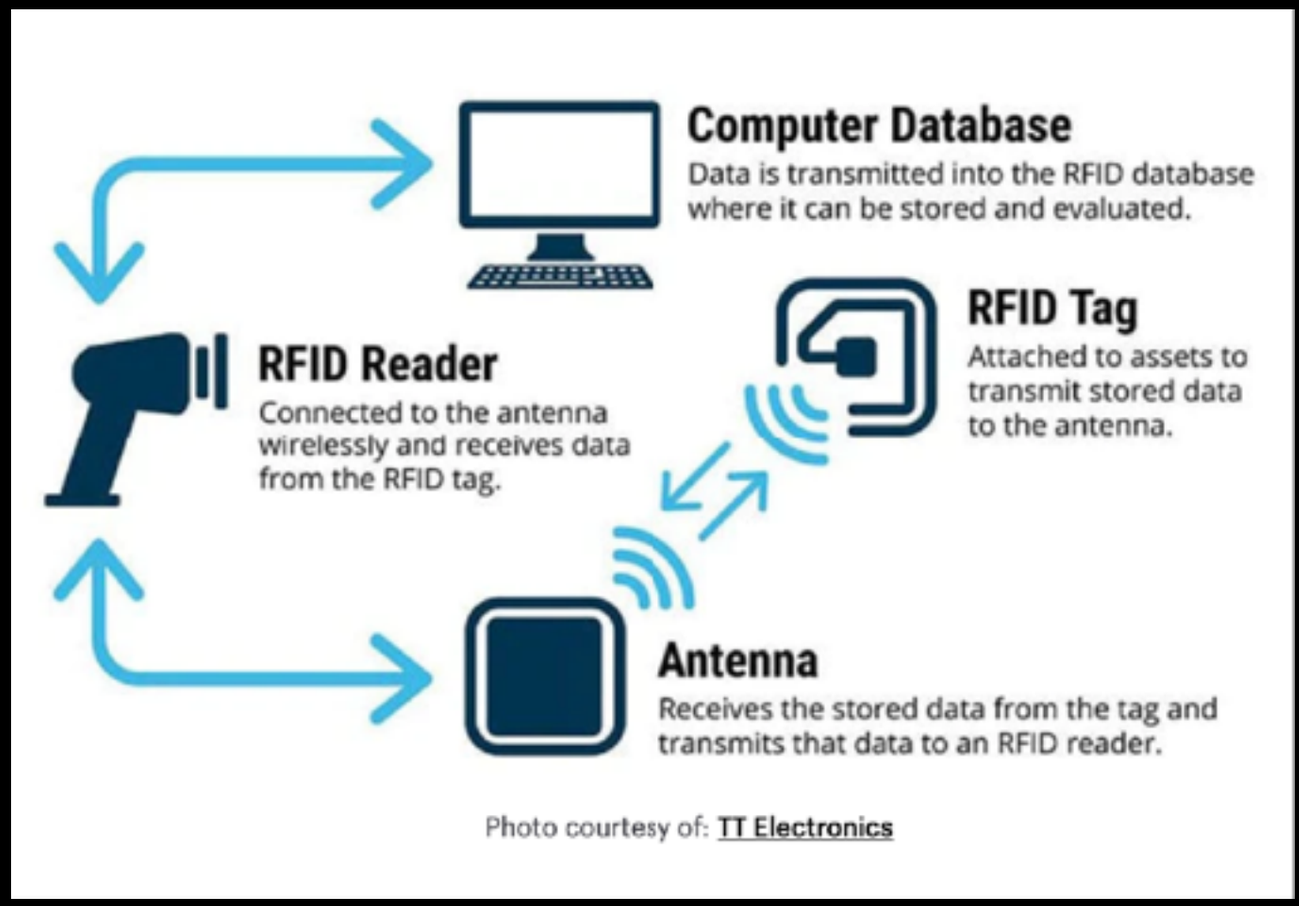
NFC Tag:
£9.75 RS Components

NFC tags
£6 for 10 on
Amazon

What is Radio Frequency Identification

RFID

- Uses electromagnetic fields to automatically identify and track tags attached to objects
- An RFID system consists of a tiny radio transponder called a tag, a radio receiver, and a transmitter.
- When triggered by an electromagnetic interrogation pulse from a nearby RFID reader device, the tag transmits digital data, usually an identifying inventory number, back to the reader.
- Passive tags are powered by energy from the RFID reader's interrogating radio waves. Active tags are powered by a battery
- US$12.08 billion spent on RFID technology in 2020

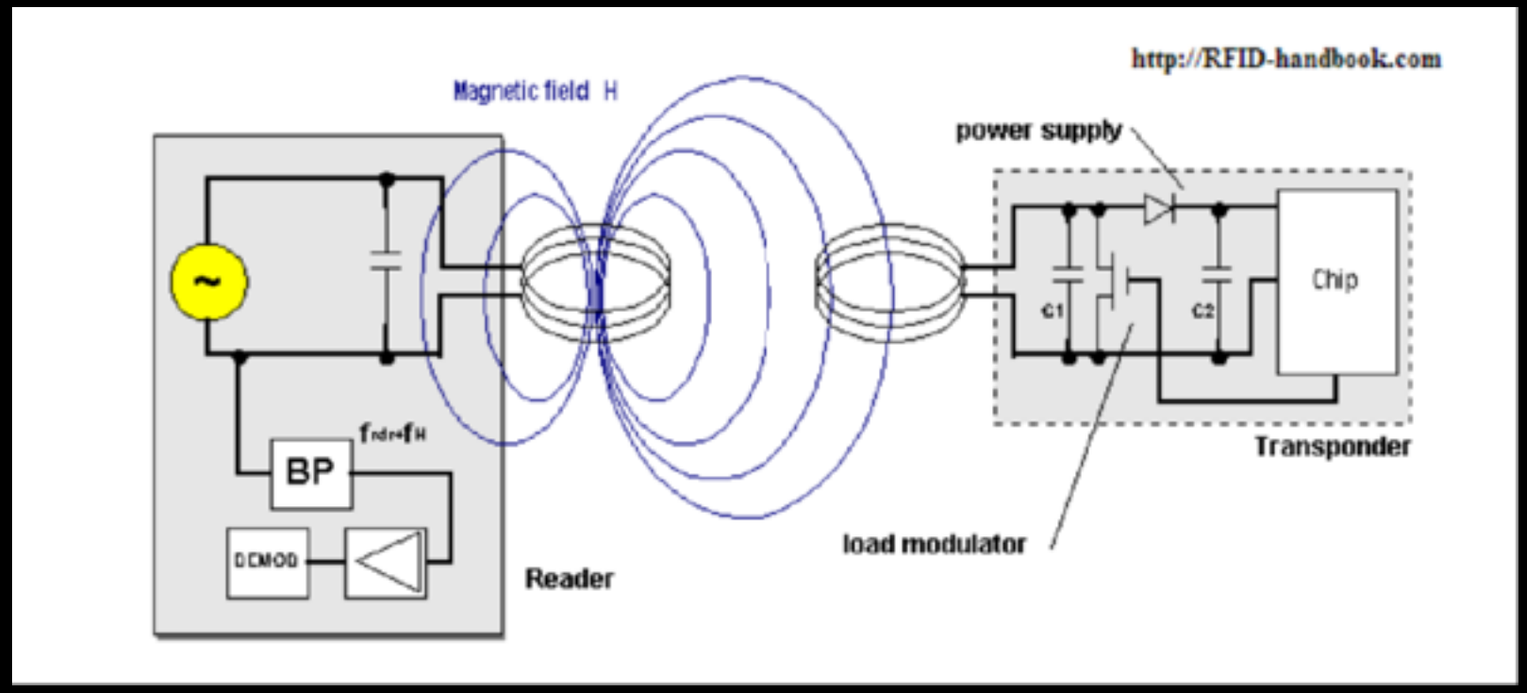


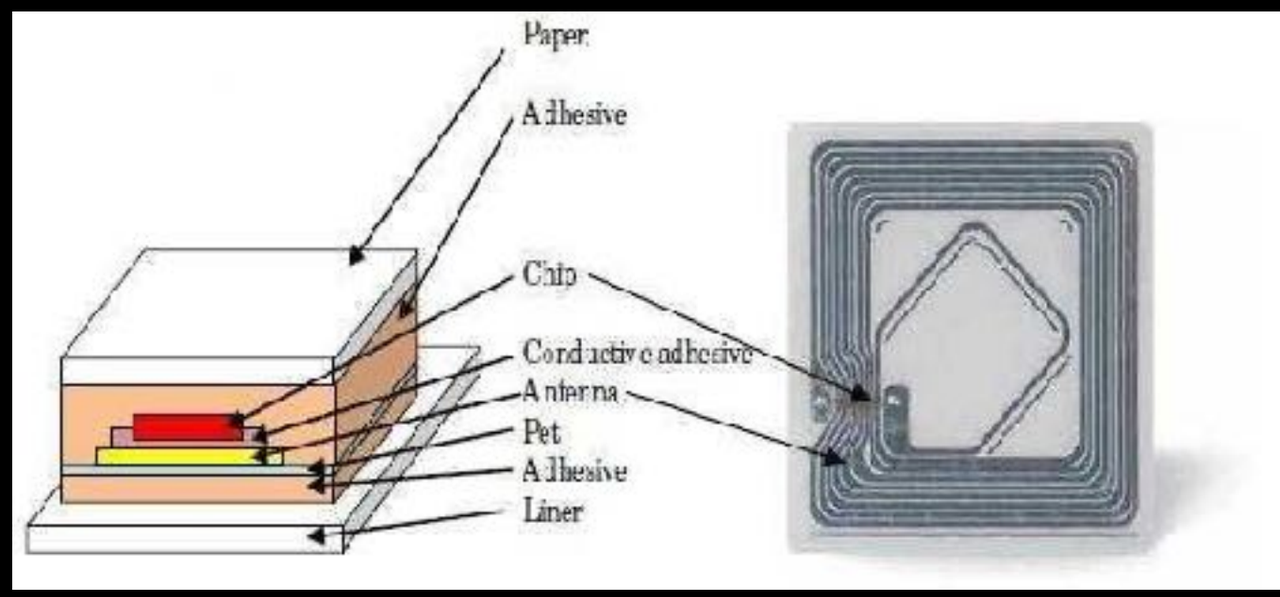
RFID Technology

RFID

RFID Tags are made up of:

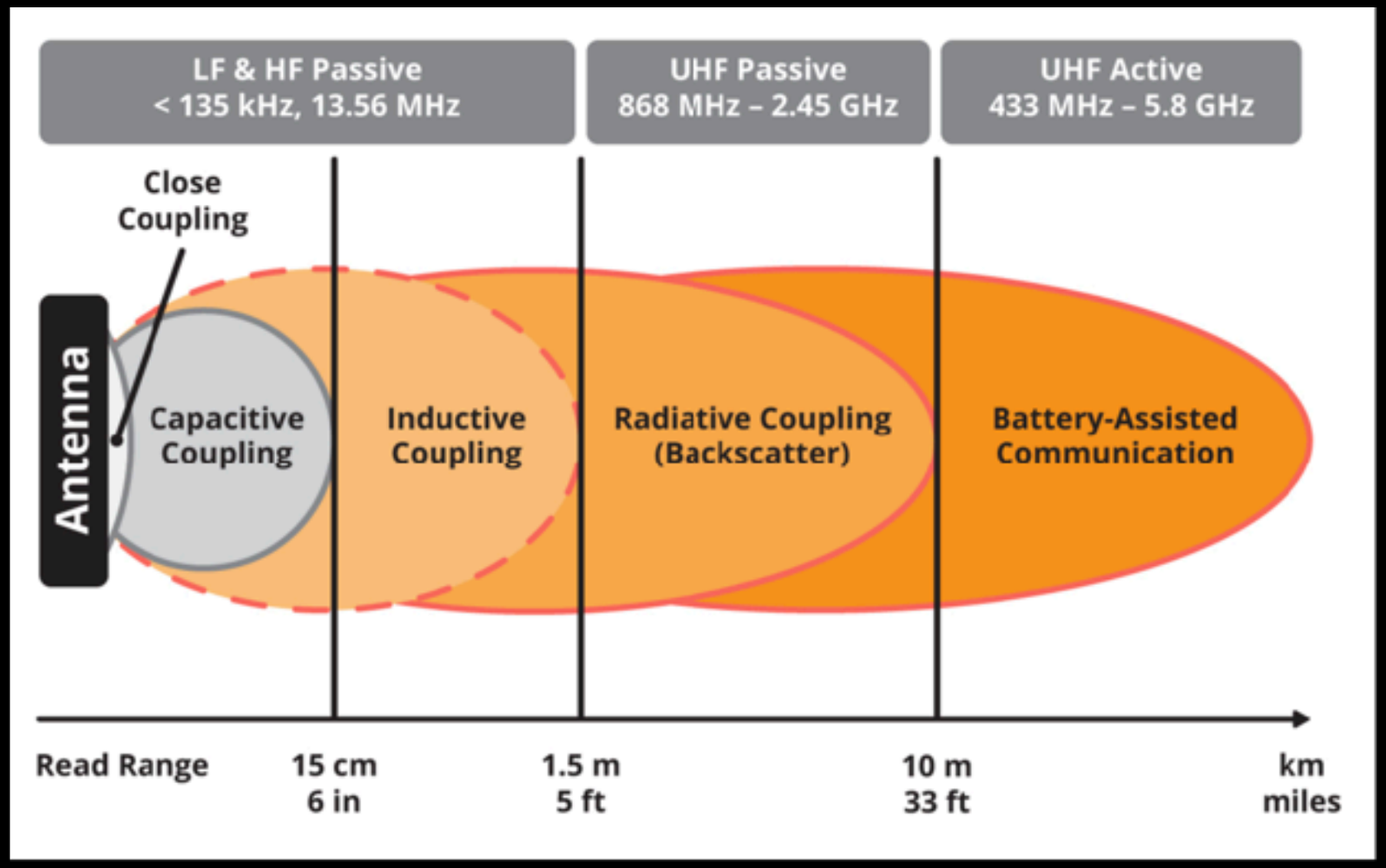
- RFID Chip (40-50,000 transistors)
  - modulates/demodulates signals
  - encodes/decodes communications
  - Implements communication protocol
  - Power management
- Antenna receives signal and power. transmit signal





RFID transmission types

RFID



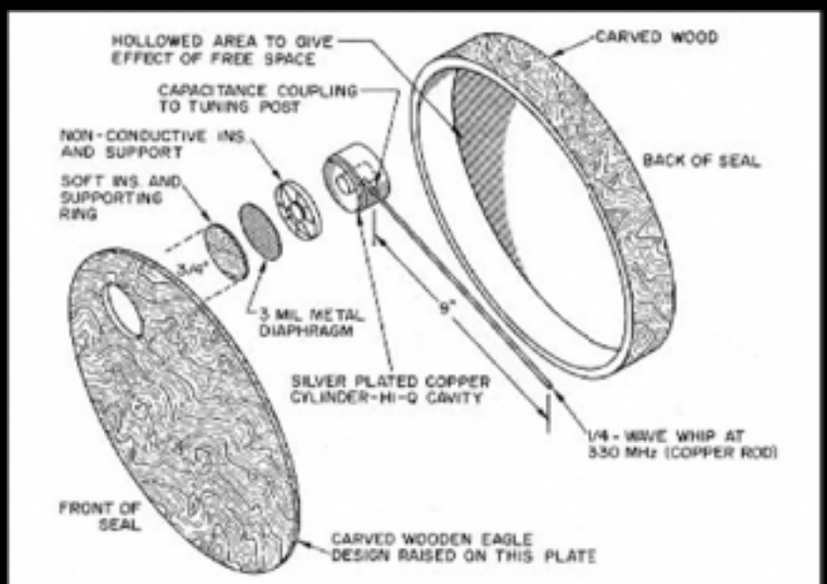
RFID covers various transmission types

- **Capacitive Coupling** – use electric currents instead of the magnetic field in order to couple. Not used widely
- **Inductive Coupling** – relies on the magnetic field of the reader. Inductive coupling is seen in LF, HF, and UHF applications that include coils/antennas in the tag infrastructure.
- **Radiative Coupling (backscatter)** – electromagnetic waves are sent from the reader antenna to the tag antenna. A small amount energy is then reflected back to the reader.

RFID History - “The Thing”

https://hackaday.com/2015/12/08/theremins-bug/

- August 4, 1945, a large, hand-carved ceremonial seal of the United States of America was given to Averell Harriman, the US ambassador by The Young Pioneer Organisation of the Soviet Union.
- “The Thing”, would not be discovered until 1952 — roughly seven years later.
- An antenna attached to a cavity with a silver diaphragm over it, serving as a microphone. There were no batteries. It was activated by radio waves beamed at the US embassy by the Soviets. It used the energy of the incoming signal to broadcast back. When that signal was switched off, The Thing would go silent. (invented by Léon Theremin)



RFID History

RFID

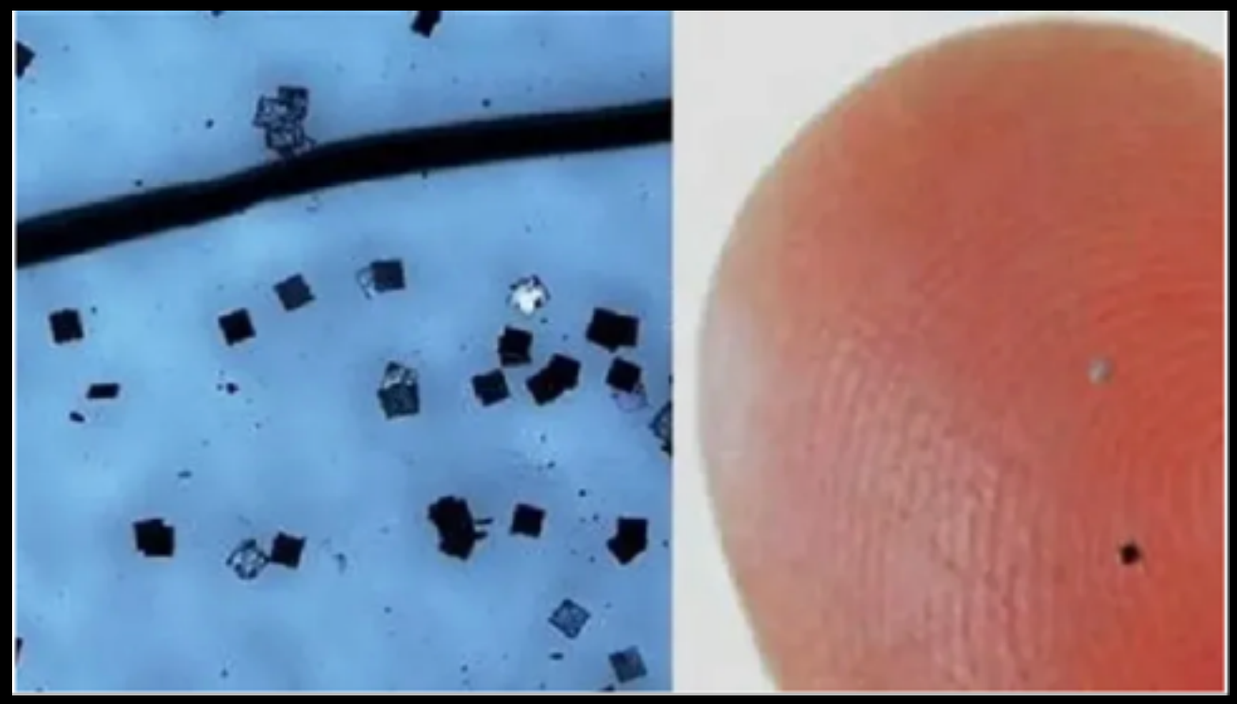
- **1948**, A paper “Communication by Means of Reflected Power.” by Harry Stockman, highlighted the possibility of point-to-point communication in which radio waves used.
- **1973**, Mario W. Cardullo created an active RFID tagging system that utilised rewritable memory.
- **1973**, a passive RFID system was patented by Charles Walton, who designed a passive responder that could unlock doors without a key
- **1970s**, the Los Alamos National Laboratories started to develop a system to track the transportation of nuclear materials securely and safely. The system included a variety of readers and transponders attached to the vehicles carrying the materials. These would then enable the truck to be identified at various points along its route.

RFID development

RFD

- RFID Tags are being used to track insects

- Hitachi has produced “Smart Dust” one of the world's smallest contactless IC chips
- Receives radio waves (2.45 GHz microwaves), and transforms it to energy to wirelessly transmit a 128 bit (1038) unique ID number.



Near Field Communications

NFC

- **March 25, 2002**: Philips and Sony agreed to establish a technology specification.
- **In 2004**, Nokia, Sony, and Philips came together to form the NFC Forum (https://nfc-forum.org/)
- **In 2006**:
  - the group produced the first set of specifications for NFC tags
  - the specifications for “smart” posters were created. Smart posters hold information that an NFC compatible device can read when passed over it
  - The first NFC-comptabile cell phone, the Nokia 6131, also surfaced during this time.

NFC Technology

NFC

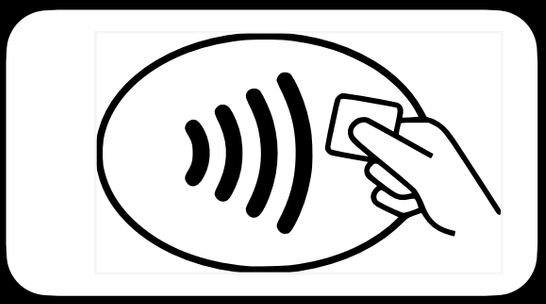
- As for RFID with:
  - Inductive coupling operating at 13.56 MHz
  - Operating distance 4cm
  - Wireless charging of up to 1W over a distance of up to 2cm.

Designed for Contactless

NFC

- The user experience for NFC is centred on a tap.
  - Very Fast Startup
  - Power Sensing
  - Short Connection Time
  - Small Data Payload
- NFC specification allows for Various Modes:
  - Card Emulation: Device looks like contactless card (bank card)
  - Reader / Writer: Device is able to read contactless tags
  - Wireless Charging: Device is able to transfer up to 1W power over an NFC connection
  - Peer-to-Peer: Two devices exchanging data
  - Secure Element based Card Emulation: enabling an application specific secure “element” to control transactions

Applications: Payment Cards



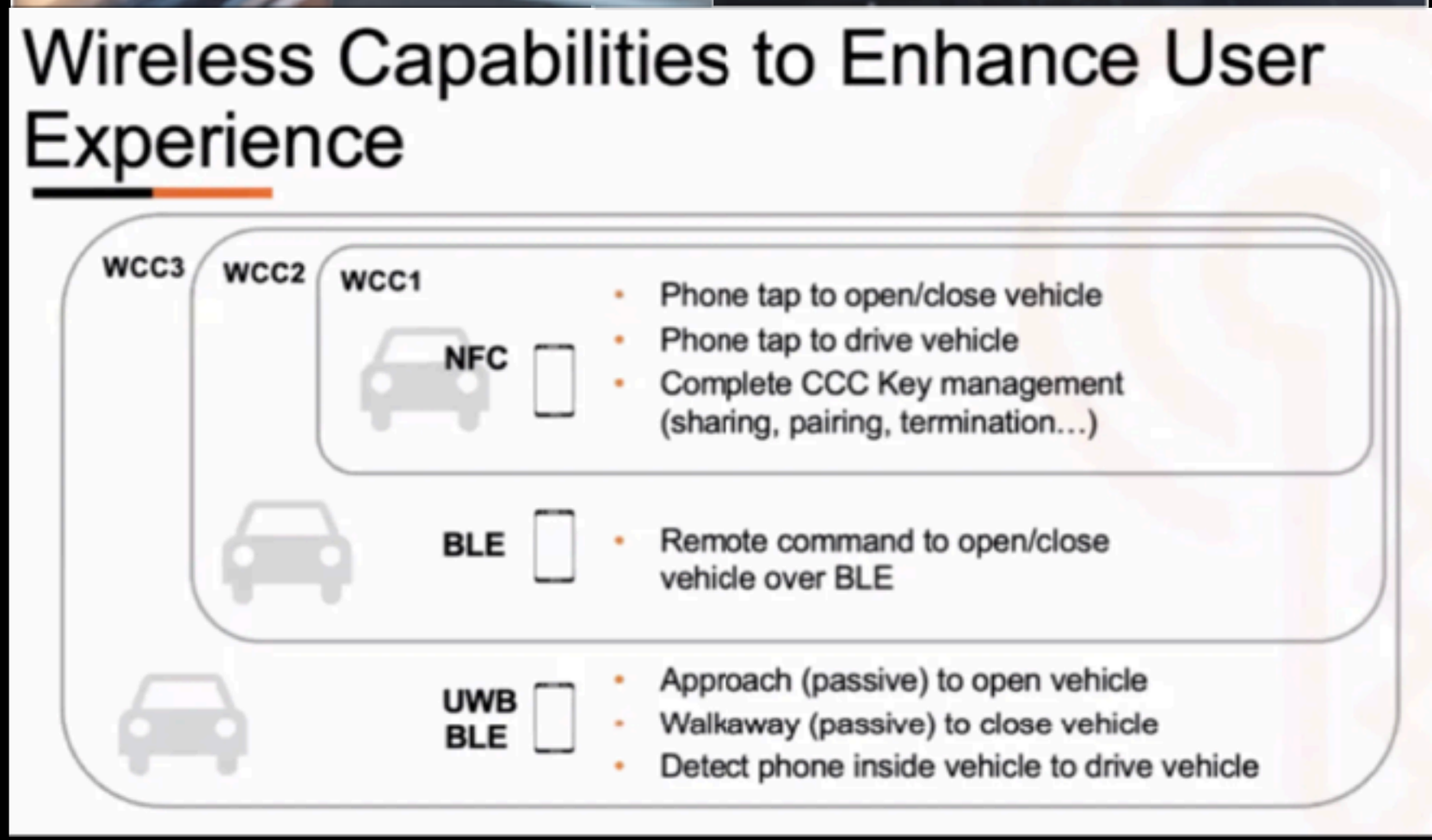
NFC / EMV

- **EMV** is the main standard for smart card payments (created by Europay, Mastercard & Visa)
- Includes the chip & pin functionality and online transactions as well as NFC
- Standard is ISO/IEC 14443 for contactless (NFC plus….)
- Security:
  - Encryption - Secret key used to generate unique card verification per transaction.
  - Dynamic data - Transactions include dynamic data unique to the transaction. Cannot be reused.
  - Authentication - offline authentication method uses data from the card to allow the EMV terminal to authenticate the card. The terminal is preloaded with keys to check complementary keys on the card for each transaction.
  - Confidentiality - transaction does not require cardholder name.

Applications: car keys

NFC

- To date - Proprietary solutions
- Car Connectivity Consortium (CCC) is producing standards
- Most major car companies, as well as Apple, Samsung, and, Google and others are members.
- At the testing and validation stage
- Will enable phones to open cars - share keys by phone



Application - Biometric passport

Passports use NFC to hold and deliver:

- the biographical information which is printed in the passport - Passport number, names, DOB, place of birth, gender. Signature (if recorded digitally)
- Digitised image of the holders photograph. Various features on the face, for example the distance between eyes, nose, mouth and ears, are digitally coded from the photograph and the information stored on the electronic chip.

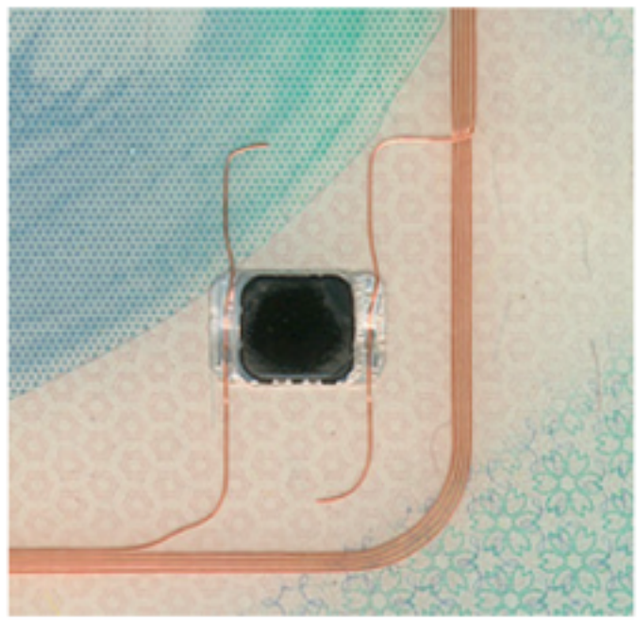


Fig. 2. Chip and antenna in UK passports

Passport security

Selected Security measures:

- **Passive Authentication**: There is an encrypted digital signature. Also all data stored is “hashed” and the hash encrypted with the country’s private key. It is verified with the country’s public key.
- **Active Authentication**: A private key, not readable, is held on the chip. Its presence is verified using a challenge-response algorithm. Verifies that the chip is authentic
- **Basic Access Control**: The inspection system must use authentication keys derived from data printed in the machine-readable zone of the data page (stops passport skimming) and also checks that chip data and printed data are the same.

Primary objectives of security:

- To prevent changes being made to a genuine passport
- To prevent making false passports
- To validate the information held is as provided by the issuing country

Biometric Passport

- Demonstration of reading the passport data using ReadID Me (available in Apple App store and Google Play)

Questions?