NFC - Near Field Communication

SmartLock Picking

Johanna Sacher

22. April 2019

Outline

Section 1

NFC Basics

NFC Basics

- communication between two devices

NFC Basics

- communication between two devices
- wireless exchange of data

NFC Basics

- communication between two devices
- wireless exchange of data
- devices in close proximity (max. 10 cm)

NFC Basics

- communication between two devices
- wireless exchange of data
- devices in close proximity (max. 10 cm)
- based on RFID-Technology

RFID

- transmit data via radiowaves

RFID

- transmit data via radiowaves
- Transponder (RFID-Tag) and Reader

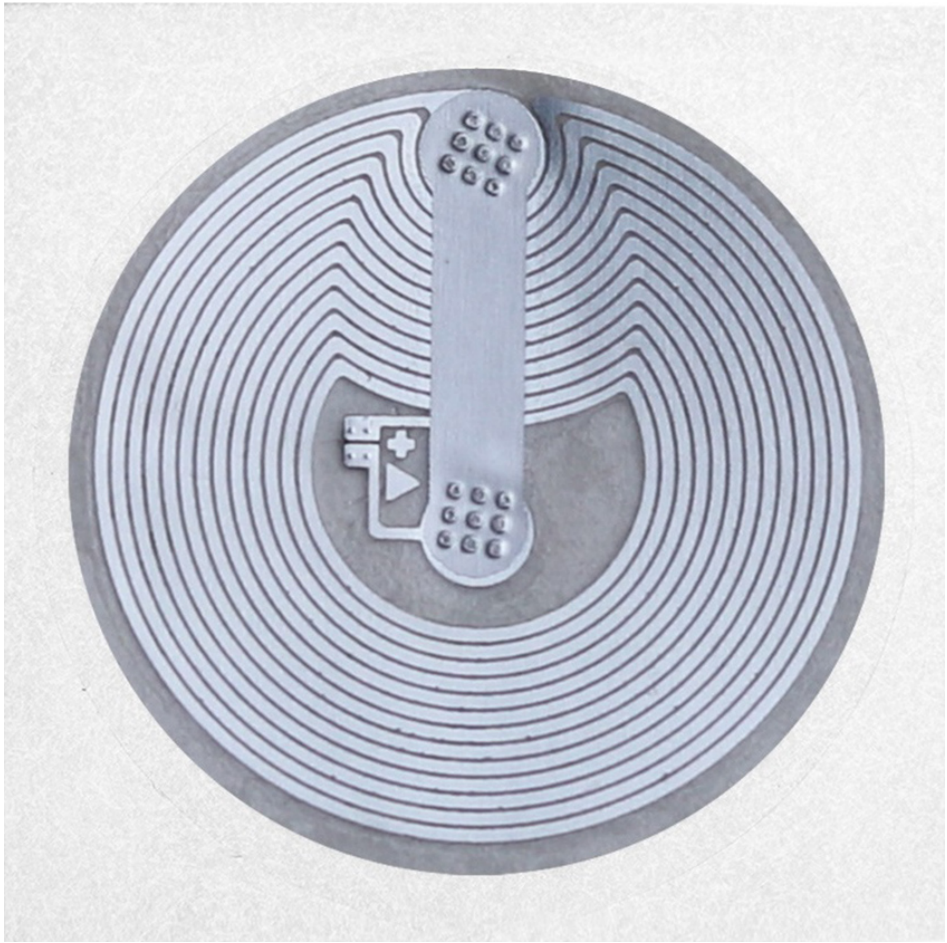
RFID

- transmit data via radiowaves
- Transponder (RFID-Tag) and Reader
- works over great distances

RFID

- transmit data via radiowaves
- Transponder (RFID-Tag) and Reader
- works over great distances
- e.g. chips for pets or cars

How NFC works



Source: NFC-Tag-Shop

How NFC works

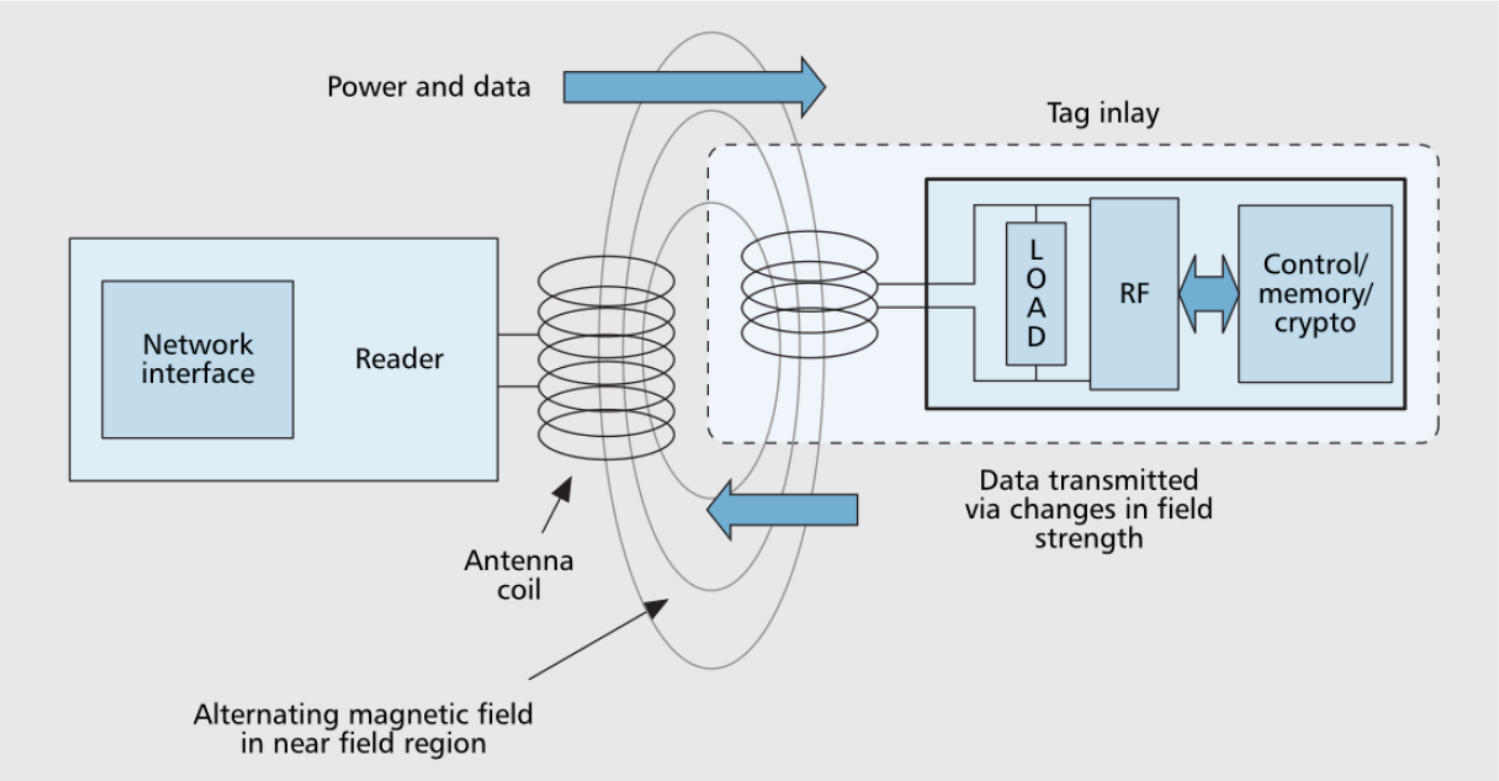
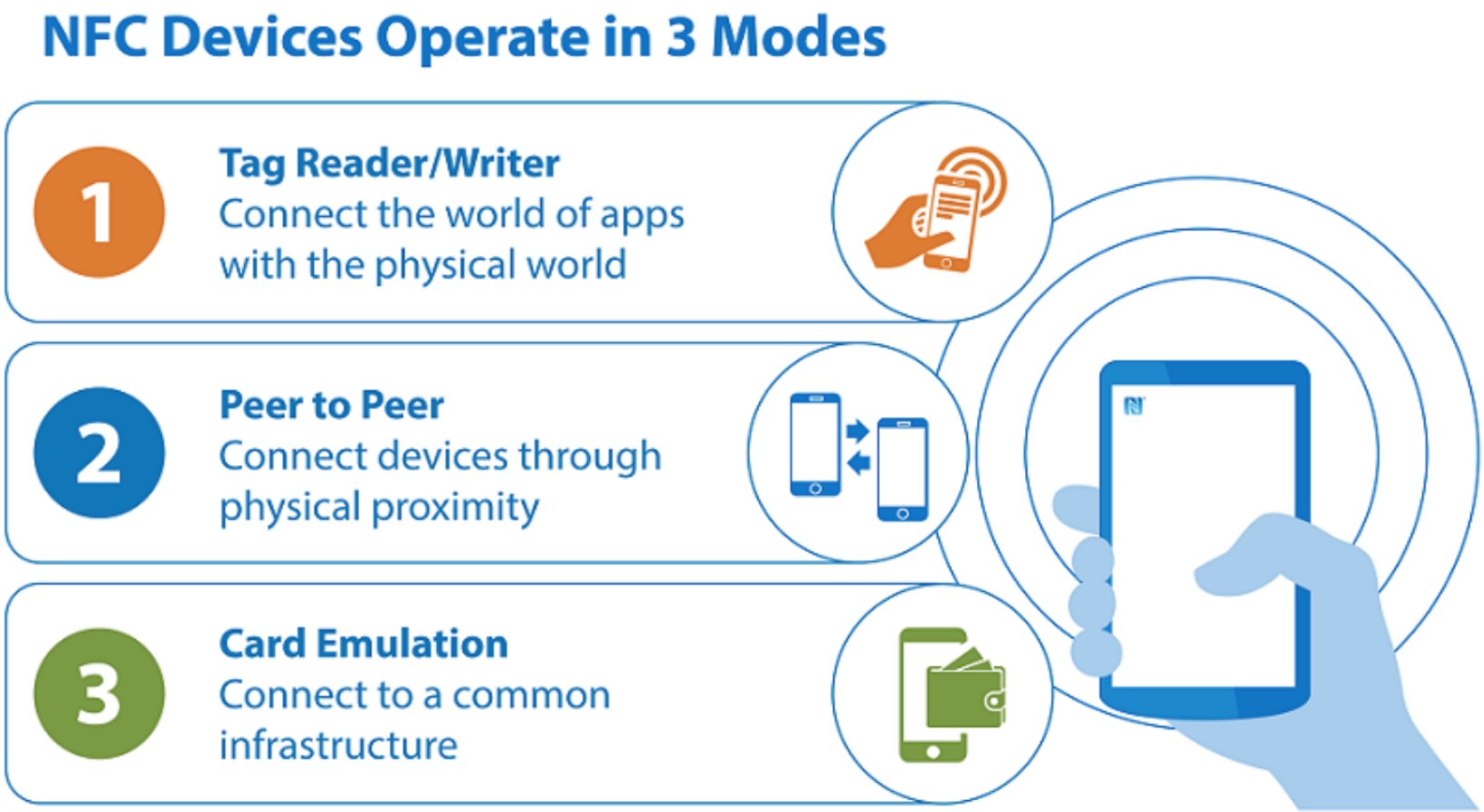


Figure 1: Magnetic Inductive Coupling between a reader and tag (Chawla and Ha, 2007).

Source: *Access Granted: On the Security of Near-Field Enabled Keycards* by Stephen J. Jones

How NFC works



Source: nfc-forum.org

Section 2

Use

Use

- pairing by user
  - $\Rightarrow$ automatic authentication

Use

- pairing by user
  - $\Rightarrow$ automatic authentication
- secure because of short distance (not really though ...)

Where we use it

Source: NFC21.de

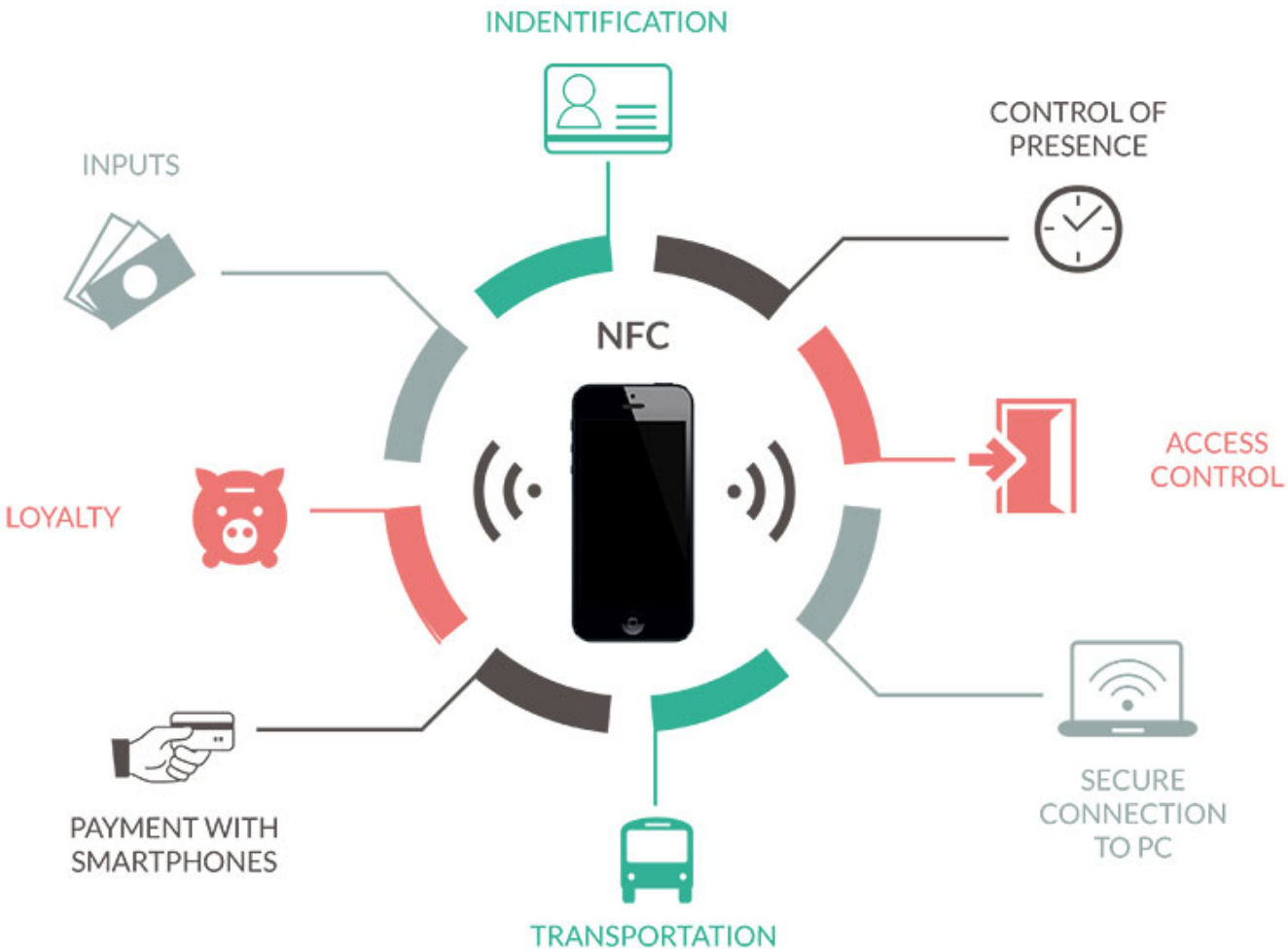
Source: dhGate.com

Source: androidauthority.com

Source: congstar.de

Source: noelsch.de

Where we use it



Source: Wonderful NFC Projects to arouse your ideas

Section 3

Security

Security

- depends on settings of the reading device

Security

- depends on settings of the reading device
- short range provides a little security

Security

- depends on settings of the reading device
- short range provides a little security
- stolen smartphone = stolen key

Possible Attacks

Phishing:

retrieve sensible data from naive users

$\Rightarrow$ by manipulation, e.g. false promises

Possible Attacks

Skimming:

unauthorised reading of data (e.g. a credit card)

- $\Rightarrow$ e.g. in order to save and replay the data
- $\Rightarrow$ possible with any reading device near enough (for example with Apps like NFCProxy or NFCGate)

Possible Attacks

Eavesdropping:

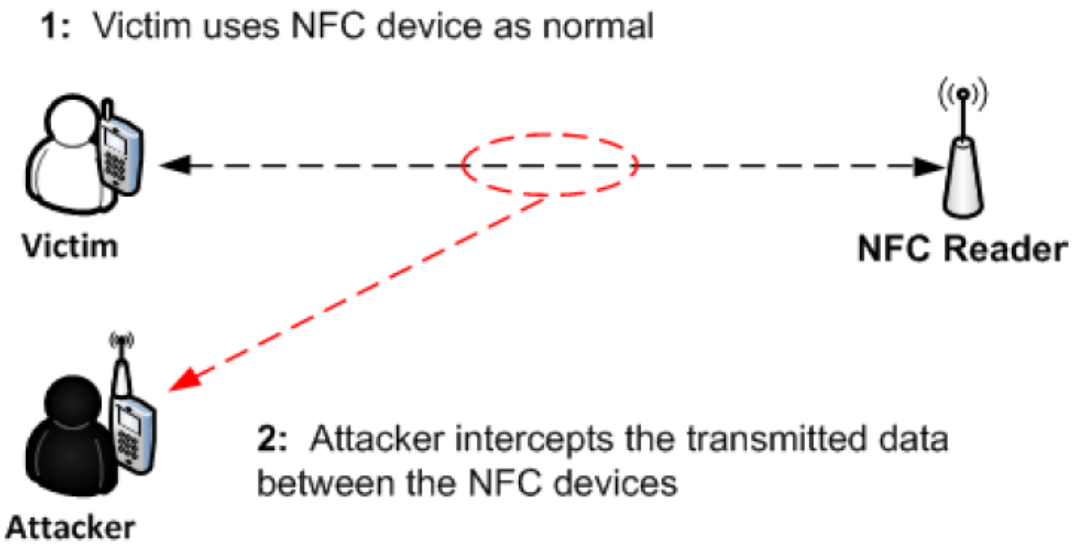


Figure 3: Eavesdropping NFC devices.

Source: *Access Granted: On the Security of Near-Field Enabled Keycards* by Stephen J. Jones

Possible Attacks

Relay Attacks:

⇒ e.g. with NFCProxy or NFCGate

Source: NFCProxy-Wiki

Section 4

NFC Tools for Android

NFC Tools for Android

NFC Reader

TagInfo

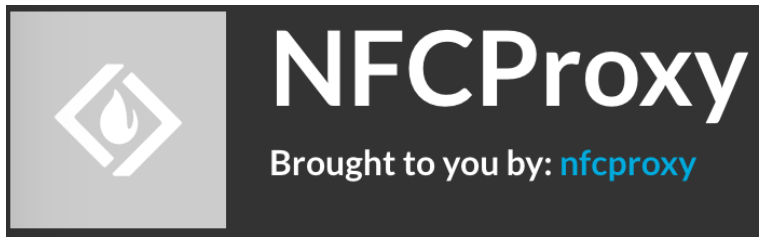
NFC Tools

NFC Tools for Android

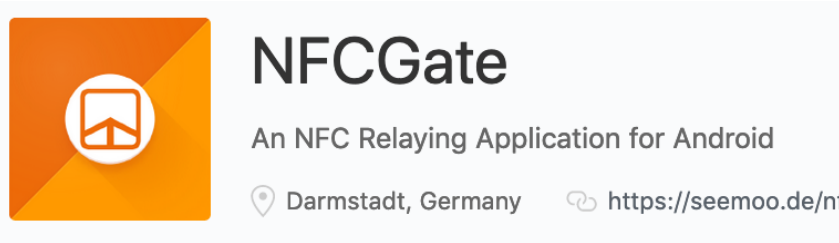
NFC Reader

TagInfo

NFC Tools

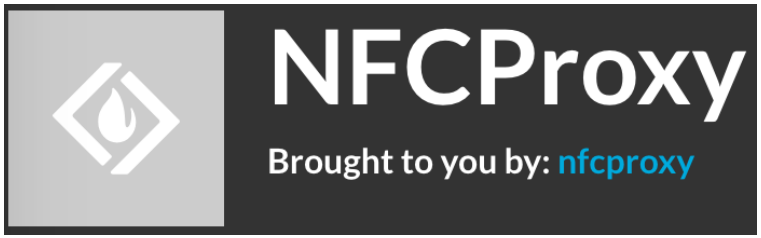


NFCProxy



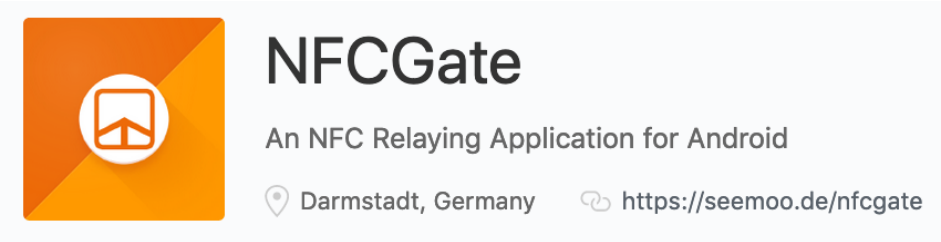
NFCGate

NFCProxy



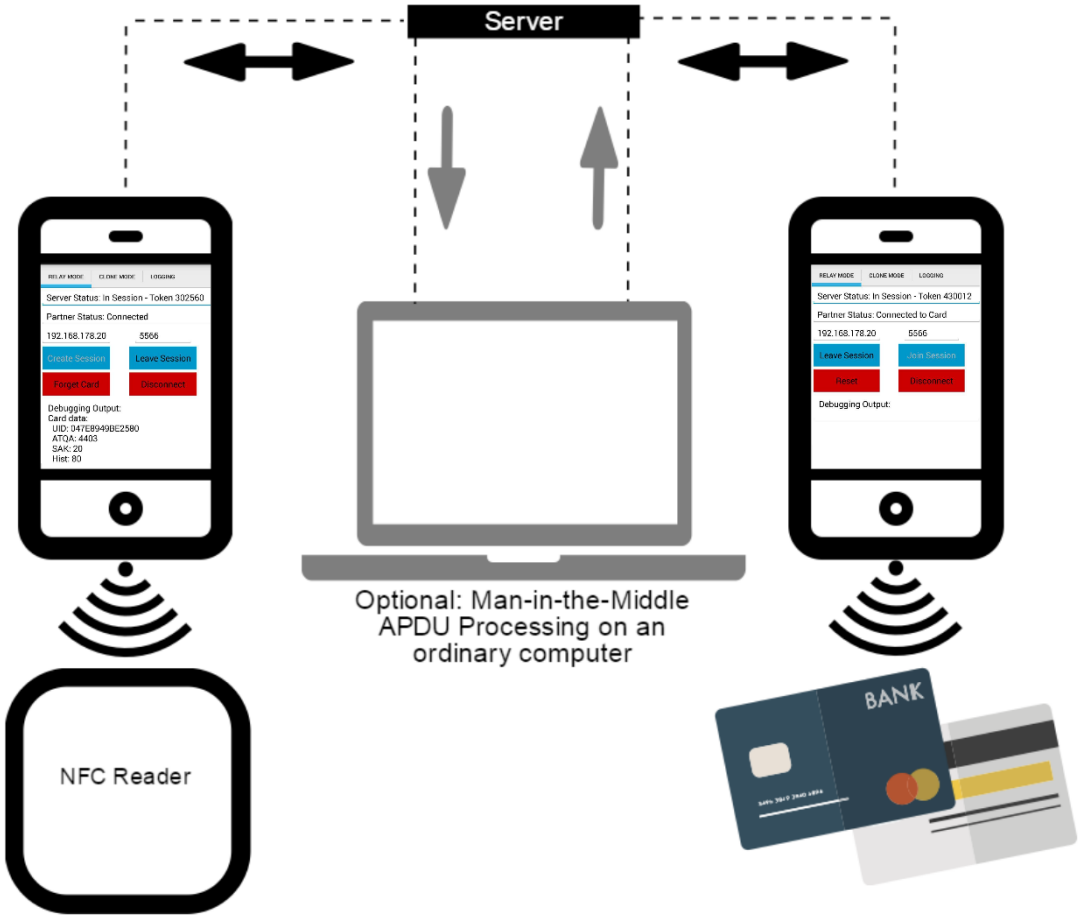
- proxy transactions between RFID credit card and reader
- replay saved transactions
- two phones: proxy and relay, read card over great distances

NFCGate



- relay communication between card and reader
  - ⇒ read cards over great distances
  - ⇒ eavesdropping

NFCGate



Source: NFCGate

Section 5

Sources

Sources

What is NFC: WikiDE, WikiEn, NFC-Forum, CONGSTAR

Wikipedia on RFID: WikiDE

RFID Basics (German): RFID Grundlagen

Difference NFC - RFID (German): Fakir.it

NFC Security: *Access Granted: On the Security of Near-Field Enabled Keycards* by Stephen J. Jones

Tool NFCProxy: NFCProxy

Tool NFCGate: NFCGate, NFCGate Video