NFC Applications and Programming

Jonathan Rapp

Overview of NFC

NFC - Near Field Communication

- Wireless data transfer
- Minimal power (host powers device)

RFID - Radio Frequency Identification

- Predecessor to NFC
- EM fields for data transmission

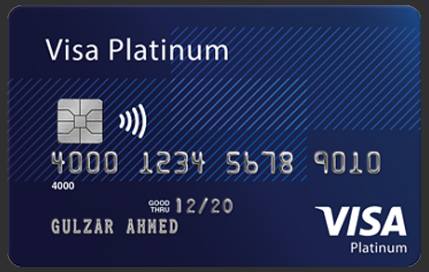
How NFC is Used

Day to day

- Commerce
- Identification / access tokens

Other instances

- Gaming
- Smartphone enhancements
- Sports



Components to Using NFC

Readers / Writers

- Smartphone
- External USB device (ACR122U)

Data Containers

- Tags
- Cards
- Figurines

Getting Started

Hardware Requirements

- A reader/writer
- NFC tag(s)

Software Requirements

- Library of choice
  - pyscard, nfcpy, nfctools, libnfc

Research

- Whatever you want to use

Utilizing the Reader and Cards

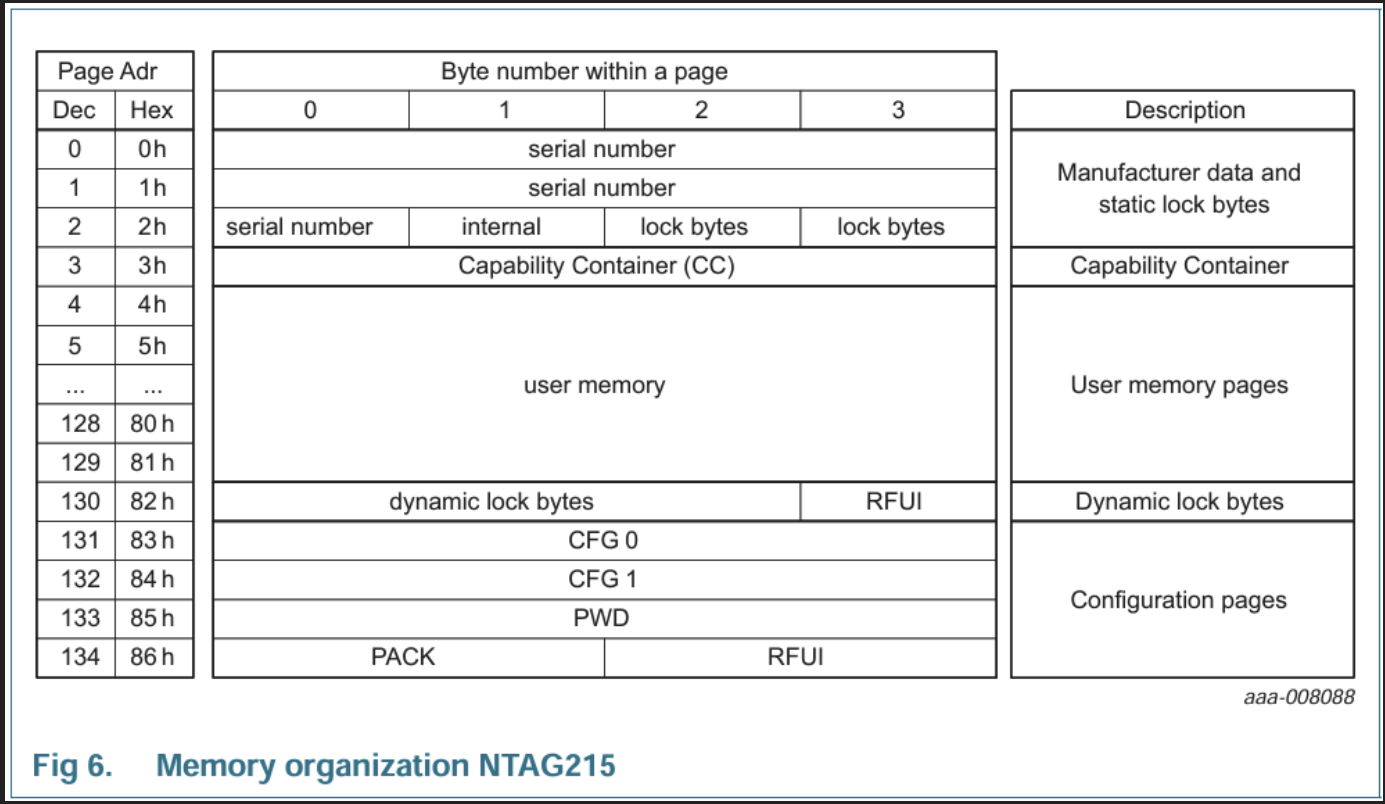
Reader/writer - ACR122U

- USB interface with computer
- Setup depends on OS
  - Windows is driver hell

NFC cards - NTAG215

- 540 bytes total (135 pages x 4 bytes)
- 504 bytes user read/write memory
- Rest is manufacturer, config, lock data

NTAG215 Memory Map



Page Adr		Byte number within a page				Description
Dec	Hex	0	1	2	3	
0	0h	serial number				Manufacturer data and static lock bytes
1	1h	serial number				
2	2h	serial number	internal	lock bytes	lock bytes	
3	3h	Capability Container (CC)				Capability Container
4	4h	user memory				User memory pages
5	5h					
...	...					
128	80 h					
129	81 h					
130	82 h	dynamic lock bytes			RFUI	Dynamic lock bytes
131	83 h	CFG 0				Configuration pages
132	84 h	CFG 1				
133	85 h	PWD				
134	86 h	PACK		RFUI		

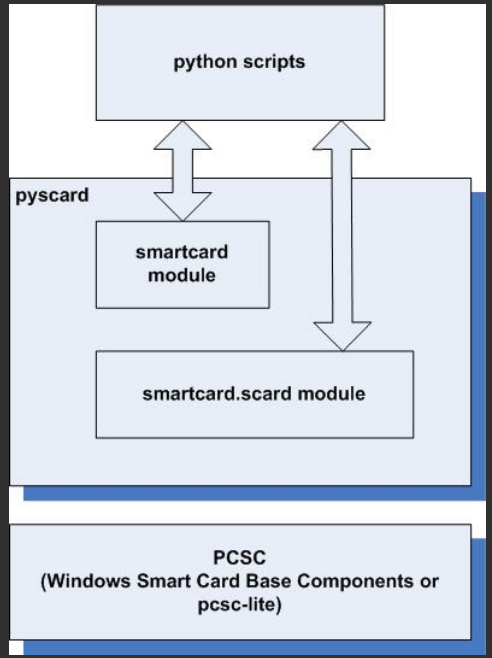
aaa-008088

Fig 6. Memory organization NTAG215

Pyscard Library Overview

Main points

- Built on PCSC API python wrapper
  - Personal Computer / Smart Card
- Development framework
- Supports Windows, MacOS, Linux



Research the Setup

Know the formats

- API of the reader/writer
- Type/standard of NFC tags
- Standard vs. custom data encoding
- Communicating - APDUs

APDU Commands

APDU - Application Protocol Data Unit

- 4 byte header - class, instruction, 2 parameters
- Send - 1 byte length, data
- Receive - 2 byte response, data

CLA	INS	P1	P2	Lc	data	→	RES	SW1	SW2
FF	B0	00	xx	yy	[]	→	[...]	90	00
FF	D6	00	xx	yy	[...]	→	[]	90	00

Demonstration Setup

Components

- ACR122U reader/writer
- NTAG215 NFC cards
- Python w/ pyscard

Goal

- Read/write data
- Build custom data encoding
- Other stuff won’t be covered

Demo and Tutorial Time

Sources

Broad NFC overview - https://www.techradar.com/news/what-is-nfc

Pyscard user guide - https://pyscard.sourceforge.io/user-guide.html

NTAG215 documentation - https://www.nxp.com/docs/en/data-sheet/NTAG213_215_216.pdf

ACR122U documentation - http://www.acs.com.hk/drivers/eng/API_ACR122U_v2.00.pdf

Misc APDU sends - https://web.archive.org/web/20090630004017/http://cheef.ru/docs/HowTo/APDU.info

Misc APDU receives - https://web.archive.org/web/20090623030155/http://cheef.ru/docs/HowTo/SW1SW2.info

Various format documentation - https://nfc-tools.github.io/resources/standards/iso14443A/