POZNAN UNIVERSITY OF TECHNOLOGY
CHAIR OF COMMUNICATIONS AND COMPUTER NETWORKS

SECURITY OF NFC TRANSMISSION IN BANKING APPLICATIONS

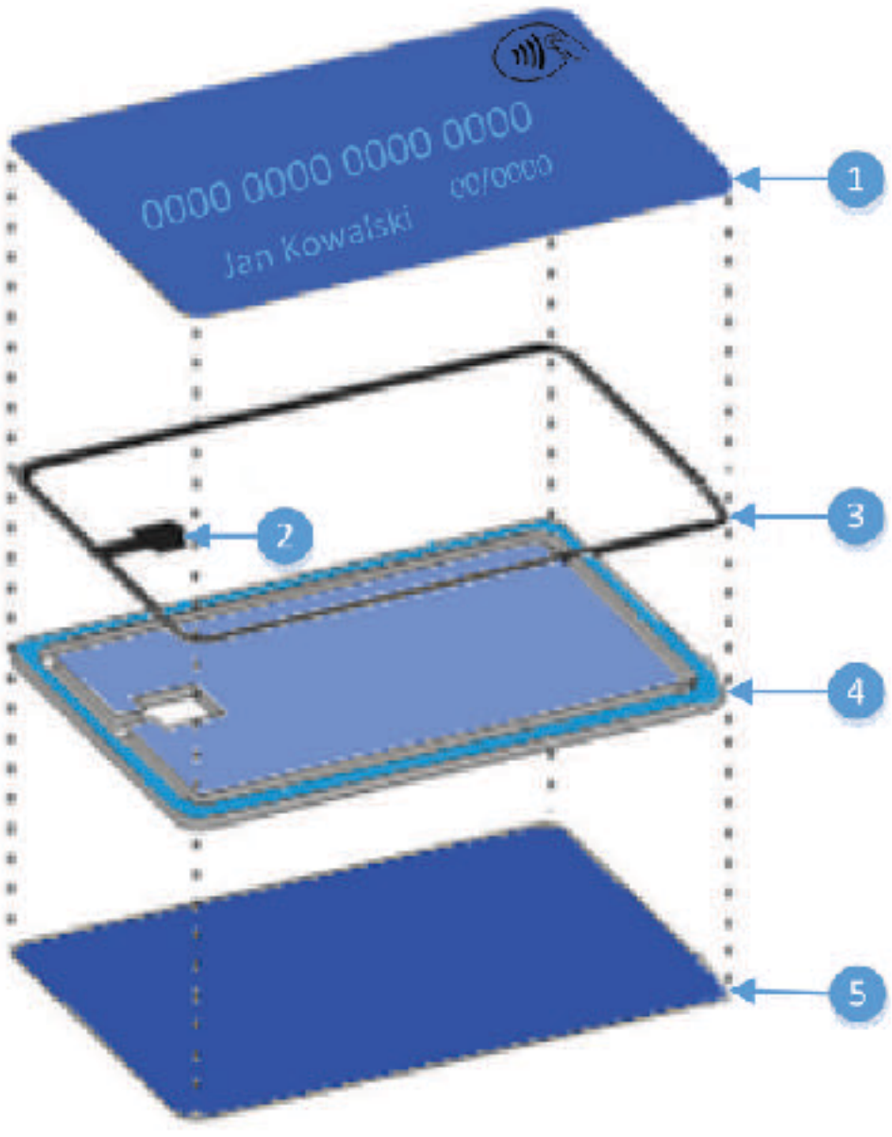
Author: Michał Weissenberg

PRESENTATION PLAN

1. PAYMENT CARD
2. WHAT IS NFC?
3. NFC IN BANKING APPLICATIONS
4. INFORMATION STORED ON THE PAYMENT CARD
5. HOW TO READ THE DATA FROM CARD?
6. SCENARIO OF ATTACK
7. WHAT NEXT?
8. HOW TO SECURE THE PAYMENT CARD?
9. SUMMARY

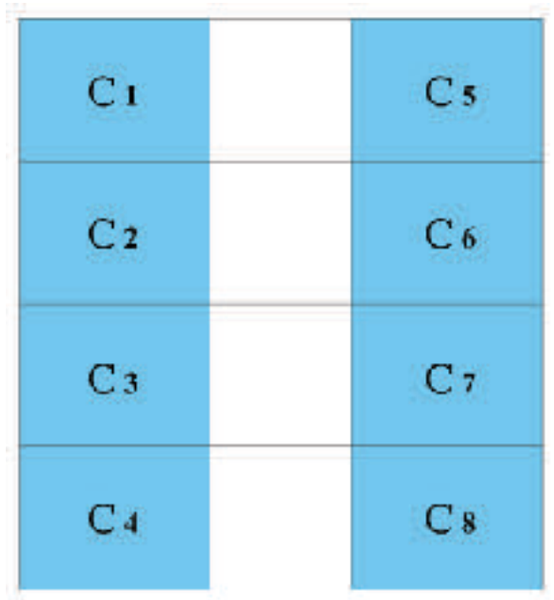
1. PAYMENT CARD

Structure



1. Card Front
2. Chip Module
3. Antenna
4. Inlay
5. Card Back

Contact designation



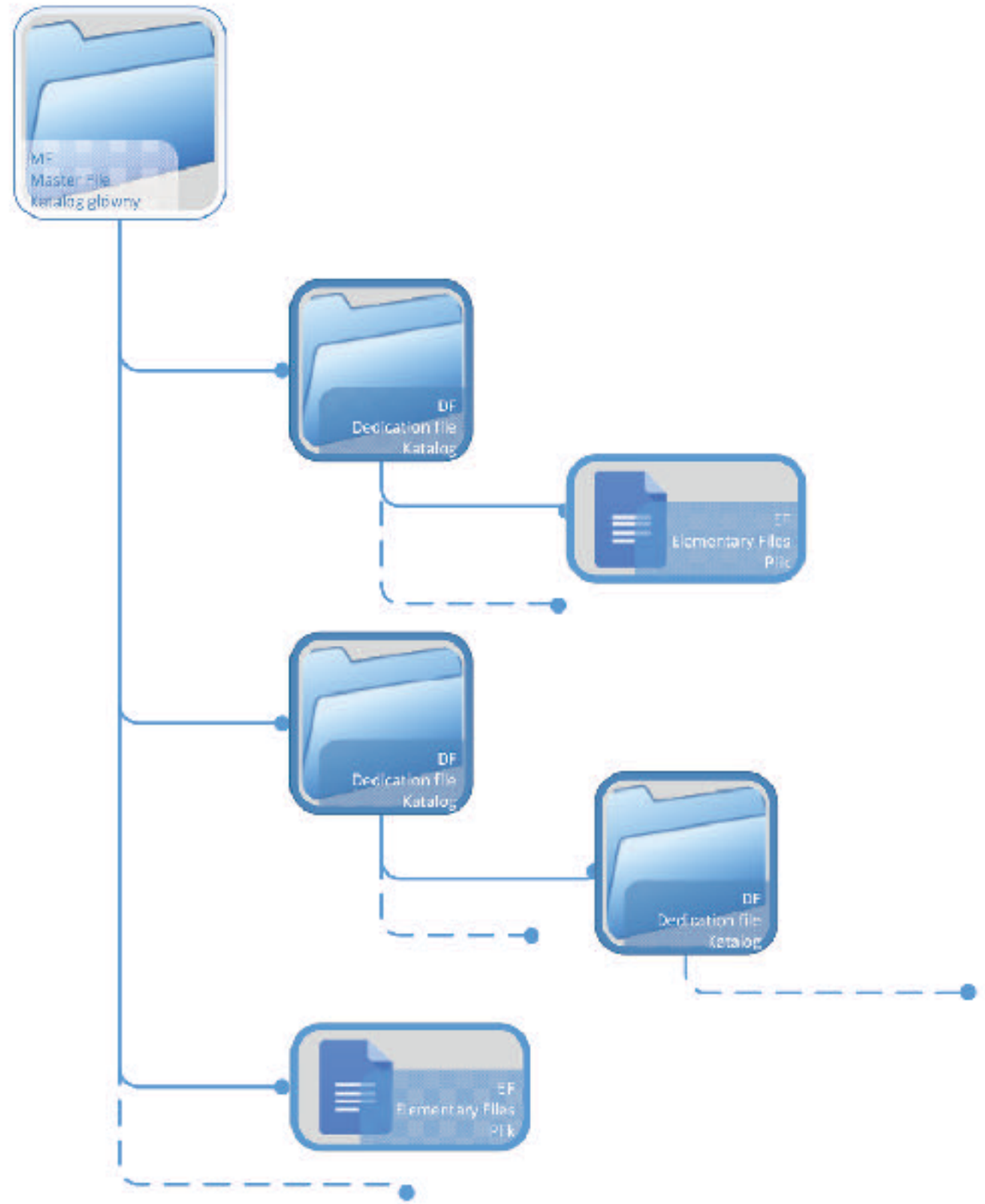
C1 - Vcc
C2 - RST
C3 - CLK
C4 & C8 - RFU
C5 - GND
C6 - Vpp
C7 - I/0

MasterCard PayPass™ *Mag Stripe, Acquirer Implementation Requirements*. 2006.

1. PAYMENT CARD

Data structure

1. Master Files
2. Dedicated Files
3. Elementary Files



1. PAYMENT CARD

Connection

1. Connection Client - Server

2. Used APDU frame

CLA	INS	P_1	P_2	L_c	DATA	L_e

Connection

DATA	SW_1	SW_2

Answer

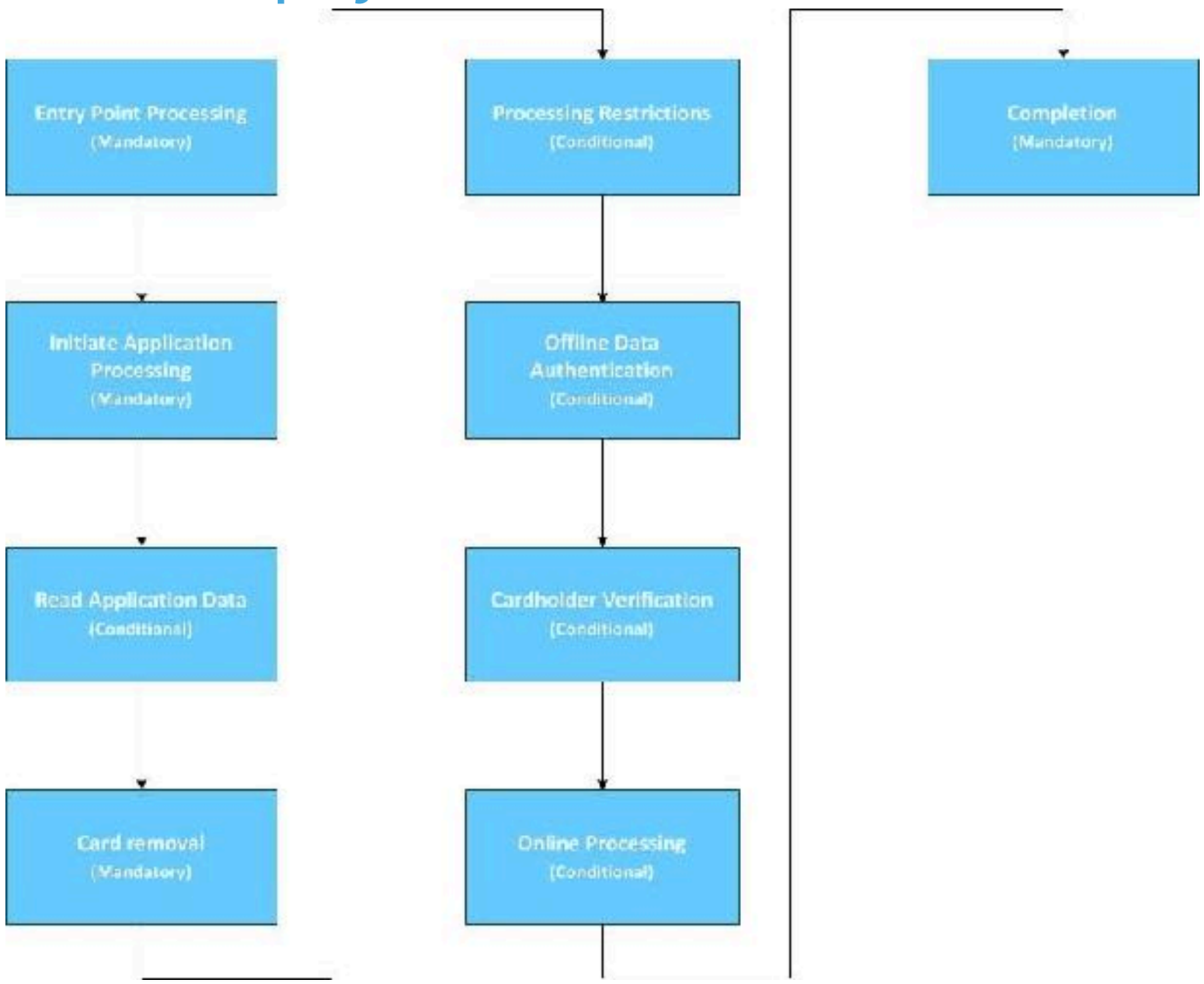
2. WHAT IS NFC?

NFC (Near Field Communication)

- Short-range wireless technologies,
- Typically requiring a separation of 10 cm or less., for payment 5 cm or less,
- NFC operates at 13.56 MHz
- Rates ranging from 106 kbit/s to 424 kbit/s.
- NFC always involves an initiator and a target
- Q&A transmission
- NFC peer-to-peer communication is possible, provided both devices are powered

3. NFC IN BANKING APPLICATION

Contactless payment



https://www.level2kernel.com/emv-visa-contactless-kernel.html

4. INFORMATION STORED ON THE PAYMENT CARD

Explicit Data

- Name and surname of the card holder
- Card expiration date
- Card number
- Number of magnetic strip 1
- Number of magnetic strip 2

Classified data

- PIN code
- Symmetric ciphers
- Public and private key
- Customer account number
- Software
- Login history

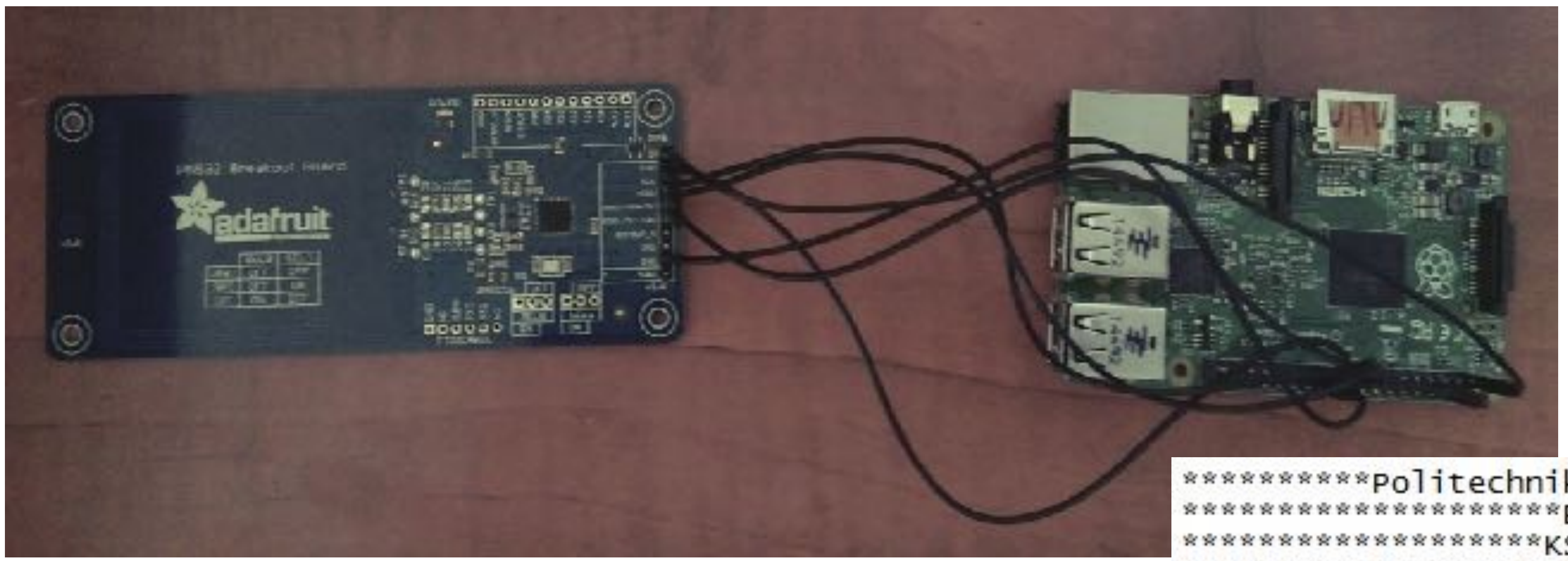
5. HOW TO READ DATA FROM THE CARD

Device and software

- Devices:
  - Raspberry Pi II
  - Adafruit PN532 Breakout Board
- Software:
  - Creating in C++

5. HOW TO READ DATA FROM THE CARD

Device and software




```
**********Politechnika Poznanska**********
*******************EiT*******************
******************KSTiK******************
****Czytanie danych z kart platniczych****
************Michal Weissenberg************

Przyloz karte
***Rozpoznanie urzadzenia***
Laczenie........

Aplikacja: DEBIT MASTERCARD
Priorytet: 0
AID: A0000000041010

Preferowany jezyk: plen
Dane wlascicela karty: WEISSENBERG/MICHAL
Track 1: 30303XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX0
Track 2: 53965XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXF
PAN: 5396 XXXX XXXX 6137
Data waznosci: 11/2013
Licznik logowan: 10
```

6. SCENARIO OF ATTACK

Relay Attack

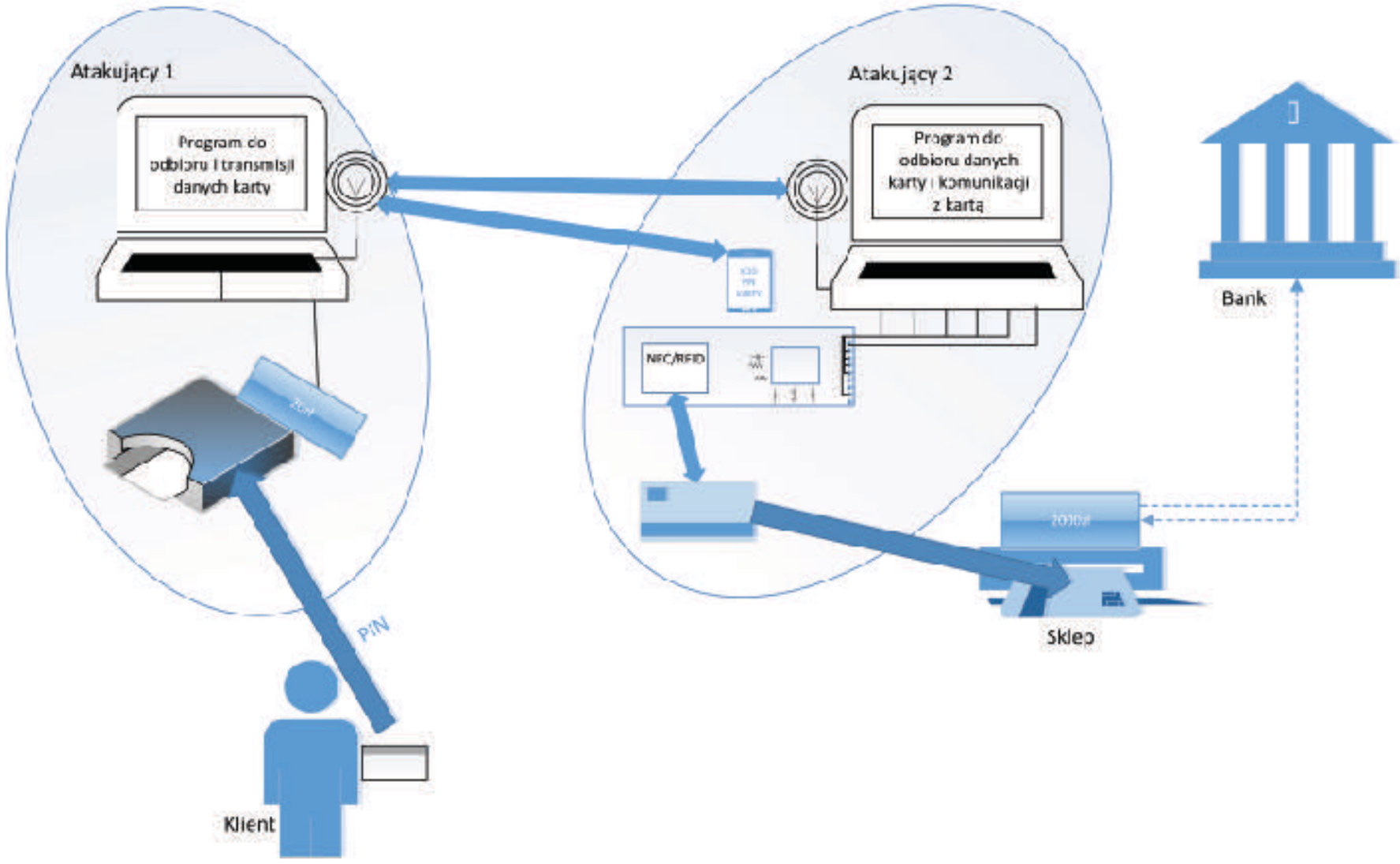
- Mafia fraud
- Attack by smartphone with NFC application

Clone Card

- Attack by smartphone with NFC application

6. SCENARIO OF ATTACK

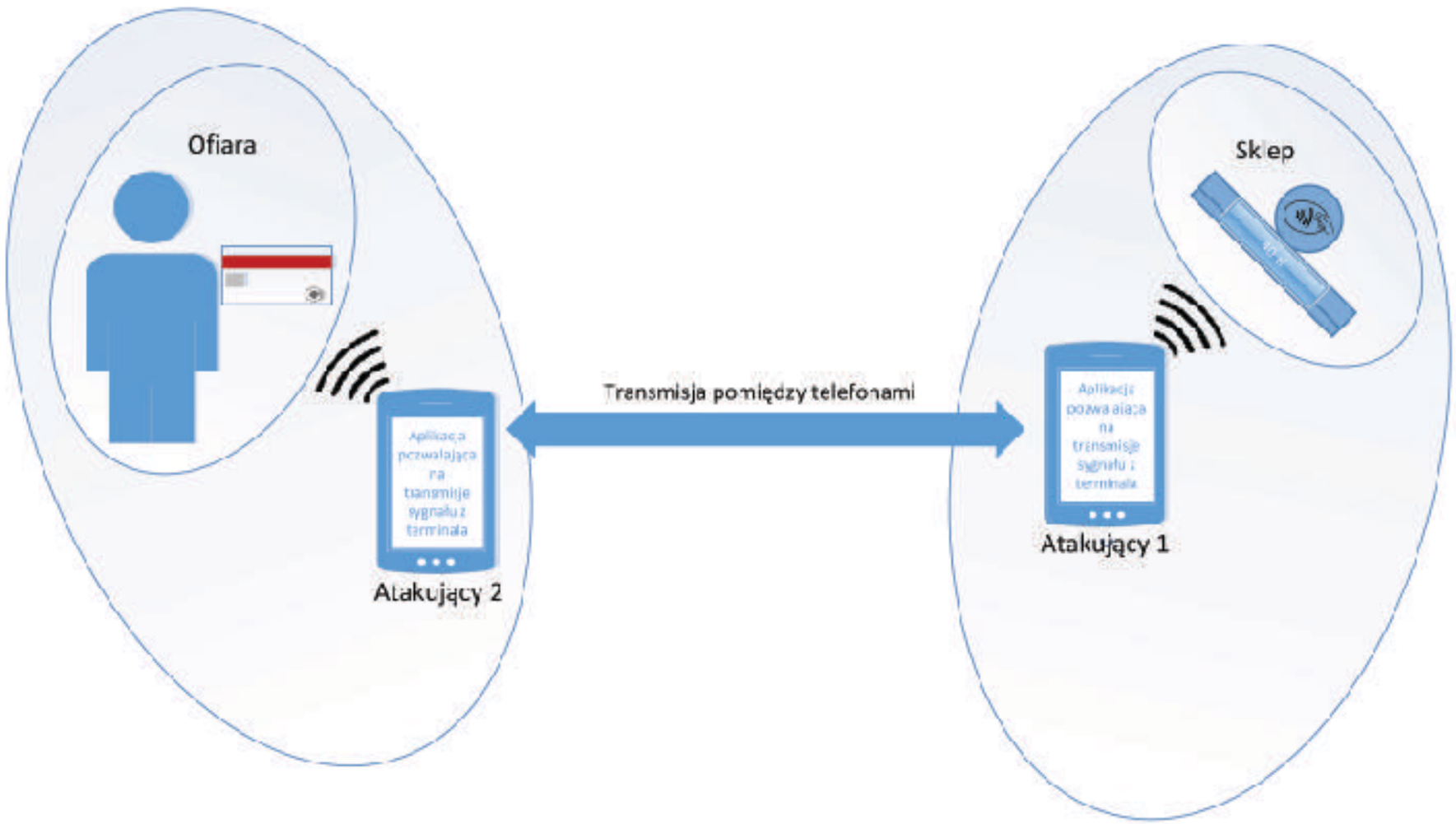
Relay Attack - Mafia Fraud



. S. Drimer, S.J. Murdoch, *Keep Your Enemies Close: Distance Bounding Against Smartcard Relay Attacks,* in USENIX Security Symposium, August 2007.

6. SCENARIO OF ATTACK

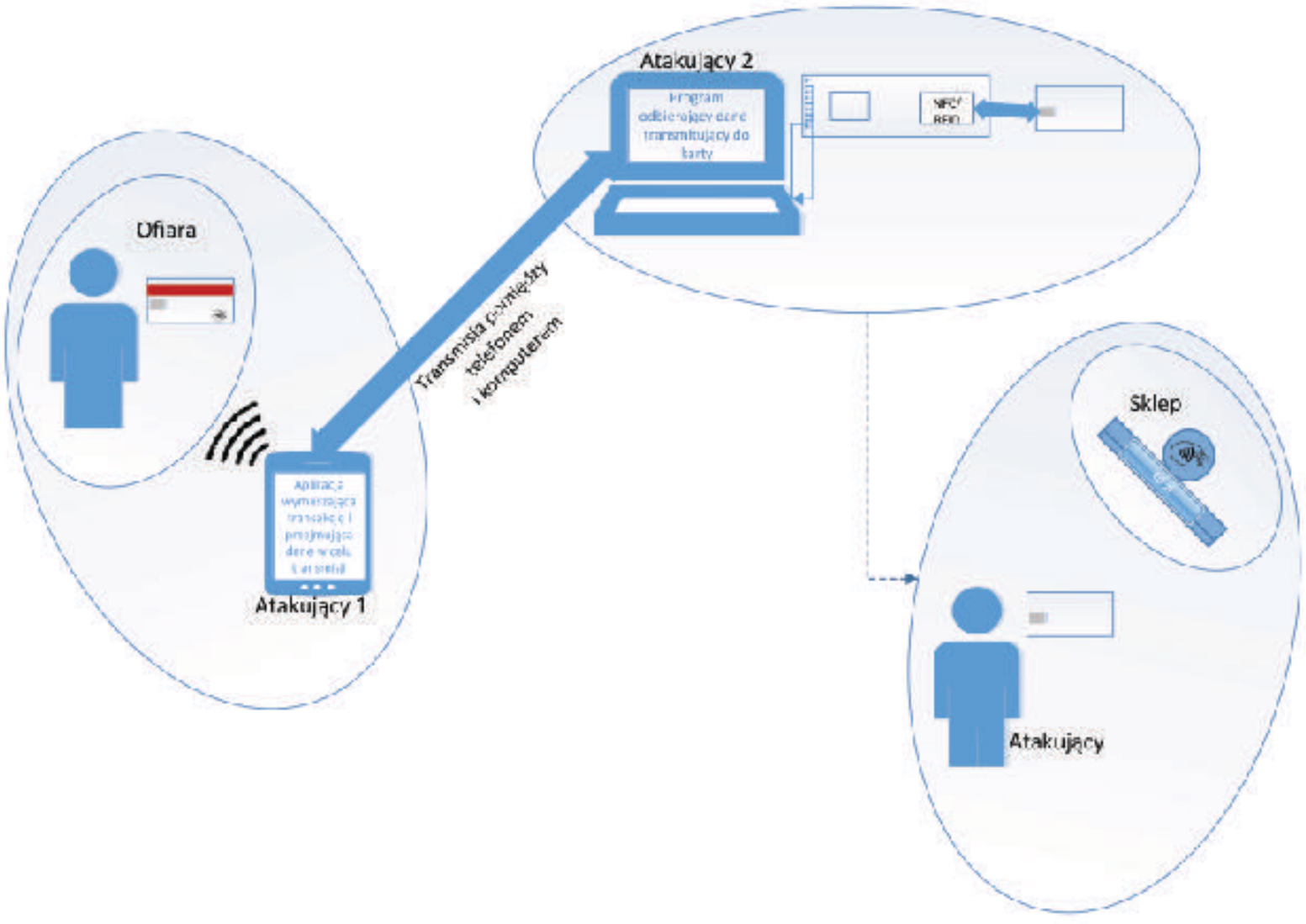
Relay Attack - Attack by smartphone with NFC



. L. Francis, G.d Hancke, K. Mayes, K. Markantonakis, *Practical Relay Attack on Contactless Transactions by Using NFC Mobile Phones*, Royal Holloway University of London, 2011.

6. SCENARIO OF ATTACK

Clone Card - Attack by smartphone with NFC



7. WHAT NEXT?

Creating an application that allows a relay attack

Issues:

- Secure communication channel
- Transmission delay
- Law in Poland and bank restrictions

8. HOW TO SECURE THE PAYMENT CARD

Simple Methods

- Shielded wallets and cases
- Aluminium foil
- Being alert

Proposed changes

- Geolocation

9. SUMMARY

- Contactless payments are one of the most popular payment systems
- Methods of authorization and security of the payment cards are constantly evolvin
- The payment cards aren’t currently resistant to relay attack
- The cardholder's personal data and basic card information about their payment ca be read without using the cryptographic systems
- Summing up:
  - It is very important to care of the security of your payment card