NFC Principles and Vulnerabilities

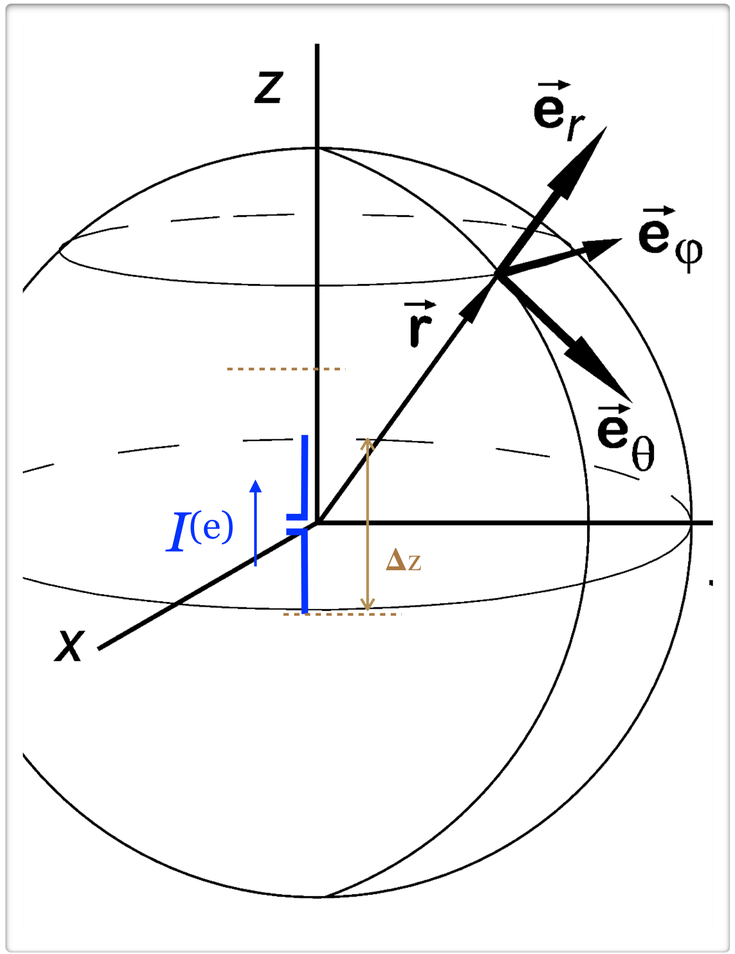
Tomáš Rosa
Cryptology and Biometrics Competence Centre of Raiffeisen Bank International
Department of Algebra, Faculty of Mathematics and Physics, Charles University in Prague

The Ideal Electric Dipole

- Electrically small, i.e. $\Delta z \ll \lambda$, uniform amplitude current element.
  - Ordinary dipole is covered by integration over these elements.
- In the far field, a donut-like pattern bearing the vertical polarisation is produced.
- In general, its field has the following components:

$$\vec{E}_{edp}(I^{(e)}) = E_{edp,\theta}(I^{(e)}) \cdot \hat{e}_{\theta} + E_{edp,r}(I^{(e)}) \cdot \hat{e}_{r}$$

$$\vec{H}_{edp}(I^{(e)}) = H_{edp,\phi}(I^{(e)}) \cdot \hat{e}_{\phi}$$



(illustration purpose only)

Ideal Dipole Element Radiation

$$\vec{H}_{edp}(I^{(e)}) = \frac{I^{(e)}\Delta z}{4\pi} j\beta\left(\frac{1}{r} + \frac{1}{j\beta r^2}\right)e^{-j\beta r}\sin\theta\cdot\hat{e}_{\phi}$$

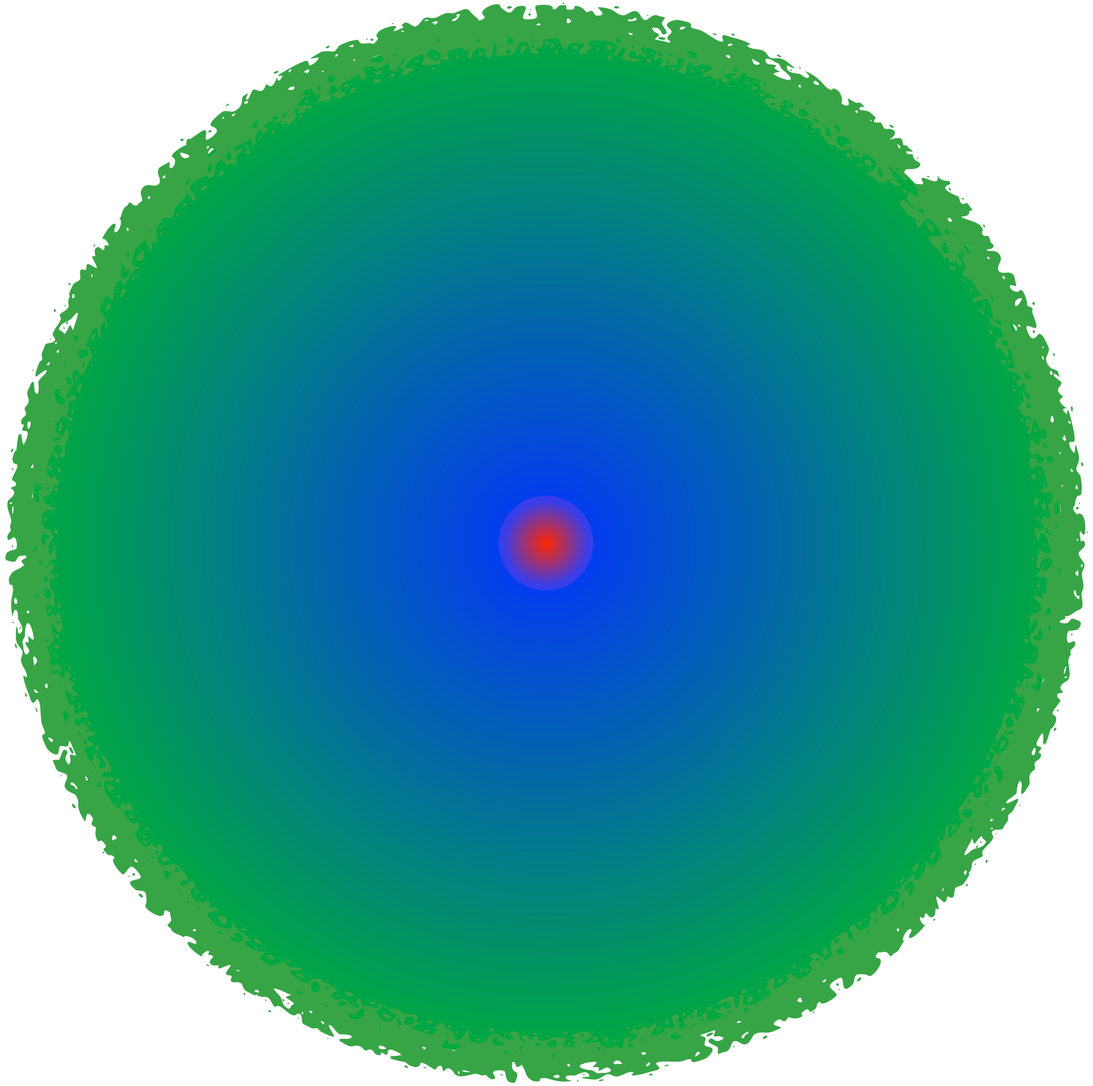
$$\vec{E}_{epd}(I^{(e)}) = \frac{I^{(e)}\Delta z}{4\pi} j\omega\mu\left(\frac{1}{r} + \frac{1}{j\beta r^2} - \frac{1}{\beta^2 r^3}\right)e^{-j\beta r}\sin\theta\cdot\hat{e}_{\theta}$$

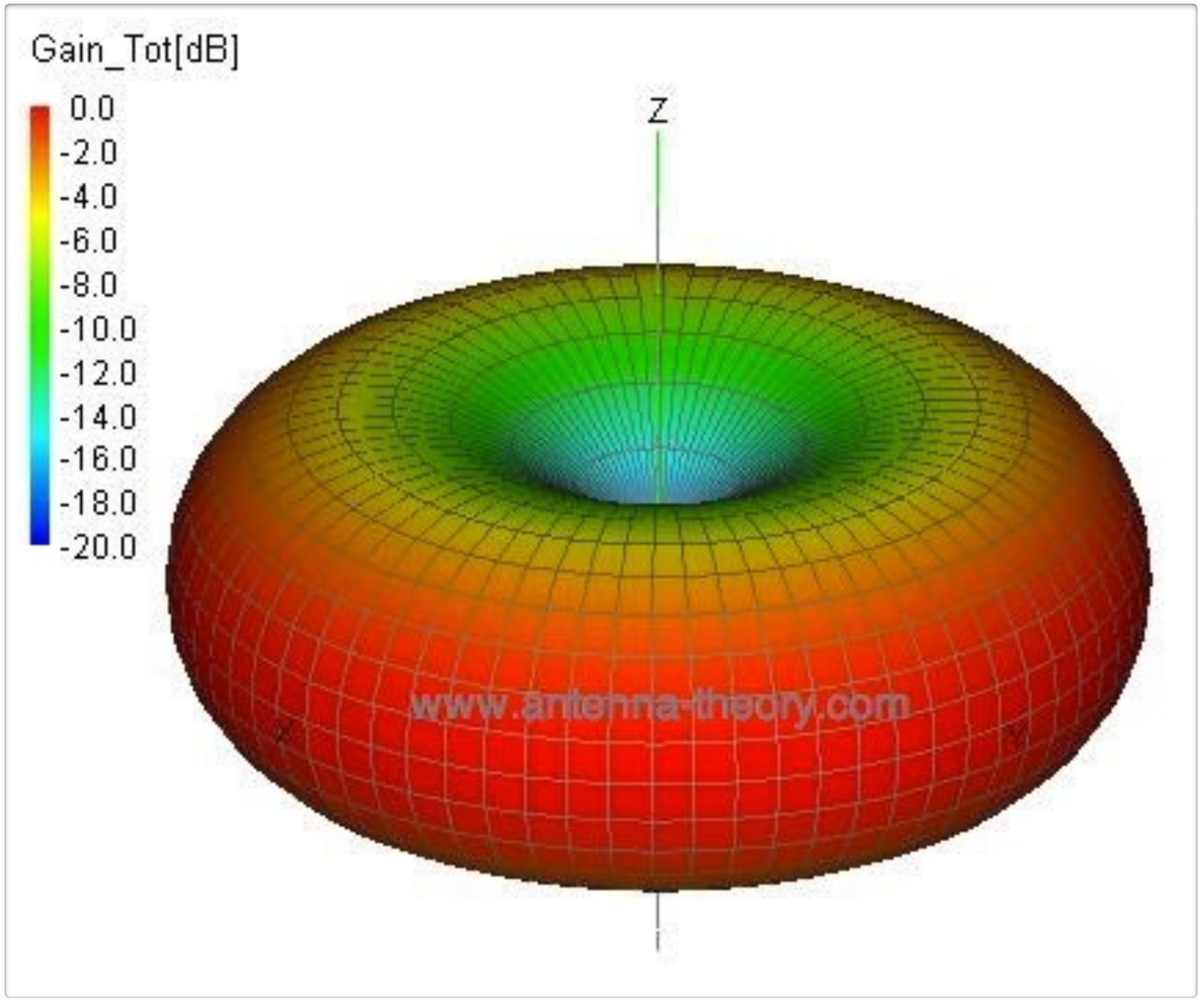
$$+\frac{I^{(e)}\Delta z}{2\pi} j\omega\mu\left(\frac{1}{j\beta r^2} - \frac{1}{\beta^2 r^3}\right)e^{-j\beta r}\cos\theta\cdot\hat{e}_{r}$$

$$= \frac{I^{(e)}\Delta z}{4\pi} j\omega\mu\left(\frac{1}{r} + \frac{1}{j\beta r^2} - \frac{1}{\beta^2 r^3}\right)e^{-j\beta r}\sin\theta\cdot\hat{e}_{\theta}$$

$$+\frac{I^{(e)}\Delta z}{2\pi}\eta\left(\frac{1}{r^2} - j\frac{1}{\beta r^3}\right)e^{-j\beta r}\cos\theta\cdot\hat{e}_{r}$$

Electromagnetic Radiation Regions





(illustration purpose only)

The Small loop

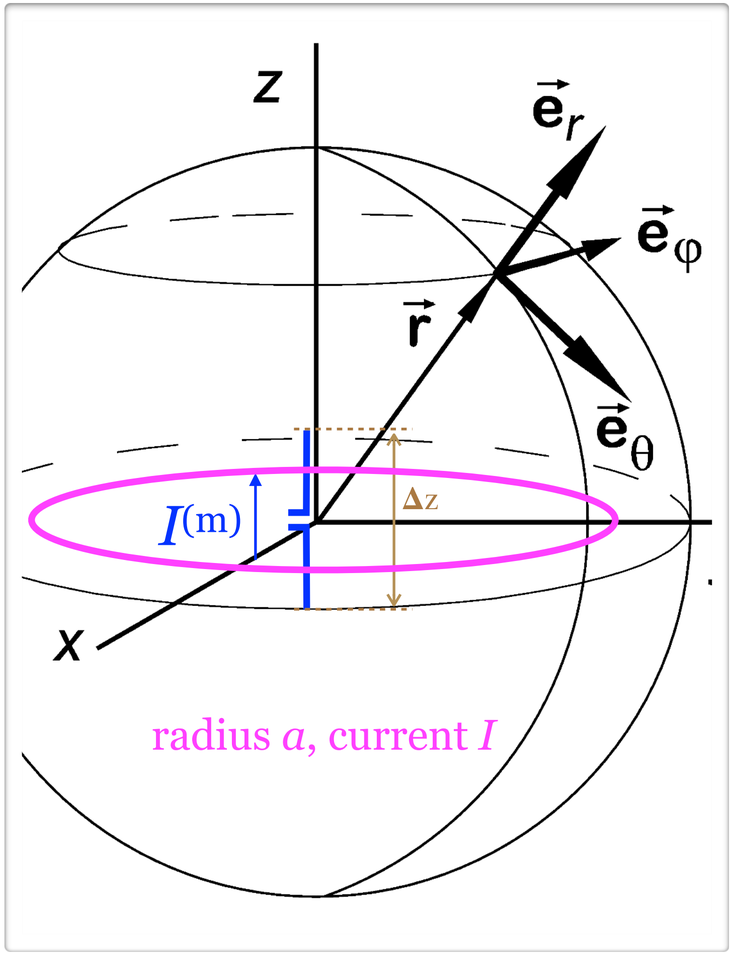
- Electrically small, i.e. $2\pi a < \lambda/10$, uniform amplitude current loop.
- Can be modelled as an ideal *magnetic* dipole which is the theoretical dual of the ideal electric dipole.
- The duality equations follow.

$$\vec{E}_{mdp}(I^{(m)}) \equiv -\vec{H}_{edp}(I^{(m)}),\ \vec{H}_{mdp}(I^{(m)}) \equiv \vec{E}_{edp}(I^{(m)})$$

$$\mu_{mdp} \equiv \varepsilon_{edp},\ \varepsilon_{mdp} \equiv \mu_{edp}$$

$$\beta_{mdp} = \omega\sqrt{\mu_{mpd}\varepsilon_{mdp}} = \omega\sqrt{\varepsilon_{edp}\mu_{edp}} = \beta_{edp}$$

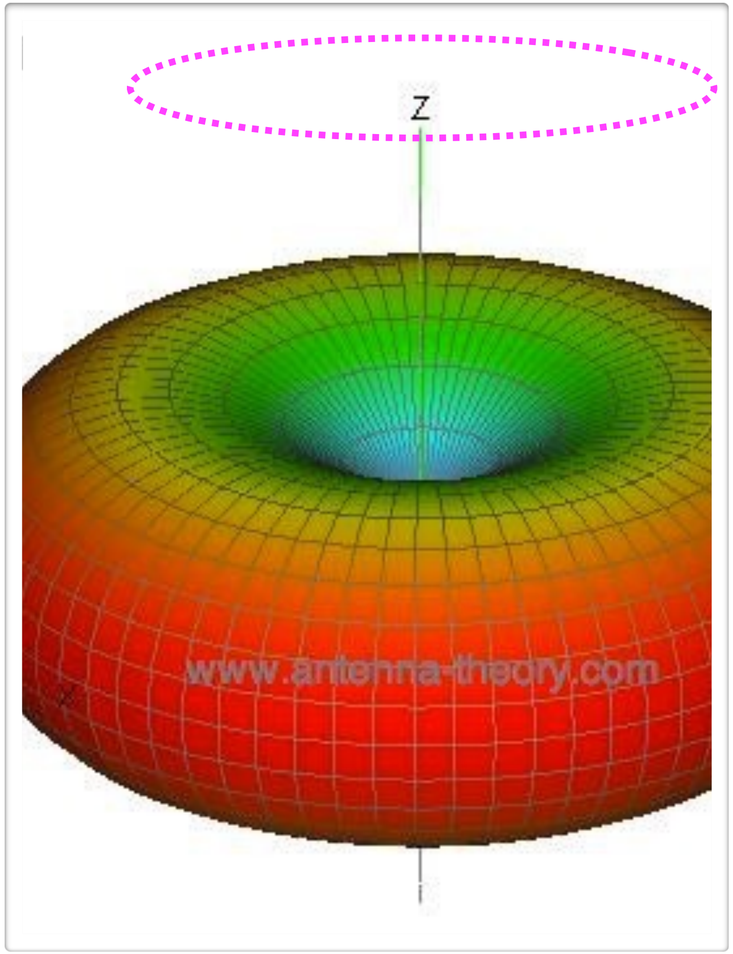
$$\text{note also } \beta = \frac{2\pi}{\lambda},\ v = \lambda f$$



(illustration purpose only)

Donut Pattern Again

- The duality with the ideal electric dipole tells us the *far field* has the donut-like form.
- The polarisation is reversed (!) - i.e. horizontal in place of vertical, now.
- In the *near field*, however, there is a significant radial component (cf. below).



(illustration purpose only)

Long Story Short

$$\vec{E}_{mdp}(I^{(m)}) = -\frac{I^{(m)}\Delta z}{4\pi} j\beta\left(\frac{1}{r} + \frac{1}{j\beta r^2}\right) e^{-j\beta r} \sin\theta \cdot \hat{e}_{\phi}$$

$$\vec{H}_{mpd}(I^{(m)}) = \frac{I^{(m)}\Delta z}{4\pi} j\omega\varepsilon\left(\frac{1}{r} + \frac{1}{j\beta r^2} - \frac{1}{\beta^2 r^3}\right) e^{-j\beta r} \sin\theta \cdot \hat{e}_{\theta}$$

$$+ \frac{I^{(m)}\Delta z}{2\pi} j\omega\varepsilon\left(\frac{1}{j\beta r^2} - \frac{1}{\beta^2 r^3}\right) e^{-j\beta r} \cos\theta \cdot \hat{e}_{r}$$

Magnetic Current of The Small Loop

$$I^{(m)}\Delta z = j\omega\mu IS$$

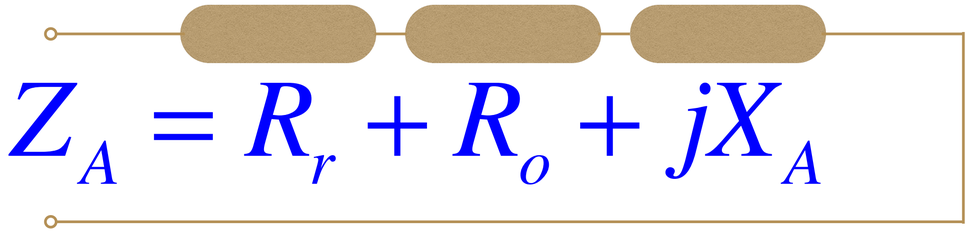
$$S = \pi a^2$$

—based on far field equivalence

Near, Far

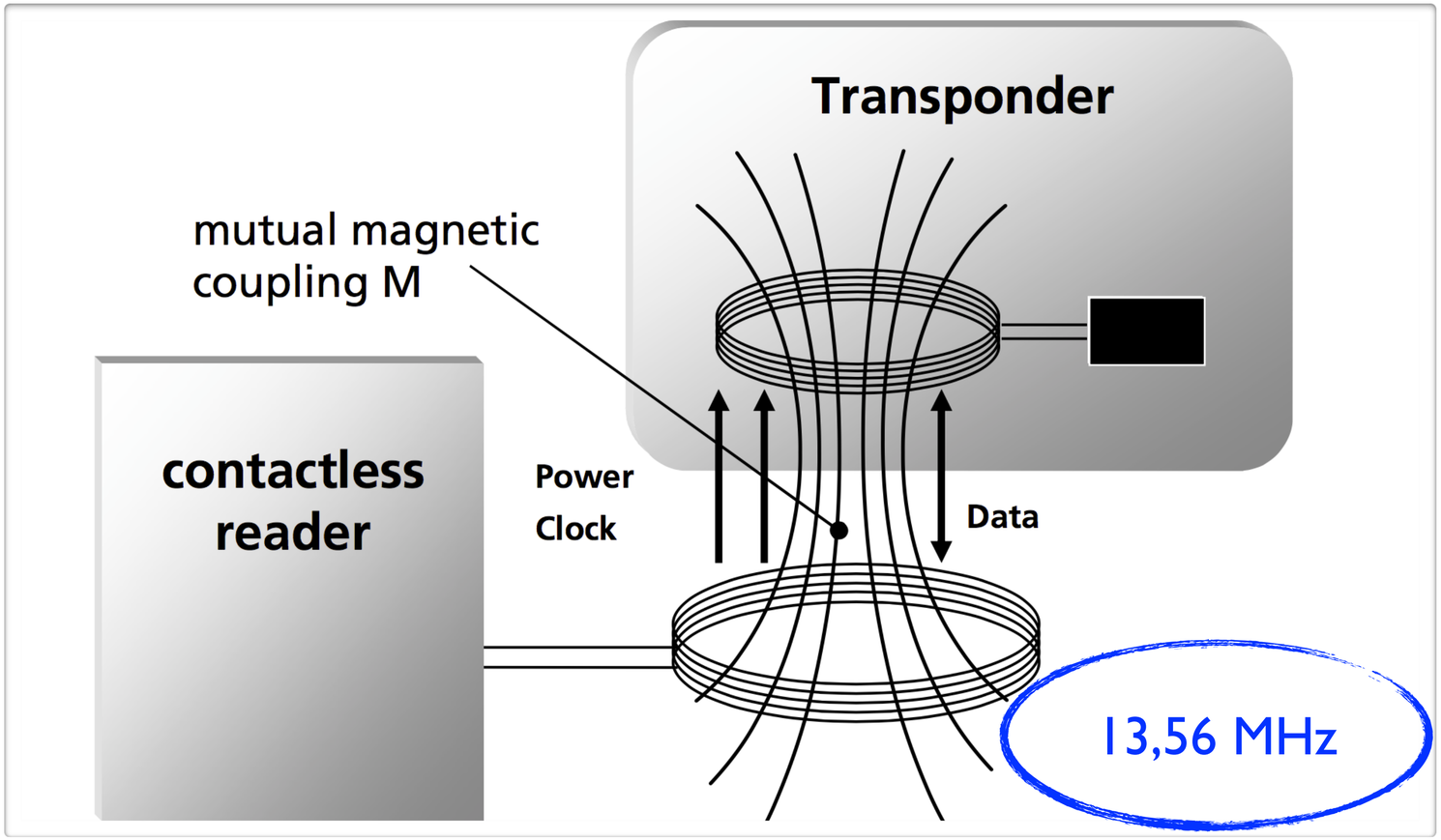
- Basing on the dominating *E*, *H* field terms, it is useful to distinguish:
  - *Reactive near field* (XNF), where the terms with $(1/r)^2$ and $(1/r)^3$ dominate. Energy is mainly stored and exchanged between *E* and *H*.
  - *Radiating near field* (Fresnel region), where the $(1/r)^2$ terms start to dominate, i.e. $r > \lambda/2\pi$. Energy is mainly radiated with unstable patterns, however.
  - *Far field* (Fraunhofer region), where the $1/r$ terms remain to dominate and the plane wave model can be used. Several conditions shall be met: $r > 2D^2/\lambda$, $r > 5D$, $r > 1.6\lambda$, where *D* is the largest antenna dimension. Energy is radiated with a distance-independent field pattern.

Antenna Impedance



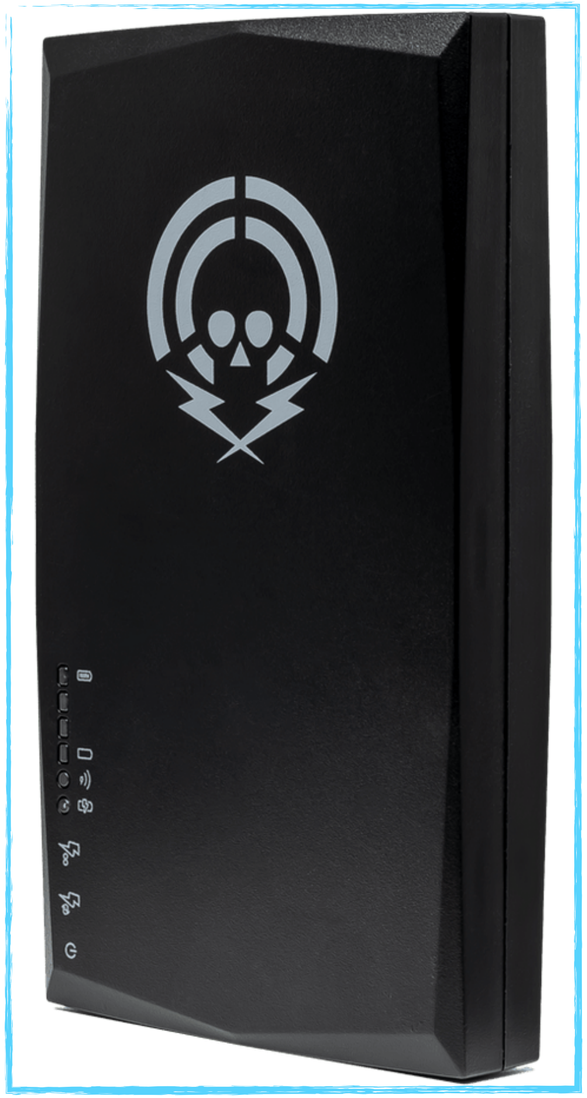
- The input impedance Z_A describes the antenna from the lumped circuit parameters viewpoint. *This is also useful to describe the antenna field action observable in those different field regions in a handy condensed way.*
  - R_r is the equivalent radiation resistance representing the energy emanated through the radio waves
  - R_o describes the dissipative energy loss
  - X_A reflects the energy exchanged back-and-forth with the reactive near field

Passive NFC Coupling

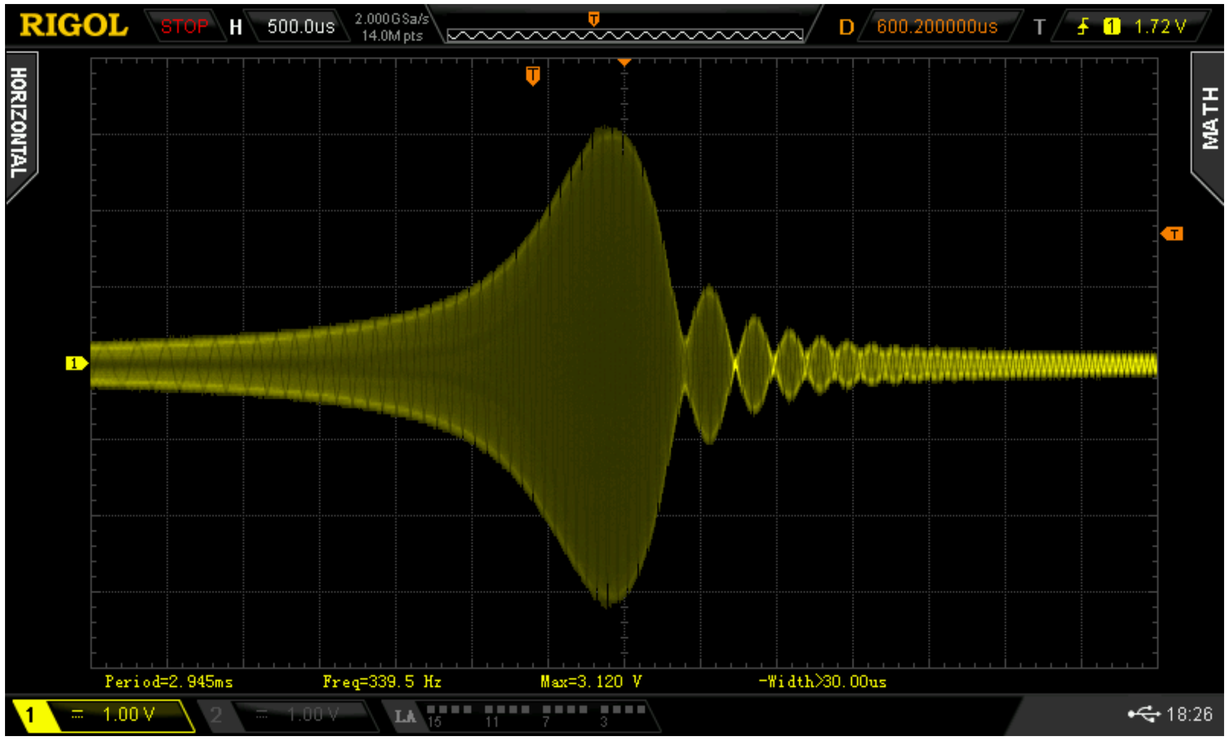


[Finkenzeller, K., 2011]

Contactless Micro-EMP Variant (NFCKill)

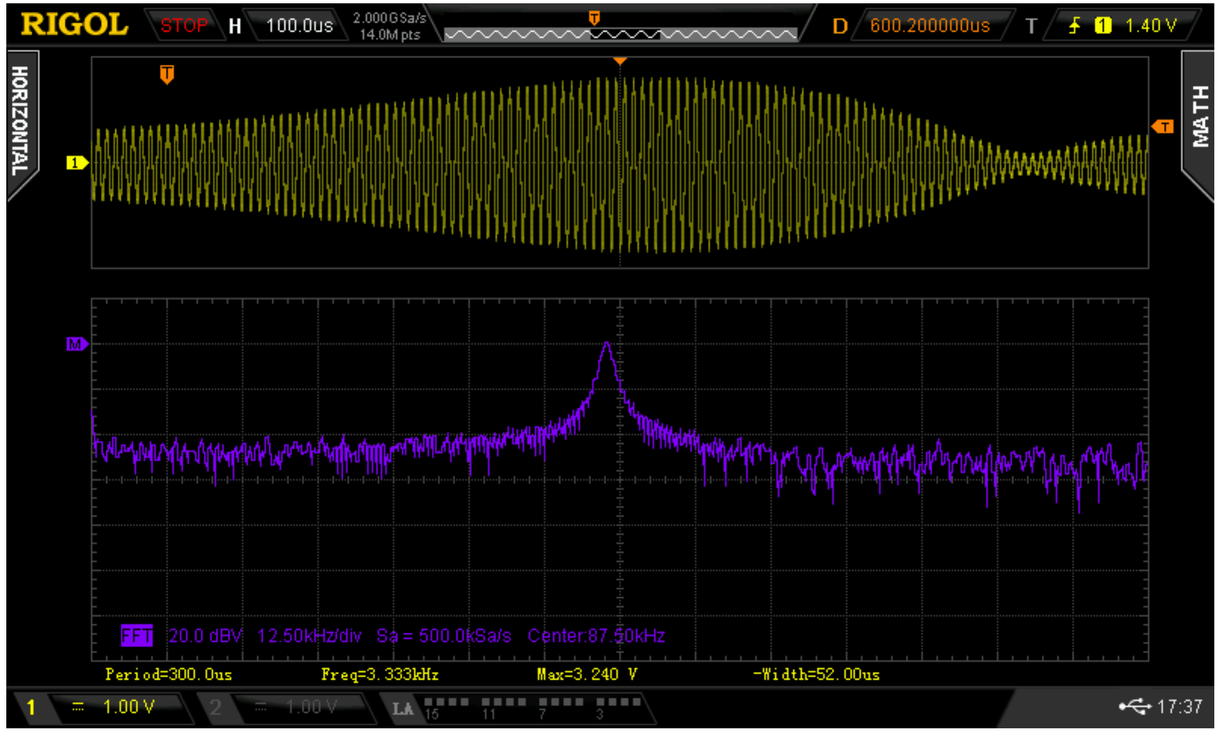


NFCKill Near-Field Magnetic Pulse (35 mm axial distance)

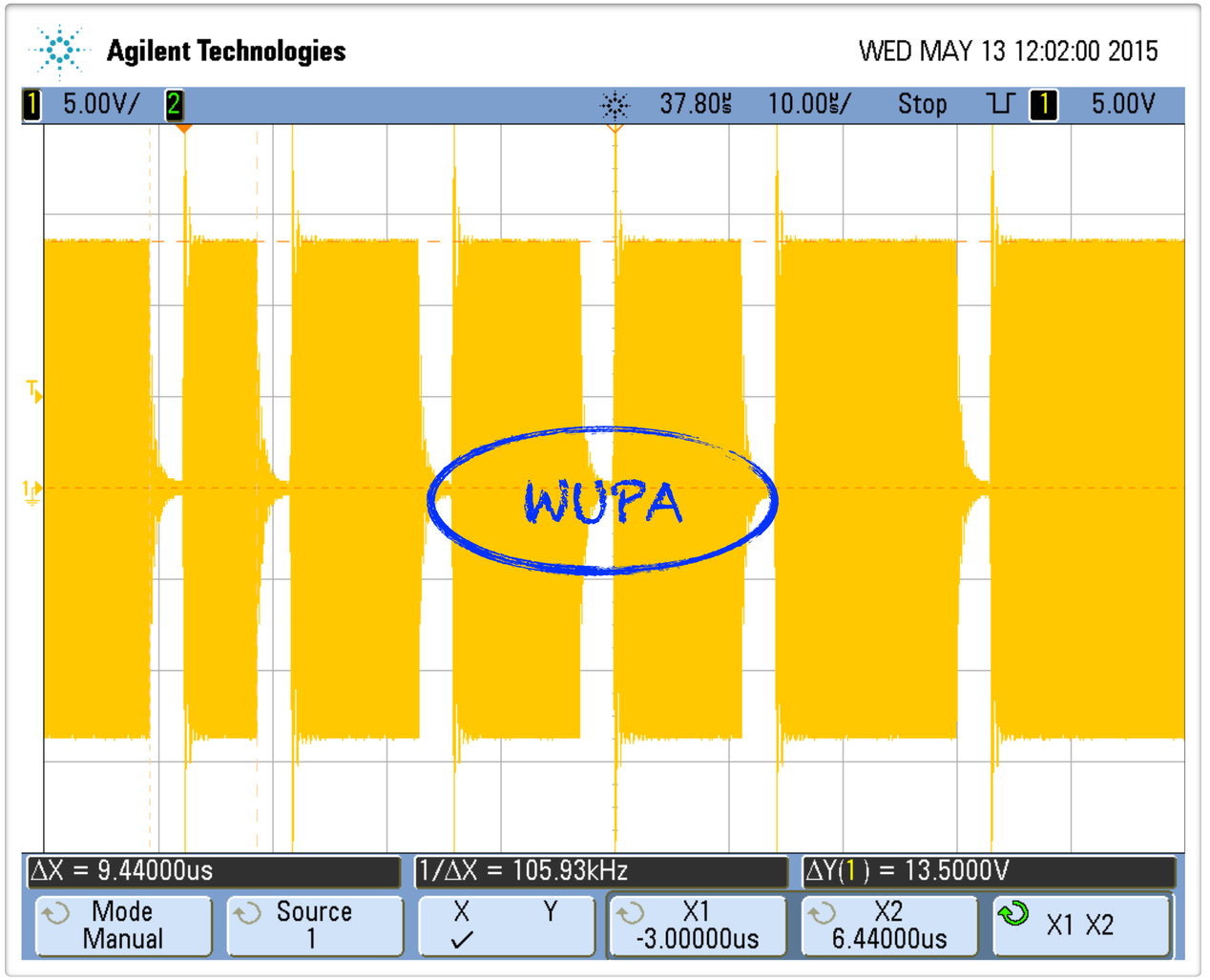


- Roughly 30-times higher peak value than for a regular NFC terminal (ACR122) in the same setup
- Will further raise sharply when approaching a closer distance
- Static discharge-like sensing observed at < 1 cm distance, their cause and effect remains unknown

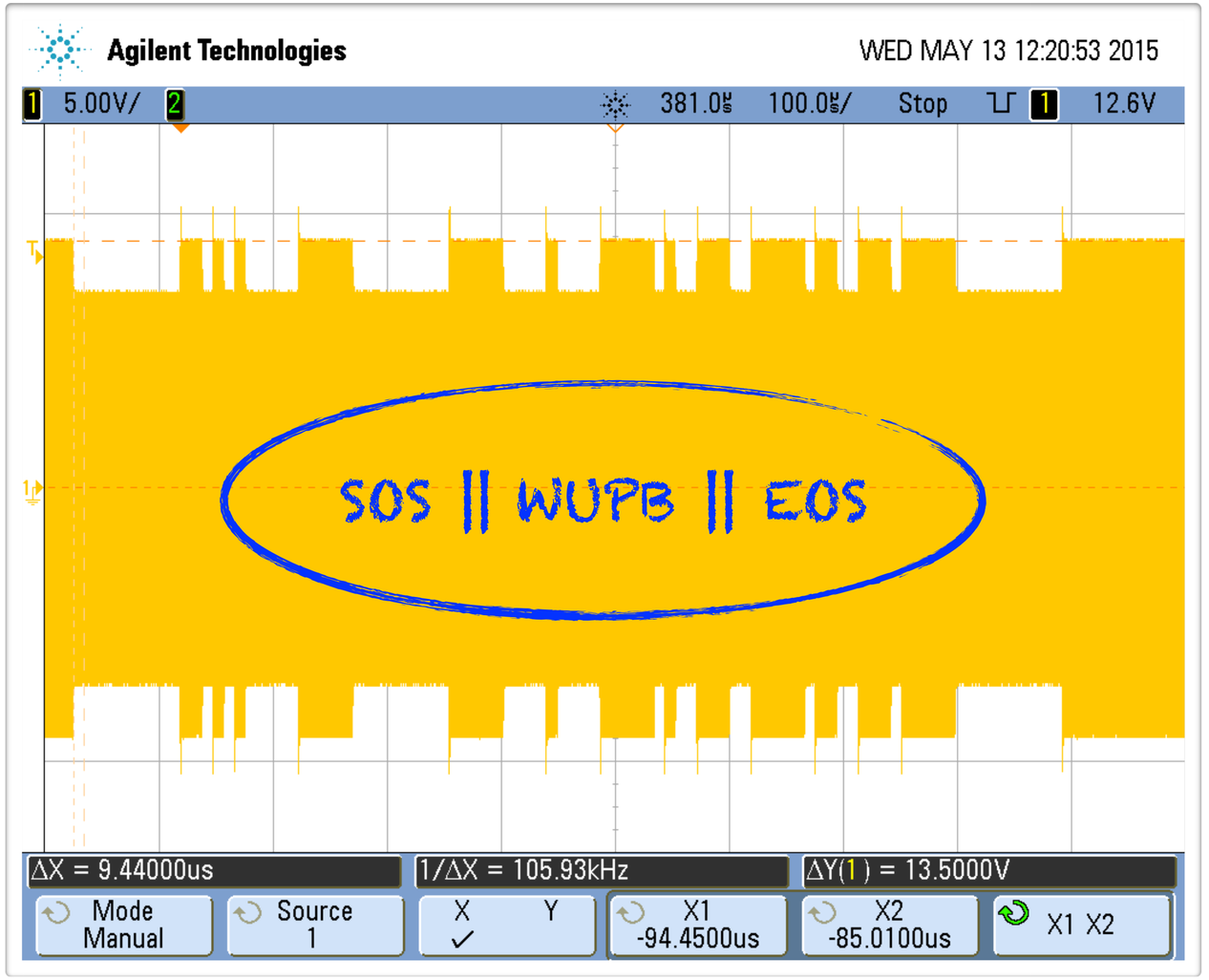
- Probably, there is a high-voltage generator discharged instantly into a primary coil, producing typical high-energy transients



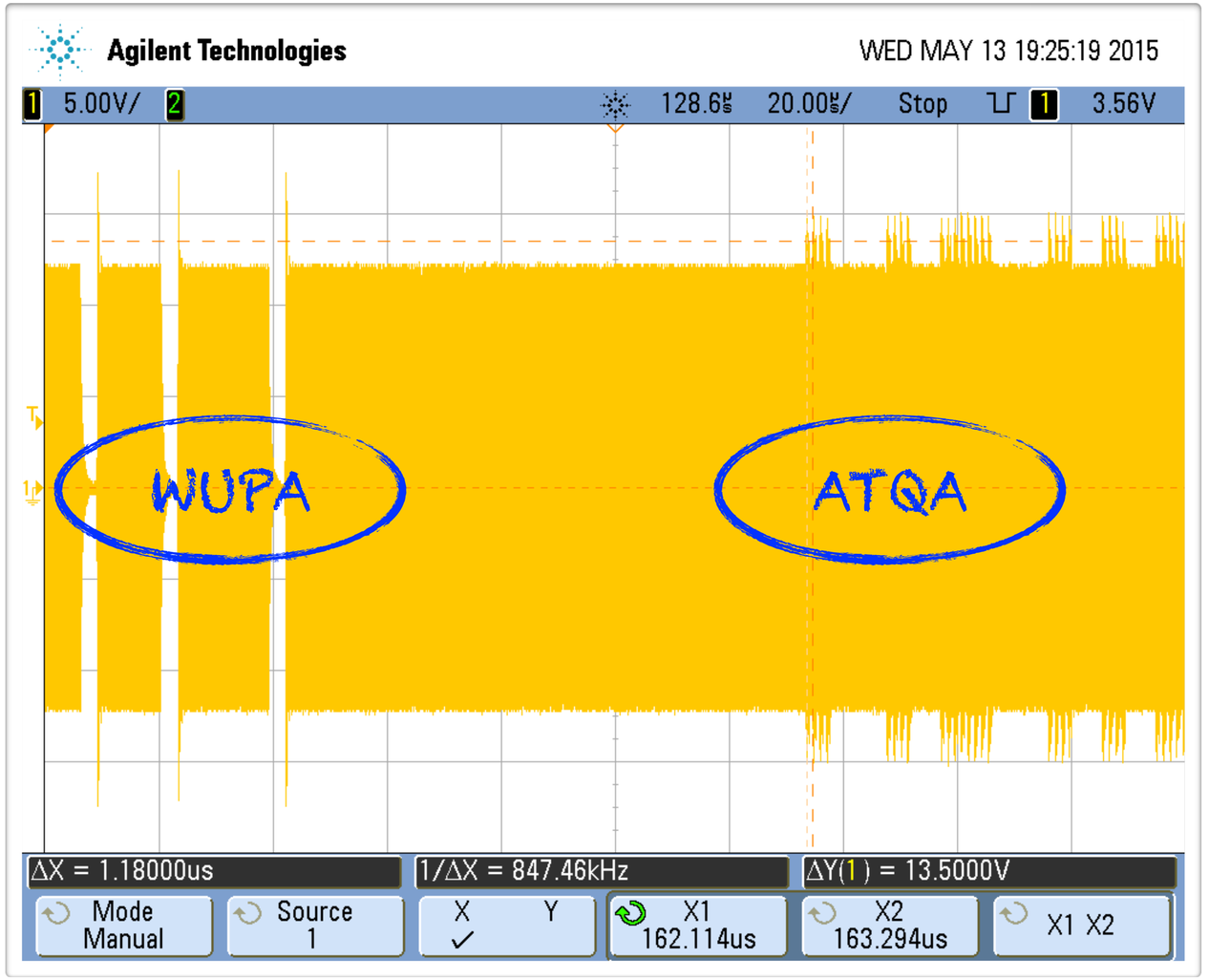
Initiator Speaking NFC-A



Initiator Speaking NFC-B

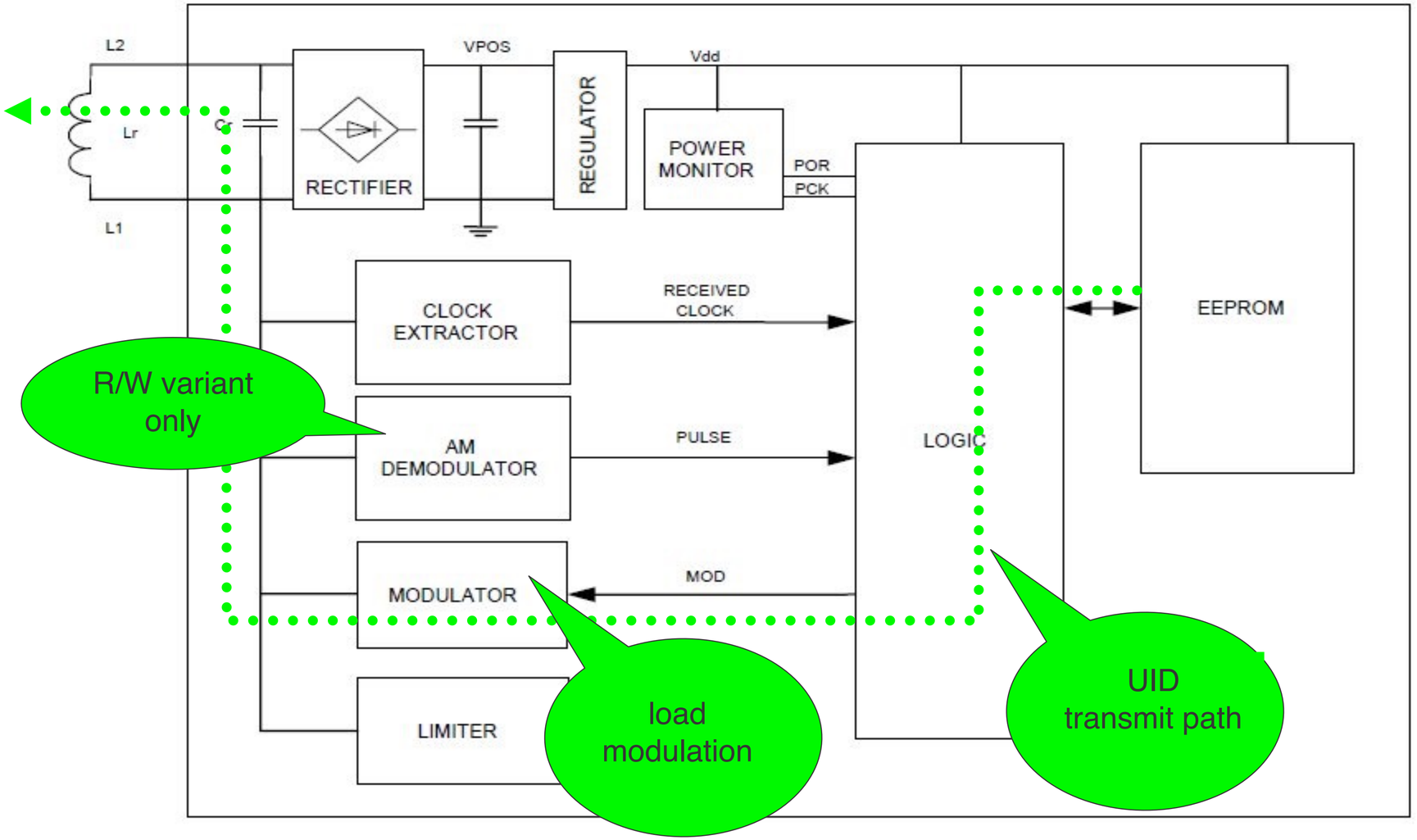


Target Response NFC-A

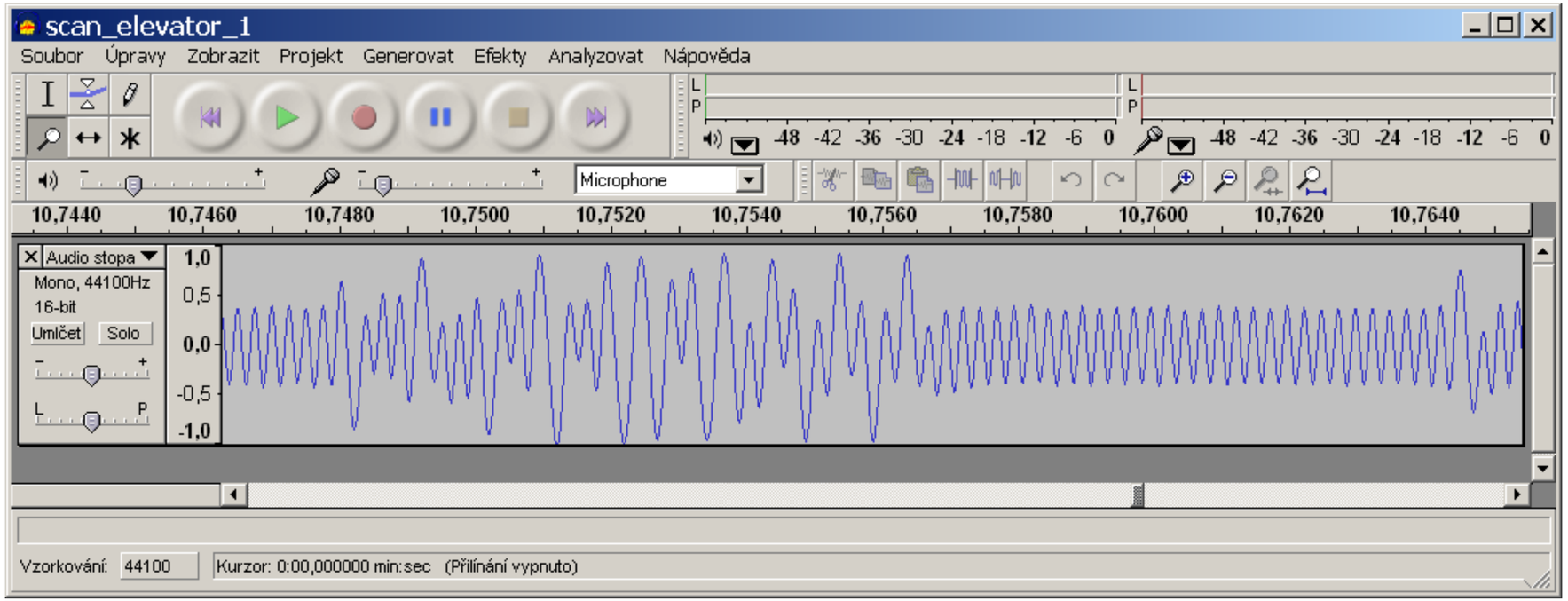


Hacking Avenue

Unique-ID Transponder Overview



Another Practical Scenario: **Eavesdropping in Elevator**

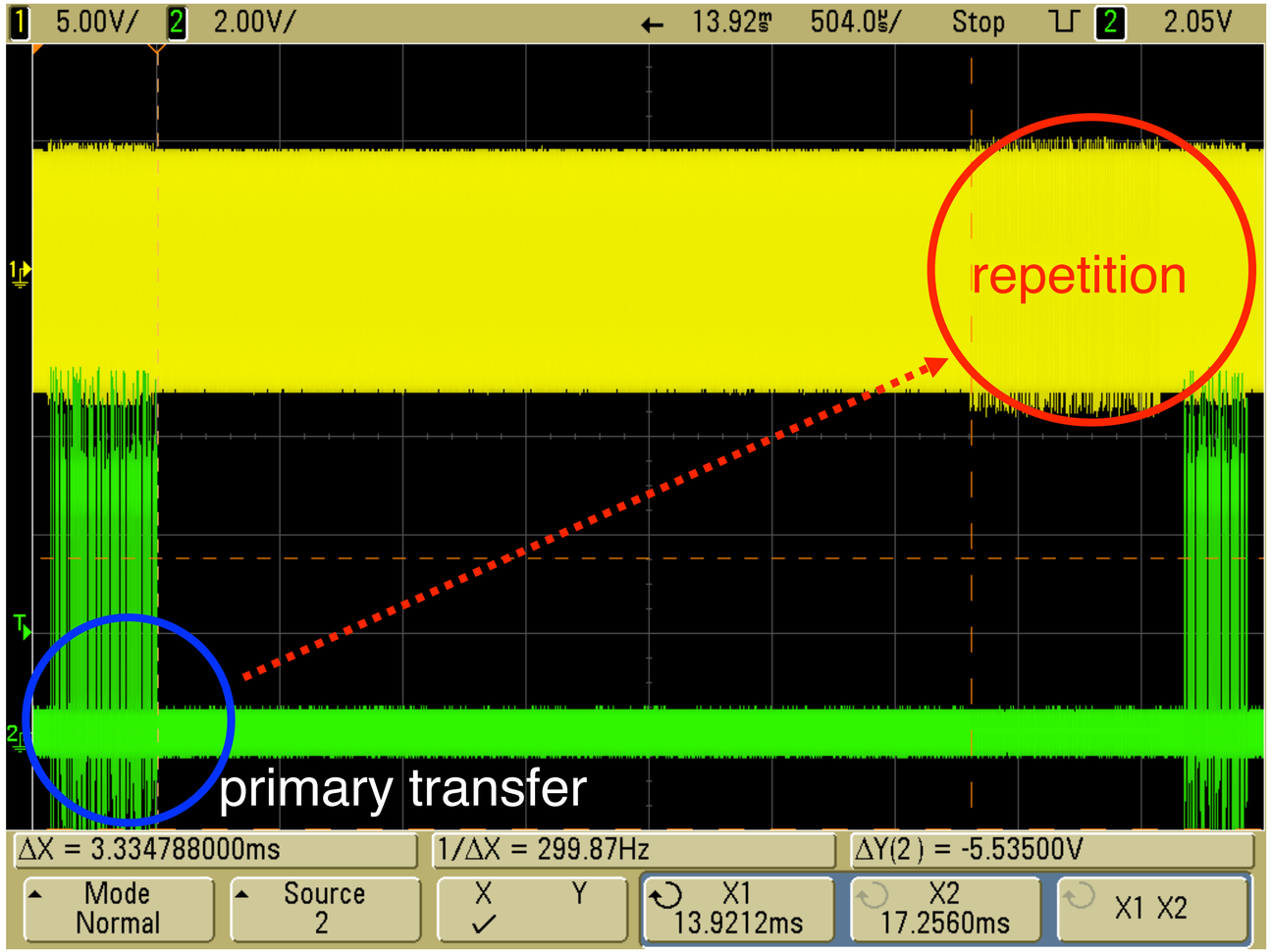


LF band transponder data intercepted while its holder was authenticating to the reader in an elevator.
Distance: cca 0,5 m.
Receiver: Sangean ATS 909W.

-- https://ok1sfu.cz/files/ST_2008_07_22_23.pdf

HF UID Interception

- Yellow trace: basic carrier
- Green trace: AM detector



All You NEED Is *LOOP*

Spying in The Lane (Still in XNF)

[https://www.youtube.com/watch?v=9QjxwejBPHs]

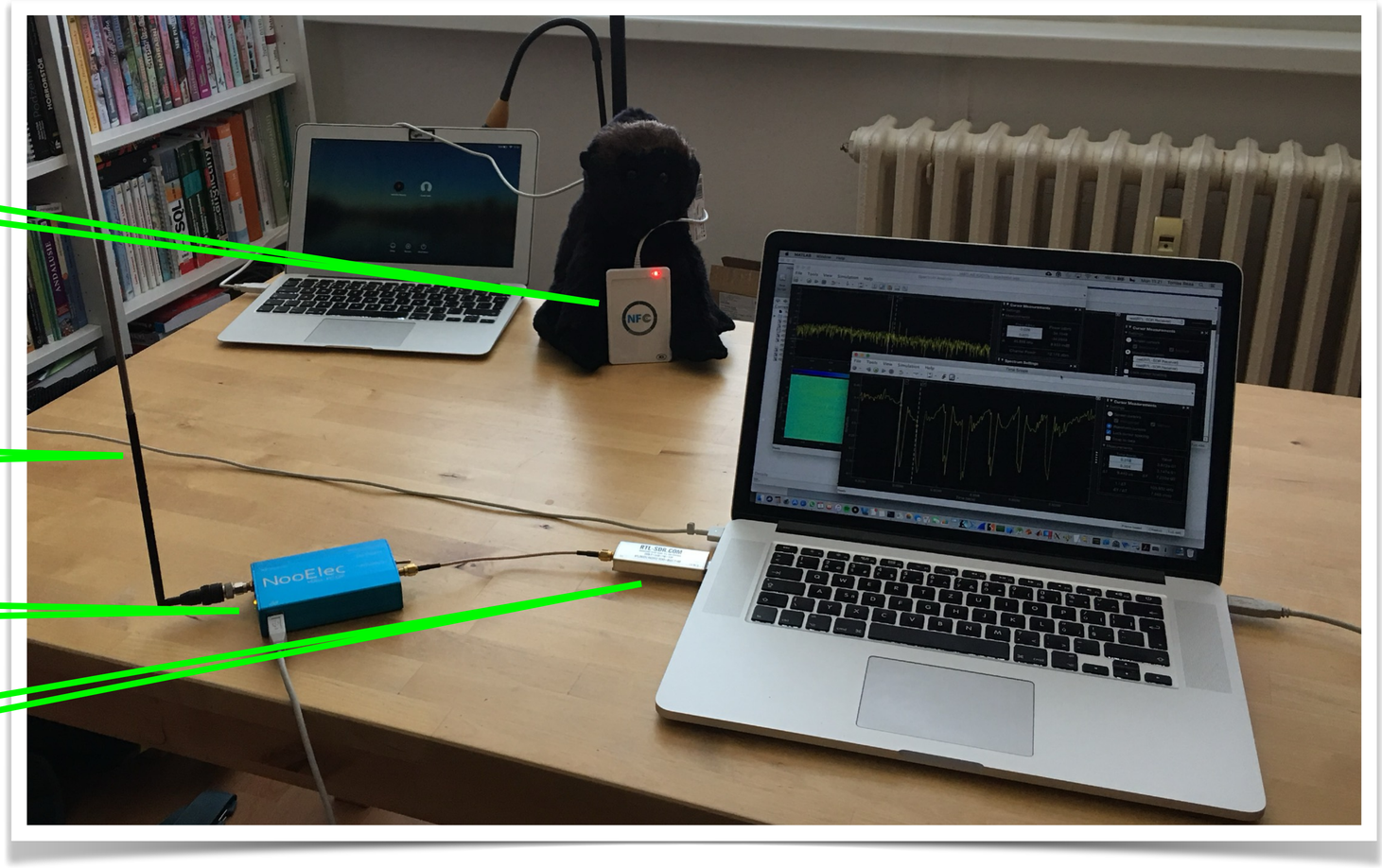
SDR Sniffer - Hardware Setup

ACR122 NFC reader

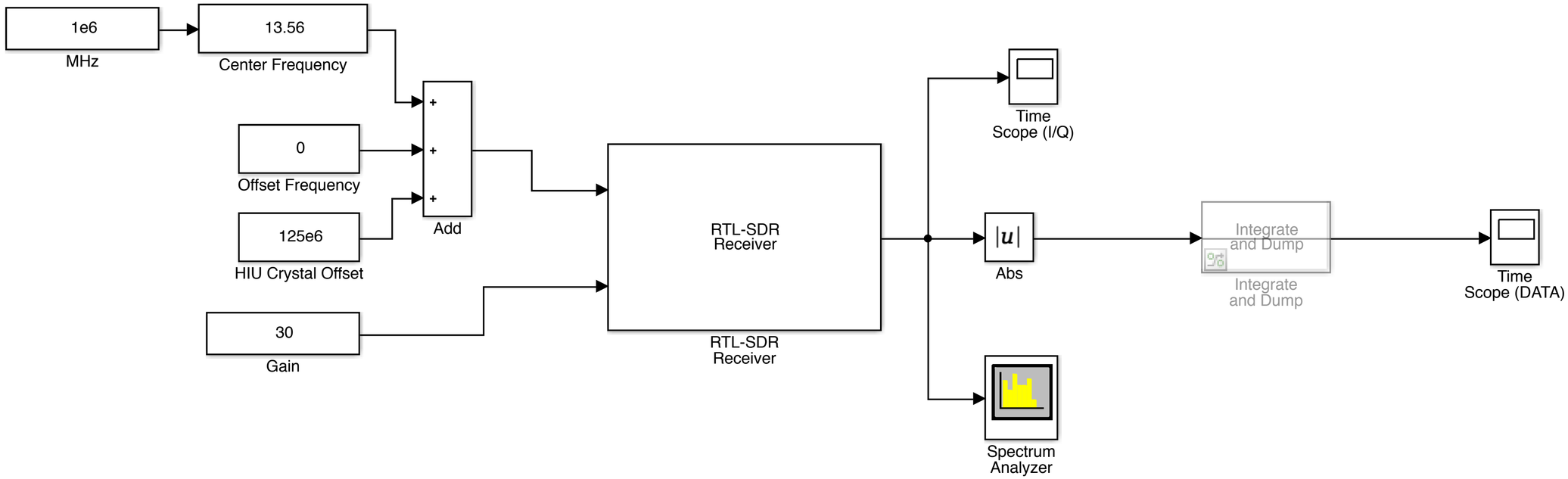
Simple telescopic antenna (untuned - a place for improvement)

NooElec HAM It Up upconverter

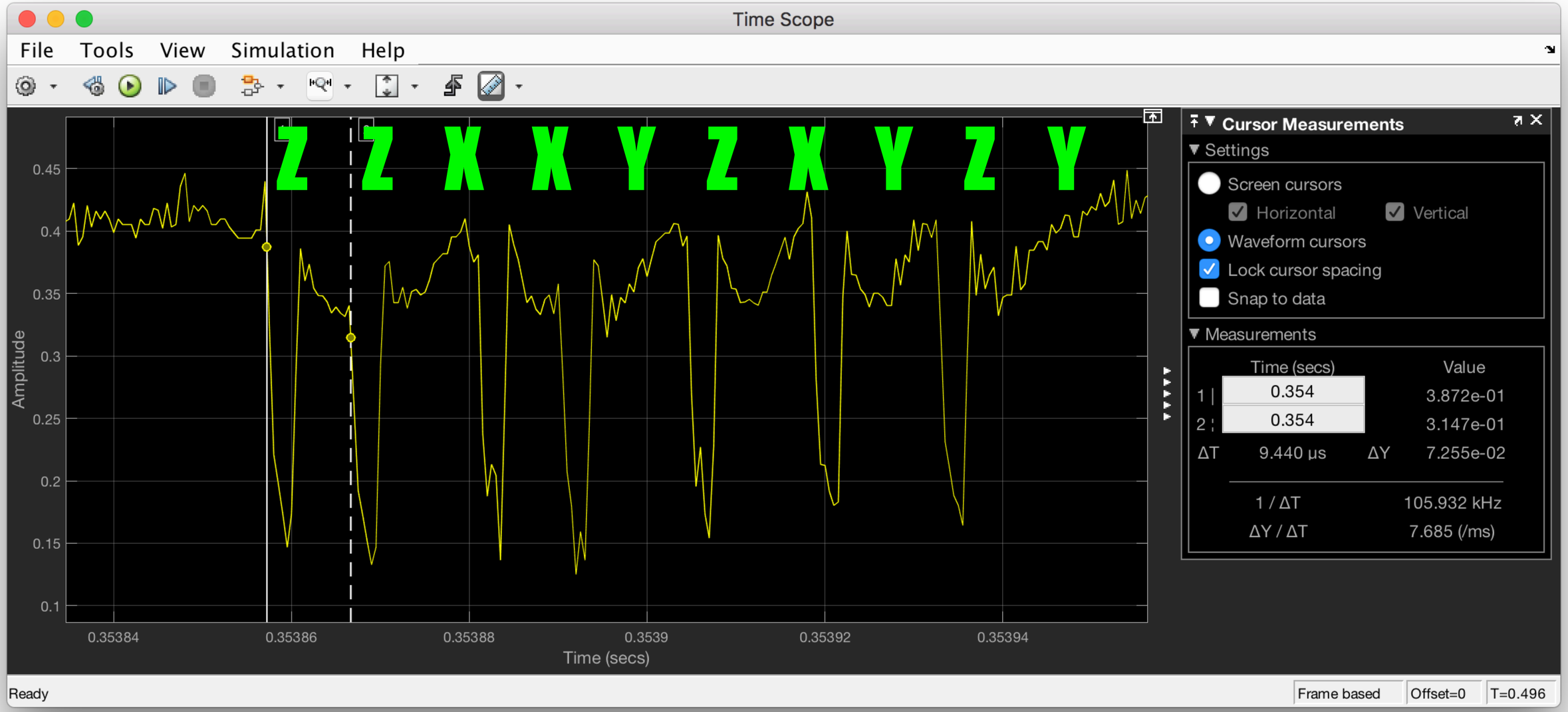
RTL-SDR v.3



Radio Definition in Simulink



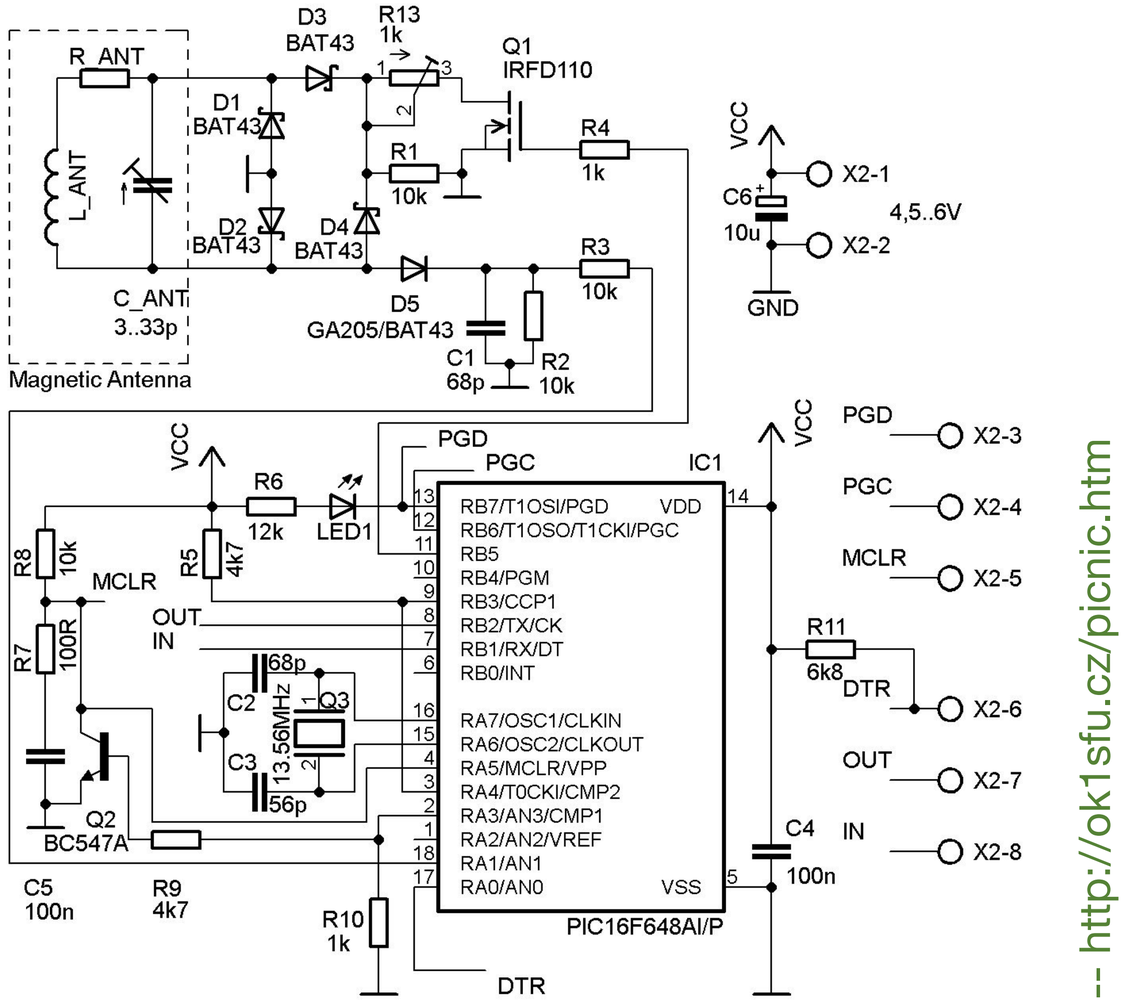
Identifying Miller Code Symbols (REQA)



Attack in Changing Room

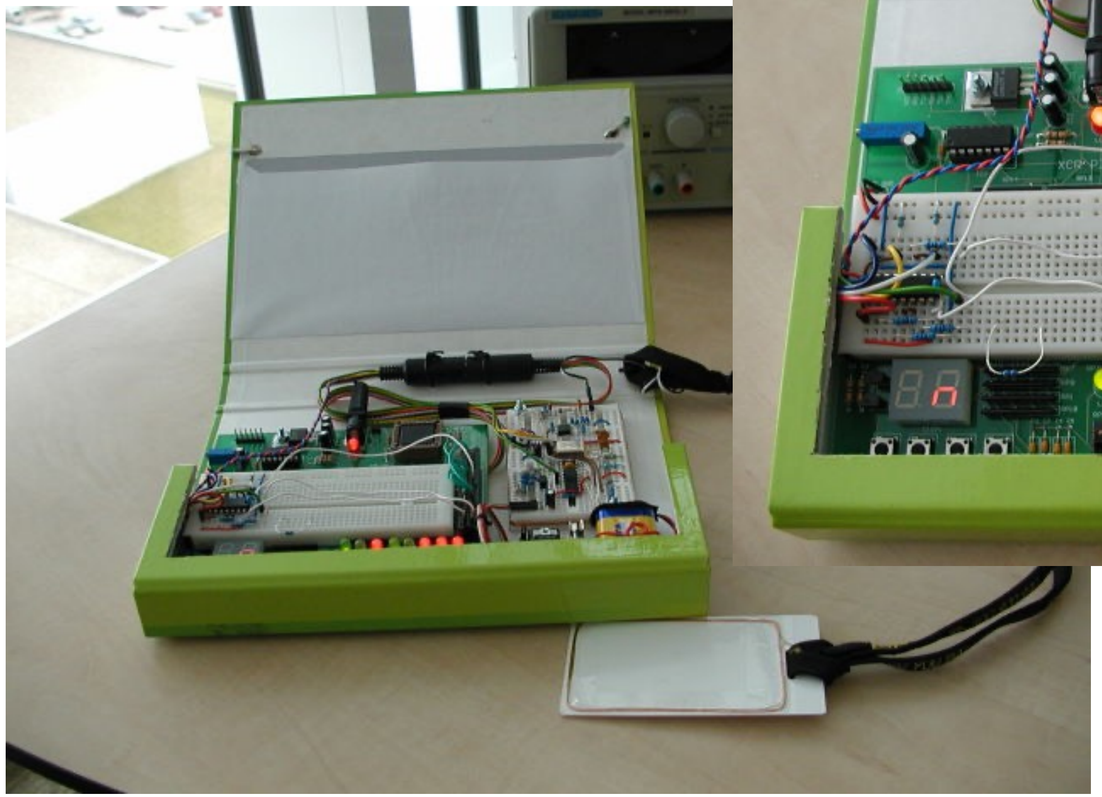
Another Real Life Scenario

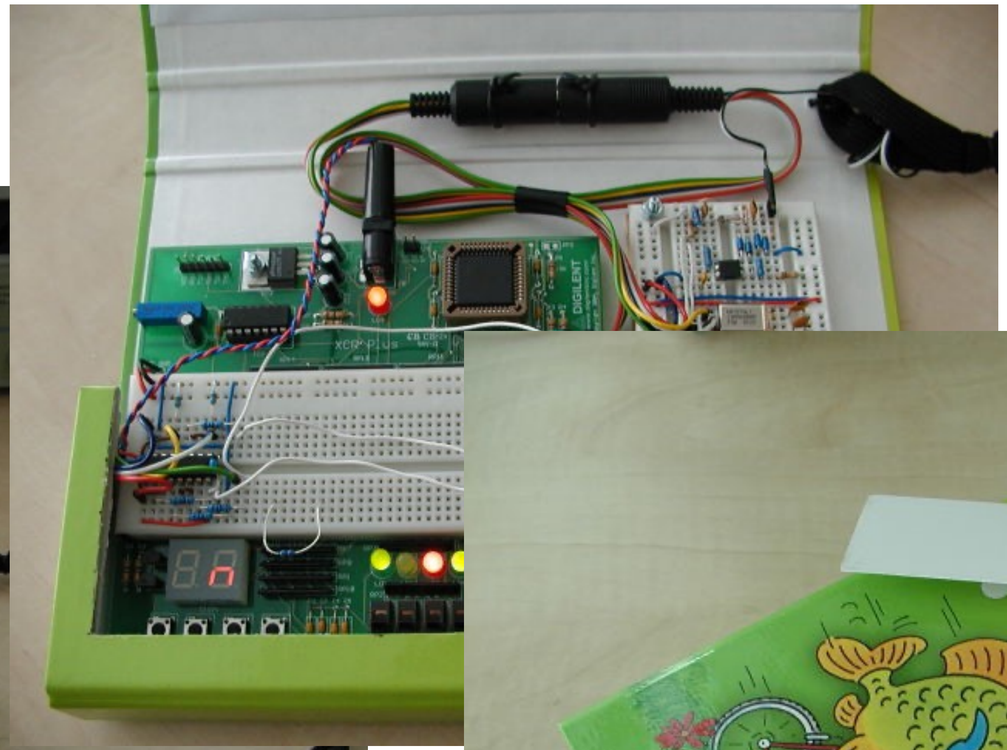
PicNic
HF Transponder Emulator



-- http://ok1sfu.cz/picnic.htm

PicNic & CPLD Coprocessor





Relay Attack Illustrated

Raiffeisen BANK

Client inspired banking

interconnection network

far field radiative coupling
(wifi, bluetooth, GSM, etc.)

Victim

Attacker A

near field inductive coupling
in between the *leech* and V's card
distance < 0,5 m (cf. following discussion)

Merchant's Term.

Attacker B

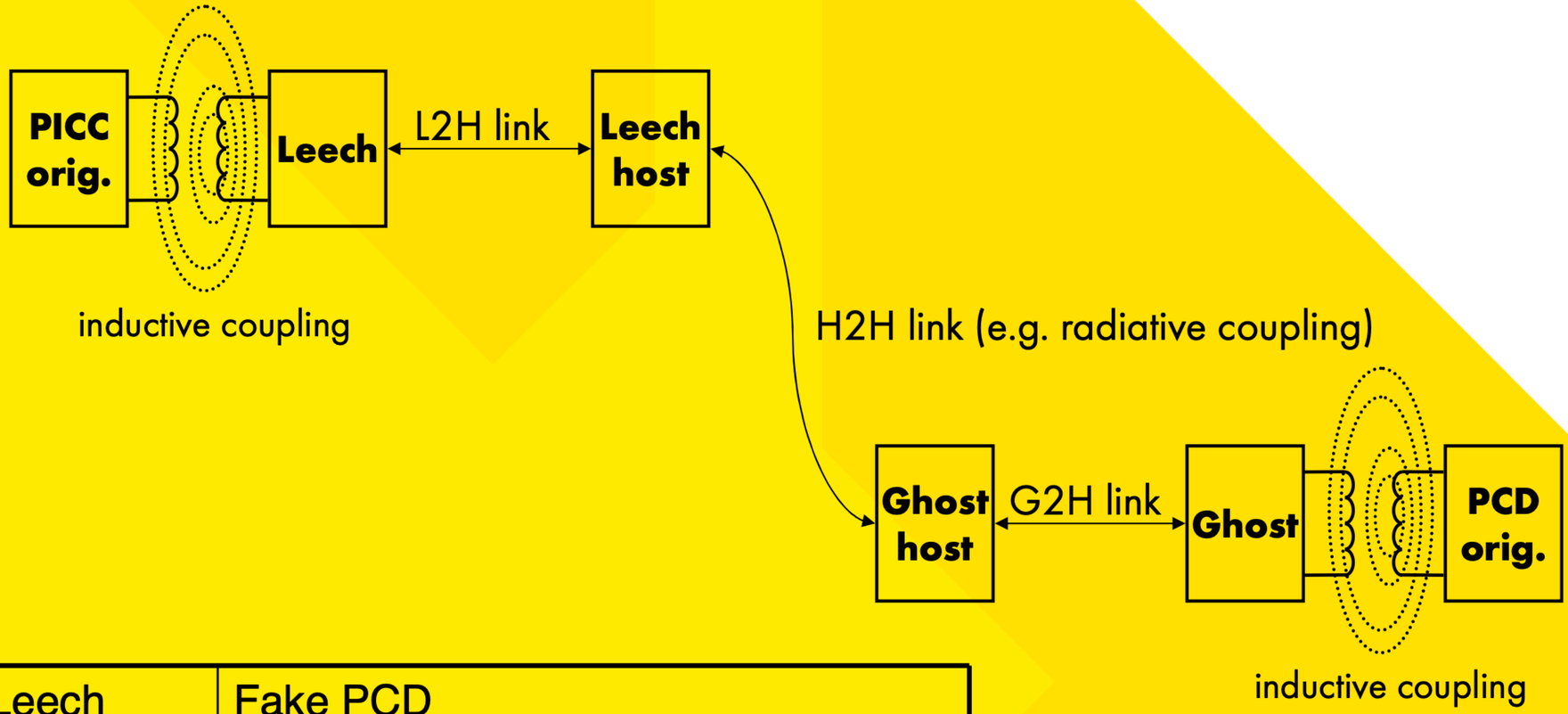
near field inductive coupling
in between the *ghost* and M's terminal

Contactless transaction with no PIN verification is assumed.

Nejdynamičtější banka roku 2010

Relay Attack Scheme

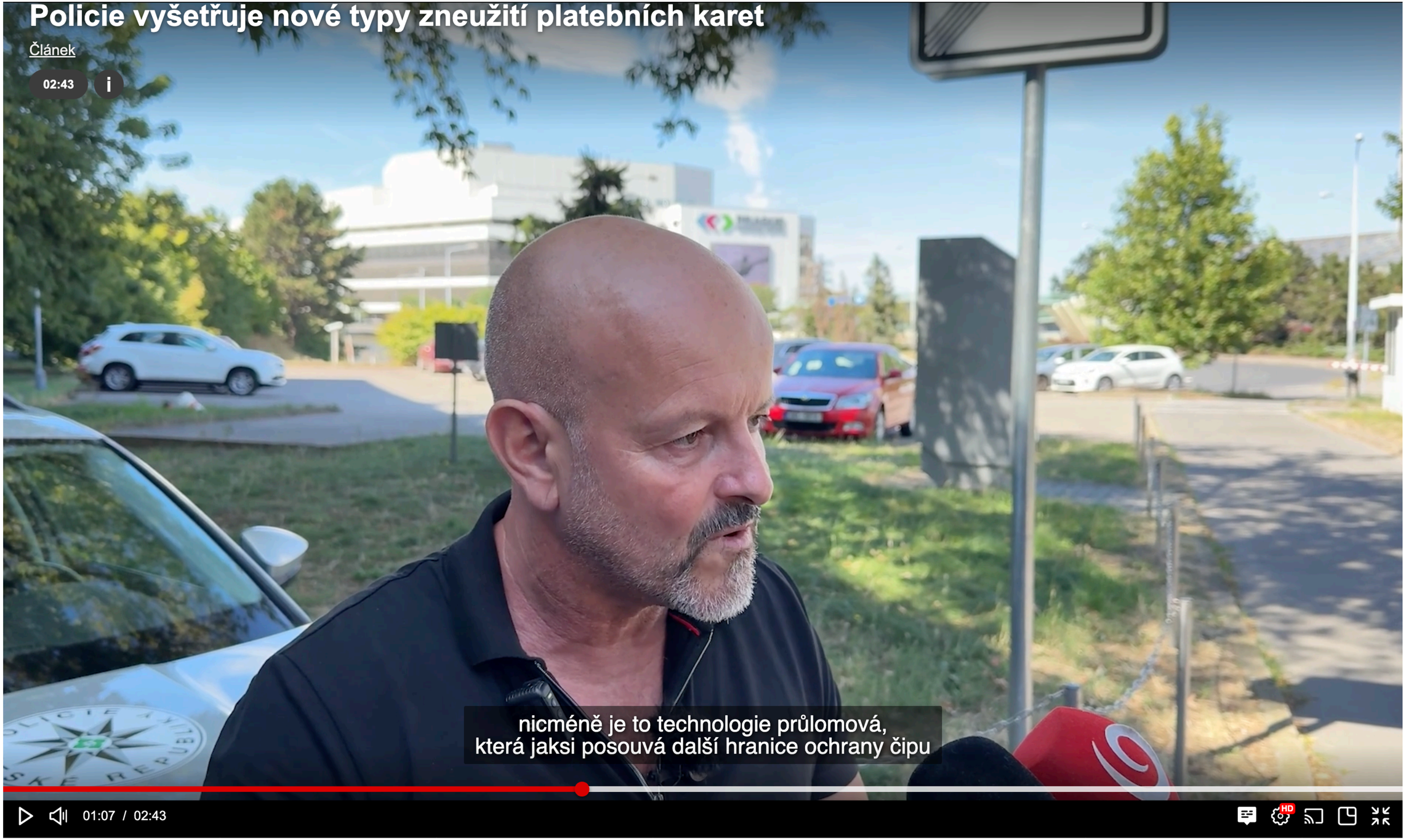
Raiffeisen BANK
Client inspired banking

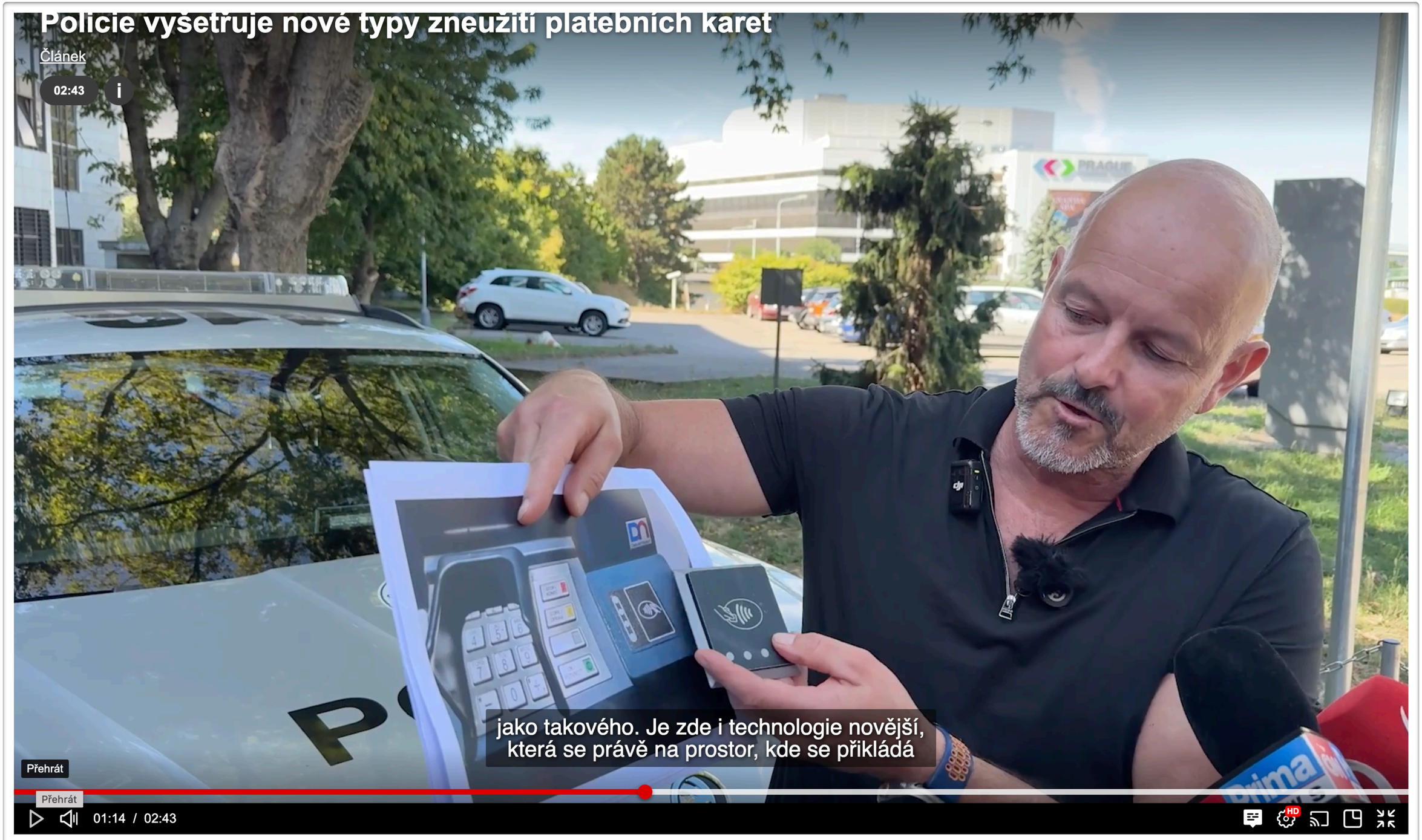


Leech	Fake PCD
Leech host	Computing device driving the leech
Ghost	Fake PICC
Ghost host	Computing device driving the ghost

Ernst & Young
Nejdynamičtější banka roku 2010

Wormhole in Access Control





HandyPay.app: Pay by card re

handypay.app

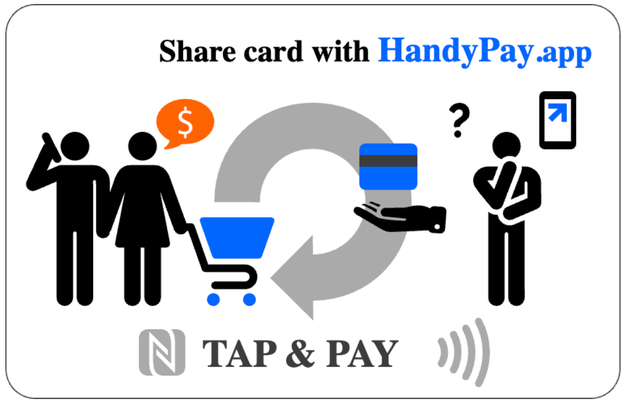
Incognito

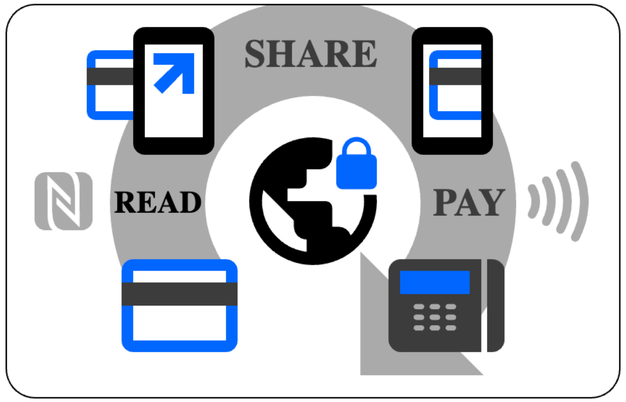
Features Pricing Tools About Sign-in

Person-to-Person payment cards share

Contactless Payment cards sharing between two linked persons.
Currently on Android Mobile phones with NFC readers.

- Person-to-Person link.
- No hidden fees.
- No geographical limits.

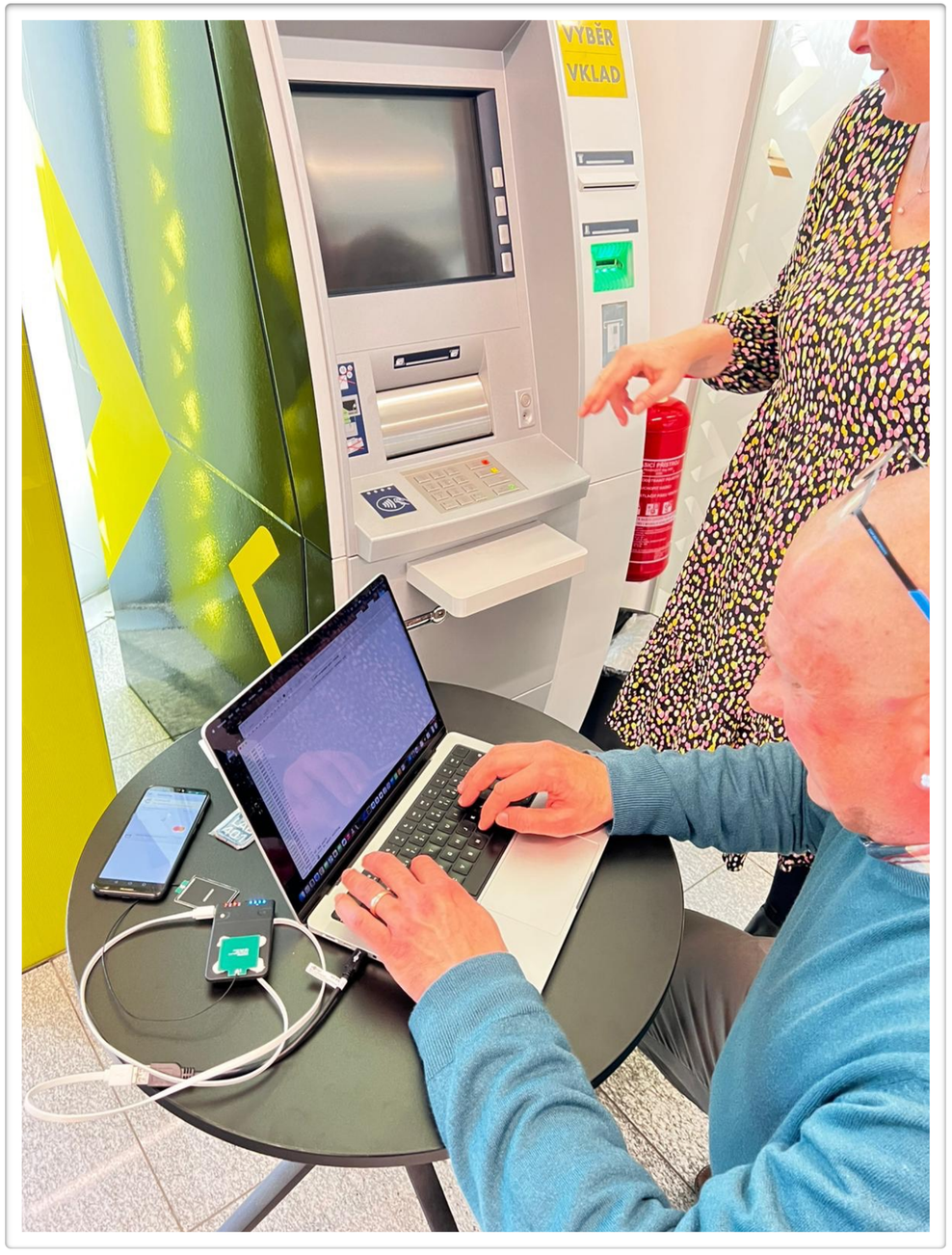




Secure NFC card payments

The application uses mobile phone's **NFC** reader on one side to read contactless card, transmit card data to the linked remote person's mobile phone, allowing to **TAP & PAY** with mobile phone like if the cardholder pay with his original card.

- Secure communication.
- Card data encryption.
- Life card processing.


VÝBĚR
VKLAD


STOP / KONEC
CORR / OPRAVA
OK / POTVRDIT
1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PQRS
8 TUV
9 WXYZ
0

HandyPay Wormhole

```
81447152 |   81462224 | Rdr |03  80  EA  00  00  04  A2  00  B4  34  00  62  E1                  | A ok|
81907396 |   81912132 | Tag |F2  01  91  40                                                      | A ok|
81922272 |   81927040 | Rdr |F2  01  91  40                                                      | A ok| S(WTX)
82372148 |   82376884 | Tag |F2  01  91  40                                                      | A ok|
82386896 |   82391664 | Rdr |F2  01  91  40                                                      | A ok| S(WTX)
82836772 |   82841508 | Tag |F2  01  91  40                                                      | A ok|
82851504 |   82856272 | Rdr |F2  01  91  40                                                      | A ok| S(WTX)
83064180 |   83083828 | Tag |03  80  0A  28  53  E8  E4  00  05  00  96  00  10  90  00  59  C5  | A ok|
```

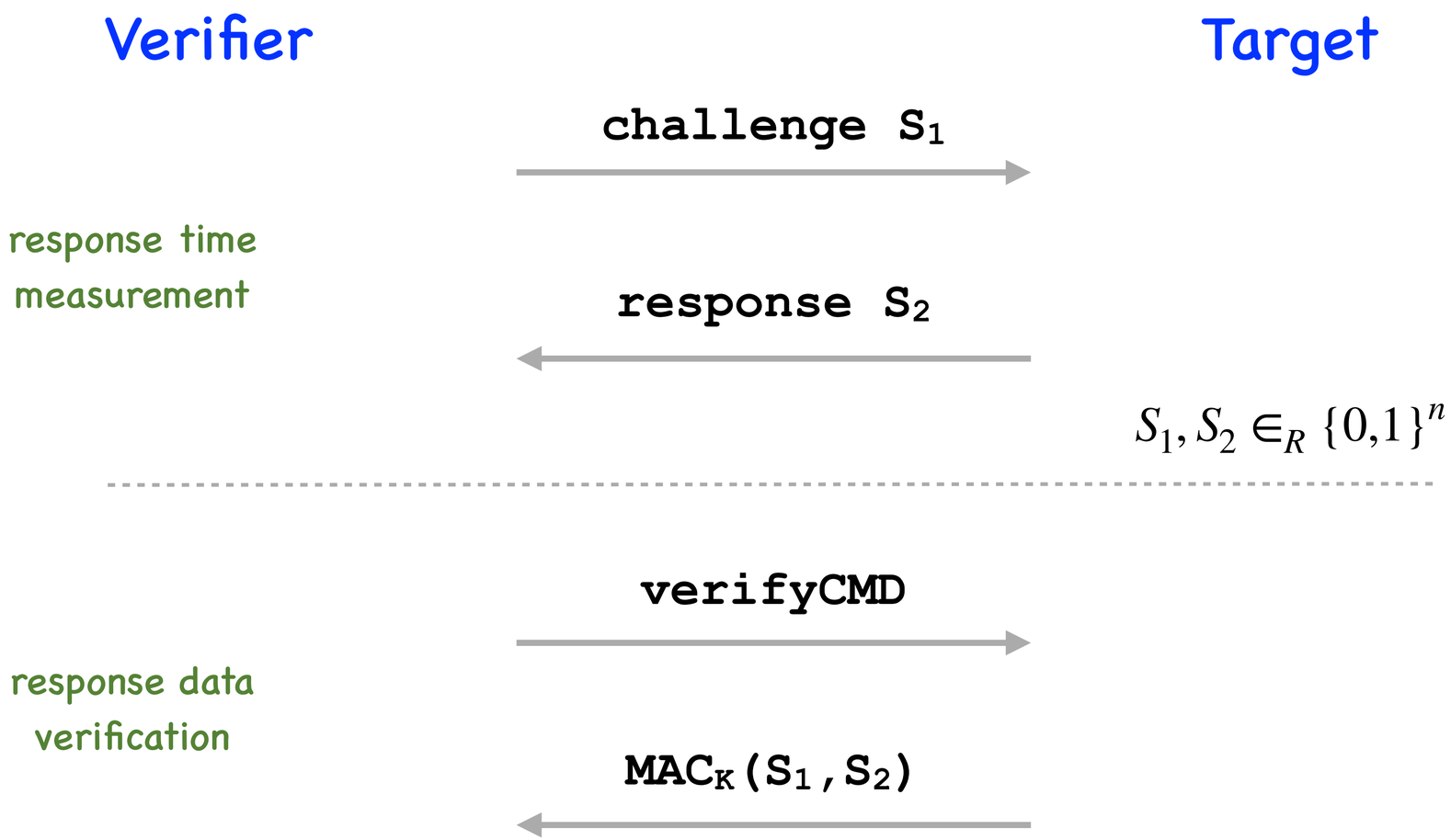
$\Delta \approx 120.7$ ms

Bare Payment Card

```
12953104 |   12968176 | Rdr |03  80  EA  00  00  04  80  B7  A3  5C  00  C3  03                  | A ok|
12976852 |   12996564 | Tag |03  80  0A  B2  88  DE  30  00  05  00  96  00  10  90  00  A4  6E  | A ok|
```

$\Delta \approx 3.2$ ms

Distance Bounding Protocol - Core Idea (one of)



Thank you for your attention

Co-funded by the European Union
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the European Cybersecurity Competence Centre can be held responsible for them

Supported by ECCC
The project funded under Grant Agreement No. 101158662 is supported by the European Cybersecurity Competence Centre

History (year-month-day format)

- 2026-04-27, version 1.0 released for CAMP at MFF UK