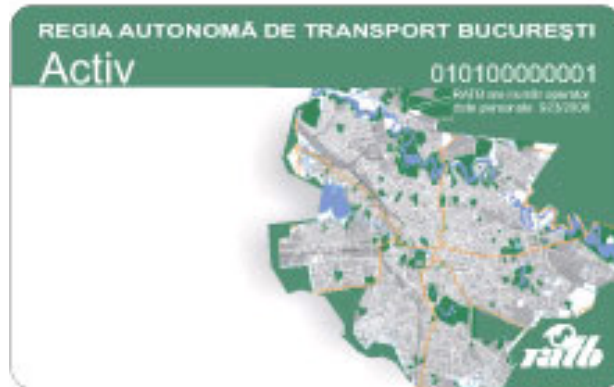


1. RATB Card Presentation (<http://card.ratb.ro>)

- a. Physical look of the customized RATB Mifare 1K card (image © RATB site)



- b. Attach link to video presentation from RATB

http://card.ratb.ro/web/static/despre_sat_card_activ.html

- c. Online account management

i. <https://online.ratb.ro/>

ii. Surface checks reveal web-application is quite well secured

iii. Not known how well the payment management is secured (not authorized)

- d. Lost/Stolen/Abandoned card management

i. http://card.ratb.ro/web/static/retea_transport.html

- e. Backoffice/backend data management

i. Present, but unknown how it works (though 24/48/72 hrs delays are in the place for some procedures, so there are some kind of End of Day jobs which are managing fraud detection, loading data to bus terminals so the online payments are charged to the cards)

2. RATB Technical details of the electronic ticketing system

- a. Mifare Classic 1k Cards

- i. About sector keys and block data

1. None of the cards have default sector keys – good choice from security point of view

2. None of the cards have sector keys which are repeating (except for sector 0 and 1) – good choice from security point of view

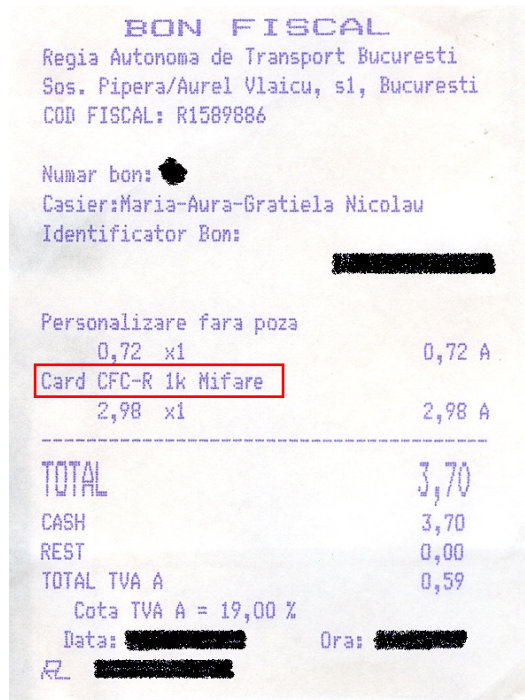
3. Sector 0 and Sector 1 have the same key of the below pattern (full key not disclosed for evident reasons)

a. c1xx1xxx5

4. Block 1 and Block 2 have these values

a. FFFFFFFFFFFFFFFFFFFFFFFFFF

ii. Attached receipt proving that – dumb thing to name your product exactly “Card CFC-R 1k Mifare” instead of “RATB Blank Card”



- iii. Attach screenshots from Omnikey Diagnostic Tool having the ATR and screenshot identifying the Mifare Classic 1k
- iv. Card is customarily pre-printed with green colors map of Bucharest
- b. Issuing boutiques - http://card.ratb.ro/web/static/retea_comerciala.html
 - i. Main issuing boutiques
 1. Have a read/write device Omnikey OK 5x21 (either Omnikey 5321 either Omnikey 5121)
 - a. http://www.hidglobal.com/prod_detail.php?prod_id=331 ~ 80 USD
 2. Have RFID cards thermal black printer to print the name and the owner ID
 - a. <http://www.rfidmexico.com.mx/ingles/impresoras.htm> - 1492 USD
 - b. <http://bsminfo.com/article.mvc/Evolis-Unveils-New-Tattoo-RW-Card-Printer-0001?VNETCOOKIE=NO>
 - ii. Secondary recharging boutiques
- c. Recharging boutiques
 - i. Have a read/write flat device (unknown yet – looks like ACR 122U, seen around things like that) ~ 30 USD
 - ii. Cannot issue a card – possibly because they do not the printer to physically personalize the card. Other reasons of not issuing the cards are yet unknown.
- d. Reading/writing terminals in buses/metro:

- i. Close to 100% they run embedded linux
 - ii. Unknown database management in use in the terminals and in the bus itself
 - iii. Metrorex entrances/RATB bus/trams/trolleys have UTI (<http://www.uti.ro>) custom developed boxes with embedded Linux (example: I have seen some non-bootable RootFS errors on some of them)
 - iv. Unknown reader/writer
3. RATB Card application level data:
- a. Types of users
 - i. http://card.ratb.ro/web/static/oferta_tarifara_tarif_redus.html
 - ii. Regular (nominal)
 - 1. Unknown authorizations of usage
 - 2. Unknown internal storage
 - iii. Controllers
 - 1. Authorizations
 - a. have access to special menu on the RATB car boxes. Controllers also have some type of portable RFID scanners looking like retail chain product scanners, possibly having some kind of DB loaded for data validation offline. Not likely that these scanners have online access though (not enough coverage, though 3G/GPRS could be used, too fast for an online DB query, etc.)
 - b. Rest of authorizations unknown
 - c. Would be useful a physical access or a sniffed conversation of such a card
 - 2. Unknown internal storage
 - iv. Elevi/Studenti
 - v. Donatori
 - vi. Pensionari
 - vii. Free - http://card.ratb.ro/web/static/oferta_tarifara_ab_gratuite.html
 - viii. TODO - Others?! (for example sysadmin, root, superuser, etc)
 - b. Types of data (http://card.ratb.ro/web/static/oferta_tarifara.html)
 - i. TODO - Information reverse engineering
 - 1. Block/sector/key?
 - 2. Which terminal boxes identify which type of data
 - 3. What is the internal format for date/RONs/type of service
 - ii. Service "Portofel electronic"
 - 1. Stores data in amount of RONs. Unknown internal format of storage.
 - 2. Max 50 RON, Min 2.5 RON
 - a. Try a boundary check (more than 50 or less than 2.5) on the system
 - iii. "Abonament fractionat toate liniile 7 zile"
 - 1. ???

- iv. “Abonament fractionat toate liniile 15 zile”
 - 1. ???
- v. “Abonament fractionat toate liniile lunar”
 - 1. ???
- vi. “Abonament Metrorex lunar”
 - 1. ???
- vii. “general RATB”
 - 1. ???
- viii. “una linie RATB”
 - 1. ???
- ix. “doua linii RATB”
 - 1. ???
- x. “lunar EXPRES 780, 783”
 - 1. ???
- xi. “10 calatorii Expres 780, 783”
 - 1. ???
- xii. “Abonament lunar valabil pe una linie preoraseneasca”
 - 1. ???
- xiii. “Abonament lunar RATB valabil pe doua linii (una linie preoraseneasca si una linie urbana)”
 - 1. ???
- xiv. TODO - Others?

4. Security

- a. Physical security
 - i. Boutiques are not very secured – look like can boxes ☺, though have some protective grillages
 - ii. Easy to break in – high \$ valuables in RFID printer and low \$ valuables in RFID reader/writer devices
- b. Network security
 - i. Boutiques possibly have some kind of network access – not analyzed
 - ii. Metrorex entrances/RATB cars are unlikely to be online – possibly the data is unloaded to backend at “end-of-day” in an offline manner
- c. Mifare and application level security
 - i. Card sniffing, cloning and emulation
 - 1. Proxmark3 – <http://www.proxmark3.org>
 - 2. ACR122U – http://www.acs.com.hk/drivers/eng/API_ACR122U.pdf
 - 3. Nokia NFC phones - <http://www.nexperts.com/typo/index.php?id=3>
 - 4. MikeyCard - Firmware for a software defined contactless smartcard, called Mikey - <http://code.google.com/p/mikeycard/>
 - 5. USRP+GNUradio (see MIT Students Hack *Boston Charlie* Cards presentation)

- d. Injection attacks into the boxes/backend
 - i. TODO
- 5. Implications and protection
 - a. Please check the listed links, as well as corresponding research papers and system integrators advices
- 6. Other (non-exhaustive) list of Mifare usage in public transport:
 - a. • Madrid
 - b. • Minneapolis
 - c. • Rio de Janeiro
 - d. • Beijing
 - e. • Sydney
 - f. • Johannesburg
 - g. • Valencia
 - h. • Houston
 - i. • São Paulo
 - j. • Nanjing
 - k. • Melbourne
 - l. • Malaga
 - m. • Boston
 - n. • Santiago de Chile
 - o. • Guangzhou
 - p. • Auckland
 - q. • Cadíz
 - r. • Seattle
 - s. • Buenos Aires
 - t. • Seoul
 - u. • Wellington
 - v. • Milan
 - w. • Guadalajara
 - x. • Montevideo
 - y. • Taipei
 - z. • Christchurch
 - aa. • Venice
 - bb. • Mexico City
 - cc. • Bogotá
 - dd. • Modena
 - ee. • Quito
 - ff. • Lyon
 - gg. • Lima
 - hh. • Valence
 - ii. • Toulouse

- jj. • Montpellier
- kk. • Luxemburg
- ll. • Oslo
- mm. • Bergen
- nn. • Stavanger
- oo. • Stockholm
- pp. • Turku
- qq. • Copenhagen
- rr. • Amsterdam
- ss. • Rotterdam
- tt. • Londra
- uu. • Liverpool
- vv. • Dublin
- ww. • Bucuresti
- xx. • Budapesta
- yy. • Varsovia
- zz. • Minsk
- aaa. • Kiev
- bbb. • Moscow
- ccc. • Kaliningrad
- ddd. • St. Petersburg
- eee. • Izmir

7. TODOs

- a. Reverse engineer through differential analysis (get full dumps in consecutive manner after changing something on the card through the legal terminals. Example: charge “Portofel electronic”, spend “Portofel Electronic”, add a new “Abonament fractionat 7 zile”, extend “Abonament fractionat 15 zile”, etc.)
 - i. Which blocks are actually used, since only the first two block have the same key
 - ii. How is the application data information is stored on the card at bit level of each data block
 - iii. How the date is being decoded from those bits to produce human-readable information when users use “Option 1 Consultare” on the terminal in the bus/metro

8. Links

- a. TOOLS/FORUMS:
 - i. <http://code.google.com/p/tk-libnfc-crapto1/>
 - ii. <http://www.proxmark.org/>
 - iii. <http://www.libnfc.org/>
- b. SEARCH:
 - i. <http://www.google.com/search?hl=en&client=firefox-a&rls=org.mozilla%3Aen-US%3Aofficial&hs=8oL&q=UTI+RATB+card&btnG=Search>

- ii. <http://www.google.com/search?hl=en&client=firefox-a&rls=org.mozilla%3Aen-US%3Aofficial&hs=w2h&q=UTI+SAT+sistem+automat+de+taxare&btnG=Search>
 - iii. <http://www.google.com/search?q=ratb+mifare&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:en-US:official&client=firefox-a>
- c. RATB, SAT, UTI:
- i. <http://metropotam.ro/La-zi/2006/11/art5391055060-Card-unic-valabil-pentru-Metrorex-si-RATB/>
 - ii. <http://www.piticu.ro/page/2?s=ratb>
 - iii. <http://card.ratb.ro/>
 - iv. http://card.ratb.ro/web/static/despre_sat_card_activ.html
 - v. <http://online.ratb.ro/>
 - vi. <http://www.adevarul.ro/articole/2007/eseul-cartelei-unice-ratb-metrorex.html>
 - vii. <http://manipularea.blogspot.com/2008/02/sute-de-mii-de-bucuresteni-pot-fi.html>
 - viii. http://www.efinance.ro/articol.php?id_revista=200805&id_sectiune=eitc&ordine_sectiune=6
 - ix. <http://www.fabricadebani.ro/news.aspx?iid=21835&sid=7>
 - x. <http://www.ziua.ro/display.php?data=2007-03-02&id=216854&ziua=8d38b019c2ac1d70705d2f8184858723>
 - xi. <http://www.ziare.com/actual/social/01-19-2009/serviciile-ratb-pot-fi-platite-cu-cardul-bcr-625033>
 - xii. <http://www.ziare.com/business/consumator/11-12-2009/bancomate-bcr-pentru-reincarcarea-cardurilor-ratb-948768>
- d. TECH:
- i. <http://tramclub.org/viewtopic.php?p=119946&sid=7530701b3e184ac44bac0d7de06430d4>
- e. KITS & DEMOs – can do nasty stuff with these :D :
- i. <http://www.youtube.com/watch?v=SDQSRpS46Fo>
 - ii. <http://www.nexperts.com/typo/index.php?id=3>