black hat ASIA 2025

# Dismantling the SEOS Protocol

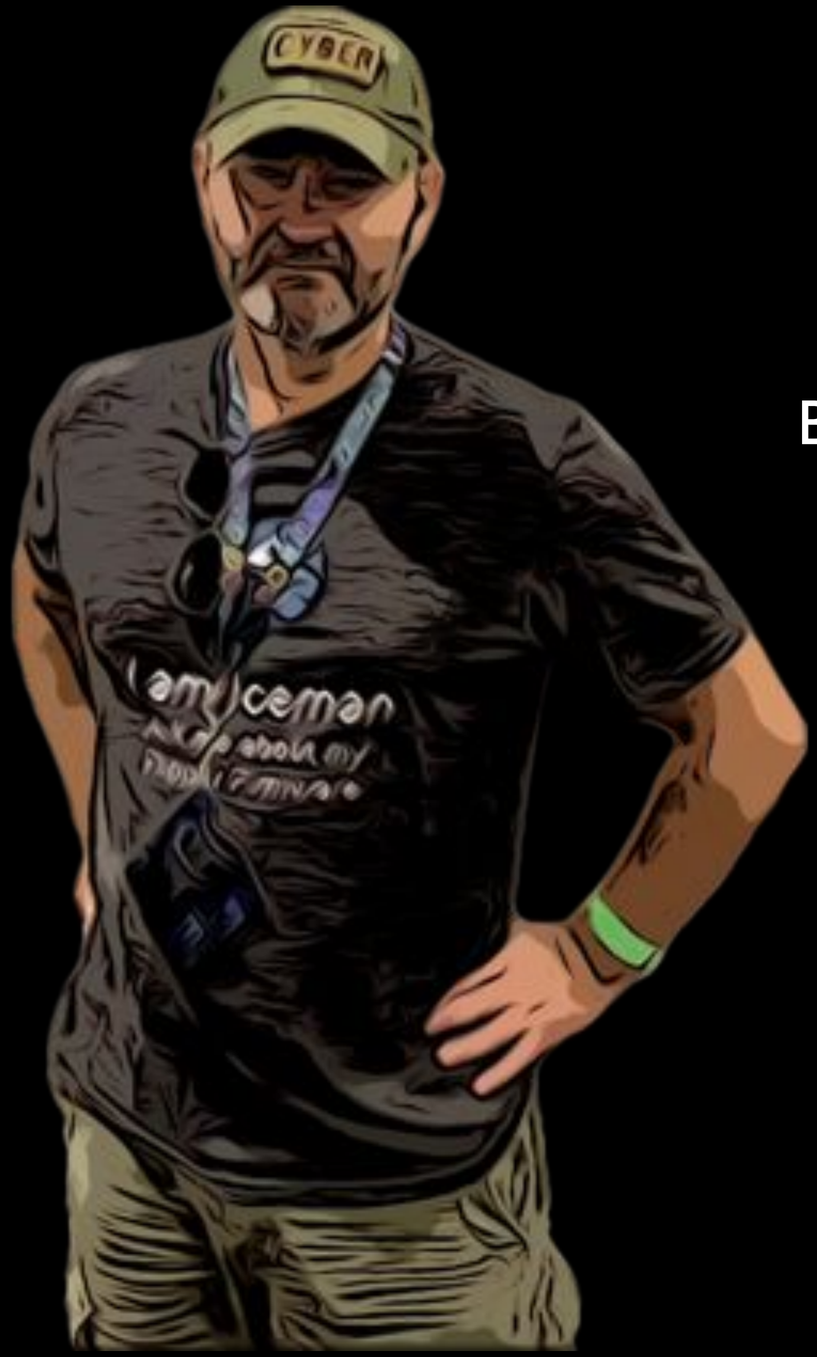
evildaemond & Iceman

# Who is evildaemond?

Day job as a Senior Penetration Tester

Almost 10 years in Physical Security
Specialises in electronics and hardware specialist

# Who is Iceman?



Been hacking RFID systems over a decade

Loves open source!

Uses 4 spaces instead of <tab>

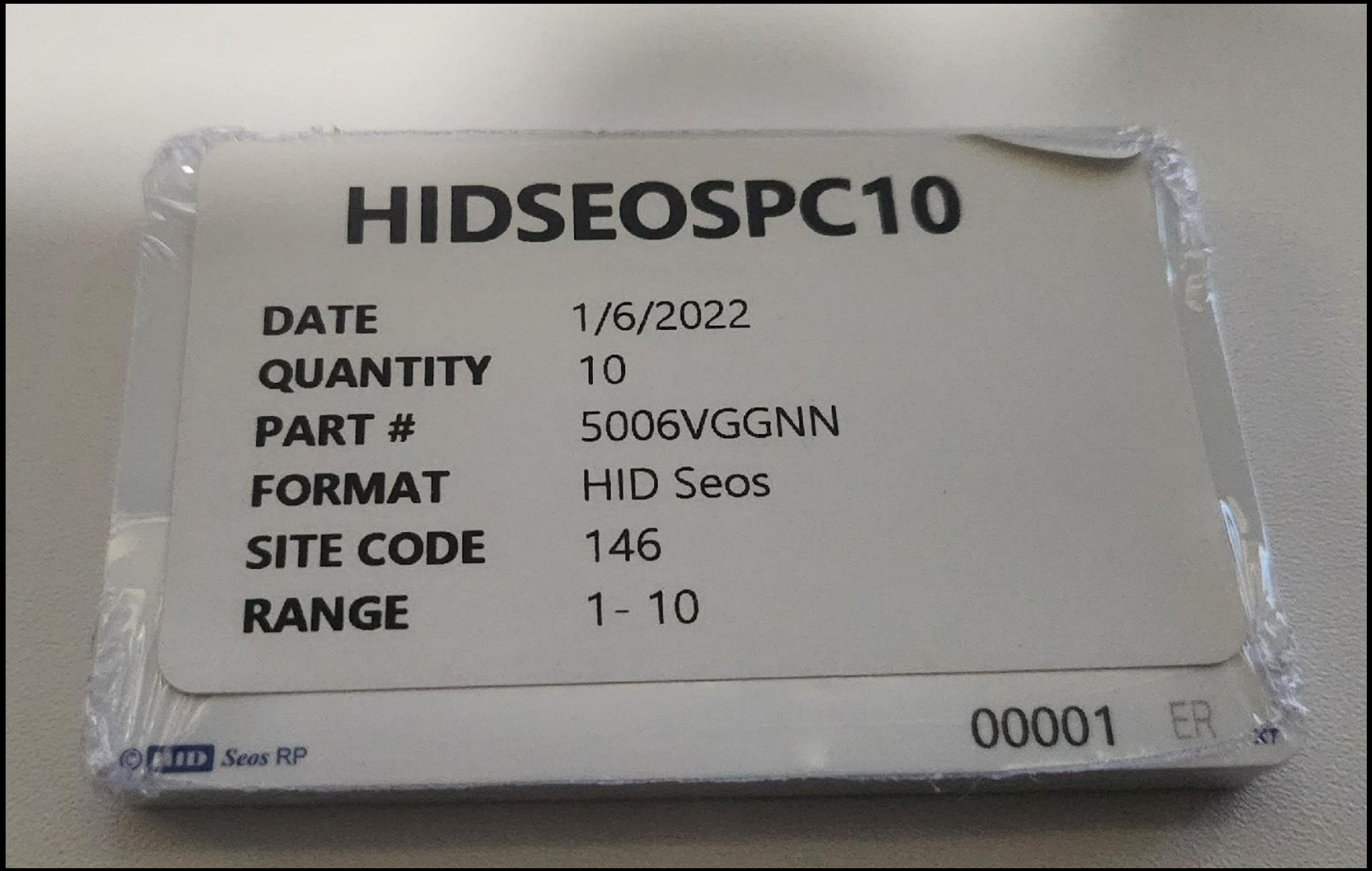
# Why?

Newest security technology

Cards came with a new access control system

No substantial any information online

Don’t trust people saying it's secure



HIDSEOSPC10

| | |
|---|---|
| DATE | 1/6/2022 |
| QUANTITY | 10 |
| PART # | 5006VGGNN |
| FORMAT | HID Seos |
| SITE CODE | 146 |
| RANGE | 1- 10 |

Understand how these systems work

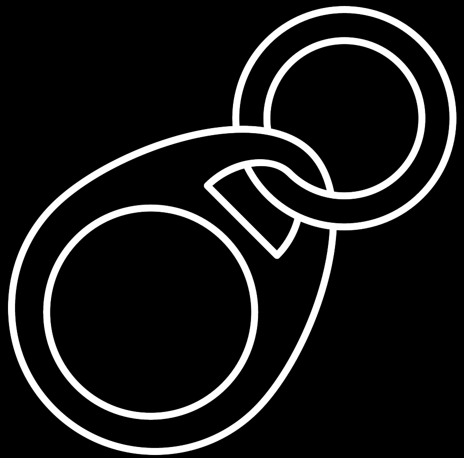
Review what the system uses

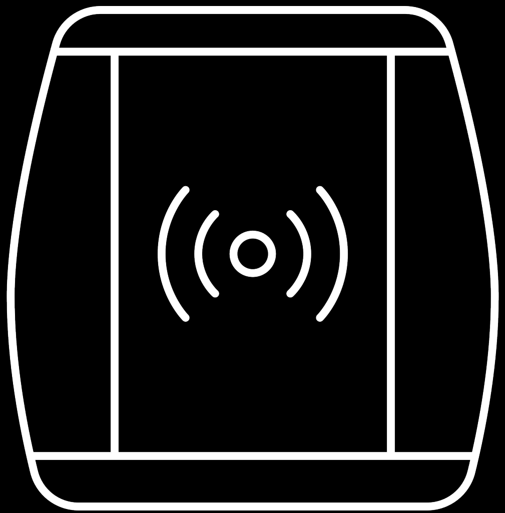
Evaluate its security

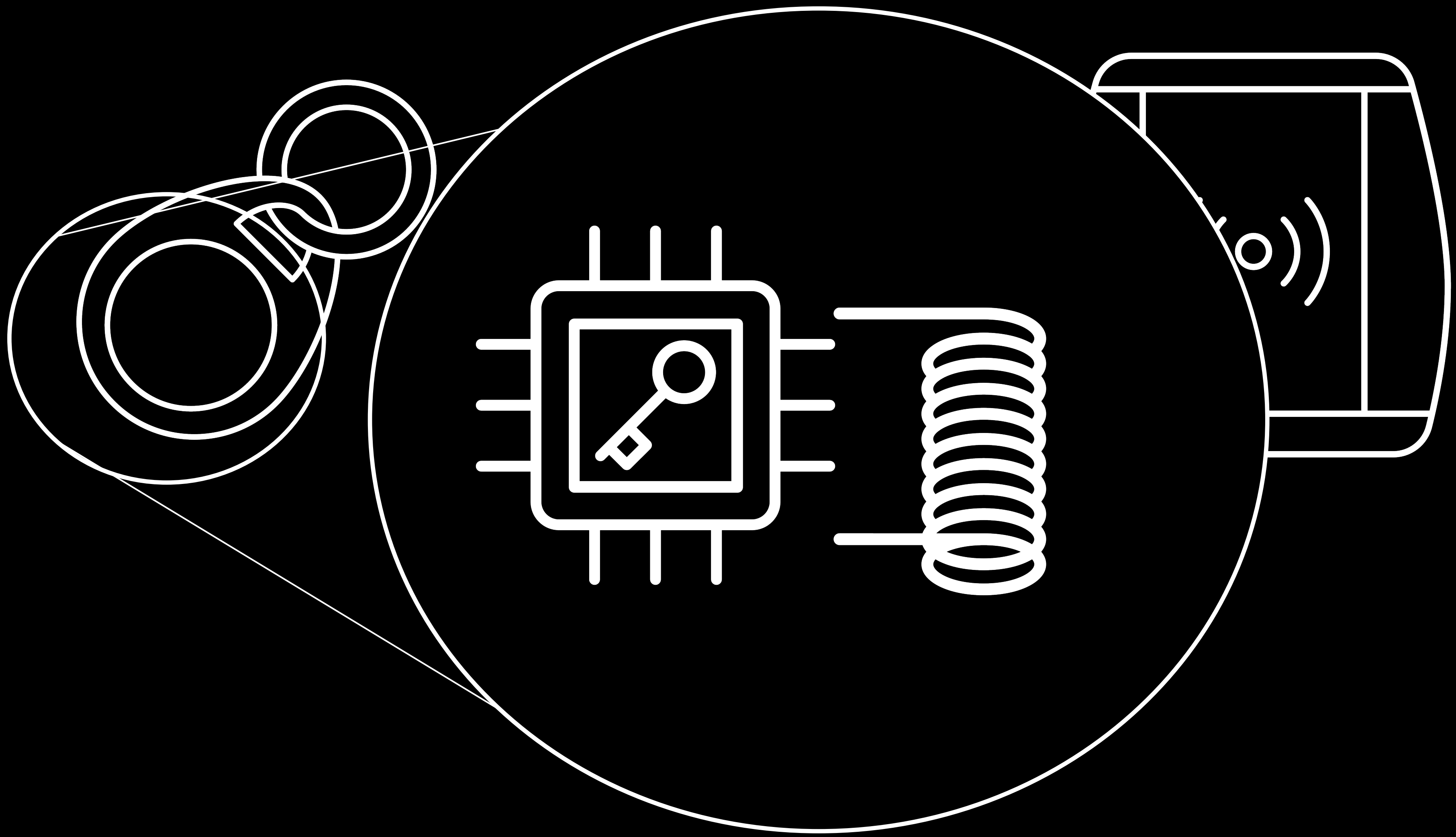
# RFID 101

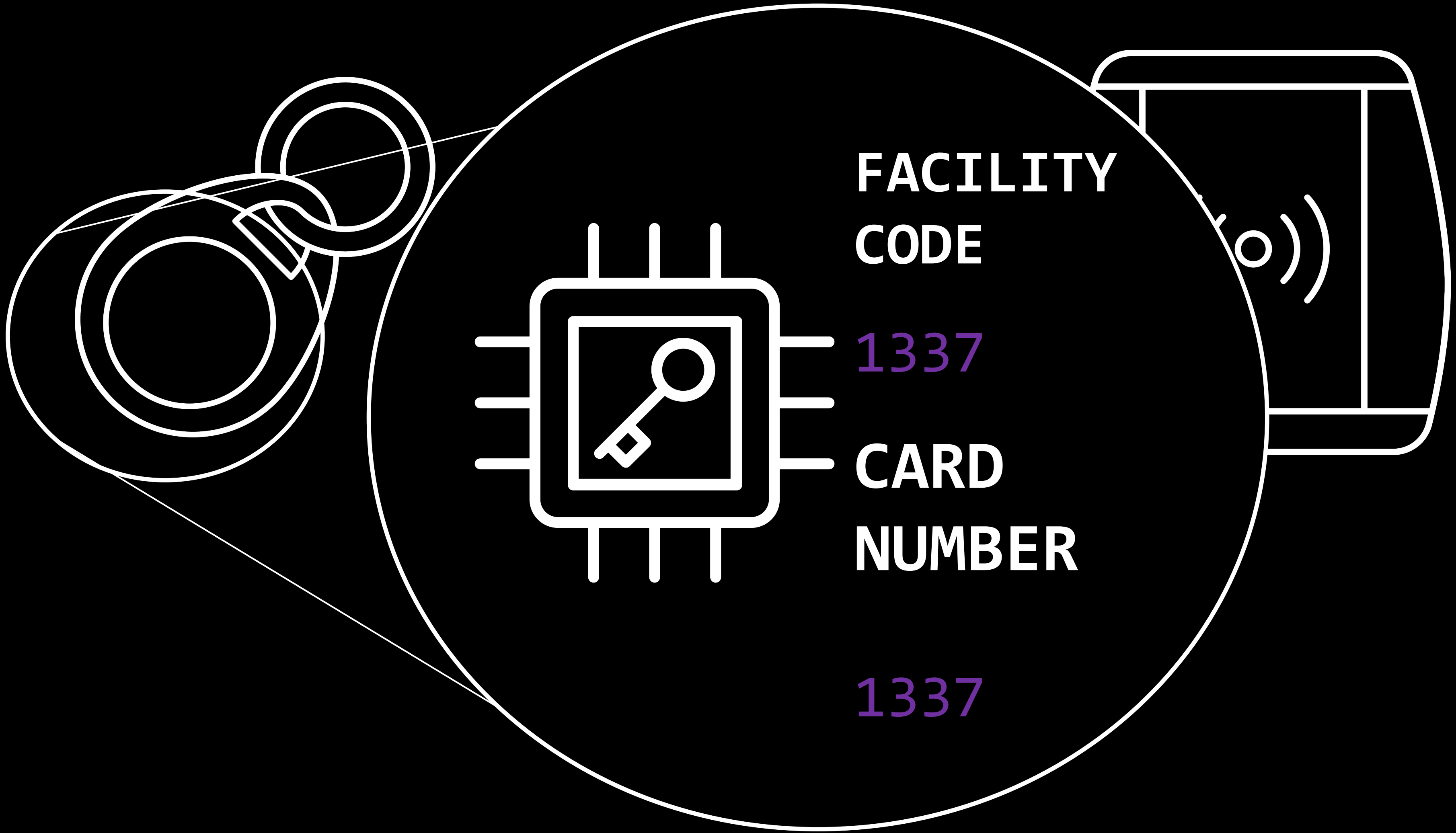
# RF - ID

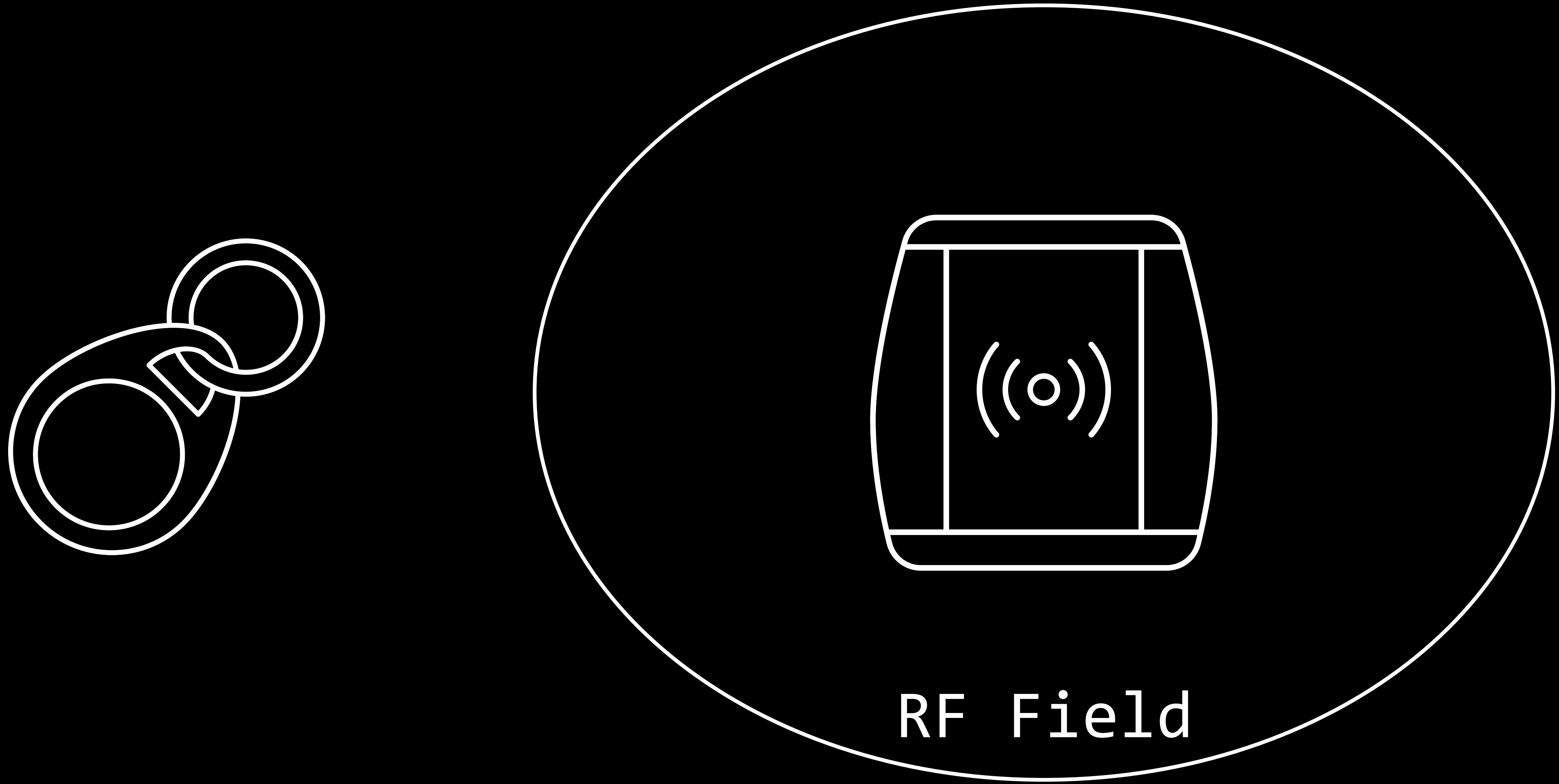
## Radio Frequency Identification

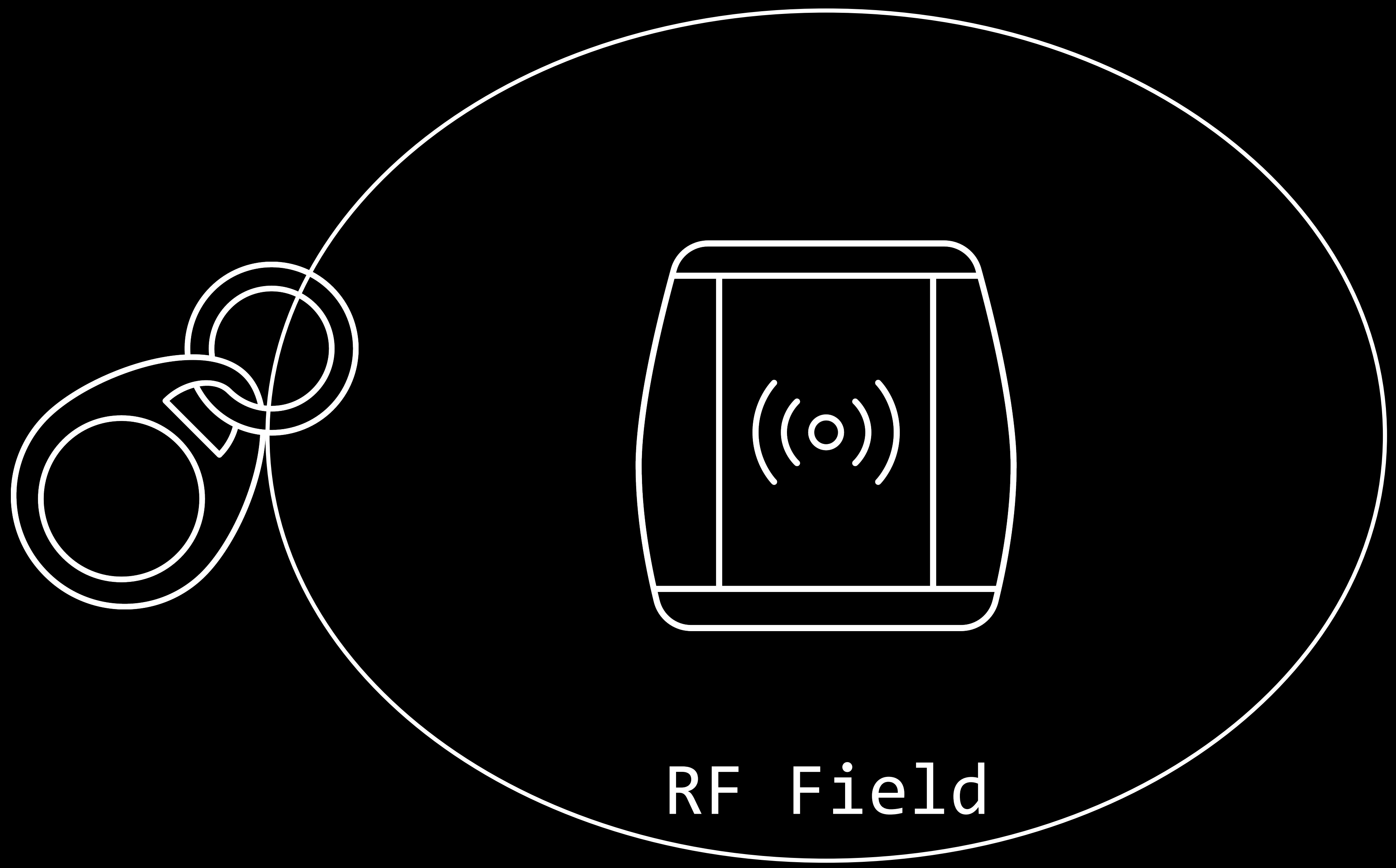




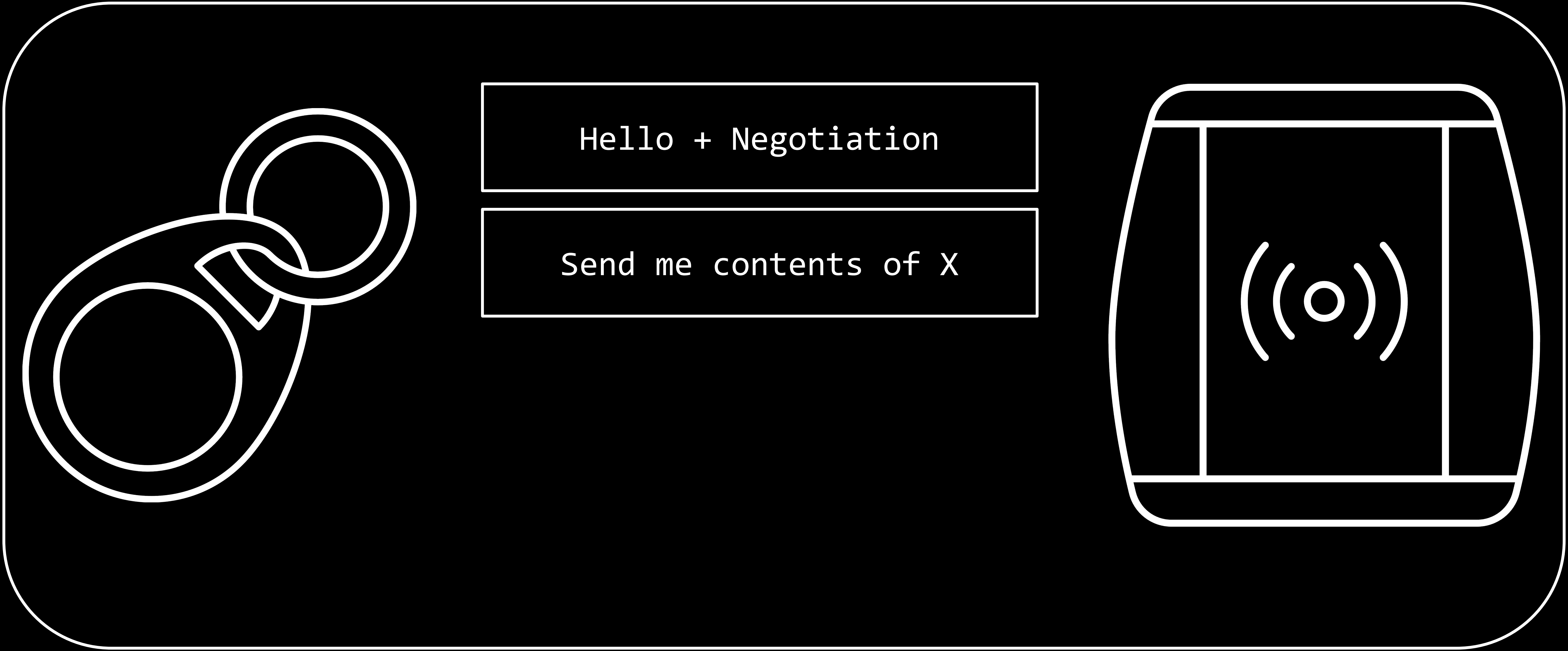



FACILITY CODE
1337
CARD NUMBER
1337


RF Field

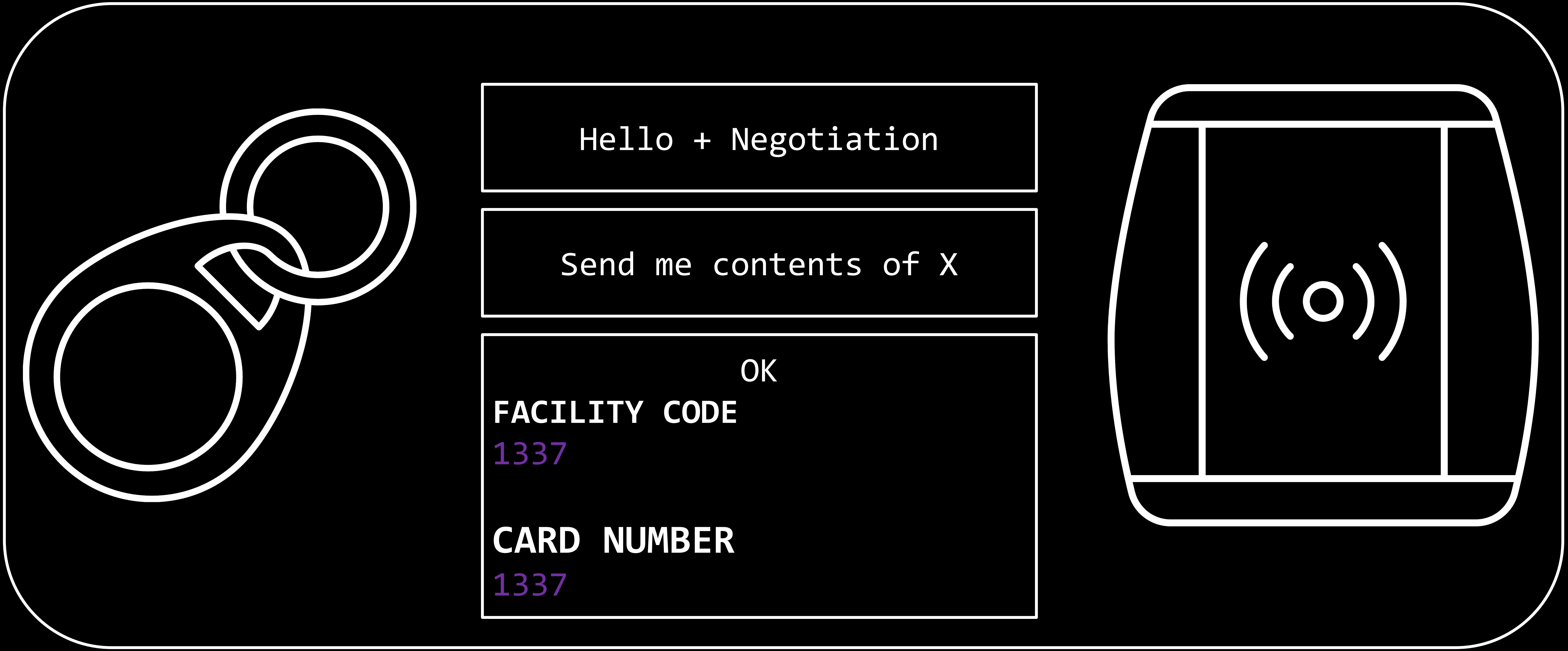

RF Field

Hello + Negotiation



Hello + Negotiation

Send me contents of X



Hello + Negotiation

Send me contents of X

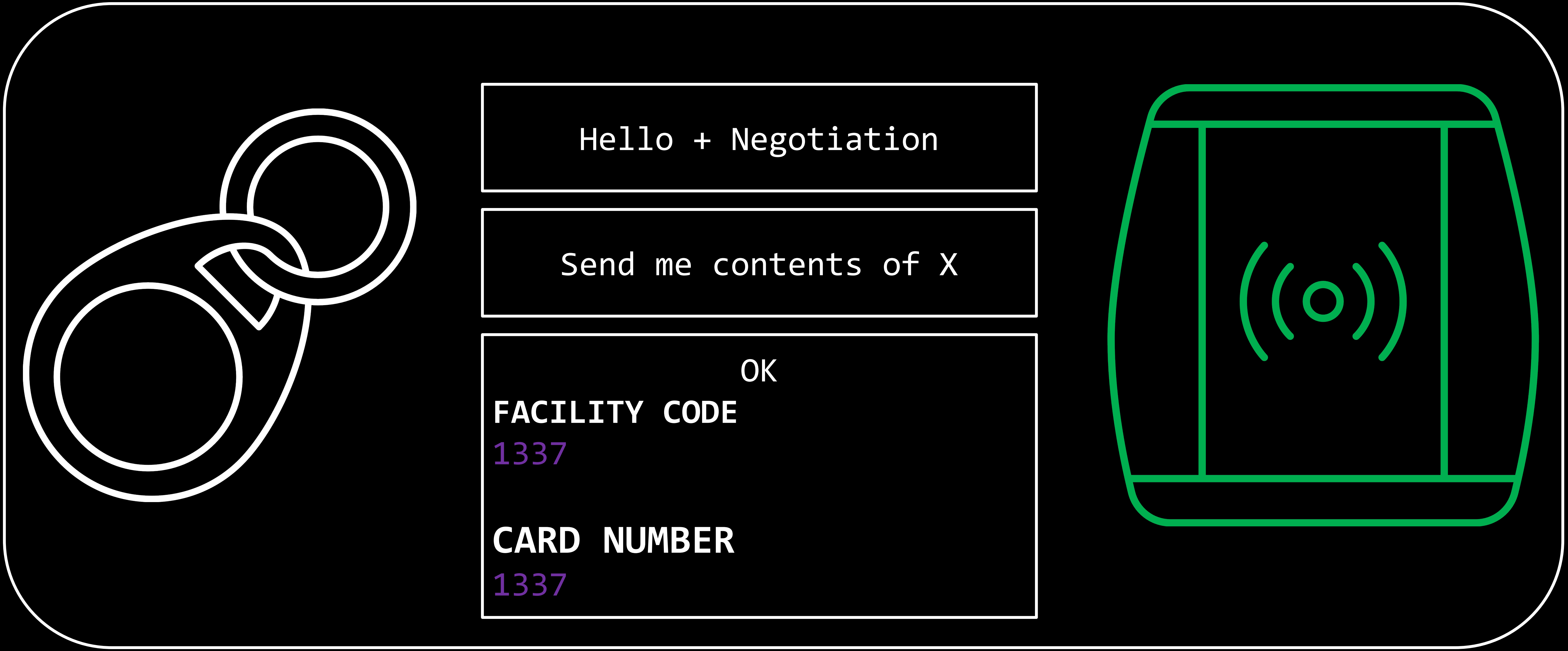
OK

**FACILITY CODE**

1337

**CARD NUMBER**

1337



Hello + Negotiation

Send me contents of X

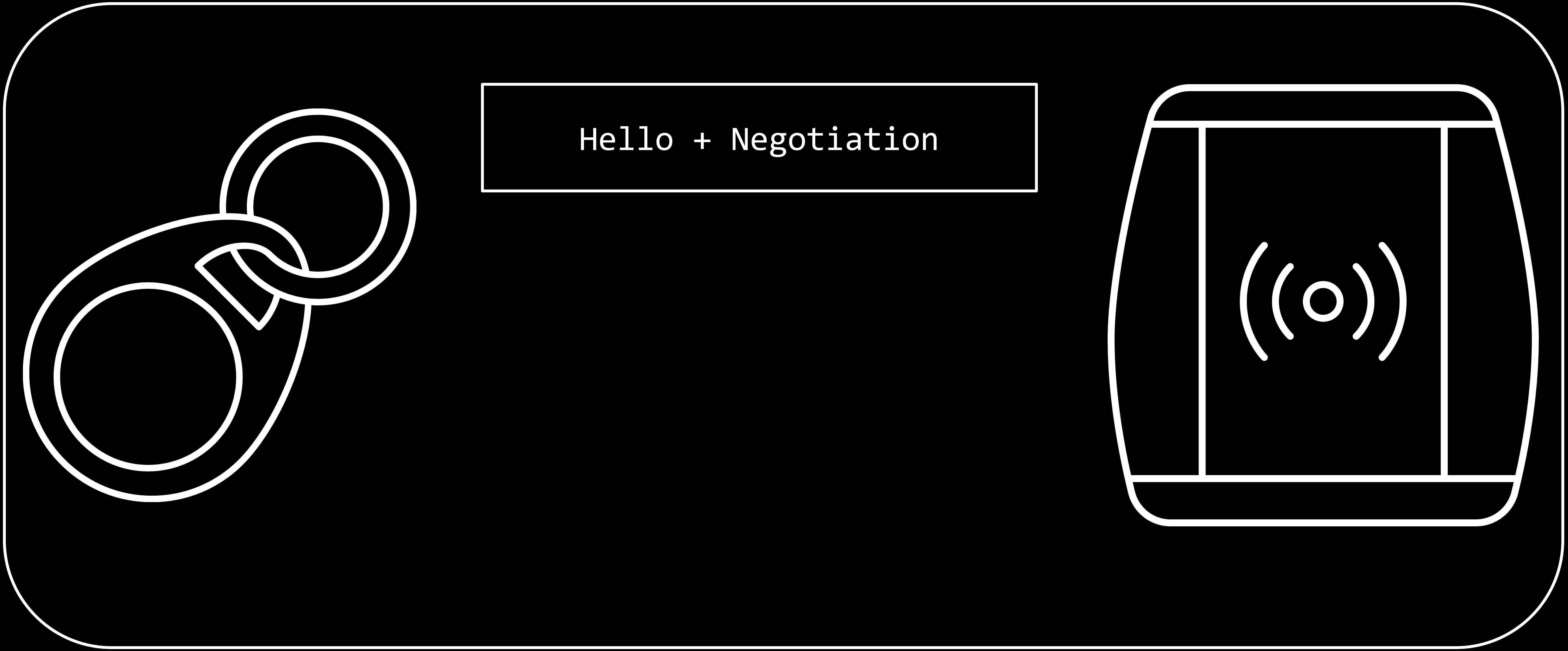
OK

**FACILITY CODE**

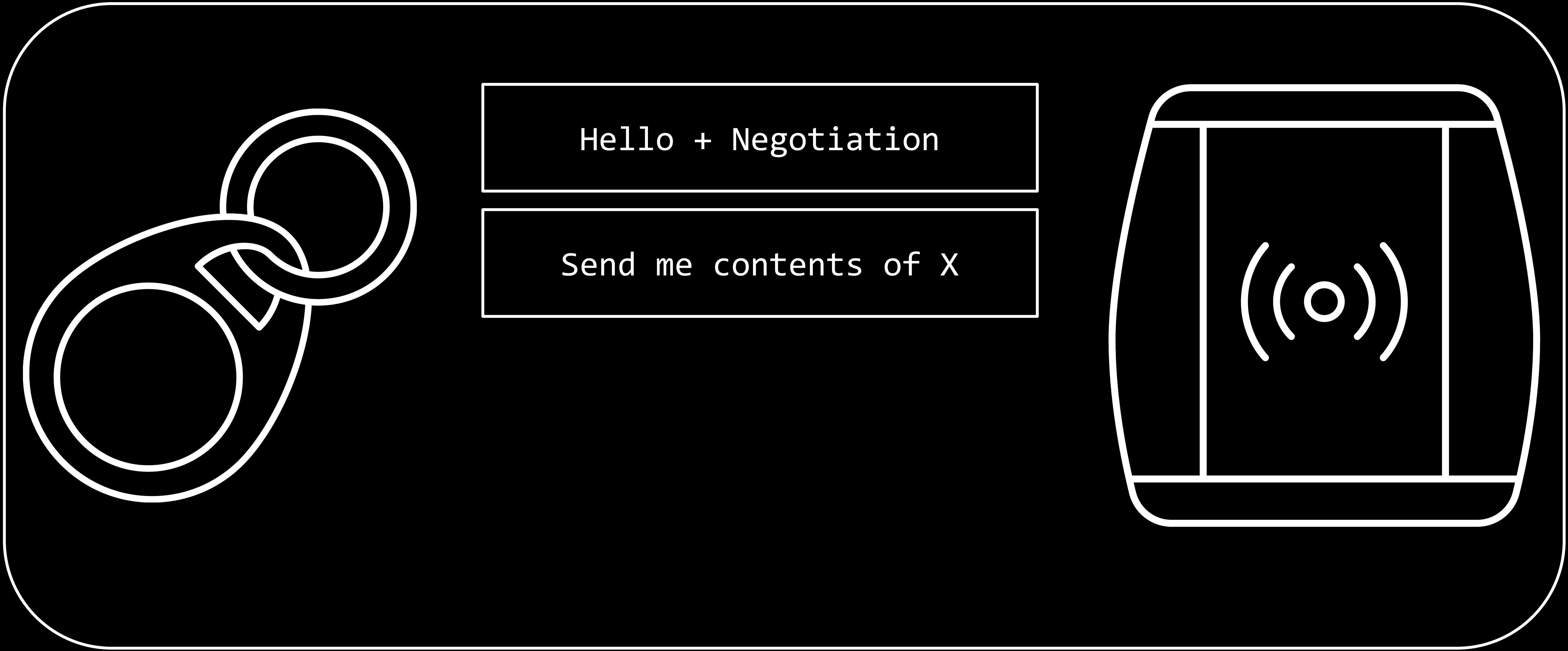
1337

**CARD NUMBER**

1337

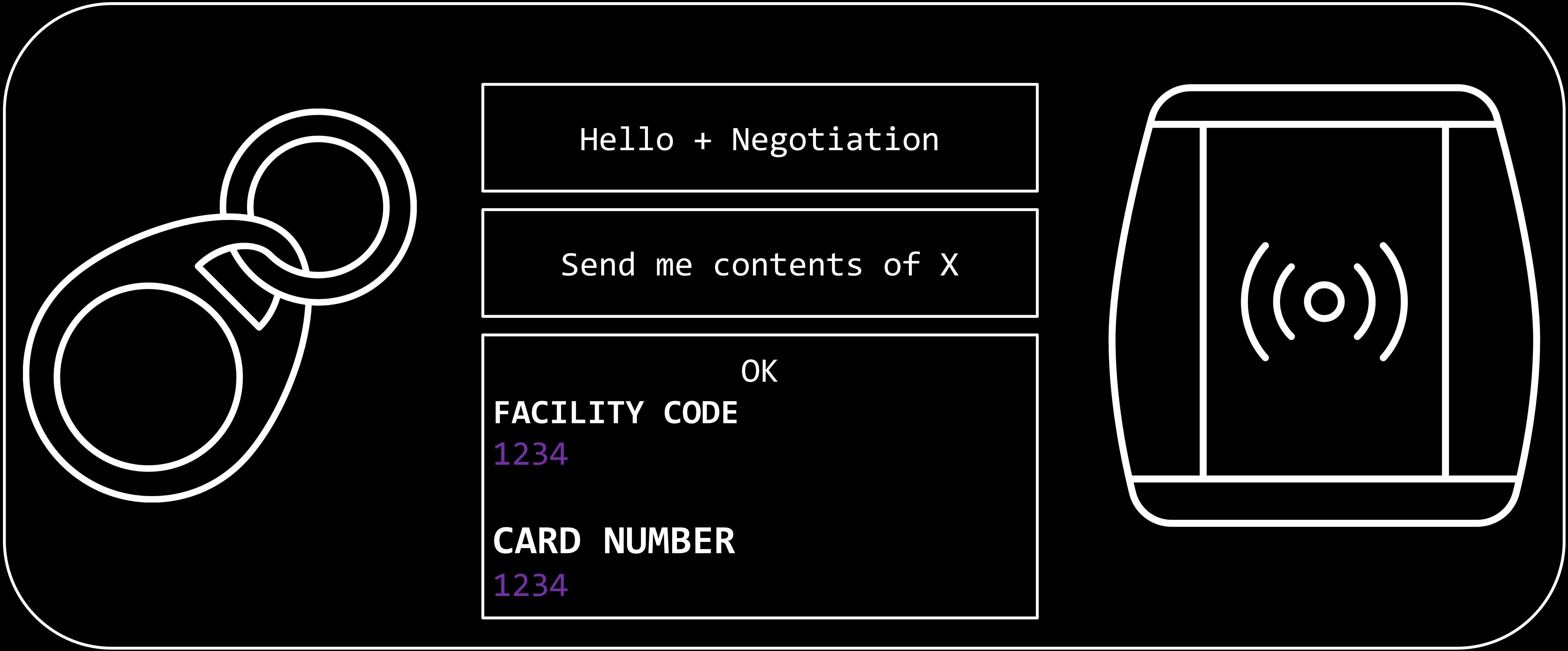


Hello + Negotiation



Hello + Negotiation

Send me contents of X



Hello + Negotiation

Send me contents of X

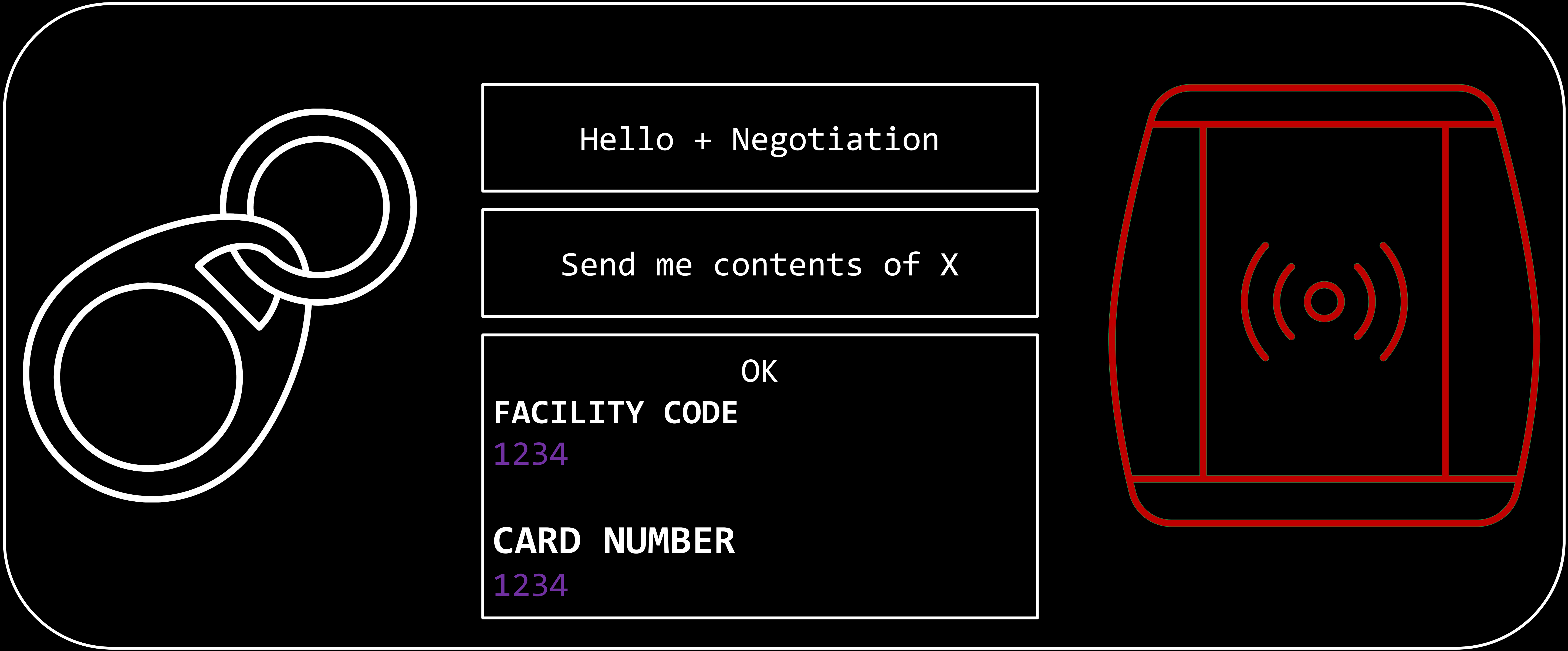
OK

**FACILITY CODE**

1234

**CARD NUMBER**

1234



Hello + Negotiation

Send me contents of X

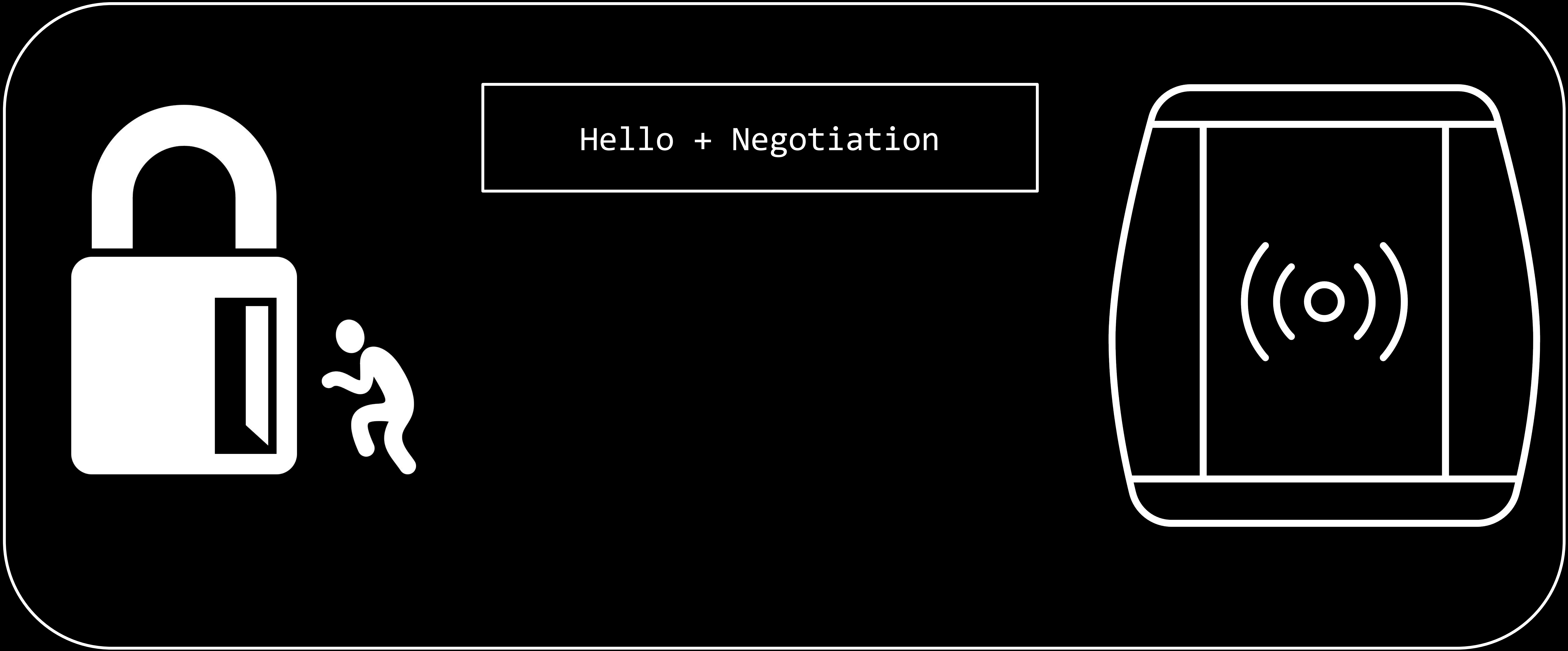
OK

**FACILITY CODE**

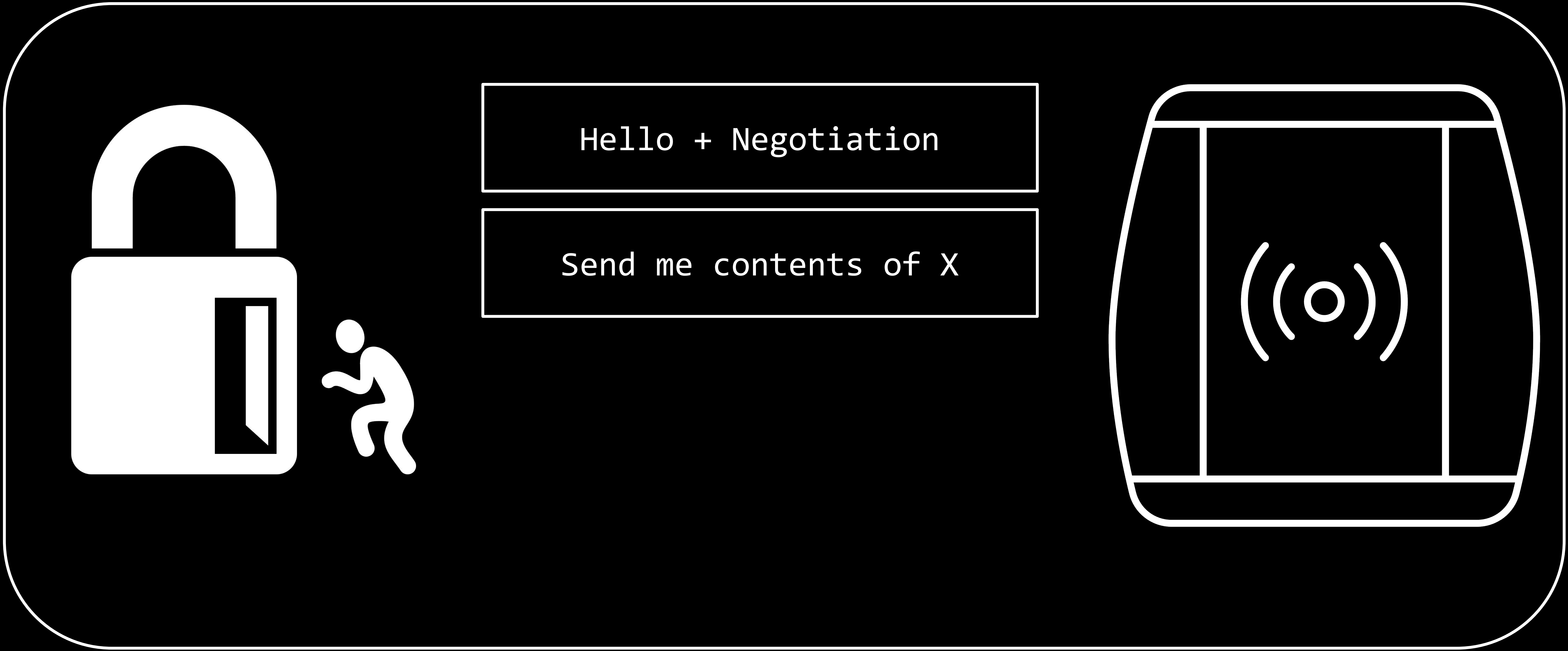
1234

**CARD NUMBER**

1234

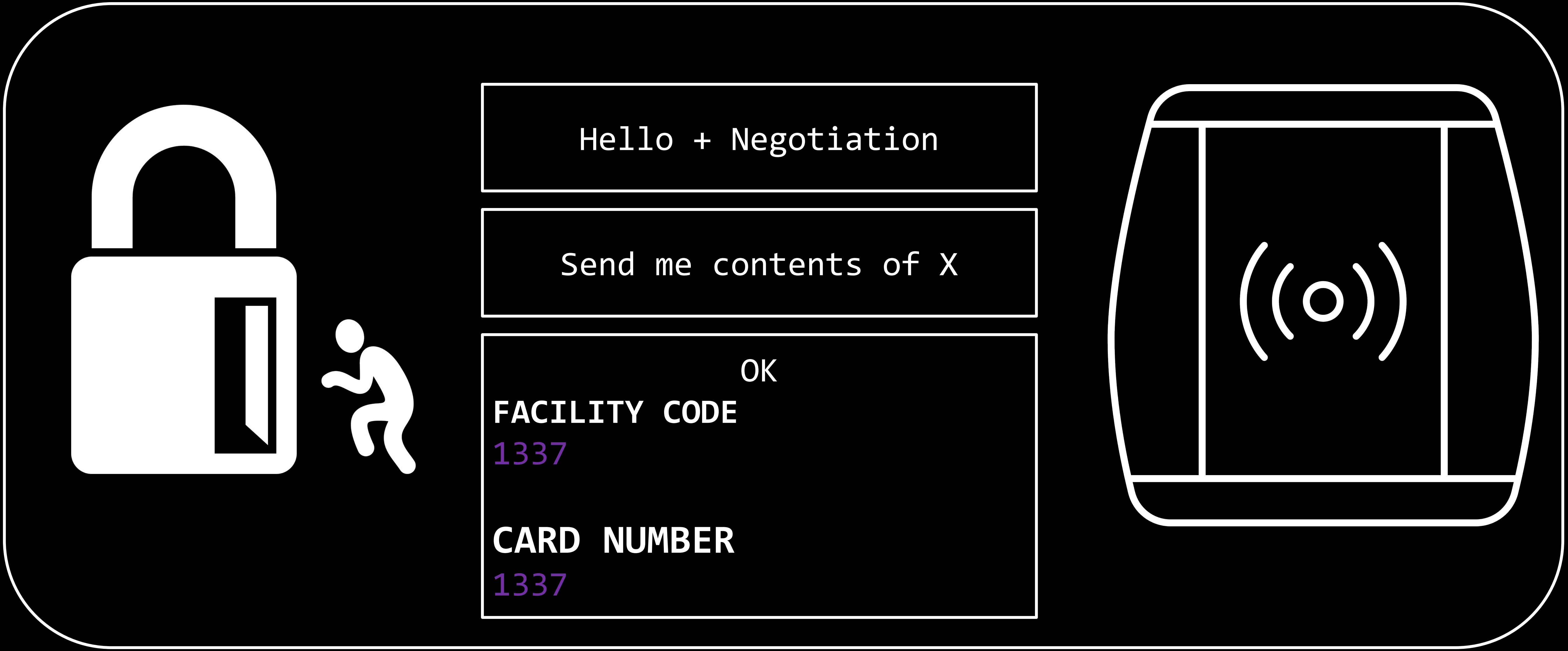


Hello + Negotiation



Hello + Negotiation

Send me contents of X



Hello + Negotiation

Send me contents of X

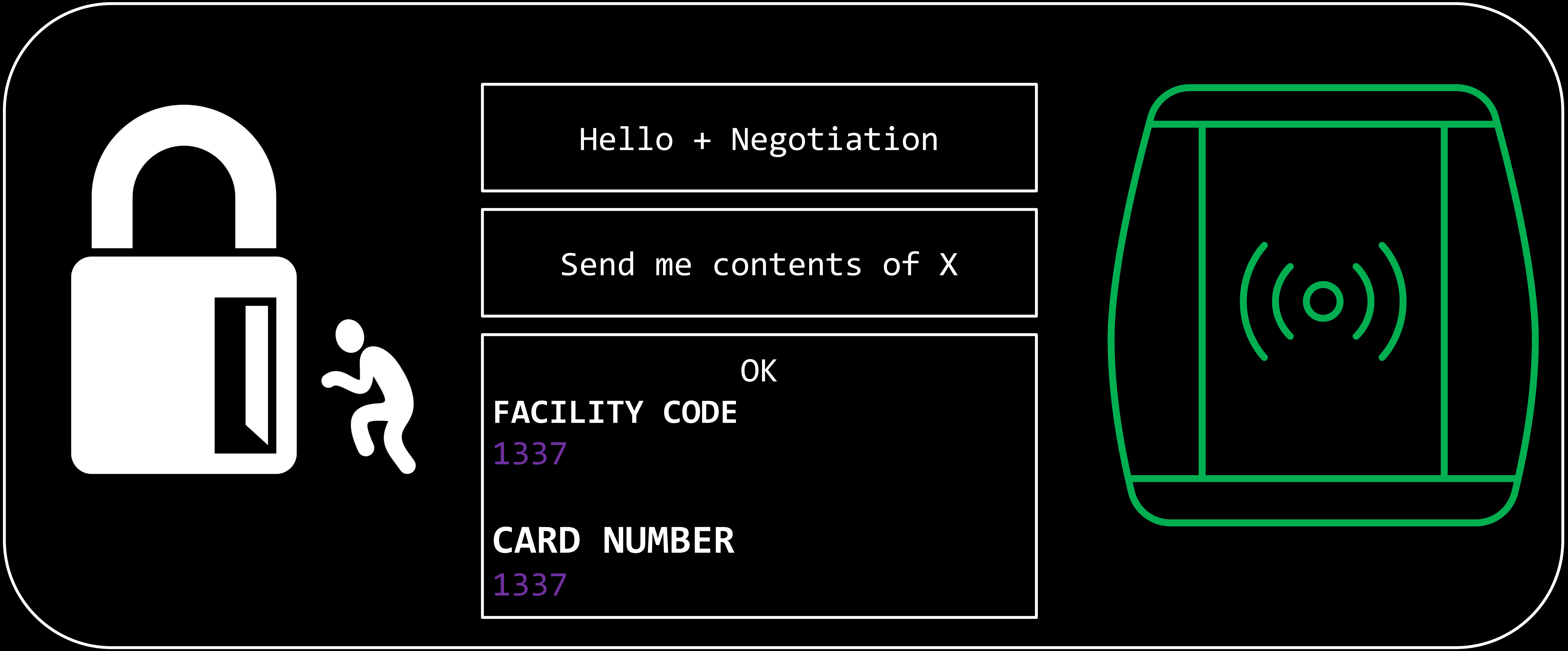
OK

**FACILITY CODE**

1337

**CARD NUMBER**

1337



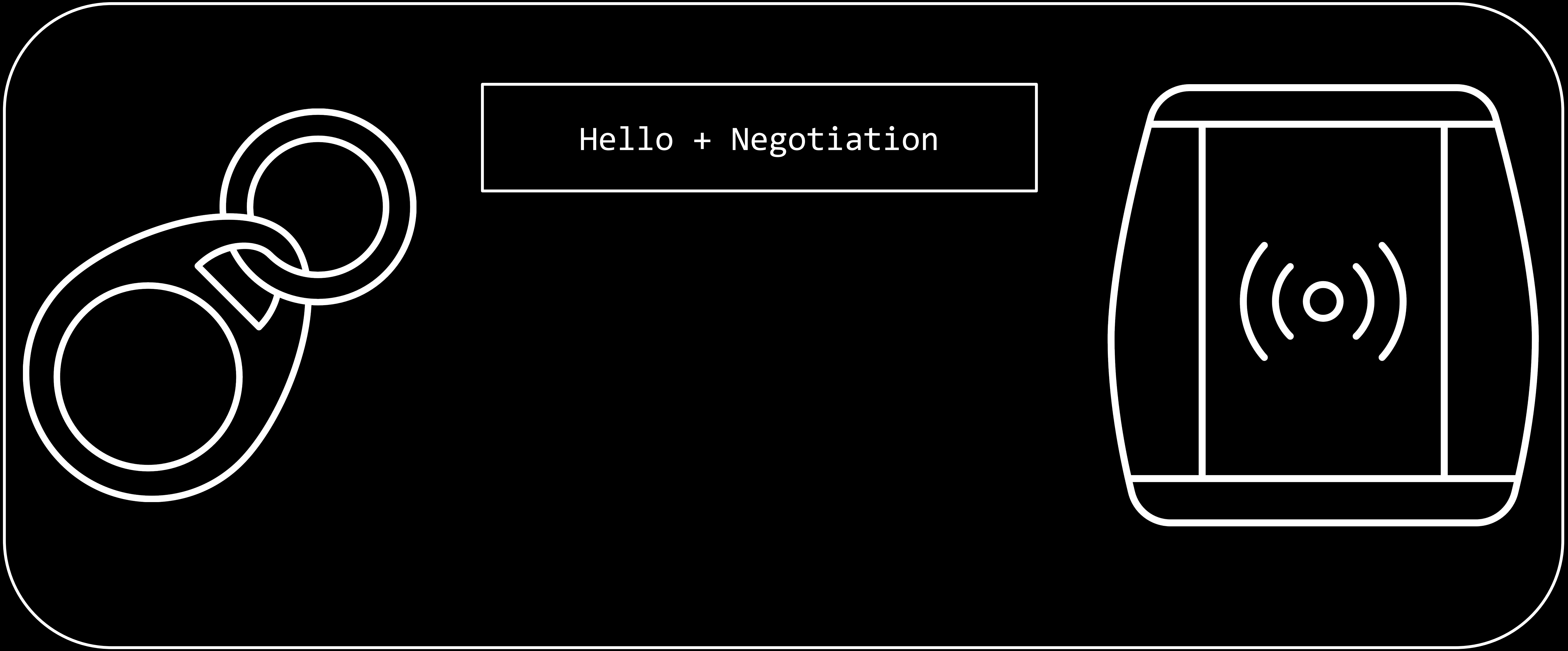
Hello + Negotiation

Send me contents of X

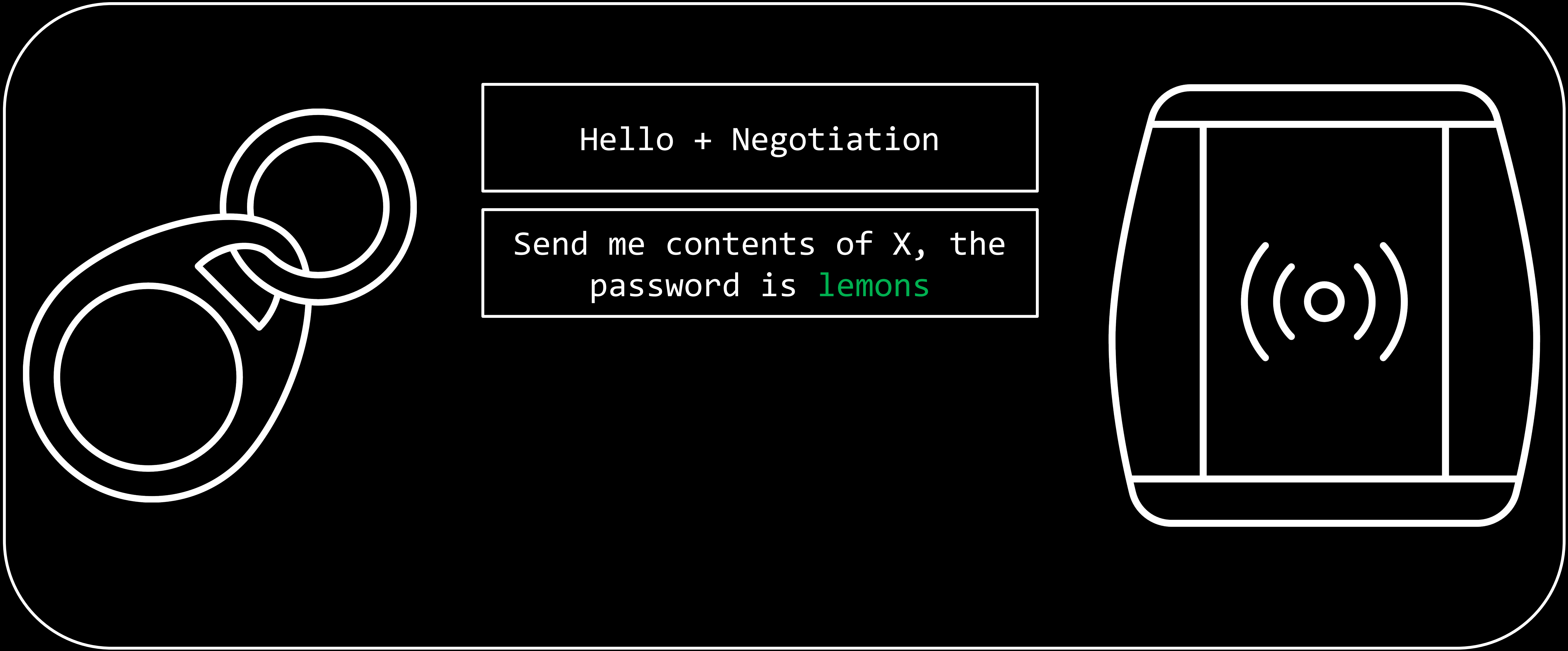
OK

**FACILITY CODE**
1337

**CARD NUMBER**
1337

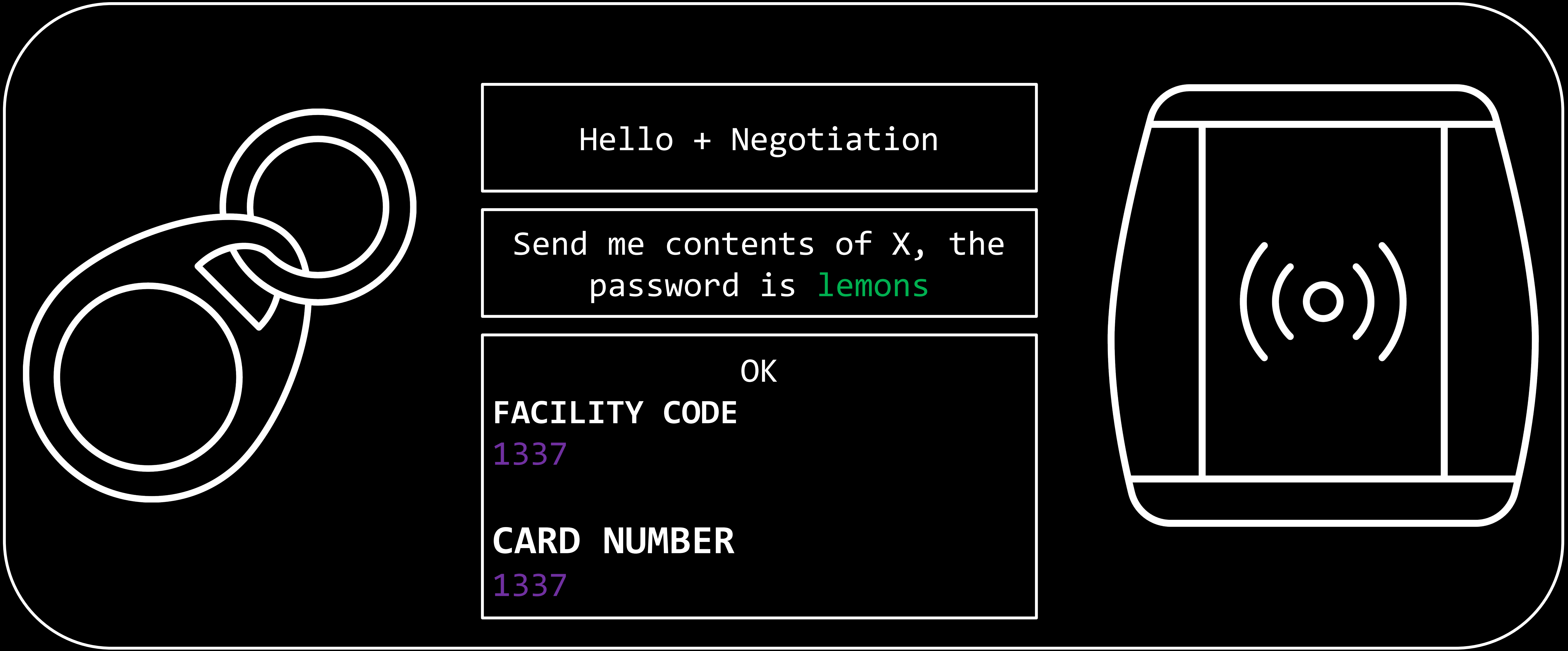


Hello + Negotiation



Hello + Negotiation

Send me contents of X, the password is lemons



Hello + Negotiation

Send me contents of X, the password is lemons

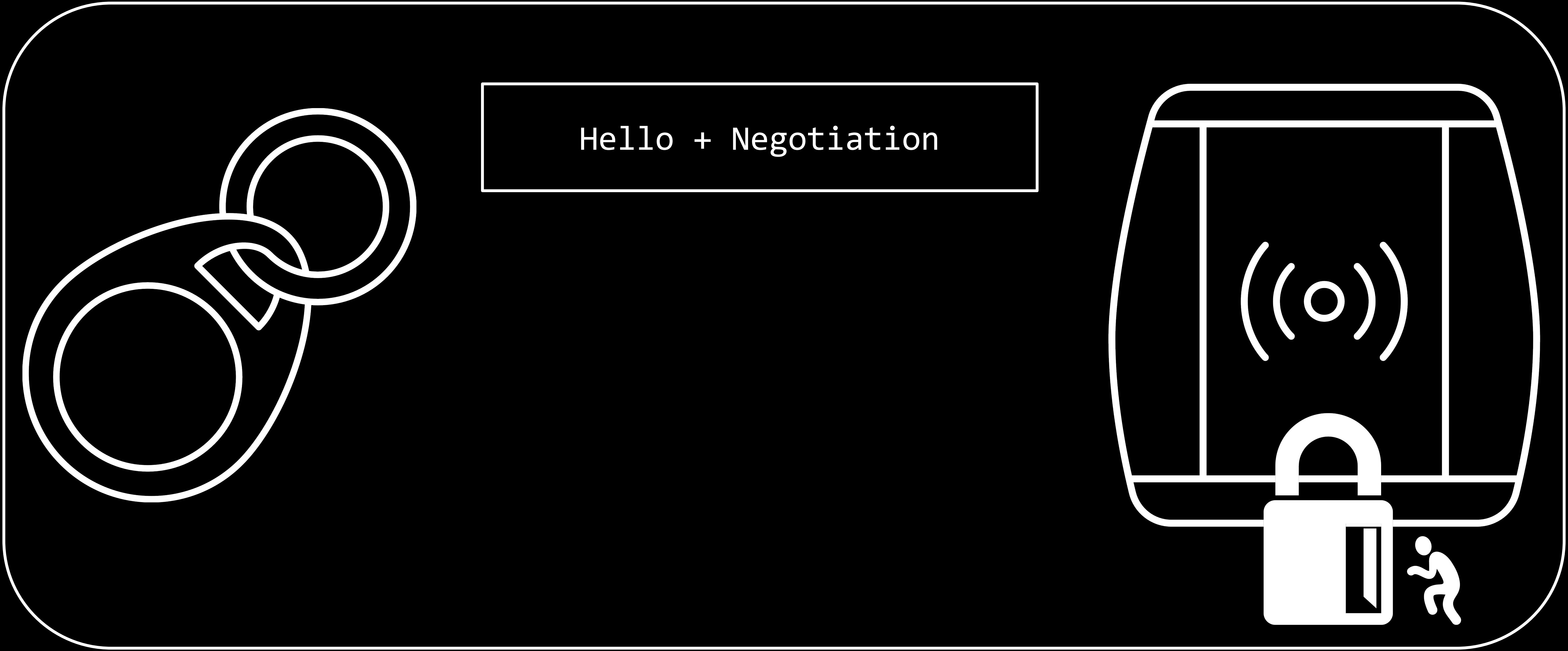
OK

**FACILITY CODE**

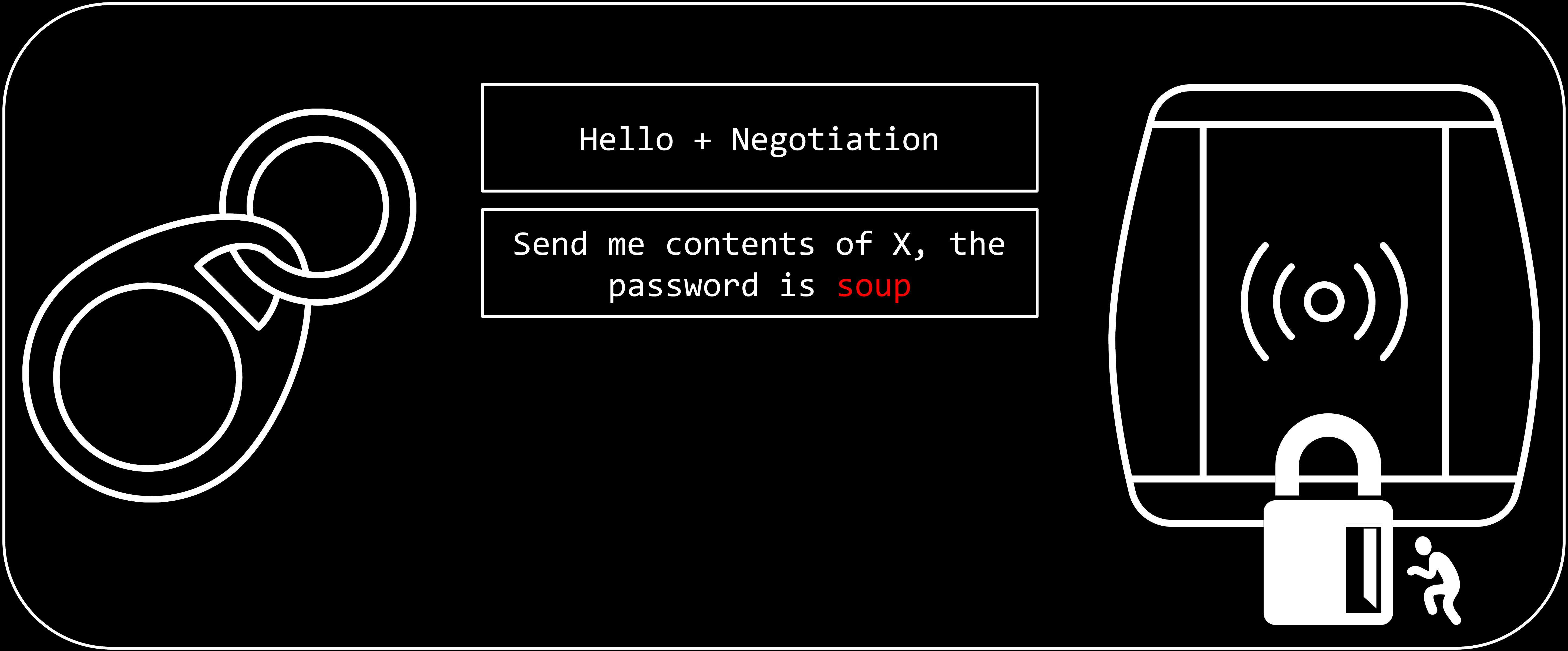
1337

**CARD NUMBER**

1337

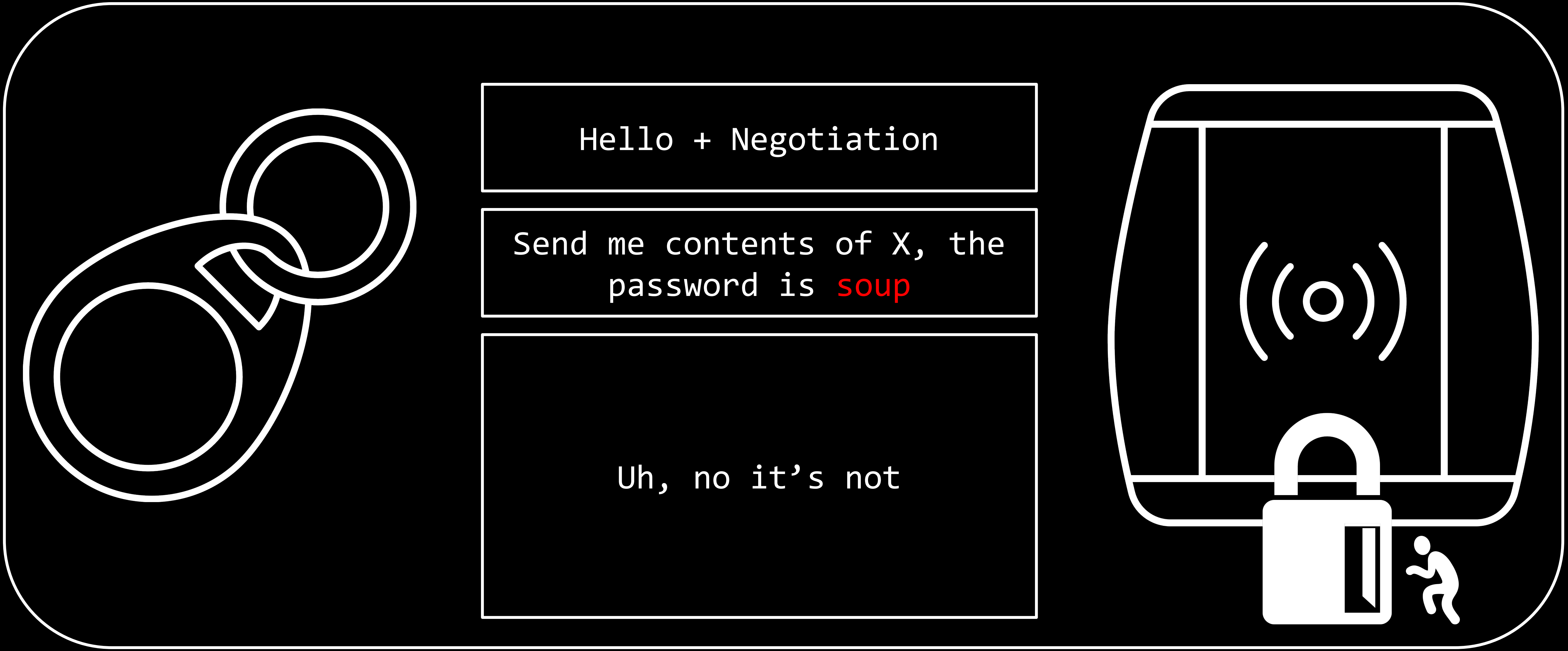


Hello + Negotiation



Hello + Negotiation

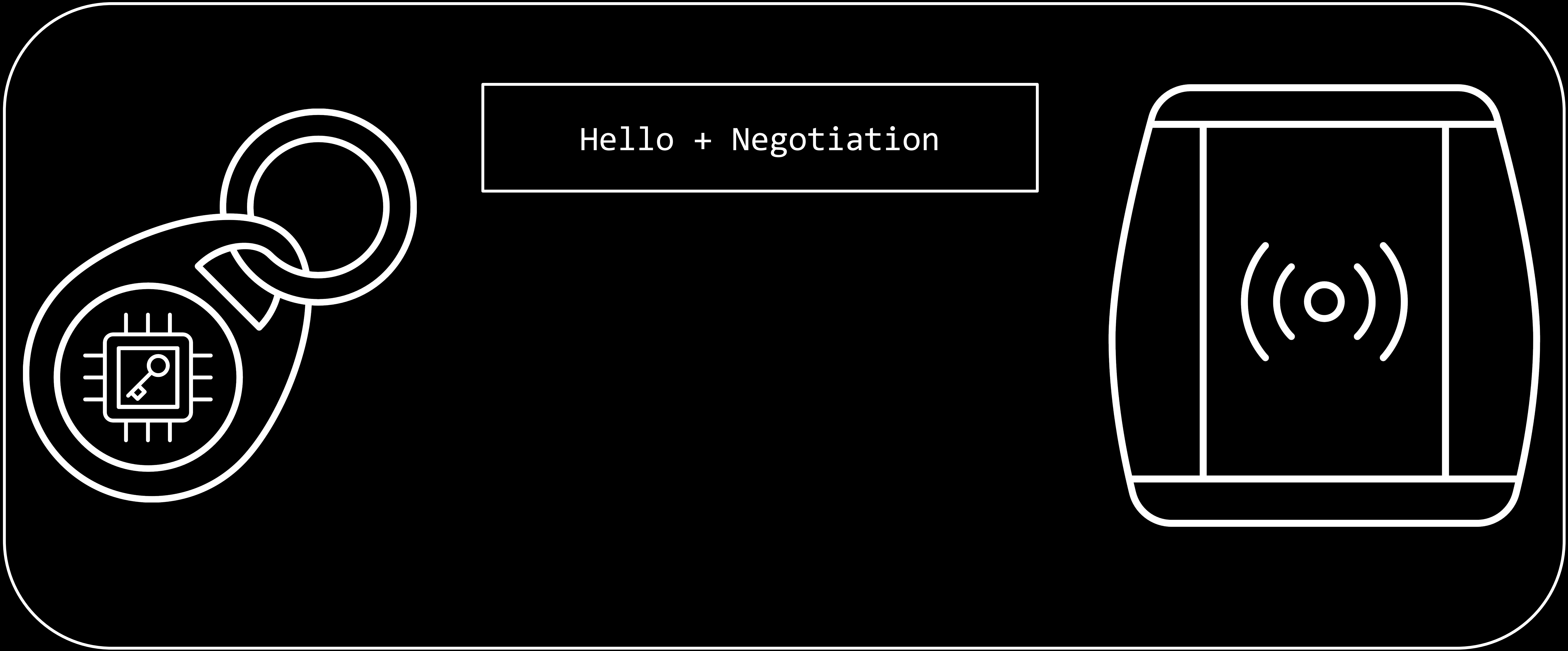
Send me contents of X, the password is soup



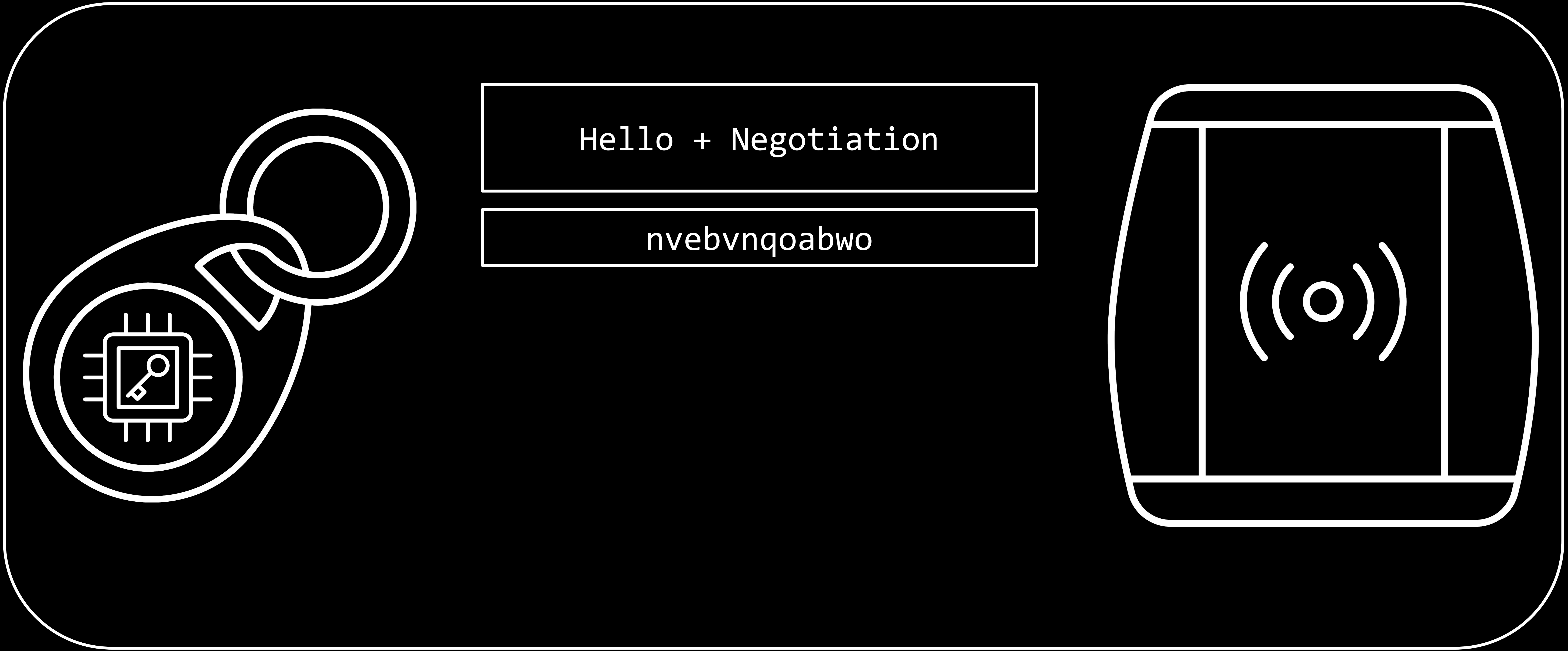
Hello + Negotiation

Send me contents of X, the password is soup

Uh, no it’s not

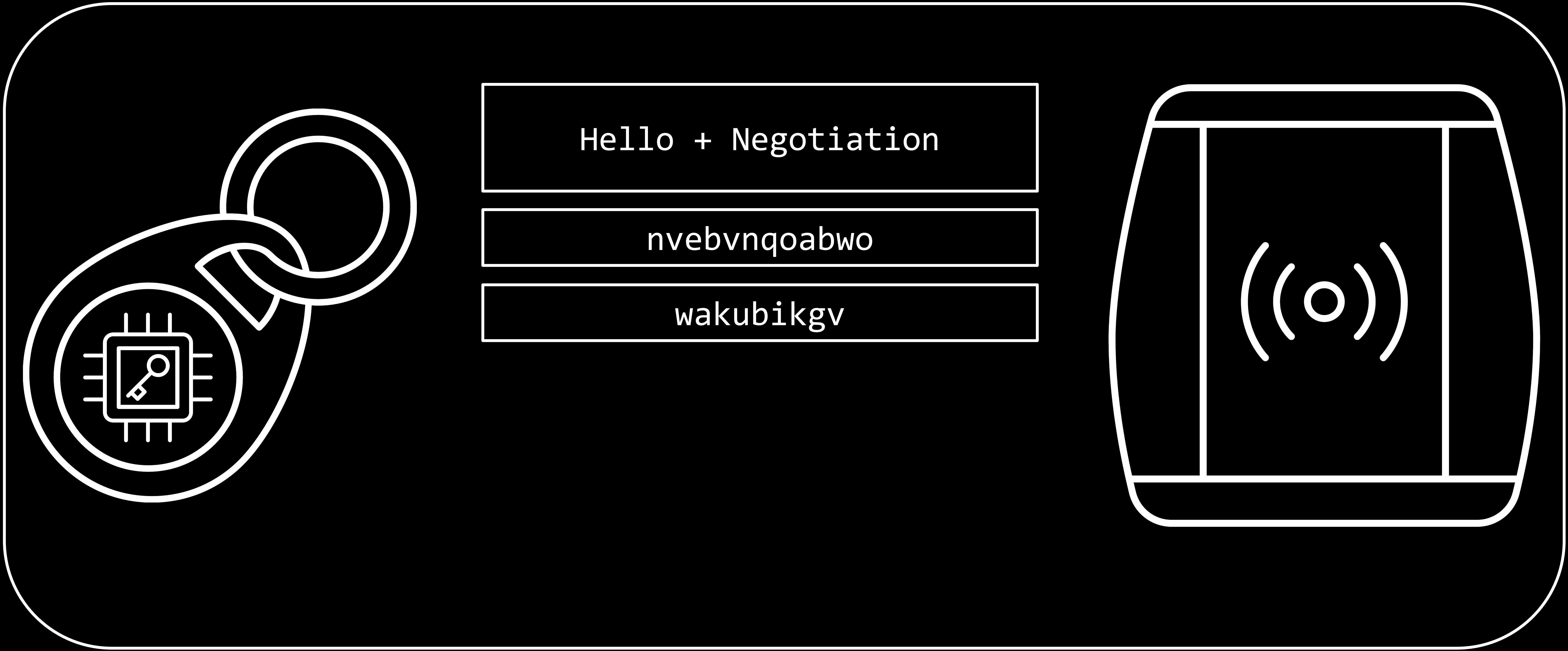


Hello + Negotiation



Hello + Negotiation

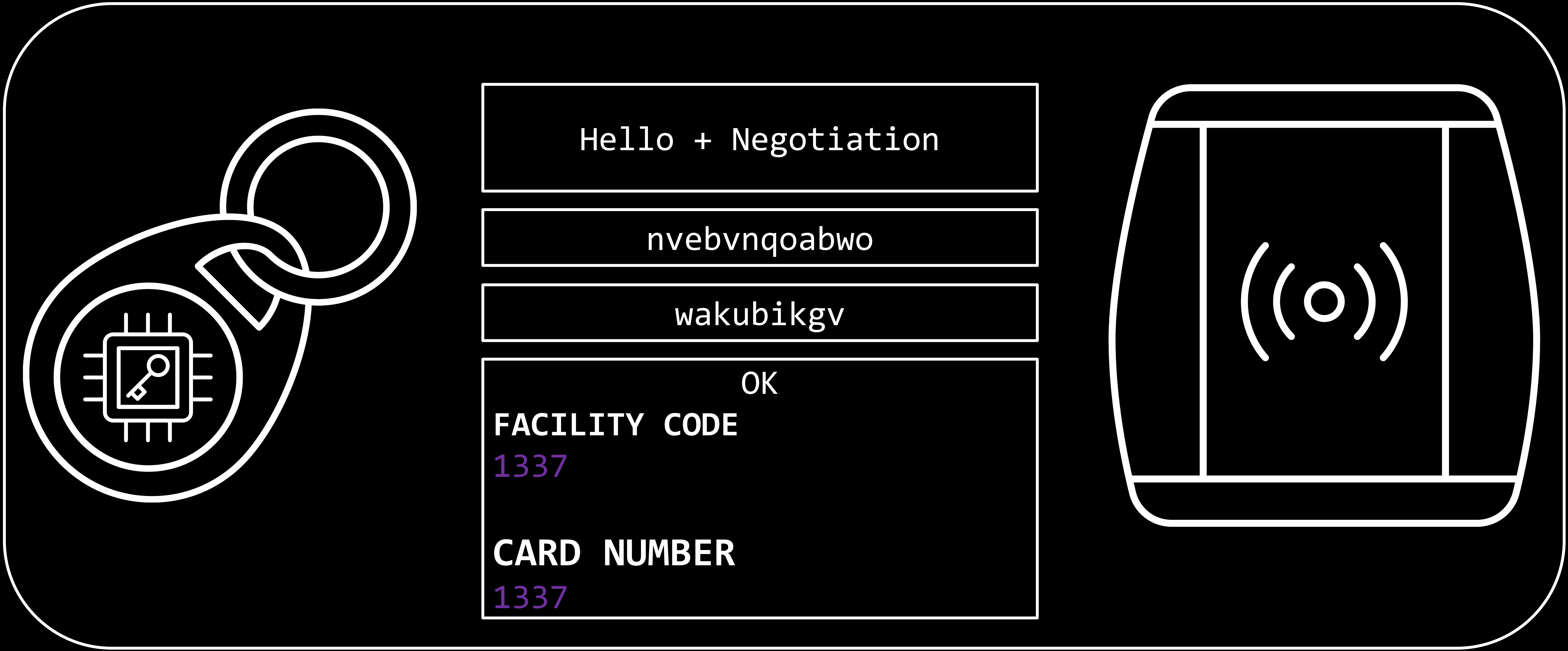
nvebvnqoabwo



Hello + Negotiation

nvebvnqoabwo

wakubikgv



Hello + Negotiation

nvebvnqoabwo

wakubikgv

OK

**FACILITY CODE**

1337

**CARD NUMBER**

1337

- HID SEOS – iCLASS SEOS

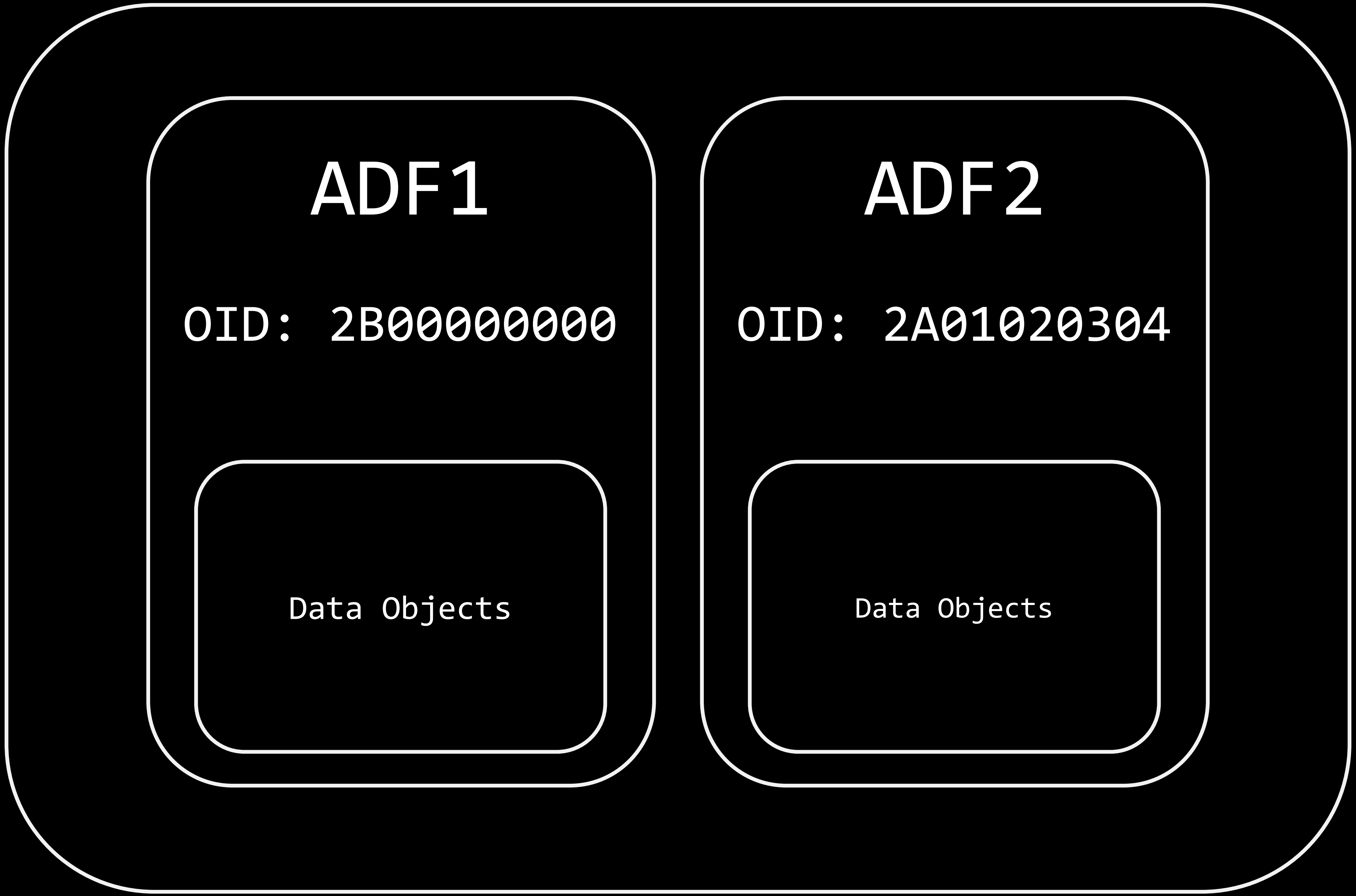
- HID Global produced
- Successor to previous iClass Generation
- Released with some information in a whitepaper
  - Strong Authentication
  - Technology Independent Security
  - Heightened Privacy Protection
  - AES Security
- Lots of discussion about this being the future

- Not much actual documentation or 3rd party support online

## Terms

| | |
|---|---|
| ADF | Application Data File |
| GDF | Global Data File |
| Diversifier | Static value on the ADF |
| ICC | Card |
| IFD | Reader |
| Priv Keyset | Keys used during the privacy exchange |
| Auth Keyset | Keys used during the Authentication Exchange |

SEOS



ADF1

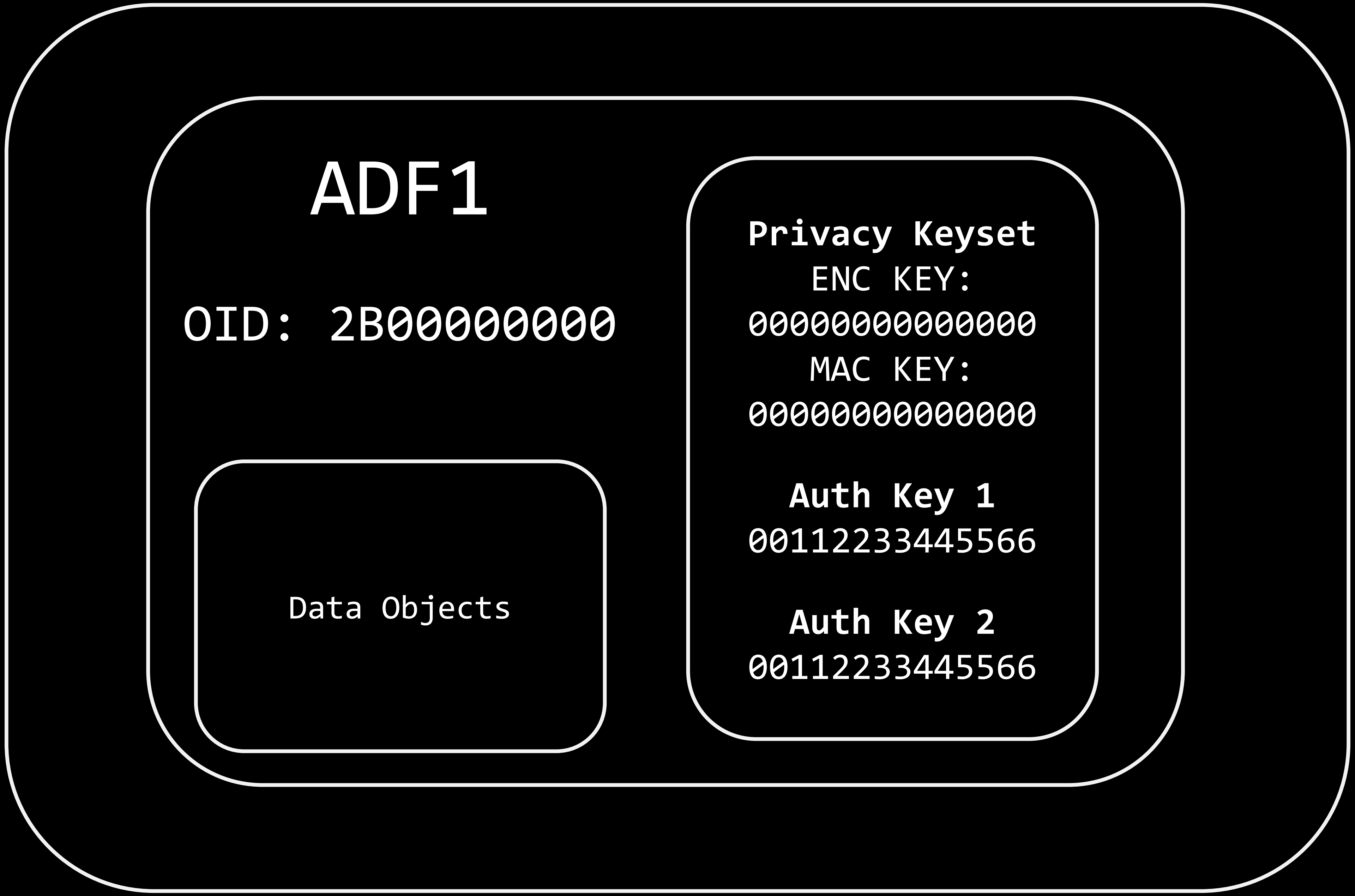
OID: 2B00000000

Data Objects

ADF2

OID: 2A01020304

Data Objects



ADF1

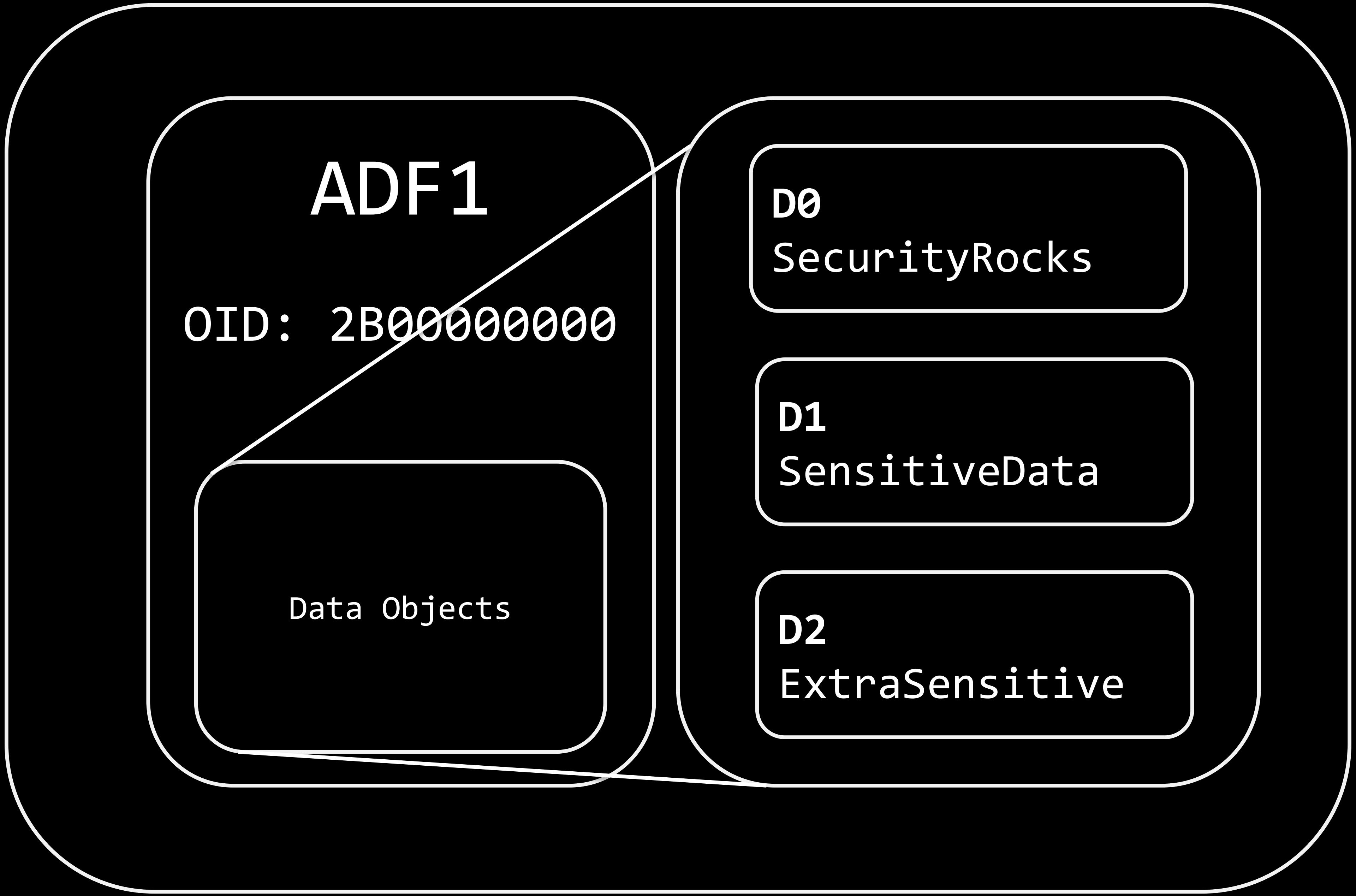
OID: 2B00000000

Data Objects

**Privacy Keyset**
ENC KEY:
00000000000000
MAC KEY:
00000000000000

**Auth Key 1**
00112233445566

**Auth Key 2**
00112233445566


ADF1
OID: 2B00000000
Data Objects
D0
SecurityRocks
D1
SensitiveData
D2
ExtraSensitive

- How do you even reverse engineer a RFID protocol?
- Doc Review
  - Public sources
    - https://www.hidglobal.com/sites/default/files/resource_files/pacs-seos-card-ds-en_0.pdf
    - https://www.digitalid.co.uk/media/download/HID-Seos-Brochure.pdf
    - https://csd.com.au/ts1523350398/attachments/ProductAttachmentGroup/4/HID-CP1000%20User%20Manual.pdf
  - Patent Information
    - Privacy preserving tag (*US10826707B2*)
    - Field revisions for a personal security device  (*EP2831802B1*)
  - Academic Papers
    - An analysis of the HID Indala and Seos protocols - Luud
    - Unlocking doors from half a continent away: A relay attack against HID Seos – Haskins, Stevado
- hf 14a sniff

```
       Start |          End | Src | Data (! denotes parity error)                                        | CRC | Annotation
-------------+--------------+-----+---------------------------------------------------------------------+-----+--------------------
           0 |         2368 | Tag |04  00                                                               |     |
     1310544 |      1312912 | Tag |04  00                                                               |     |
     2621248 |      2623616 | Tag |04  00                                                               |     |
     2654560 |      2660384 | Tag |08  3C  7F  7E  35                                                   | !!  |
     2690992 |      2694576 | Tag |20  FC  70                                                           | A ok|
     2731808 |      2740000 | Tag |05  78  77  94  02  6D  C8                                           | A ok|
     2839600 |      2843120 | Tag |D0  73  87                                                           | A ok|
     3098560 |      3105600 | Tag |0A  00  69  86  DD  D9                                               | A ok|
     3174368 |      3181344 | Tag |0B  00  69  86  66  C5                                               | A ok|
     3243808 |      3250848 | Tag |0A  00  69  86  DD  D9                                               | A ok|
     3356976 |      3363952 | Tag |0B  00  69  86  66  C5                                               | A ok|
     3487440 |      3510608 | Tag |0A  00  6F  0C  84  0A  A0  00  00  04  40  00  01  01  00  01  90  00 |     |
             |              |     |6F  A4                                                               | A ok|
     3742416 |      3807951 | Tag |0B  00  CD  02  09  07  85  40  19  7F  CD  5B  7B  AD  9B  1A  B1  92 |     |
             |              |     |49  E4  5D  69  AE  5E  39  A0  40  B8  4C  B5  ED  EF  E5  06  E8  A8 |     |
             |              |     |76  C9  CF  90  AC  07  22  4D  39  AB  D8  37  5B  70  50  26  48  08 |     |
             |              |     |A3  CE  CC  27  E3  18  4B  14  8B  9A  A2  FA  75  DE  F7  5D  F8  DD |     |
             |              |     |8E  08  E0  B0  DD  56  8F  B1  1F  04  90  00  C6  02               | A ok|
     4127296 |      4148160 | Tag |0A  00  7C  0A  81  08  01  81  E4  38  01  01  02  01  90  00  1C  46 | A ok|
     4652016 |      4709744 | Tag |0B  00  7C  2A  82  28  B4  7D  5E  94  93  B6  2E  76  DE  29  B7  86 |     |
             |              |     |6D  90  2D  91  C9  01  7A  2B  FA  72  2B  52  05  B9  BB  FC  3D  C0 |     |
             |              |     |4C  16  94  D5  3E  35  9D  CF  36  20  90  00  7B  9D               | A ok|
     5115232 |      5180767 | Tag |0A  00  85  40  1D  8A  DB  06  2E  D5  64  80  F4  CC  A5  56  55  42 |     |
             |              |     |3C  83  B0  16  E9  3A  EC  2F  86  1E  50  86  D6  1C  C8  F1  15  C4 |     |
             |              |     |A4  1D  05  D5  94  96  4B  64  95  6C  07  96  9B  31  B3  2C  65  76 |     |
             |              |     |A5  94  58  B2  96  80  B9  9B  7B  F9  E1  7C  DC  C3  99  02  90  00 |     |
             |              |     |8E  08  BB  4B  96  E7  B8  0C  42  B6  90  00  FE  4B               | A ok|
     5524976 |      5529712 | Tag |CA  00  7A  29                                                       | A ok|
    15006960 |     15009328 | Tag |04  00                                                               |     |
    15029088 |     15034976 | Tag |08  DD  FF  C5  EF                                                   | !!  |
0B00A404000AA00000044000010100010039C
```

```
0A007C0A81080181E4380101020190001C46
```

```
0B0380A504001306112B0601040181E438010102011801010202008A4C
```

```
0B00CD0209078540197FCD5B7BAD9B1AB19249E45D69AE5E39A040B84CB5EDEFE506
E8A876C9CF90AC07224D39ABD8375B7050264808A3CECC27E3184B148B9AA2FA75DE
F75DF8DD8E08E0B0DD568FB11F049000C602
```

```
0A0300870001047C0281000041DB
```

```
0A007C0A81080181E4380101020190001C46
```

```
0B007C2A8228B47D5E9493B62E76DE29B7866D902D91C9017A2BFA722B5205B9BBFC
3DC04C1694D53E359DCF362090007B9D
```

```
0B00A404000AA0000004400001010001000039C
```

```
0A007C0A81080181E43801010201900001C46
```

```
0B00CD0209078540197FCD5B7BAD9B1AB19249E45D69AE5E39A040B84CB5EDEFE506
E8A876C9CF90AC07224D39ABD8375B7050264808A3CECC27E3184B148B9AA2FA75DE
F75DF8DD8E08E0B0DD568FB11F049000C602
```

```
0A007C0A81080181E43801010201900001C46
```

```
0B007C2A8228B47D5E9493B62E76DE29B7866D902D91C9017A2BFA722B5205B9BBFC
3DC04C1694D53E359DCF362090007B9D
```

```
0A0085401D8ADB062ED56480F4CCA55655423C83B016E93AEC2F861E5086D61CC8F1
15C4A41D05D594964B64956C07969B31B32C6576A59458B29680B99B7BF9E17CDCC3
990290008E08BB4B96E7B80C42B69000FE4B
```

```
0B00A404000AA000004400000101000100039C
```

```
        0B       00A404000AA000004400000101000100       039C
Encapsulation                  APDU                       CRC
```

```
F75DF8DD8E08E0B0DD568FB11F049000C602
```

```
0A007C0A81080181E4380101020190001C46
```

```
0B007C2A8228B47D5E9493B62E76DE29B7866D902D91C9017A2BFA722B5205B9BBFC
3D04C1694D53E359DCF362090007B9D
```

```
0A0085401D8ADB062ED56480F4CCA55655423C83B016E93AEC2F861E5086D61CC8F1
15C4A41D05D594964B64956C07969B31B32C6576A59458B29680B99B7BF9E17CDCC3
990290008E08BB4B96E7B80C42B69000FE4B
```

```
0B00A404000AA000000440000101000100039C
```

```
      0B        00A404000AA0000004400001010001000       039C
Encapsulation                APDU                      CRC
```

```
E75DF8DD8E08E0B0DD568FB11F049000C602
```

```
00 A4 04 00 0A A0000004400001010001000
         ISO7816 – SELECT FILE
```

```
0B007C2A8228B47D5E9493B62E76DE29B7866D902D91C9017A2BFA722B5205B9BBFC
3DC04C1694D53E359DCF362090007B9D
```

```
0A0085401D8ADB062ED56480F4CCA55655423C83B016E93AEC2F861E5086D61CC8F1
15C4A41D05D594964B64956C07969B31B32C6576A59458B29680B99B7BF9E17CDCC3
990290008E08BB4B96E7B80C42B69000FE4B
```

```
0B00A404000AA000000440000101000100039C
```

```
0B              00A404000AA000000440000101000100     039C
Encapsulation                 APDU                    CRC
```

E75DF8DD8E08E0B0DD568FB11F049000C602

```
00 A4 04 00 0A A000000440000101000100
        ISO7816 – SELECT FILE
```

0B007C2A8228B47D5E9493B62E76DE29B7866D902D91C9017A2BFA722B5205B9BBFC

```
          0A                 A000000440 000101000100
   Length of Data          Application ID (RID + PIX)
```

990290008E08BB4B96E7B80C42B69000FE4B

```
0B00A404000AA000000440000101000100039C
```

```
0A007C0A81080181E4380101020190001C46
```

```
007C0A81080181E43801010201        9000 (OK)
APDU                   Response Code
```

```
0A007C0A81080181E4380101020190001C46
```

```
0B007C2A8228B47D5E9493B62E76DE29B7866D902D91C9017A2BFA722B5205B9BBFC
3DC04C1694D53E359DCF362090007B9D
```

```
0A0085401D8ADB062ED56480F4CCA55655423C83B016E93AEC2F861E5086D61CC8F1
15C4A41D05D594964B64956C07969B31B32C6576A59458B29680B99B7BF9E17CDCC3
990290008E08BB4B96E7B80C42B69000FE4B
```

0B00A404000AA0000004400001010001000039C

0A007C0A81080181E43801010201900001C46

007C0A81080181E43801010201 9000 (OK)

APDU Response Code

00 7C 0A81080181E43801010201

ISO7816 – SELECT FILE Response

0A 81080181E43801010201

Length Data

```
0B00A404000AA00000044000010100010003 9C
```

```
0A007C0A81080181E4380101020190001C46
```

```
0B0380A504001306112B0601040181E43801010201180101020200 8A4C
```

```
0B00CD0209078540197FCD5B7BAD9B1AB19249E45D69AE5E39A040B84CB5EDEFE506
E8A876C9CF90AC07224D39ABD8375B7050264808A3CECC27E3184B148B9AA2FA75DE
F75DF8DD8E08E0B0DD568FB11F049000C602
```

```
0A0300870001047C0281000041DB
```

```
0A007C0A81080181E4380101020190001C46
```

```
0B007C2A8228B47D5E9493B62E76DE29B7866D902D91C9017A2BFA722B5205B9BBFC
3DC04C1694D53E359DCF362090007B9D
```

```
0B0380A504001306112B0601040181E43801010201180101020200 8A4C
```

```
80   A5 04 001306112B0601040181E43801010201180101020200
  SM    Mutual Auth (Challenge RND ICC)
```

```
0B00CD020907854 0197FCD5B7BAD9B1AB19249E45D69AE5E39A040B84CB5EDEFE506
E8A876C9CF90AC07224D39ABD8375B7050264808A3CECC27E3184B148B9AA2FA75DE
F75DF8DD8E08E0B0DD568FB11F049000C602
```

```
0A03008700010 47C0281000041DB
```

```
0A007C0A81080181E43801010201900 01C46
```

```
0B007C2A8228B47D5E9493B62E76DE29B7866D902D91C9017A2BFA722B5205B9BBFC
3DC04C1694D53E359DCF362090007B9D
```

```
0B0380A504001306112B0601040181E438010102011801010202008A4C
```

```
80   A5 04 001306112B0601040181E43801010201180101020200
  SM    SEOS Command - Get ADF


A5   = INS Header for Get ADF
04   = Get ADF from OID (Object ID)

Modifying 04 to 07 has been seen for the GDF
```

```
0B007C2A8228B47D5E9493B62E76DE29B7866D902D91C9017A2BFA722B5205B9BBFC
3DC04C1694D53E359DCF362090007B9D
```

```
0B0380A504001306112B0601040181E4380101020118010102020008A4C
```

```
80  A5 04 001306112B0601040181E43801010201180101020200
  SM   GET ADF Command
```

```
13  06[11] 2B0601040181E438010102011801010202 00
 DataLen     ASN1         OID
```

```
0A007C0A81080181E4380101020190001C46
```

```
0B007C2A8228B47D5E9493B62E76DE29B7866D902D91C9017A2BFA722B5205B9BBFC
3DC04C1694D53E359DCF362090007B9D
```

```
0B0380A504001306112B0601040181E438010102011801010202008A4C
```

```
    80   A5 04 001306112B0601040181E43801010201180101020200
      SM    GET ADF Command
```

```
      13  06[11] 2B0601040181E438010102011801010202 00
       DataLen      ASN1            OID
```

```
ADF OID: 1.3.6.1.4.1.29240.1.1.2.1.24.1.1.2
```

```
3DC04C1694D53E359DCF362090007B9D
```

```
0B00A404000AA0000004400001010001000039C
```

```
0A007C0A81080181E438010102019001C46
```

```
0B0380A504001306112B0601040181E43801010201180101020200 8A4C
```

```
0B00CD0209078540197FCD5B7BAD9B1AB19249E45D69AE5E39A040B84CB5EDEFE506
E8A876C9CF90AC07224D39ABD8375B7050264808A3CECC27E3184B148B9AA2FA75DE
F75DF8DD8E08E0B0DD568FB11F049000C602
```

```
0A0300870001047C0281000041DB
```

```
0A007C0A81080181E438010102019001C46
```

```
0B007C2A8228B47D5E9493B62E76DE29B7866D902D91C9017A2BFA722B5205B9BBFC
3DC04C1694D53E359DCF362090007B9D
```

```
0B00CD0209078540197FCD5B7BAD9B1AB19249E45D69AE5E39A040B84CB5EDEFE506
E8A876C9CF90AC07224D39ABD8375B7050264808A3CECC27E3184B148B9AA2FA75DE
F75DF8DD8E08E0B0DD568FB11F049000C602
```

```
CD0209078540197FCD5B7BAD9B1AB19249E45D69AE5E39A040B84CB5EDEFE506E8A8
76C9CF90AC07224D39ABD8375B7050264808A3CECC27E3184B148B9AA2FA75DEF75D
F8DD8E08E0B0DD568FB11F04 9000 (OK)
```

```
0A0300870001047C0281000041DB
```

```
0A007C0A81080181E43801010201900001C46
```

```
0B007C2A8228B47D5E9493B62E76DE29B7866D902D91C9017A2BFA722B5205B9BBFC
3DC04C1694D53E359DCF362090007B9D
```

```
0B00CD0209078540197FCD5B7BAD9B1AB19249E45D69AE5E39A040B84CB5EDEFE506
E8A876C9CF90AC07224D39ABD8375B7050264808A3CECC27E3184B148B9AA2FA75DE
F75DF8DD8E08E0B0DD568FB11F049000C602
```

```
CD0209078540197FCD5B7BAD9B1AB19249E45D69AE5E39A040B84CB5EDEFE506E8A8
76C9CF90AC07224D39ABD8375B7050264808A3CECC27E3184B148B9AA2FA75DEF75D
F8DD8E08E0B0DD568FB11F04 9000 (OK)
```

```
CD [02]
  09 07

85 [40]
197FCD5B7BAD9B1AB19249E45D69AE5E39A040B84CB5EDEFE506E8A876C9CF90AC0
7224D39ABD8375B7050264808A3CECC27E3184B148B9AA2FA75DEF75DF8DD

8E [08]
  E0B0DD568FB11F04
```

```
0B00CD0209078540197FCD5B7BAD9B1AB19249E45D69AE5E39A040B84CB5EDEFE506
E8A876C9CF90AC07224D39ABD8375B7050264808A3CECC27E3184B148B9AA2FA75DE
F75DF8DD8E08E0B0DD568FB11F049000C602
```

```
CD [02] =  Encryption and Hash Mechanism
  09 =    AES-128 CBC
  07 =    SHA-256

85 [40]
197FCD5B7BAD9B1AB19249E45D69AE5E39A040B84CB5EDEFE506E8A876C9CF90AC
07224D39ABD8375B7050264808A3CECC27E3184B148B9AA2FA75DEF75DF8DD

8E [08]
E0B0DD568FB11F04
```

```
0B00CD0209078540197FCD5B7BAD9B1AB19249E45D69AE5E39A040B84CB5EDEFE506
E8A876C9CF90AC07224D39ABD8375B7050264808A3CECC27E3184B148B9AA2FA75DE
F75DF8DD8E08E0B0DD568FB11F049000C602
```

```
CD [02] =  Encryption and Hash Mechanism
  09 =    AES-128 CBC
  07 =    SHA-256

85 [40] =  Cryptogram (Encrypted with our Privacy keyset)
197FCD5B7BAD9B1AB19249E45D69AE5E39A040B84CB5EDEFE506E8A876C9CF90AC
07224D39ABD8375B7050264808A3CECC27E3184B148B9AA2FA75DEF75DF8DD

8E [08]
E0B0DD568FB11F04
```

```
0B00CD0209078540197FCD5B7BAD9B1AB19249E45D69AE5E39A040B84CB5EDEFE506
E8A876C9CF90AC07224D39ABD8375B7050264808A3CECC27E3184B148B9AA2FA75DE
F75DF8DD8E08E0B0DD568FB11F049000C602
```

```
CD [02] =  Encryption and Hash Mechanism
  09 =    AES-128 CBC
  07 =    SHA-256

85 [40] =  Cryptogram (Encrypted with our Privacy keyset)
197FCD5B7BAD9B1AB19249E45D69AE5E39A040B84CB5EDEFE506E8A876C9CF90AC
07224D39ABD8375B7050264808A3CECC27E3184B148B9AA2FA75DEF75DF8DD

8E [08] = MAC (Encrypted with our Privacy Keyset)
E0B0DD568FB11F04
```

```
0B00CD0209078540197FCD5B7BAD9B1AB19249E45D69AE5E39A040B84CB5EDEFE506
E8A876C9CF90AC07224D39ABD8375B7050264808A3CECC27E3184B148B9AA2FA75DE
F75DF8DD8E08E0B0DD568FB11F049000C602
```

```
Cryptogram

197FCD5B7BAD9B1AB19249E45D69AE5E39A040B84CB5EDEFE506E8A876C9CF90AC
07224D39ABD8375B7050264808A3CECC27E3184B148B9AA2FA75DEF75DF8DD

Decrypted

06 [11] = ADF OID
    2B0601040181E438010102011801010202
CF [07] = External ID
    11223344556677
```

```
0B00A404000AA0000004400001010001000039C
```

```
0A007C0A81080181E4380101020190001C46
```

```
0B0380A504001306112B0601040181E4380101020118010102020008A4C
```

```
0B00CD0209078540197FCD5B7BAD9B1AB19249E45D69AE5E39A040B84CB5EDEFE506
E8A876C9CF90AC07224D39ABD8375B7050264808A3CECC27E3184B148B9AA2FA75DE
F75DF8DD8E08E0B0DD568FB11F049000C602
```

```
0A0300870001047C0281000041DB
```

```
0A007C0A81080181E4380101020190001C46
```

```
0B007C2A8228B47D5E9493B62E76DE29B7866D902D91C9017A2BFA722B5205B9BBFC
3DC04C1694D53E359DCF362090007B9D
```

```
0A0300870001047C0281000041DB000100039C
```

```
00 87 00 01 04 7C02810000
ISO7816 – Secure Messaging
```

```
0B00CD0209078540197FCD5B7BAD9B1AB19249E45D69AE5E39A040B84CB5EDEFE506
E8A876C9CF90AC07224D39ABD8375B7050264808A3CECC27E3184B148B9AA2FA75DE
F75DF8DD8E08E0B0DD568FB11F049000C602
```

```
0A007C0A81080181E438010102019000 1C46
```

```
0B007C2A8228B47D5E9493B62E76DE29B7866D902D91C9017A2BFA722B5205B9BBFC
3DC04C1694D53E359DCF362090007B9D
```

```
0A0300870001047C0281000041DB0001000039C
```

```
00 87 00 01 04 7C02810000
```

```
87 =  Secure Messaging APDU Instruction
00
01 = Authentication Keyslot
04 = Type of Instruction (RND.ICC)
```

```
0A007C0A81080181E4380101020190001C46
```

```
0B007C2A8228B47D5E9493B62E76DE29B7866D902D91C9017A2BFA722B5205B9BBFC
3DC04C1694D53E359DCF362090007B9D
```

```
0A0300870001047C0281000041DB0001000039C
```

```
00 87 00 01 04 7C02810000
```

87 = Secure Messaging APDU Instruction
00
01 = Authentication Keyslot
04 = Type of Instruction (RND.ICC)

```
0A007C0A81080181E4380101020190001C46
```

Authentication Keyslots go from 0x00 to 0x0F

```
0B00A404000AA00000044000010100010003 9C
```

```
0A007C0A81080181E4380101020190001C46
```

```
0B0380A504001306112B0601040181E43801010201180101020 2008A4C
```

```
0B00CD0209078540197FCD5B7BAD9B1AB19249E45D69AE5E39A040B84CB5EDEFE506
E8A876C9CF90AC07224D39ABD8375B7050264808A3CECC27E3184B148B9AA2FA75DE
F75DF8DD8E08E0B0DD568FB11F049000C602
```

```
0A03008700010 47C0281000041DB
```

```
0A007C0A81080181E4380101020190001C46
```

```
0B007C2A8228B47D5E9493B62E76DE29B7866D902D91C9017A2BFA722B5205B9BBFC
3DC04C1694D53E359DCF362090007B9D
```

```
0A007C0A81080181E4380101020190001C46
```

```
007C0A81080181E43801010201 9000 (OK)
```

```
0B00CD02090785401 97FCD5B7BAD9B1AB19249E45D69AE5E39A040B84CB5EDEFE506
E8A876C9CF90AC07224D39ABD8375B7050264808A3CECC27E3184B148B9AA2FA75DE
F75DF8DD8E08E0B0DD568FB11F049000C602
```

```
0A0300870001047C0281000041DB
```

```
0B007C2A8228B47D5E9493B62E76DE29B7866D902D91C9017A2BFA722B5205B9BBFC
3DC04C1694D53E359DCF362090007B9D
```

```
0A007C0A81080181E4380101020190001C469C
```

```
007C0A81080181E43801010201 9000 (OK)
```

```
    00 7C 0A 81[08] 0181E43801010201
ASN.1       RND.ICC
```

```
0A0300870001047C0281000041DB
```

```
0B007C2A8228B47D5E9493B62E76DE29B7866D902D91C9017A2BFA722B5205B9BBFC
3DC04C1694D53E359DCF362090007B9D
```

```
0A007C0A81080181E4380101020190001C469C
```

```
007C0A81080181E43801010201 9000 (OK)
```

```
      00 7C 0A 81 [08] 0181E43801010201
ASN.1         RND.ICC
```

```
RND.ICC = 0181E43801010201
```

Depending on configuration, this can be static across different cards, this is not the case across all cards

```
0A03008700092C7C2A8228203FB3BF4F476BBDA5C8B01D76A9FAF6557D57D5AE8D88
EC2066D0016A1551006ACC3FD3AFF2B41A00719B
```

```
0A037C2A8228F6AB0D0E72289F8C4DF1C0E0C429930F1424461B7E300AC72F46DD56
2EDAED304FD673CC06DE888F9000B152
```

```
0A020CCB3FFF168508A556FCB38B03D6F697008E085B17E7B6D7479E360096A0
```

```
0A0085401D8ADB062ED56480F4CCA55655423C83B016E93AEC2F861E5086D61CC8F
115C4A41D05D594964B64956C07969B31B32C6576A59458B29680B99B7BF9E17CDC
C3990290008E08BB4B96E7B80C42B69000FE4B
```

```
0A03008700092C7C2A8228203FB3BF4F476BBDA5C8B01D76A9FAF6557D57D5AE8D88
EC2066D0016A1551006ACC3FD3AFF2B41A00719B
```

```
87 00 09 2C
ISO7816 - Secure Messaging

7C [2A] - ASN1 Tag
82 [28] - ASN1 Tag
203FB3BF4F476BBDA5C8B01D76A9FAF6557D57D5AE8D88EC2066D0016A1551006AC
C3FD3AFF2B41A
```

```
0A0085401D8ADB062ED56480F4CCA55655423C83B016E93AEC2F861E5086D61CC8F
115C4A41D05D594964B64956C07969B31B32C6576A59458B29680B99B7BF9E17CDC
C3990290008E08BB4B96E7B80C42B69000FE4B
```

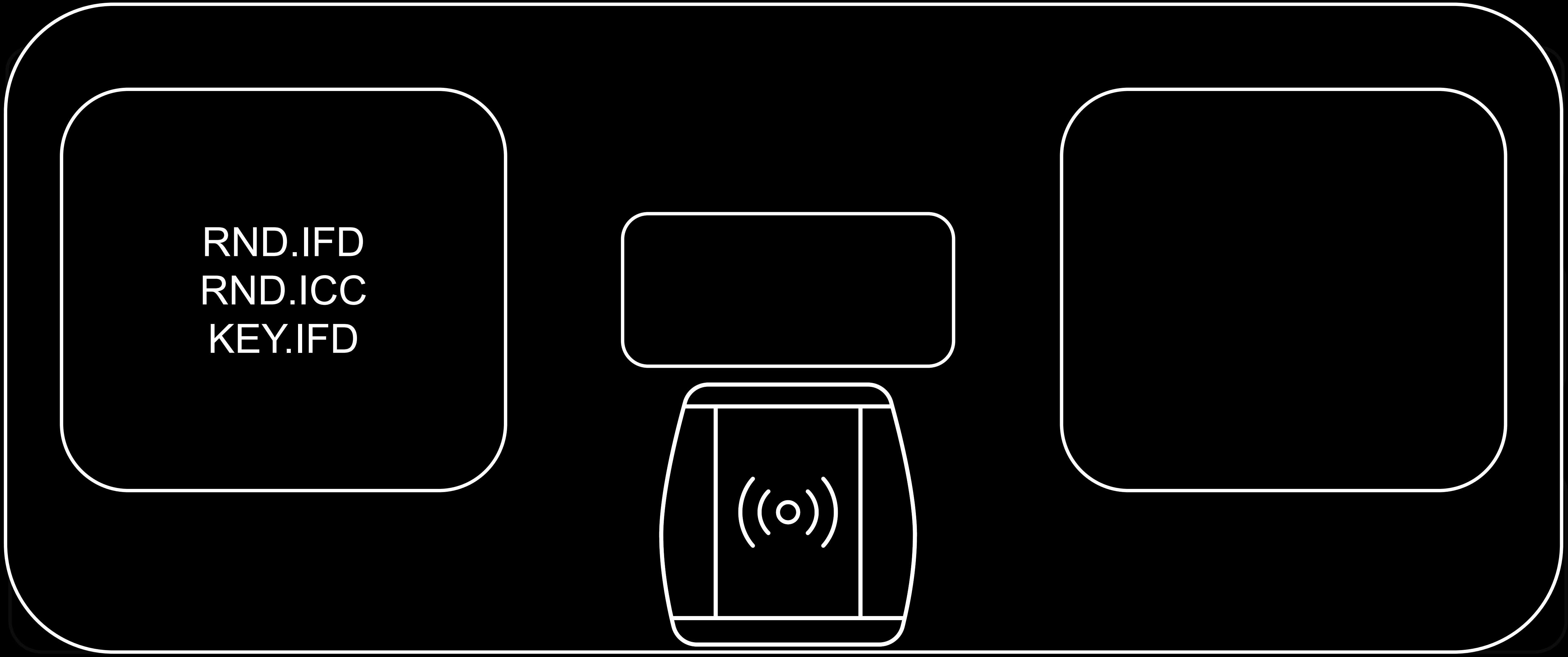
```
0A03008700092C7C2A8228203FB3BF4F476BBDA5C8B01D76A9FAF6557D57D5AE8D88
EC2066D0016A1551006ACC3FD3AFF2B41A00719B
```

87 00 09 2C
ISO7816 - Secure Messaging

7C [2A] - ASN1 Tag
82 [28] - ASN1 Tag
203FB3BF4F476BBDA5C8B01D76A9FAF6557D57D5AE8D88EC2066D0016A1551006AC
C3FD3AFF2B41A

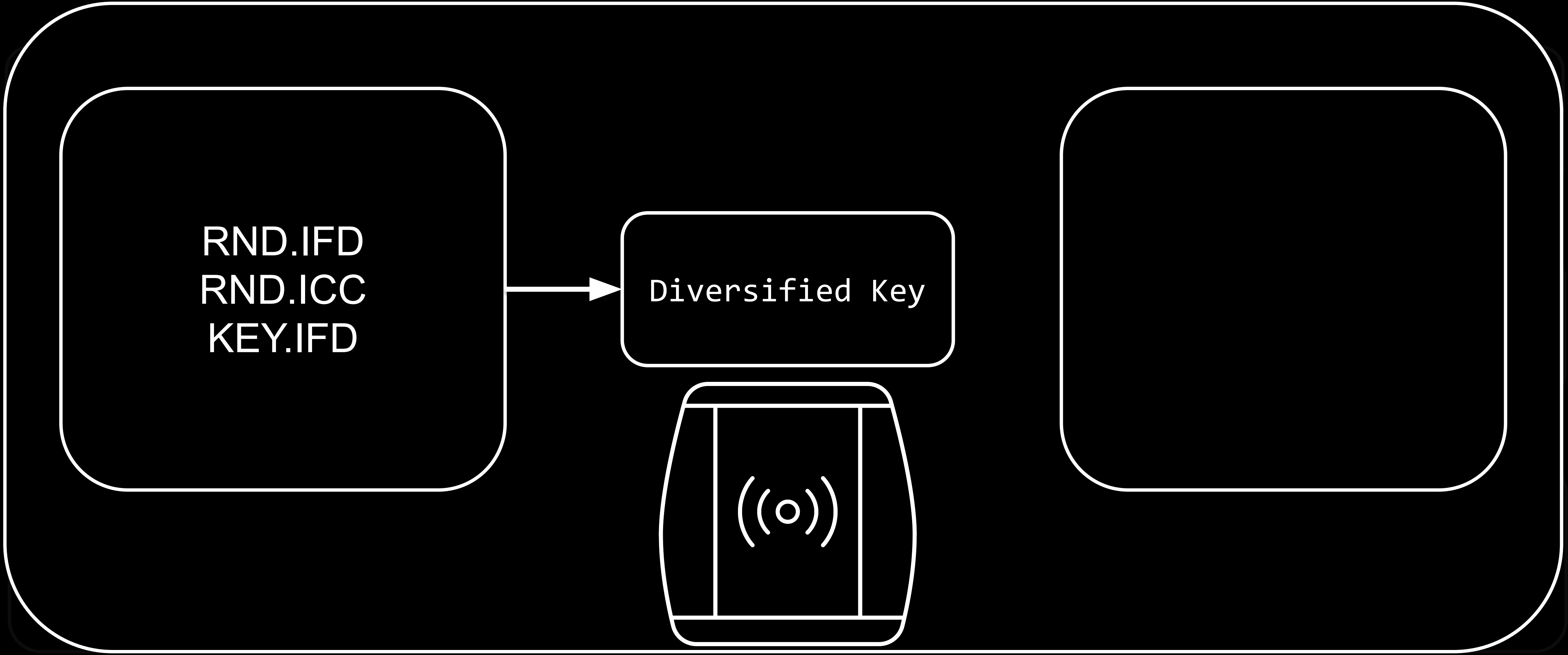
**Cryptogram -**
203FB3BF4F476BBDA5C8B01D76A9FAF6557D57D5AE8D88EC2066D0016A155100
**MAC -**
6ACC3FD3AFF2B41A

```
0A03008700092C7C2A8228203FB3BF4F476BBDA5C8B01D76A9FAF6557D57D5AE8D88
EC2066D0016A1551006ACC3FD3AFF2B41A00719B
```

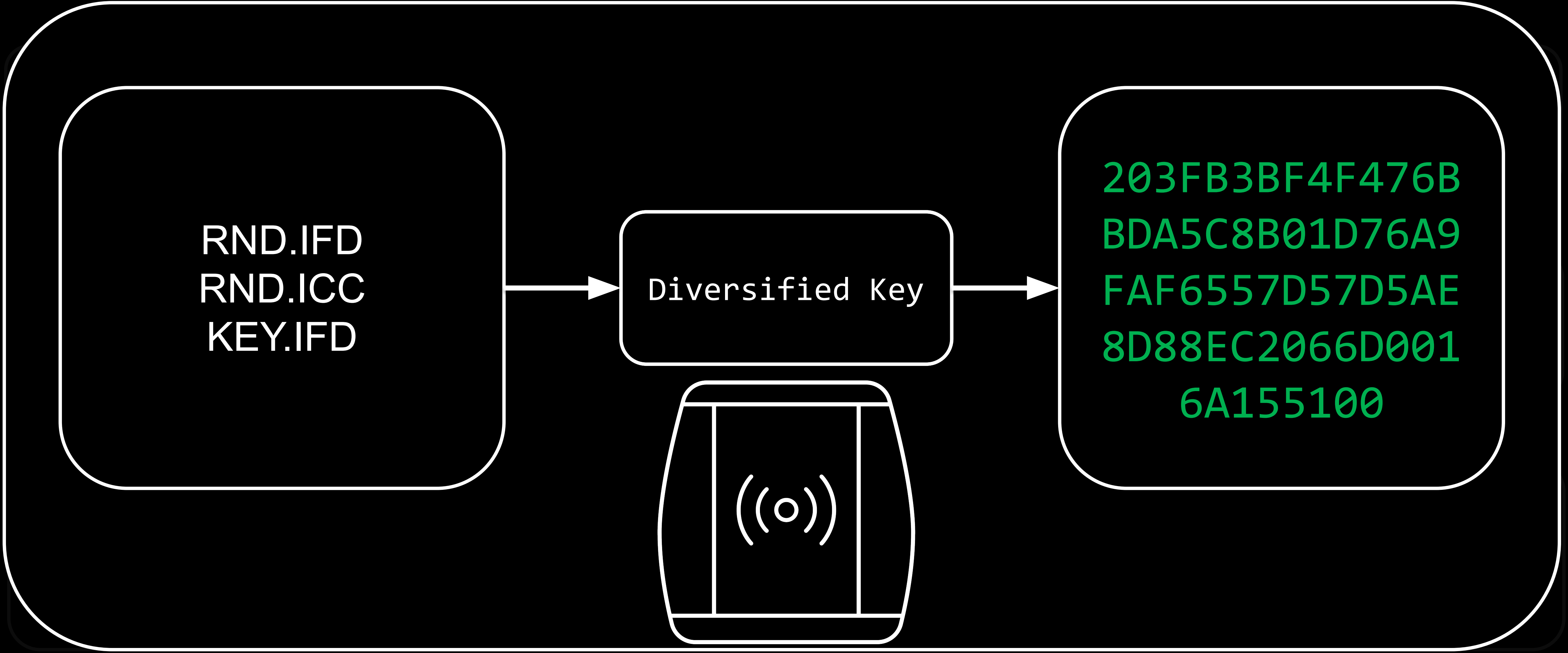


RND.IFD
RND.ICC
KEY.IFD

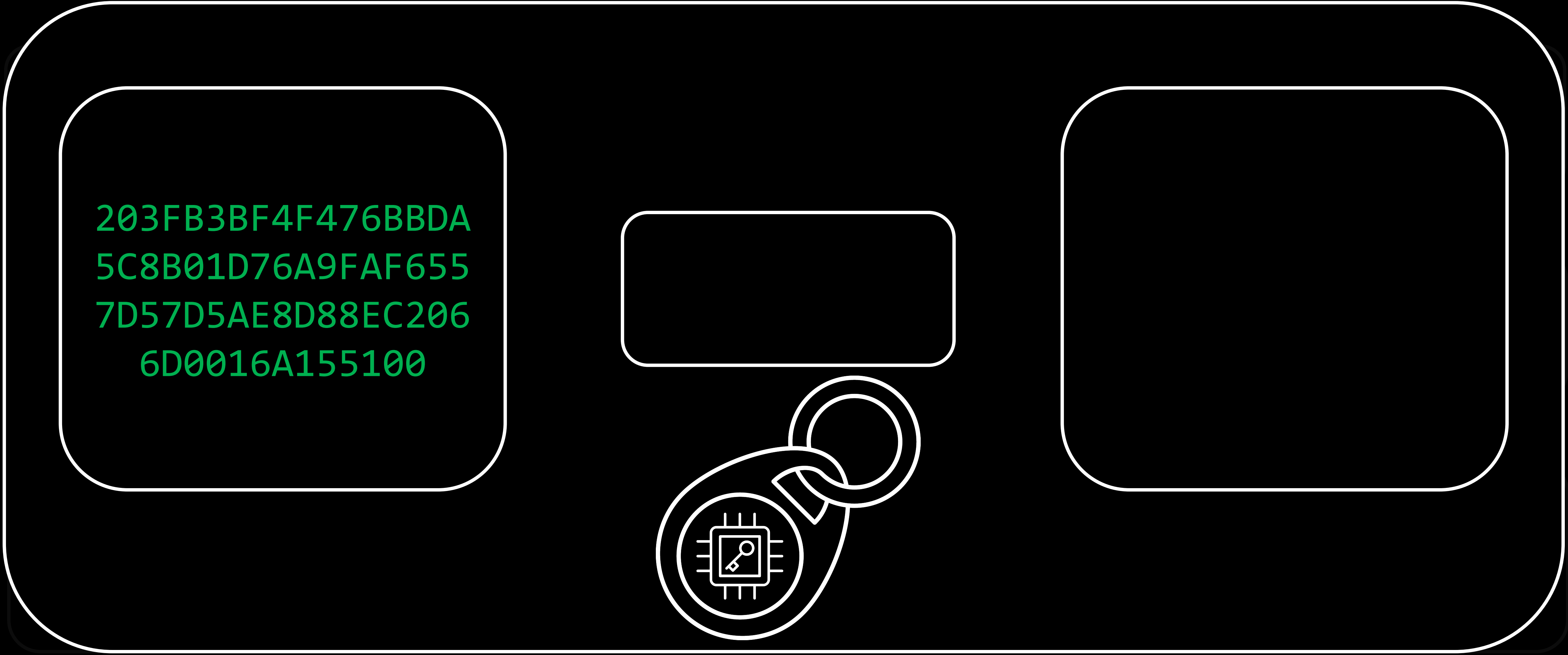
```
0A03008700092C7C2A8228203FB3BF4F476BBDA5C8B01D76A9FAF6557D57D5AE8D88
EC2066D0016A1551006ACC3FD3AFF2B41A00719B
```



```
0A03008700092C7C2A8228203FB3BF4F476BBDA5C8B01D76A9FAF6557D57D5AE8D88
EC2066D0016A1551006ACC3FD3AFF2B41A00719B
```

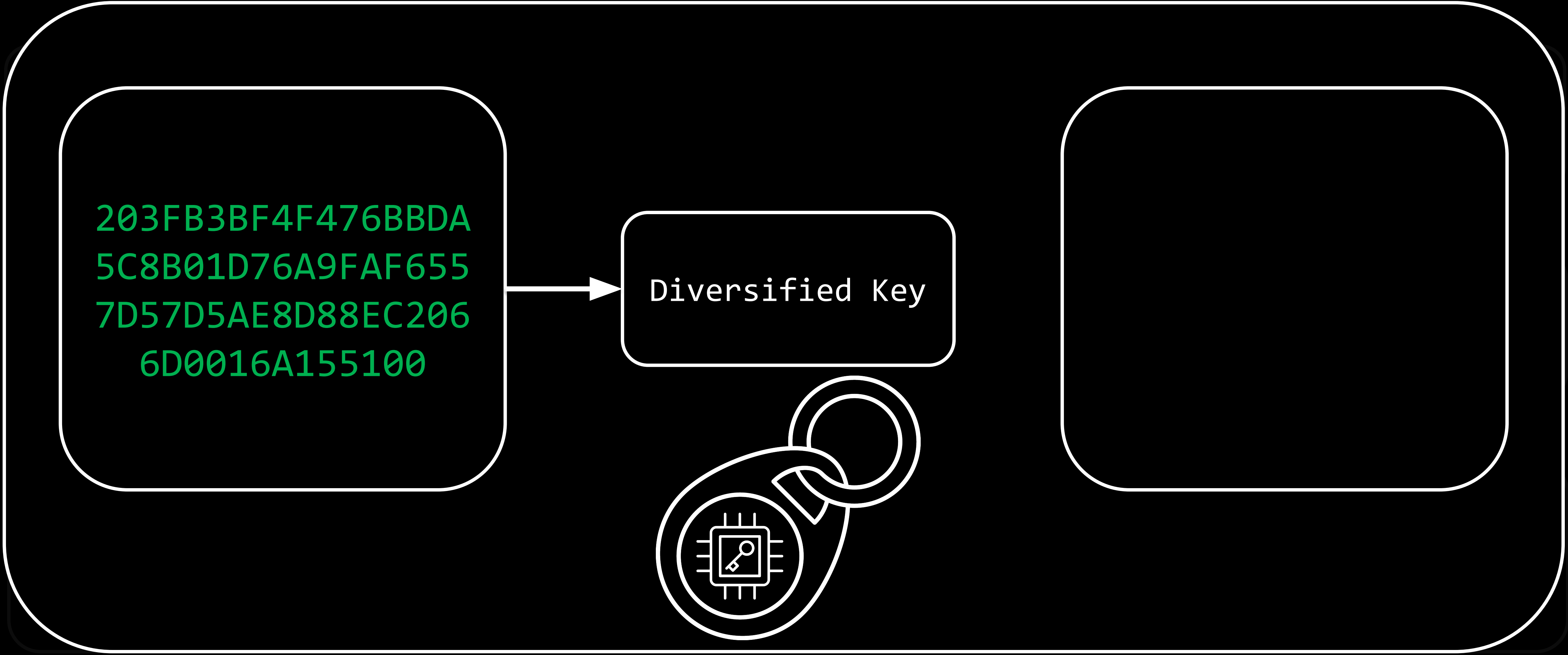


```
0A03008700092C7C2A8228203FB3BF4F476BBDA5C8B01D76A9FAF6557D57D5AE8D88
EC2066D0016A1551006ACC3FD3AFF2B41A00719B
```



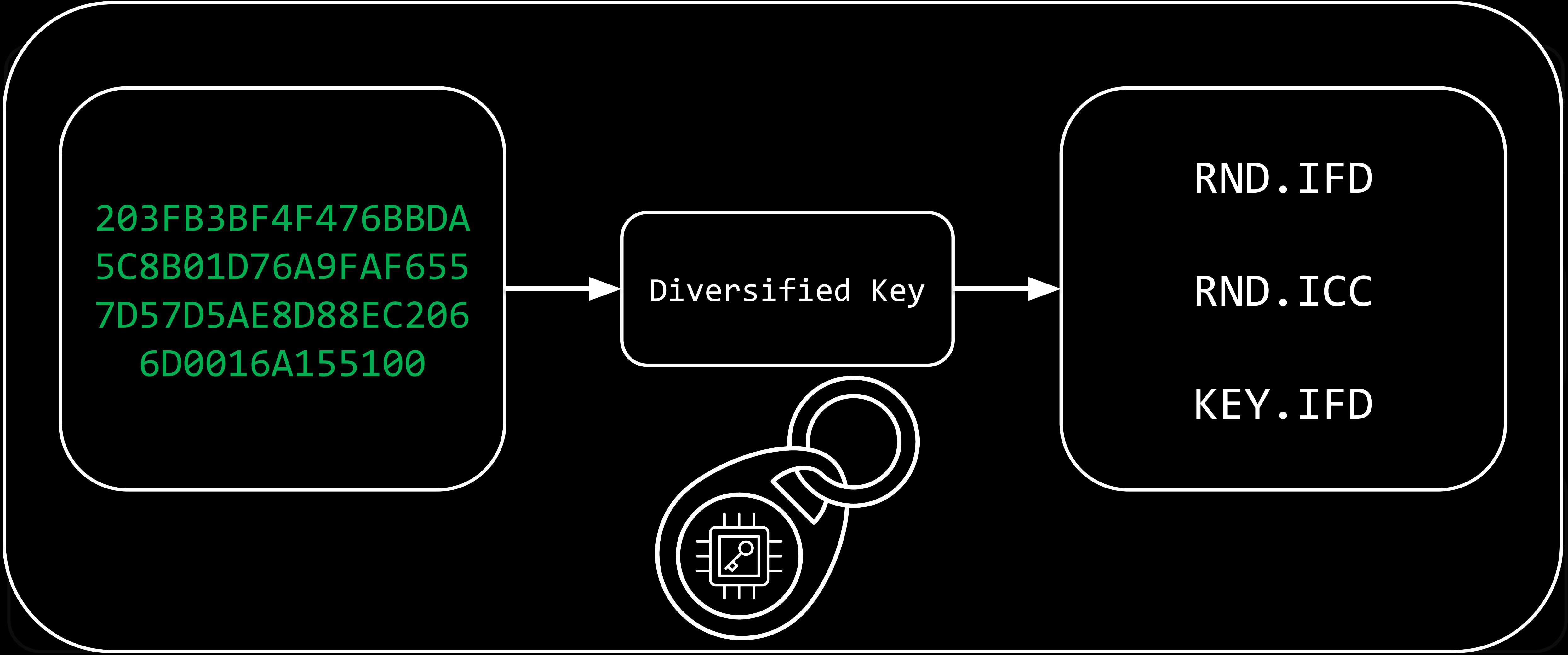
```
203FB3BF4F476BBDA
5C8B01D76A9FAF655
7D57D5AE8D88EC206
6D0016A155100
```

```
0A03008700092C7C2A8228203FB3BF4F476BBDA5C8B01D76A9FAF6557D57D5AE8D88
EC2066D0016A1551006ACC3FD3AFF2B41A00719B
```



```
203FB3BF4F476BBDA
5C8B01D76A9FAF655
7D57D5AE8D88EC206
6D0016A155100
```

```
0A03008700092C7C2A8228203FB3BF4F476BBDA5C8B01D76A9FAF6557D57D5AE8D88
EC2066D0016A1551006ACC3FD3AFF2B41A00719B
```



203FB3BF4F476BBDA
5C8B01D76A9FAF655
7D57D5AE8D88EC206
6D0016A155100

Diversified Key

RND.IFD

RND.ICC

KEY.IFD

```
0A03008700092C7C2A8228203FB3BF4F476BBDA5C8B01D76A9FAF6557D57D5AE8D88
EC2066D0016A1551006ACC3FD3AFF2B41A00719B
```

```
0A037C2A8228F6AB0D0E72289F8C4DF1C0E0C429930F1424461B7E300AC72F46DD56
2EDAED304FD673CC06DE888F9000B152
```

```
0A020CCB3FFF168508A556FCB38B03D6F697008E085B17E7B6D7479E360096A0
```

```
0A0085401D8ADB062ED56480F4CCA55655423C83B016E93AEC2F861E5086D61CC8F
115C4A41D05D594964B64956C07969B31B32C6576A59458B29680B99B7BF9E17CDC
C3990290008E08BB4B96E7B80C42B69000FE4B
```

```
0A037C2A8228F6AB0D0E72289F8C4DF1C0E0C429930F1424461B7E300AC72F46DD56
2EDAED304FD673CC06DE888F9000B152
```

```
7C2A8228F6AB0D0E72289F8C4DF1C0E0C429930F1424461B7E300AC72F46DD562EDA
ED304FD673CC06DE888F 9000 (OKAY)
```

```
0A020CCB3FFF168508A556FCB38B03D6F697008E085B17E7B6D7479E360096A0
```

```
0A0085401D8ADB062ED56480F4CCA55655423C83B016E93AEC2F861E5086D61CC8F
115C4A41D05D594964B64956C07969B31B32C6576A59458B29680B99B7BF9E17CDC
C3990290008E08BB4B96E7B80C42B69000FE4B
```

```
0A037C2A8228F6AB0D0E72289F8C4DF1C0E0C429930F1424461B7E300AC72F46DD56
2EDAED304FD673CC06DE888F9000B152
```

```
7C [2A] = ASN1 Tag
82 [28] = ASN1 Tag
F6AB0D0E72289F8C4DF1C0E0C429930F1424461B7E300AC72F46DD562EDAED304FD
673CC06DE888F
```

**Cryptogram -**

F6AB0D0E72289F8C4DF1C0E0C429930F1424461B7E300AC72F46DD562EDAED30

**MAC -**

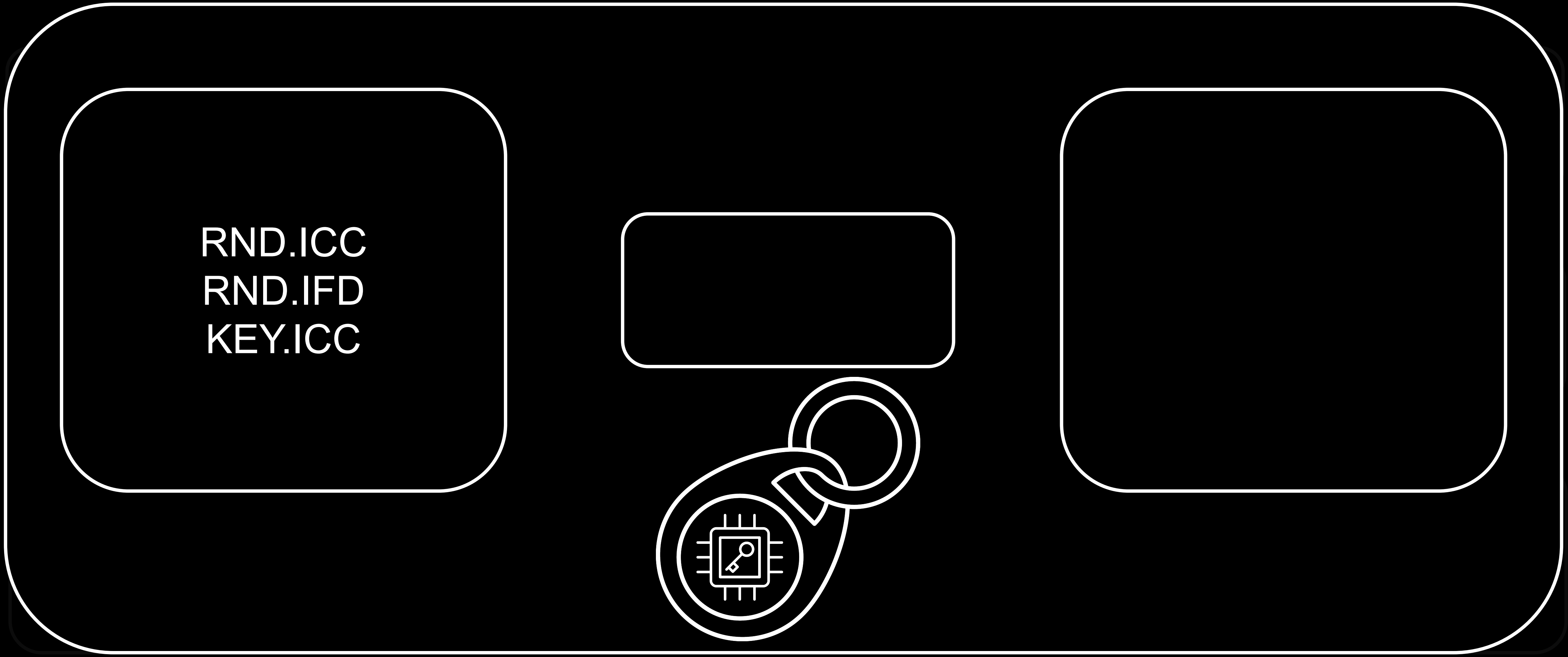
4FD673CC06DE888F

0A037C2A8228F6AB0D0E72289F8C4DF1C0E0C429930F1424461B7E300AC72F46DD56
2EDAED304FD673CC06DE888F9000B152

7C [2A] = ASN1 Tag
82 [28] = ASN1 Tag
F6AB0D0E72289F8C4DF1C0E0C429930F1424461B7E300AC72F46DD562EDAED304FD
673CC06DE888F

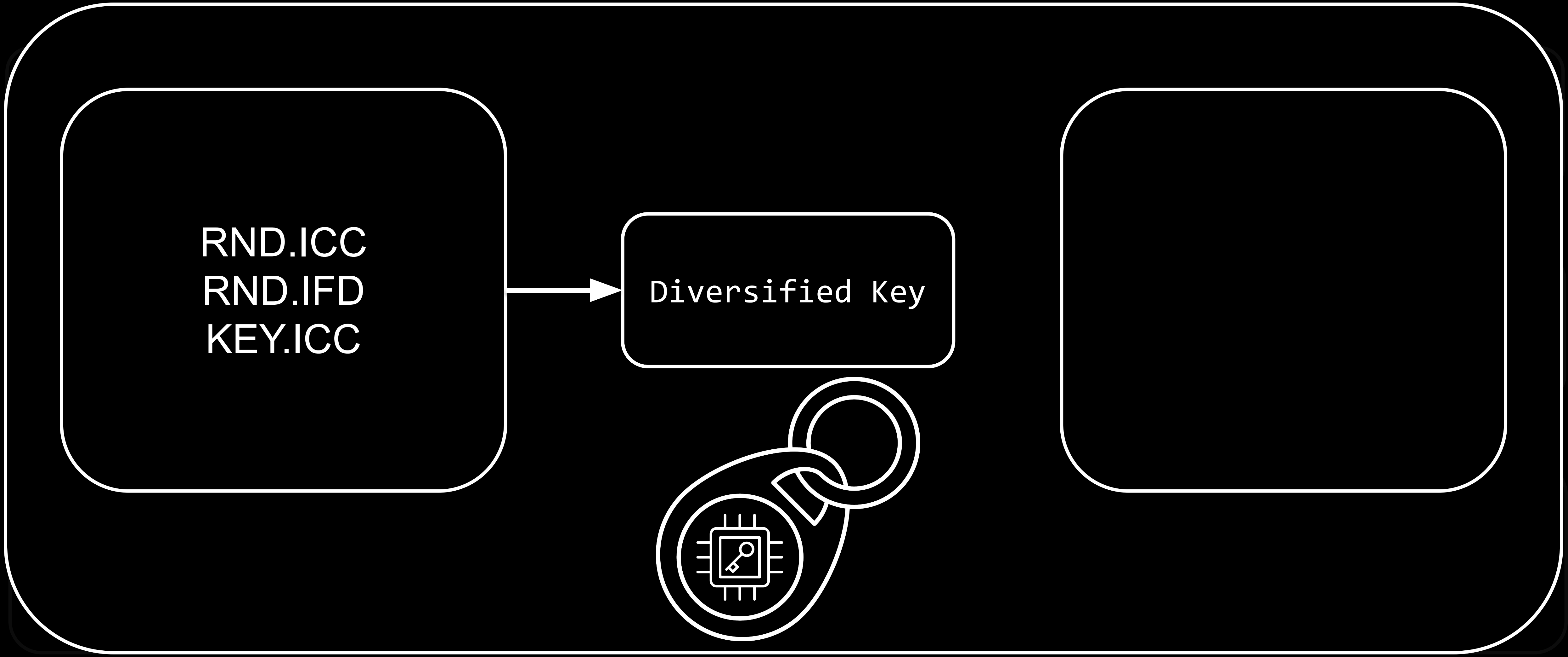
**Cryptogram -**
F6AB0D0E72289F8C4DF1C0E0C429930F1424461B7E300AC72F46DD562EDAED30
**MAC -**
4FD673CC06DE888F

```
0A03008700092C7C2A8228203FB3BF4F476BBDA5C8B01D76A9FAF6557D57D5AE8D88
EC2066D0016A1551006ACC3FD3AFF2B41A00719B
```



RND.ICC
RND.IFD
KEY.ICC

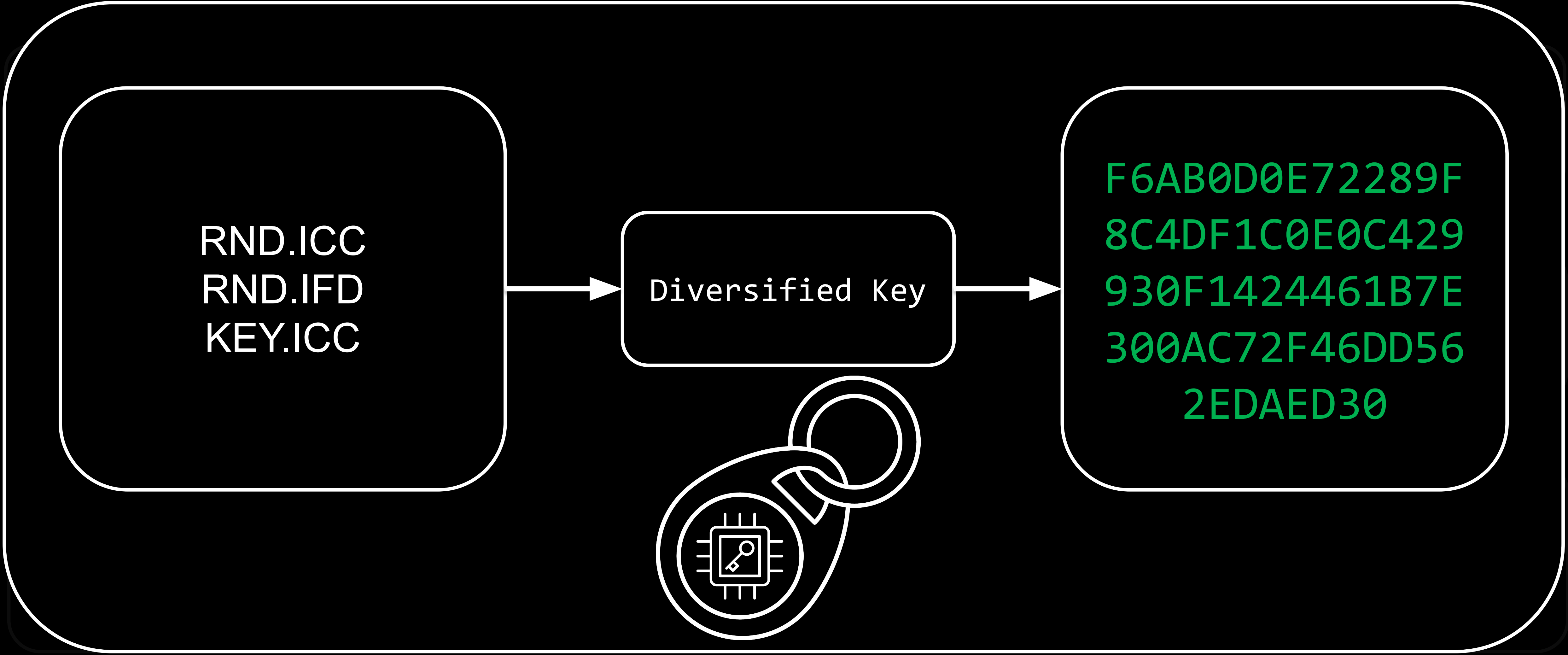
```
0A03008700092C7C2A8228203FB3BF4F476BBDA5C8B01D76A9FAF6557D57D5AE8D88
EC2066D0016A1551006ACC3FD3AFF2B41A00719B
```



RND.ICC
RND.IFD
KEY.ICC

Diversified Key

```
0A03008700092C7C2A8228203FB3BF4F476BBDA5C8B01D76A9FAF6557D57D5AE8D88
EC2066D0016A1551006ACC3FD3AFF2B41A00719B
```

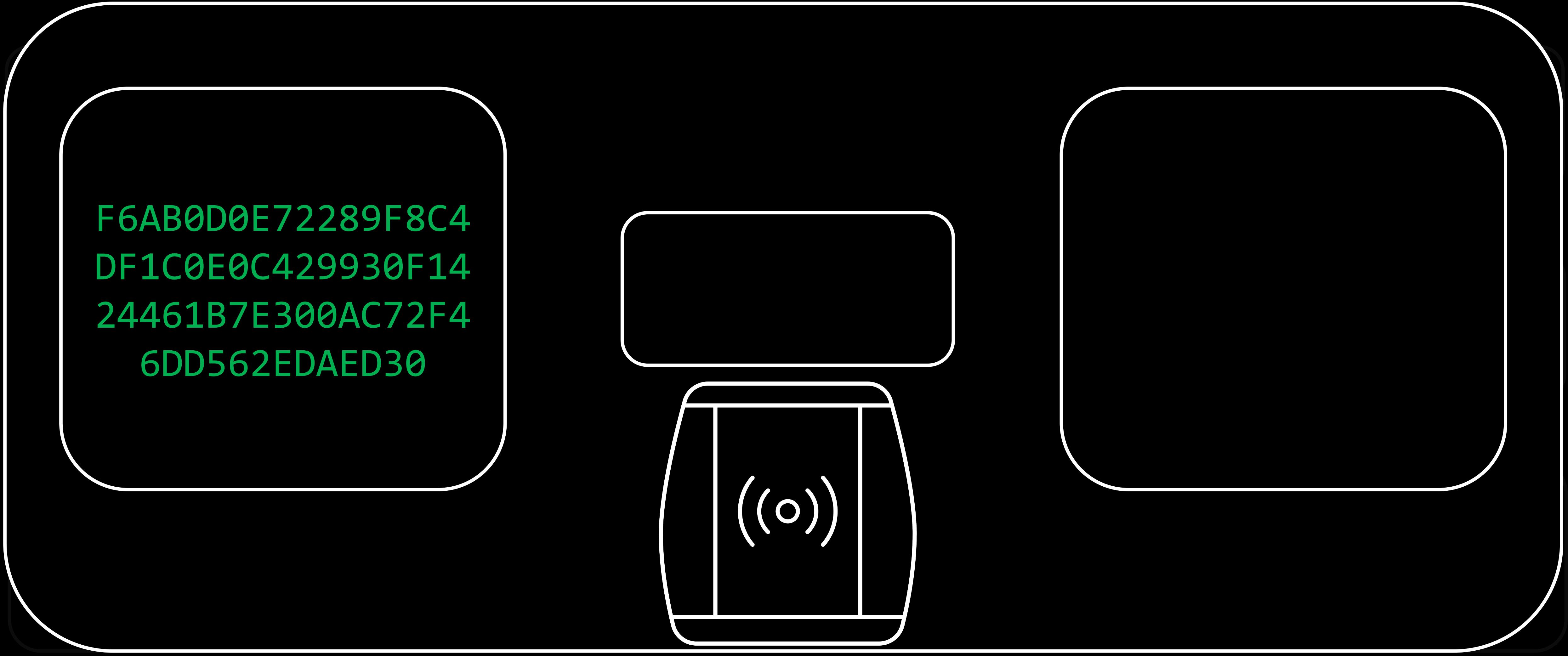


RND.ICC
RND.IFD
KEY.ICC

Diversified Key

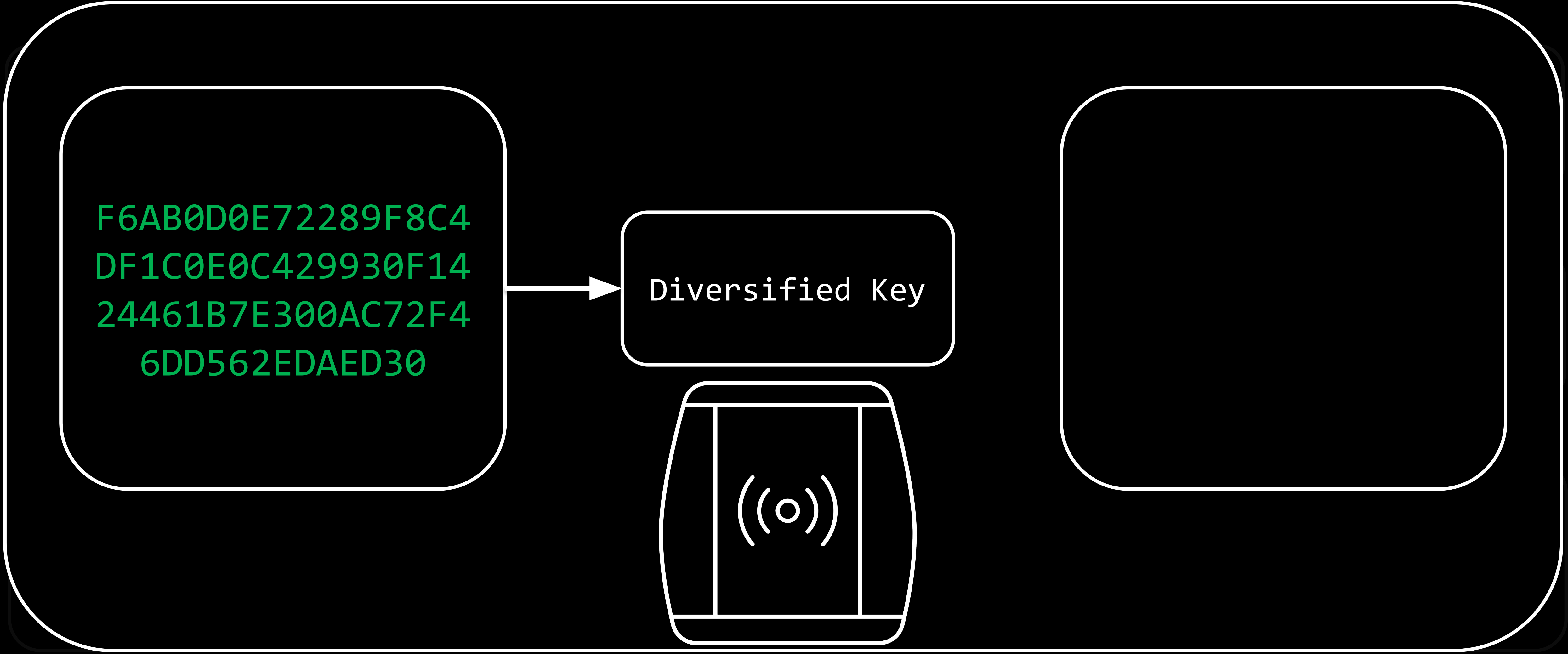
```
F6AB0D0E72289F
8C4DF1C0E0C429
930F1424461B7E
300AC72F46DD56
2EDAED30
```

```
0A03008700092C7C2A8228203FB3BF4F476BBDA5C8B01D76A9FAF6557D57D5AE8D88
EC2066D0016A1551006ACC3FD3AFF2B41A00719B
```



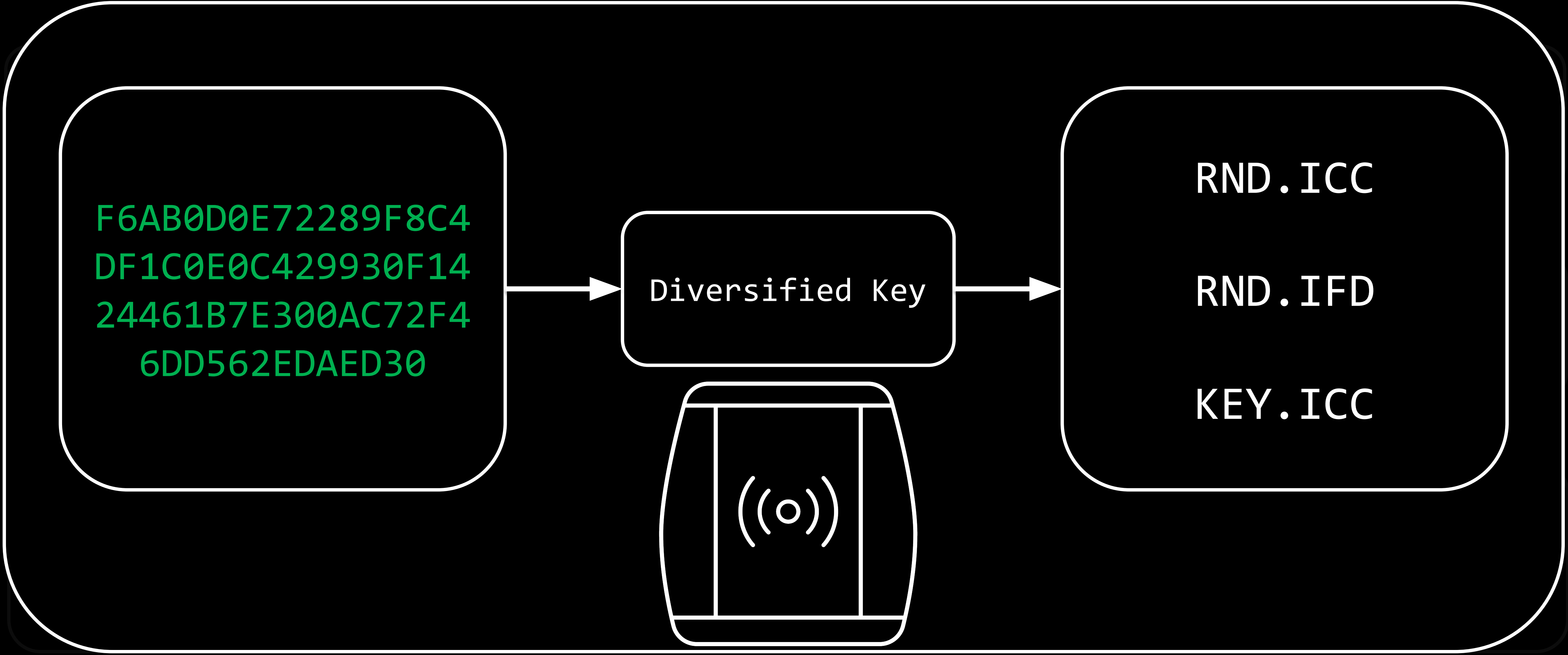
```
F6AB0D0E72289F8C4
DF1C0E0C429930F14
24461B7E300AC72F4
6DD562EDAED30
```

```
0A03008700092C7C2A8228203FB3BF4F476BBDA5C8B01D76A9FAF6557D57D5AE8D88
EC2066D0016A1551006ACC3FD3AFF2B41A00719B
```



```
F6AB0D0E72289F8C4
DF1C0E0C429930F14
24461B7E300AC72F4
6DD562EDAED30
```

```
0A03008700092C7C2A8228203FB3BF4F476BBDA5C8B01D76A9FAF6557D57D5AE8D88
EC2066D0016A1551006ACC3FD3AFF2B41A00719B
```



F6AB0D0E72289F8C4
DF1C0E0C429930F14
24461B7E300AC72F4
6DD562EDAED30

Diversified Key

RND.ICC

RND.IFD

KEY.ICC

```
0A03008700092C7C2A8228203FB3BF4F476BBDA5C8B01D76A9FAF6557D57D5AE8D88
EC2066D0016A1551006ACC3FD3AFF2B41A00719B
```

```
0A037C2A8228F6AB0D0E72289F8C4DF1C0E0C429930F1424461B7E300AC72F46DD56
2EDAED304FD673CC06DE888F9000B152
```

```
0A020CCB3FFF168508A556FCB38B03D6F697008E085B17E7B6D7479E360096A0
```

```
0A0085401D8ADB062ED56480F4CCA55655423C83B016E93AEC2F861E5086D61CC8F
115C4A41D05D594964B64956C07969B31B32C6576A59458B29680B99B7BF9E17CDC
C3990290008E08BB4B96E7B80C42B69000FE4B
```

```
0A020CCB3FFF168508A556FCB38B03D6F697008E085B17E7B6D7479E360096A0
```

```
0A03008700092C7C2A8228203FB3BF4F476BBDA5C8B01D76A9FAF6557D57D5AE8D88
EC2066D0016A1551006ACC3FD3AFF2B41A00719B
```

```
0A037C2A8228F6AB0D0E72289F8C4DF1C0E0C429930F1424461B7E300AC72F46DD56
2EDAED304FD673CC06DE888F9000B152
```

```
0A0085401D8ADB062ED56480F4CCA55655423C83B016E93AEC2F861E5086D61CC8F
115C4A41D05D594964B64956C07969B31B32C6576A59458B29680B99B7BF9E17CDC
C3990290008E08BB4B96E7B80C42B69000FE4B
```

```
0A03008700092C7C2A8228203FB3BF4F476BBDA5C8B01D76A9FAF6557D57D5AF8D88
EC2066D0016A1551006ACC3FD3AFF2B41A00719B
```

```
0A020CCB3FFF168508A556FCB38B03D6F697008E085B17E7B6D7479E360096A0
```

```
0A037C2A8228F6AB0D0E7228 [illegible] 424461B7E300AC72F46DD56
2EDAED304FD673CC06DE888F9000B152
```

0C CB 3F FF

SEOS GET Data Command

16

Length

8508A556FCB38B03D6F697008E085B17E7B6D7479E3600

APDU

```
0A0085401D8ADB062ED56480F4CCA55655423C83B016E93AEC2F861E5086D61CC8F
115C4A41D05D594964B64956C07969B31B32C6576A59458B29680B99B7BF9E17CDC
C3990290008E08BB4B96E7B80C42B69000FE4B
```

```
0A020CCB3FFF168508A556FCB38B03D6F697008E085B17E7B6D7479E360096A0
```

```
0C CB 3F FF
SEOS GET Data Command
16
Length

8508A556FCB38B03D6F697008E085B17E7B6D7479E3600
APDU
```

```
85 [08]
A556FCB38B03D6F6
97 [00]
8E [08]
5B17E7B6D7479E36
```

```
0A020CCB3FFF168508A556FCB38B03D6F697008E085B17E7B6D7479E360096A0
```

```
0C CB 3F FF
```

SEOS GET Data Command

```
16
```

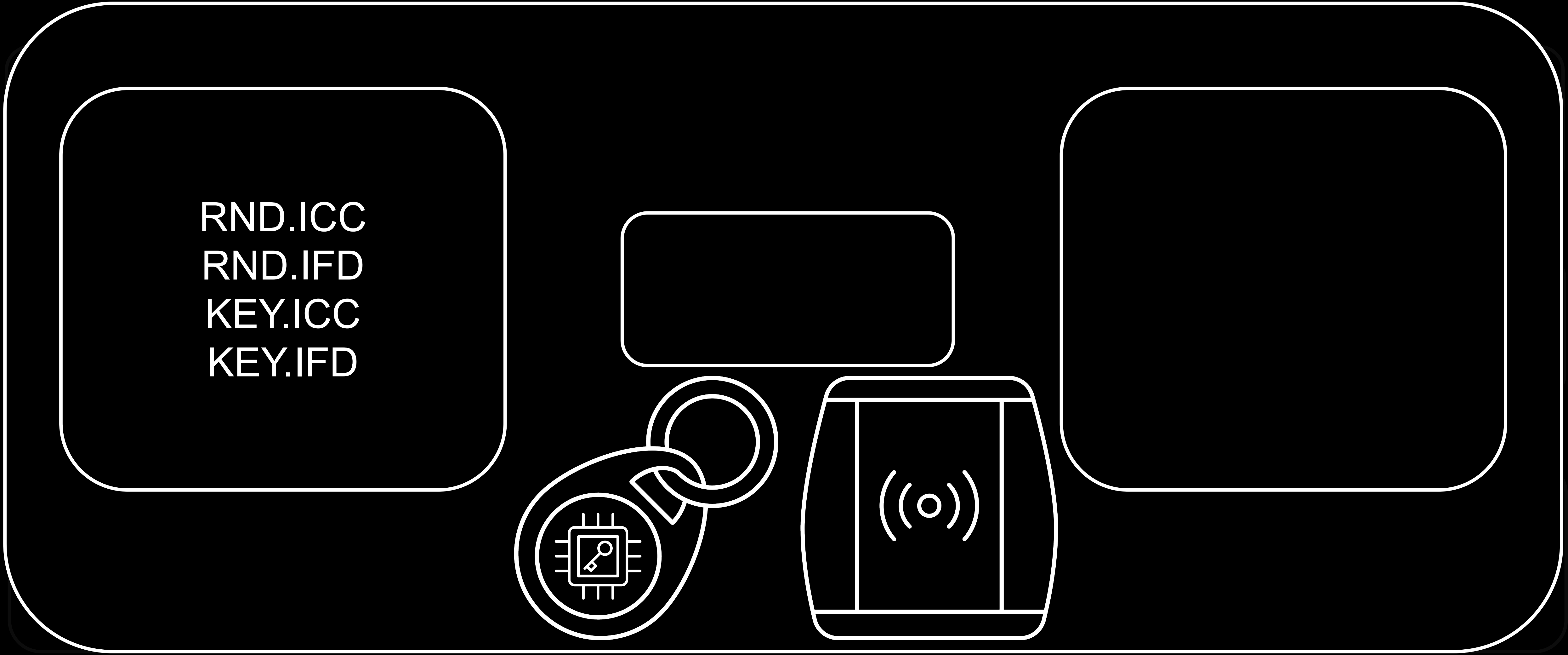
Length

```
8508A556FCB38B03D6F697008E085B17E7B6D7479E3600
```

APDU

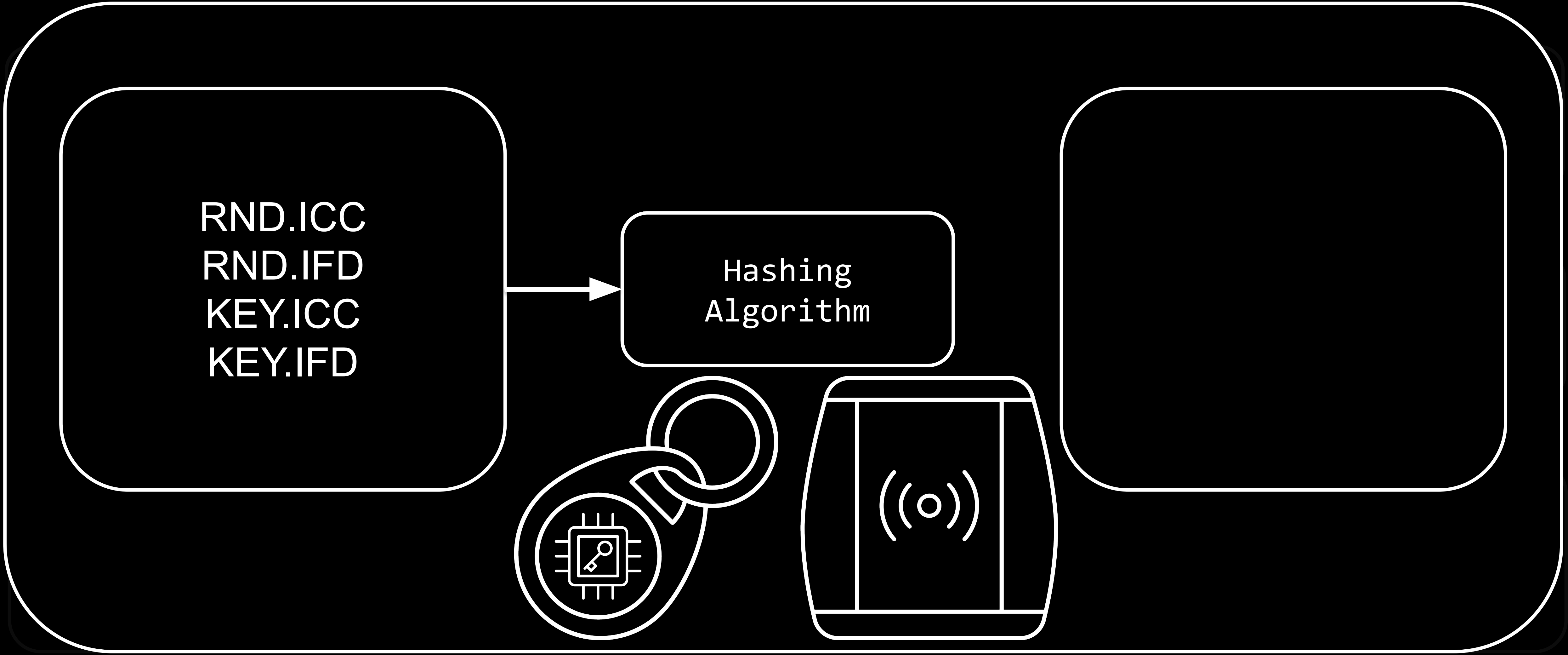
```
85 [08] = Cryptogram
A556FCB38B03D6F6
97 [00]
8E [08] = MAC
5B17E7B6D7479E36
```

```
0A020CCB3FFF168508A556FCB38B03D6F697008E085B17E7B6D7479E360096A0
```



RND.ICC
RND.IFD
KEY.ICC
KEY.IFD

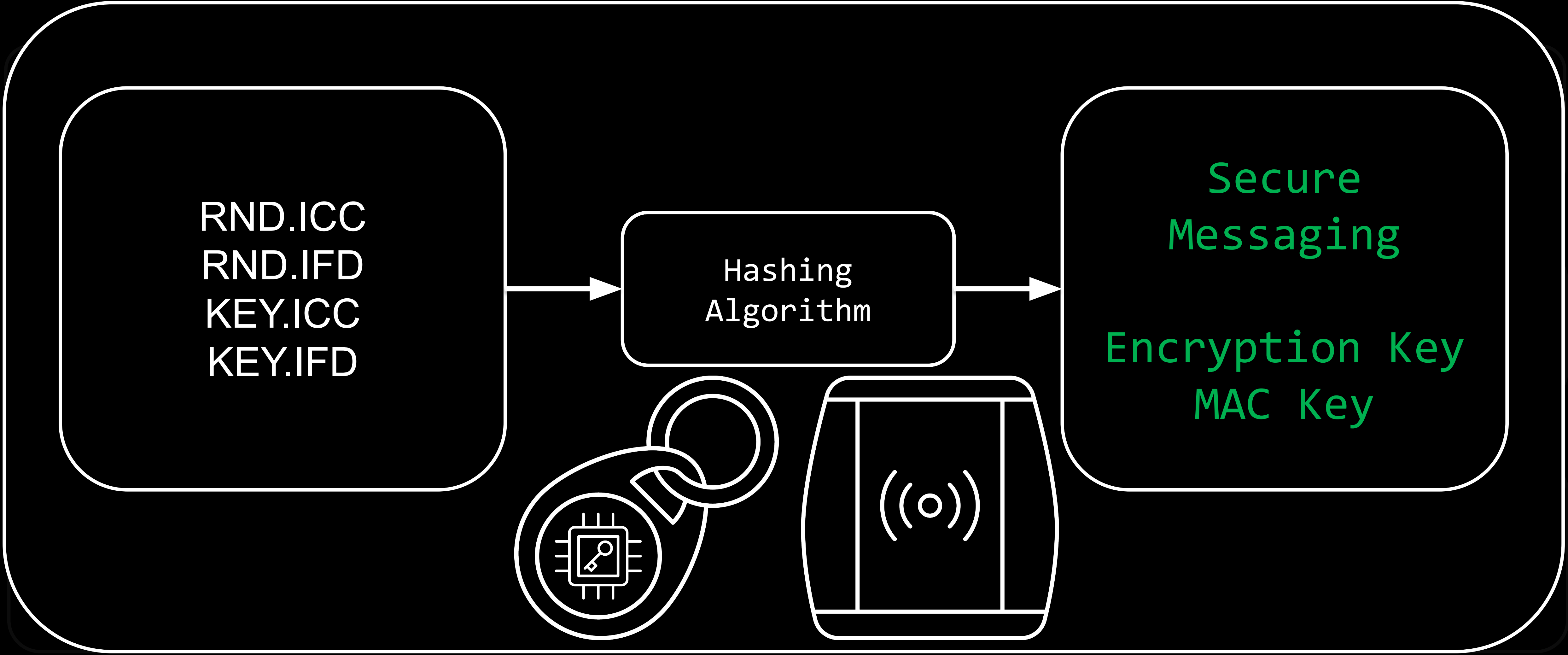
```
0A020CCB3FFF168508A556FCB38B03D6F697008E085B17E7B6D7479E360096A0
```



RND.ICC
RND.IFD
KEY.ICC
KEY.IFD

Hashing Algorithm

```
0A020CCB3FFF168508A556FCB38B03D6F697008E085B17E7B6D7479E360096A0
```



RND.ICC
RND.IFD
KEY.ICC
KEY.IFD

Hashing Algorithm

Secure Messaging

Encryption Key
MAC Key

```
0A020CCB3FFF168508A556FCB38B03D6F697008E085B17E7B6D7479E360096A0
```

```
85 [08] = Cryptogram
A556FCB38B03D6F6

97 [00]

8E [08] = MAC
5B17E7B6D7479E36
```

## MAC Chaining

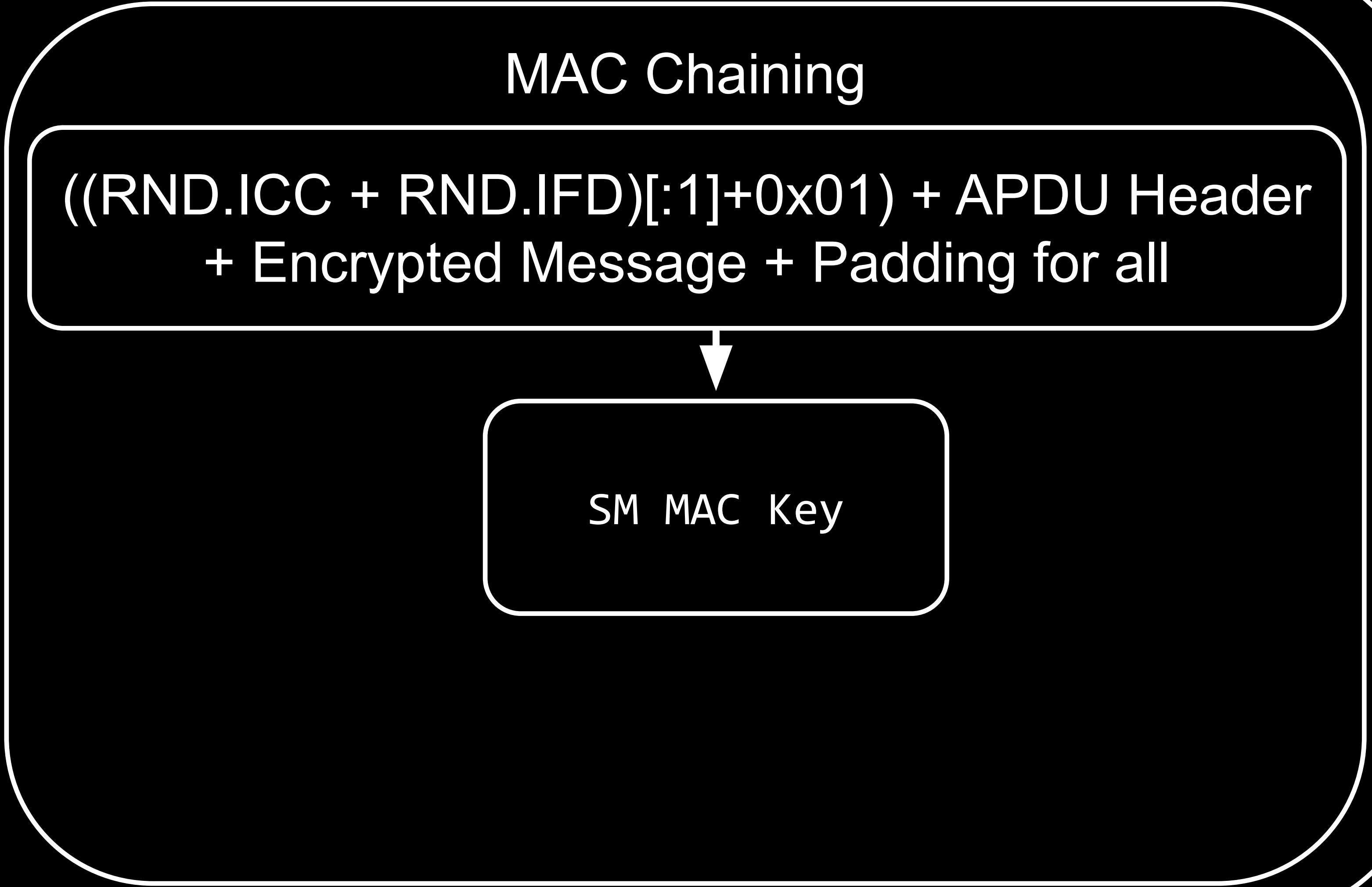
((RND.ICC + RND.IFD)[:1]+0x01) + APDU Header + Encrypted Message + Padding for all

```
0A020CCB3FFF168508A556FCB38B03D6F697008E085B17E7B6D7479E360096A0
```

```
85 [08] = Cryptogram
A556FCB38B03D6F6

97 [00]

8E [08] = MAC
5B17E7B6D7479E36
```



MAC Chaining

((RND.ICC + RND.IFD)[:1]+0x01) + APDU Header + Encrypted Message + Padding for all

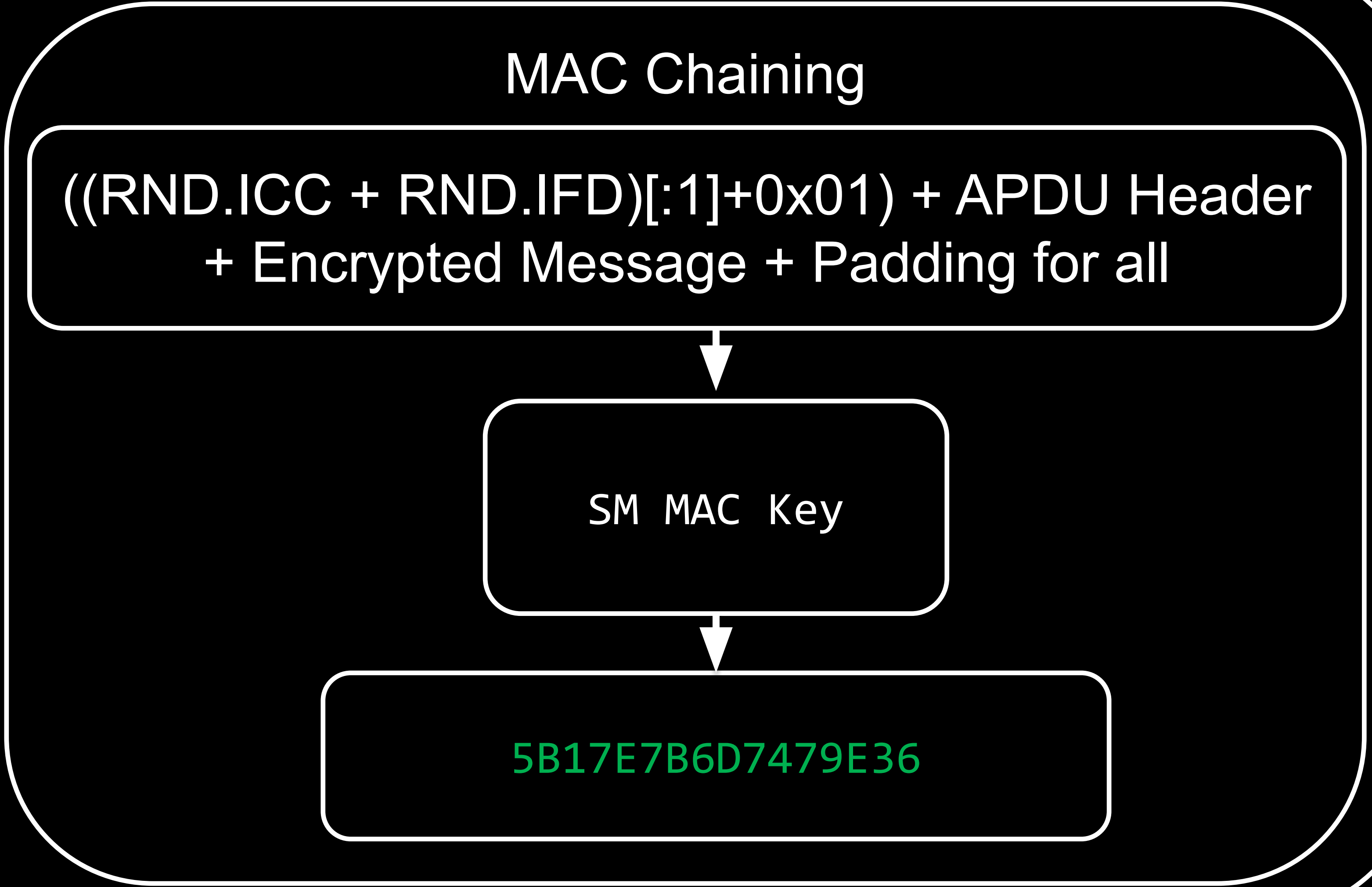
SM MAC Key

```
0A020CCB3FFF168508A556FCB38B03D6F697008E085B17E7B6D7479E360096A0
```

```
85 [08] = Cryptogram
A556FCB38B03D6F6

97 [00]

8E [08] = MAC
5B17E7B6D7479E36
```



MAC Chaining

((RND.ICC + RND.IFD)[:1]+0x01) + APDU Header + Encrypted Message + Padding for all

SM MAC Key

5B17E7B6D7479E36

```
0A020CCB3FFF168508A556FCB38B03D6F697008E085B17E7B6D7479E360096A0
```

```
85 [08] = Cryptogram
A556FCB38B03D6F6

97 [00]

8E [08] = MAC
5B17E7B6D7479E36
```

### Command Decryption

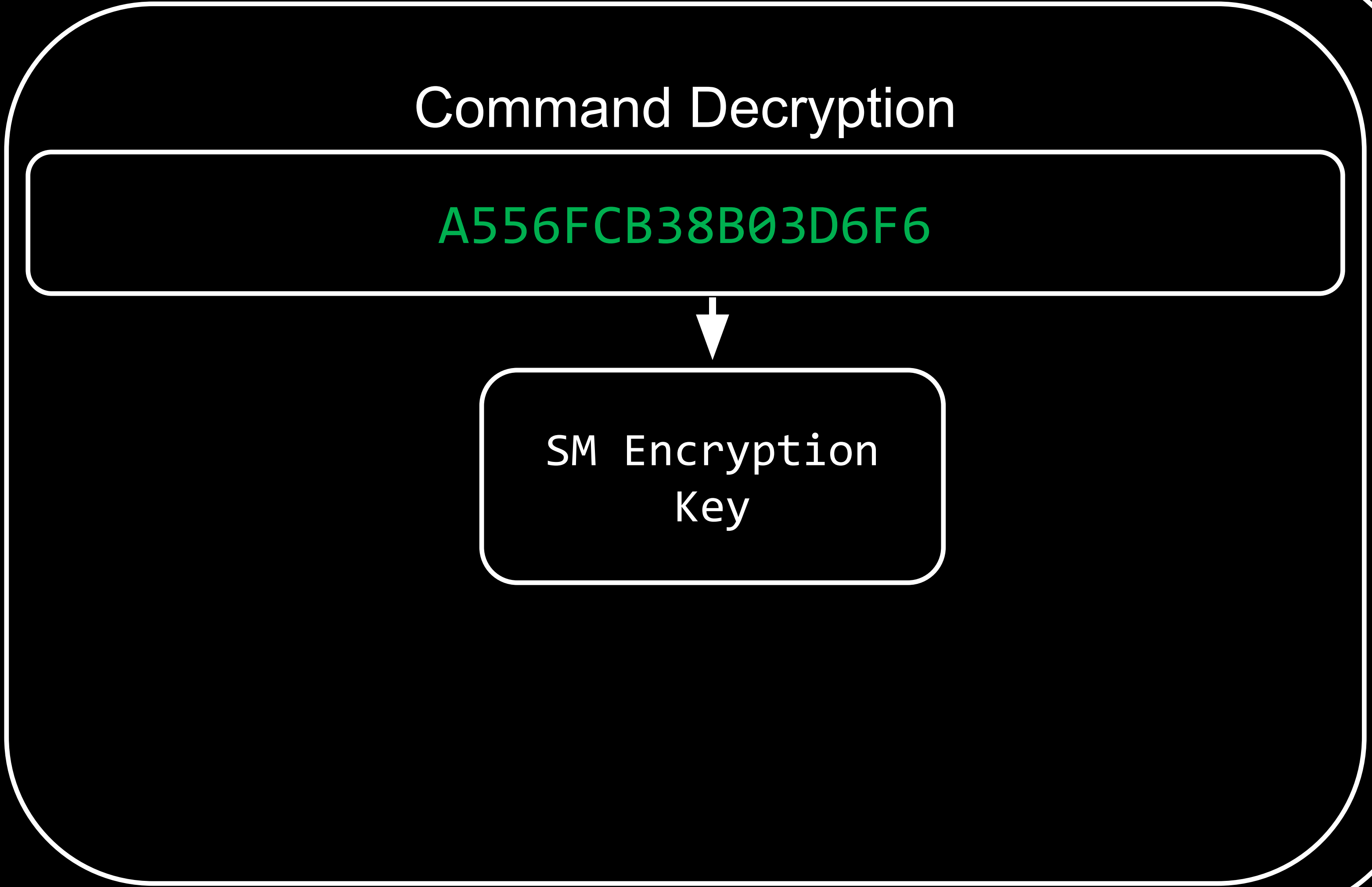
```
A556FCB38B03D6F6
```

0A020CCB3FFF168508A556FCB38B03D6F697008E085B17E7B6D7479E360096A0

85 [08] = Cryptogram
A556FCB38B03D6F6

97 [00]

8E [08] = MAC
5B17E7B6D7479E36



Command Decryption

A556FCB38B03D6F6

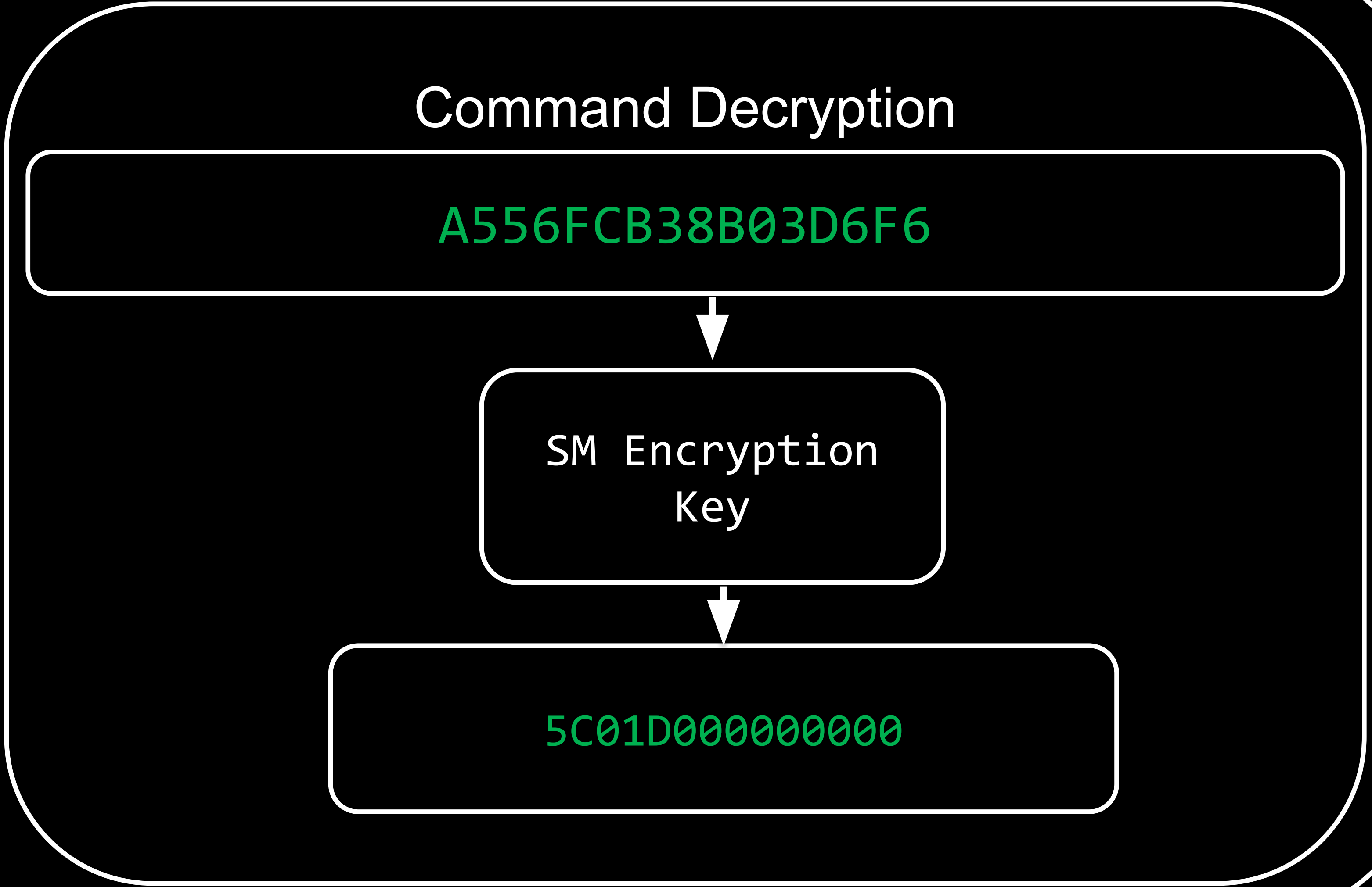
SM Encryption
Key

```
0A020CCB3FFF168508A556FCB38B03D6F697008E085B17E7B6D7479E360096A0
```

```
85 [08] = Cryptogram
A556FCB38B03D6F6

97 [00]

8E [08] = MAC
5B17E7B6D7479E36
```



Command Decryption

A556FCB38B03D6F6

SM Encryption Key

5C01D000000000

```
0A020CCB3FFF168508A556FCB38B03D6F697008E085B17E7B6D7479E360096A0
```

```
5C [01]   = ASN1 Tag
D0      = Object to get

00000000  = Padding
```

```
0A03008700092C7C2A8228203FB3BF4F476BBDA5C8B01D76A9FAF6557D57D5AE8D88
EC2066D0016A1551006ACC3FD3AFF2B41A00719B
```

```
0A037C2A8228F6AB0D0E72289F8C4DF1C0E0C429930F1424461B7E300AC72F46DD56
2EDAED304FD673CC06DE888F9000B152
```

```
0A020CCB3FFF168508A556FCB38B03D6F697008E085B17E7B6D7479E360096A0
```

```
0A0085401D8ADB062ED56480F4CCA55655423C83B016E93AEC2F861E5086D61CC8F
115C4A41D05D594964B64956C07969B31B32C6576A59458B29680B99B7BF9E17CDC
C3990290008E08BB4B96E7B80C42B69000FE4B
```

```
0A0085401D8ADB062ED56480F4CCA55655423C83B016E93AEC2F861E5086D61CC8F
115C4A41D05D594964B64956C07969B31B32C6576A59458B29680B99B7BF9E17CDC
C3990290008E08BB4B96E7B80C42B69000FE4B
```

```
0A037C2A8228F6AB0D0E72289F8C4DF1C0E0C429930F1424461B7E300AC72F46DD56
2EDAED304FD673CC06DE888F9000B152
```

```
0A020CCB3FFF168508A556FCB38B03D6F697008E085B17E7B6D7479E360096A0
```

```
0A0085401D8ADB062ED56480F4CCA55655423C83B016E93AEC2F861E5086D61CC8F
115C4A41D05D594964B64956C07969B31B32C6576A59458B29680B99B7BF9E17CDC
C3990290008E08BB4B96E7B80C42B69000FE4B
```

```
85401D8ADB062ED56480F4CCA55655423C83B016E93AEC2F861E5086D61CC8F115C
4A41D05D594964B64956C07969B31B32C6576A59458B29680B99B7BF9E17CDCC399
0290008E08BB4B96E7B80C42B6 9000 (OKAY)
```

```
0A020CCB3FFF168508A556FCB38B03D6F697008E085B17E7B6D7479E360096A0
```

```
0A0085401D8ADB062ED56480F4CCA55655423C83B016E93AEC2F861E5086D61CC8F
115C4A41D05D594964B64956C07969B31B32C6576A59458B29680B99B7BF9E17CDC
C3990290008E08BB4B96E7B80C42B69000FE4B
```

```
0A037C2A8228F6AB0D0E72289F8C4DF1C0E0C429930F1424461B7E300AC72F46DD56
2EDAED304FD673CC06DE888F9000B152
```

```
85 [40]
1D8ADB062ED56480F4CCA55655423C83B016E93AEC2F861E5086D61CC8F115C4A
41D05D594964B64956C07969B31B32C6576A59458B29680B99B7BF9E17CDCC3
99 [02]
9000
8E [08]
BB4B96E7B80C42B6
```

```
0A0085401D8ADB062ED56480F4CCA55655423C83B016E93AEC2F861E5086D61CC8F
115C4A41D05D594964B64956C07969B31B32C6576A59458B29680B99B7BF9E17CDC
C3990290008E08BB4B96E7B80C42B69000FE4B
```

```
0A037C2A8228F6AB0D0E72289F8C4DF1C0E0C429930F1424461B7E300AC72F46DD56
2EDAED304FD673CC06DE888F9000B152
```

```
85 [40] = ASN1 Tag for Cryptogram
1D8ADB062ED56480F4CCA55655423C83B016E93AEC2F861E5086D61CC8F115C4A
41D05D594964B64956C07969B31B32C6576A59458B29680B99B7BF9E17CDCC3
99 [02] = ASN1 Tag for Response Code
9000
8E [08] = ASN1 Tag for MAC
BB4B96E7B80C42B6
```

```
0A0085401D8ADB062ED56480F4CCA55655423C83B016E93AEC2F861E5086D61CC8F1
15C4A41D05D594964B64956C07969B31B32C6576A59458B29680B99B7BF9E17CDCC3
990290008E08BB4B96E7B80C42B69000FE4B
```

```
85 [40]
1D8ADB062ED56480F4CCA5565
5423C83B016E93AEC2F861E50
86D61CC8F115C4A41D05D5949
64B64956C07969B31B32C6576
A59458B29680B99B7BF9E17CD
CC3

99 [02]
9000

8E [08]
BB4B96E7B80C42B6
```

## MAC Chaining

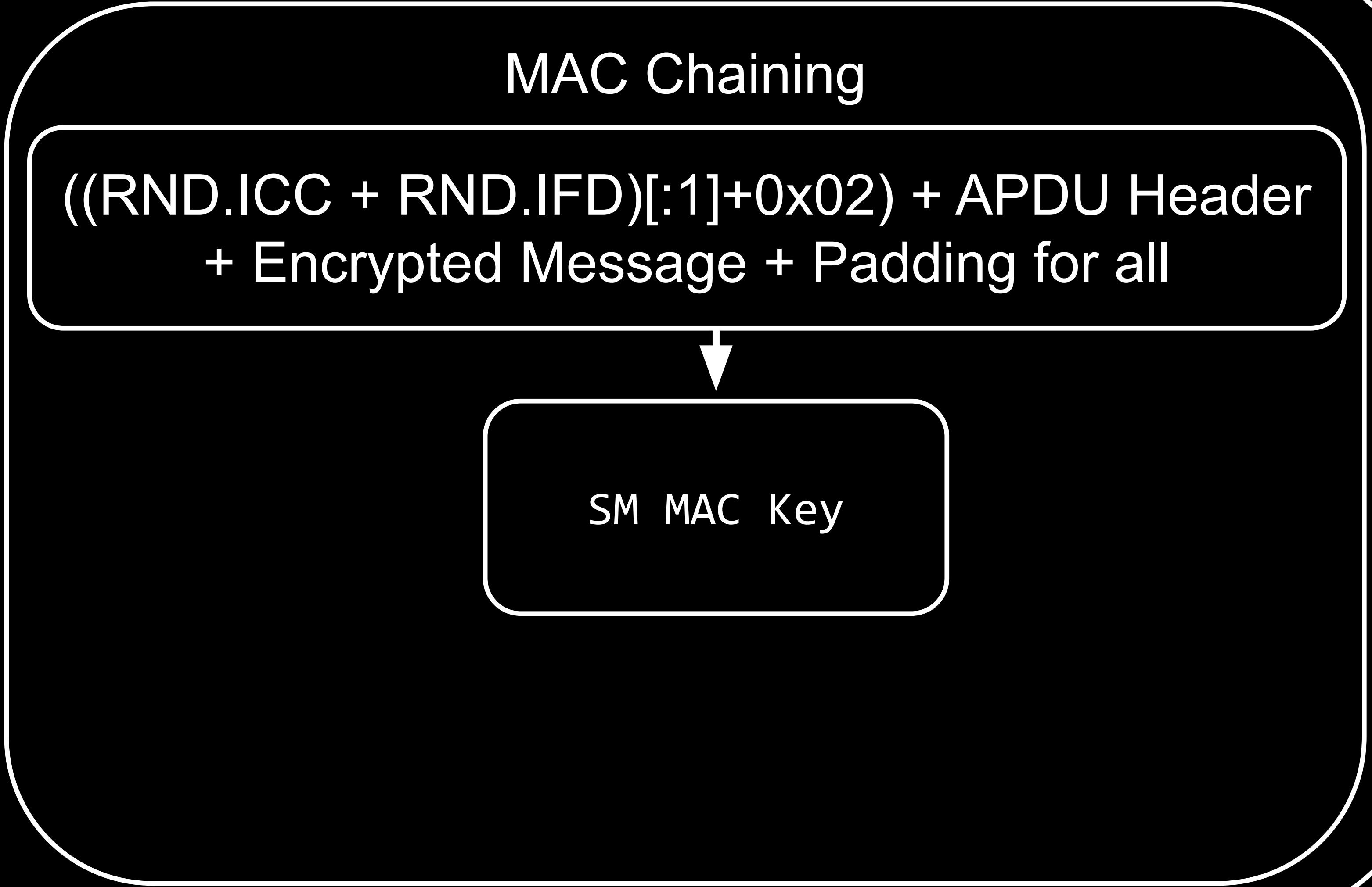
((RND.ICC + RND.IFD)[:1]+0x02) + APDU Header + Encrypted Message + Padding for all

```
0A0085401D8ADB062ED56480F4CCA55655423C83B016E93AEC2F861E5086D61CC8F1
15C4A41D05D594964B64956C07969B31B32C6576A59458B29680B99B7BF9E17CDCC3
990290008E08BB4B96E7B80C42B69000FE4B
```

```
85 [40]
1D8ADB062ED56480F4CCA5565
5423C83B016E93AEC2F861E50
86D61CC8F115C4A41D05D5949
64B64956C07969B31B32C6576
A59458B29680B99B7BF9E17CD
CC3

99 [02]
9000

8E [08]
BB4B96E7B80C42B6
```


MAC Chaining

((RND.ICC + RND.IFD)[:1]+0x02) + APDU Header + Encrypted Message + Padding for all

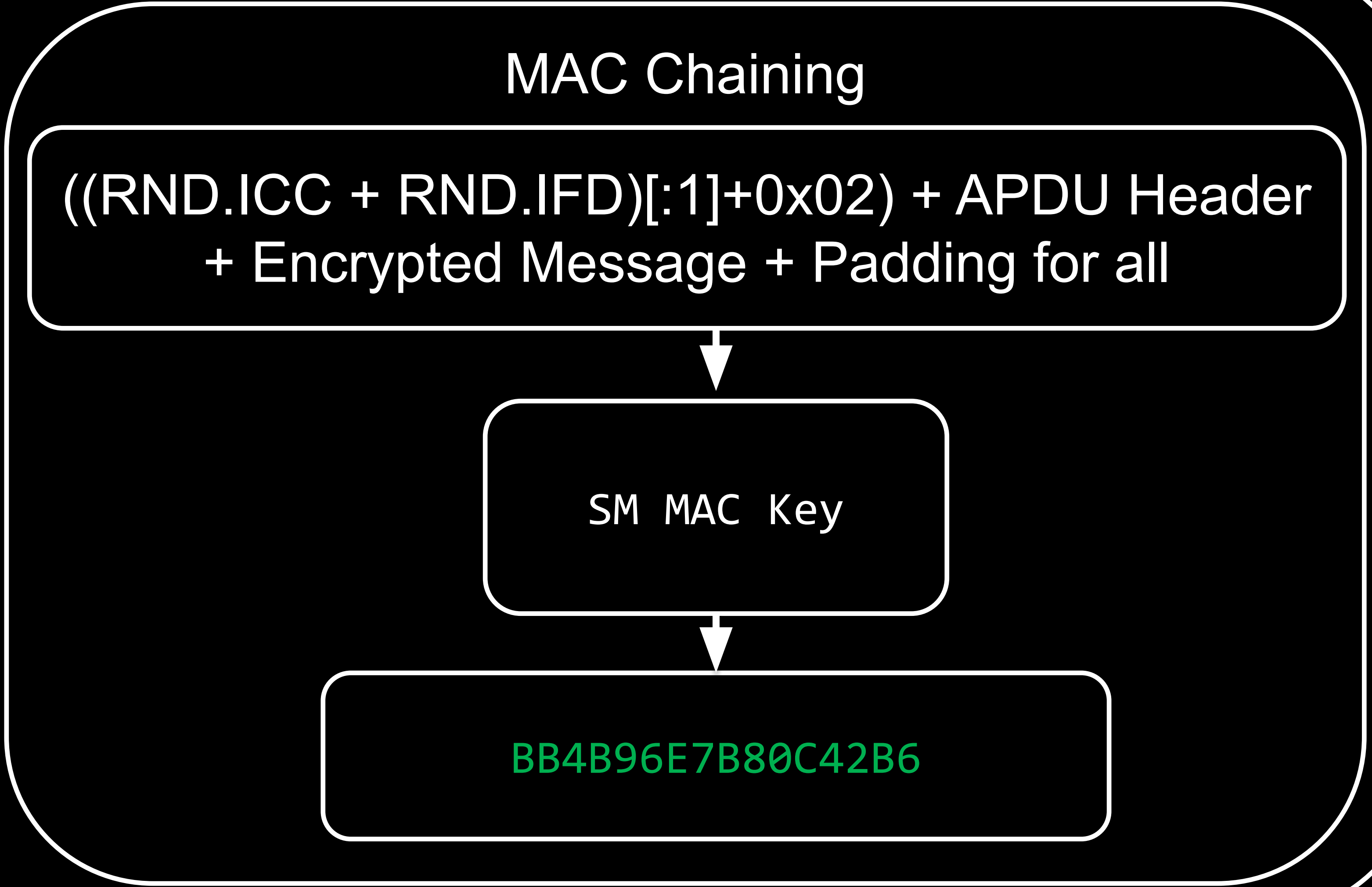
SM MAC Key

```
0A0085401D8ADB062ED56480F4CCA55655423C83B016E93AEC2F861E5086D61CC8F1
15C4A41D05D594964B64956C07969B31B32C6576A59458B29680B99B7BF9E17CDCC3
990290008E08BB4B96E7B80C42B69000FE4B
```

```
85 [40]
1D8ADB062ED56480F4CCA5565
5423C83B016E93AEC2F861E50
86D61CC8F115C4A41D05D5949
64B64956C07969B31B32C6576
A59458B29680B99B7BF9E17CD
CC3

99 [02]
9000

8E [08]
BB4B96E7B80C42B6
```



MAC Chaining

((RND.ICC + RND.IFD)[:1]+0x02) + APDU Header + Encrypted Message + Padding for all

SM MAC Key

BB4B96E7B80C42B6

```
0A0085401D8ADB062ED56480F4CCA55655423C83B016E93AEC2F861E5086D61CC8F1
15C4A41D05D594964B64956C07969B31B32C6576A59458B29680B99B7BF9E17CDCC3
990290008E08BB4B96E7B80C42B69000FE4B
```

```
85 [40]
1D8ADB062ED56480F4CCA5565
5423C83B016E93AEC2F861E50
86D61CC8F115C4A41D05D5949
64B64956C07969B31B32C6576
A59458B29680B99B7BF9E17CD
CC3

99 [02]
9000

8E [08]
BB4B96E7B80C42B6
```

## Command Decryption

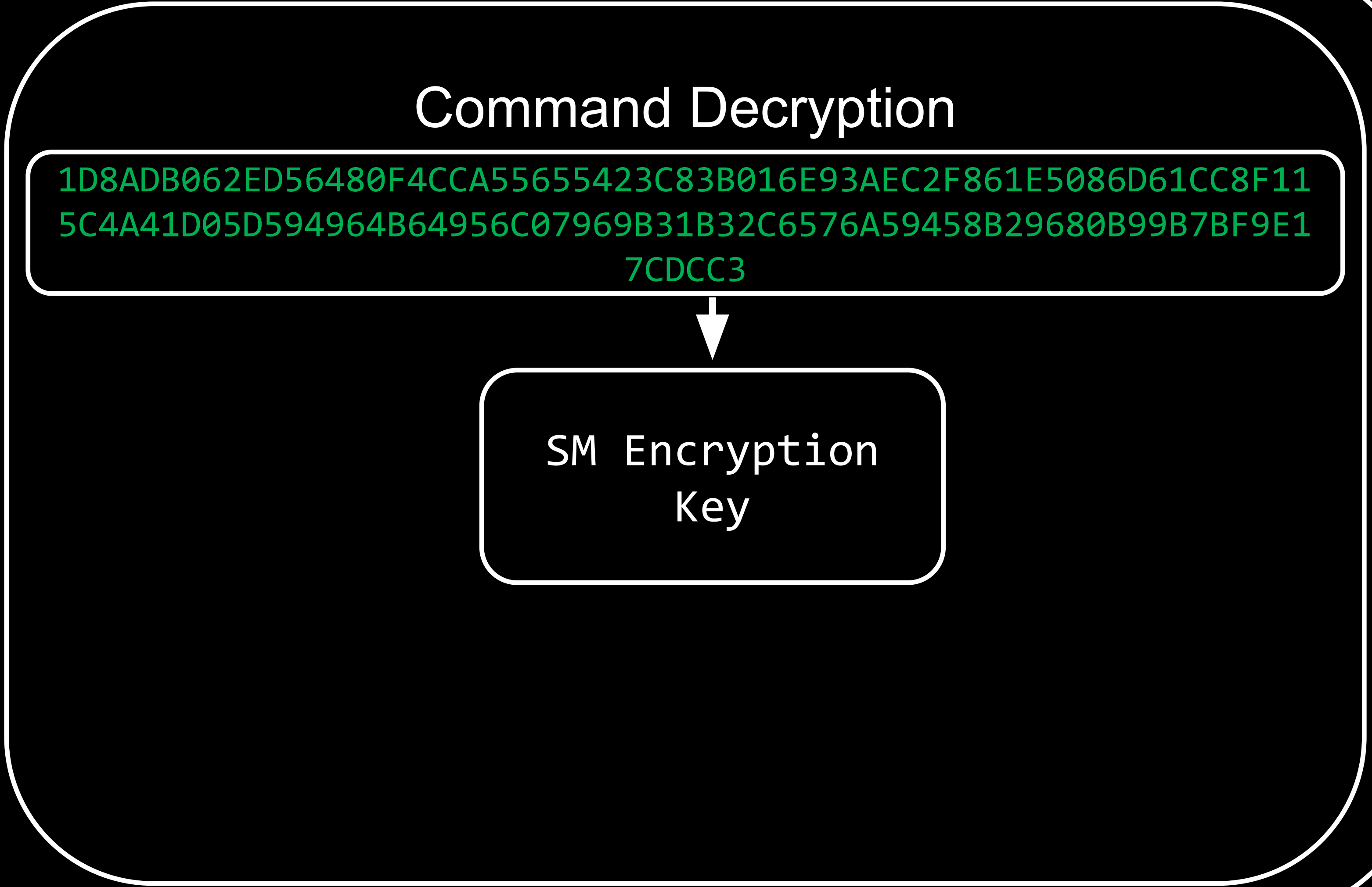
```
1D8ADB062ED56480F4CCA55655423C83B016E93AEC2F861E5086D61CC8F11
5C4A41D05D594964B64956C07969B31B32C6576A59458B29680B99B7BF9E1
7CDCC3
```

```
0A0085401D8ADB062ED56480F4CCA55655423C83B016E93AEC2F861E5086D61CC8F1
15C4A41D05D594964B64956C07969B31B32C6576A59458B29680B99B7BF9E17CDCC3
990290008E08BB4B96E7B80C42B69000FE4B
```

```
85 [40]
1D8ADB062ED56480F4CCA5565
5423C83B016E93AEC2F861E50
86D61CC8F115C4A41D05D5949
64B64956C07969B31B32C6576
A59458B29680B99B7BF9E17CD
CC3

99 [02]
9000

8E [08]
BB4B96E7B80C42B6
```



Command Decryption

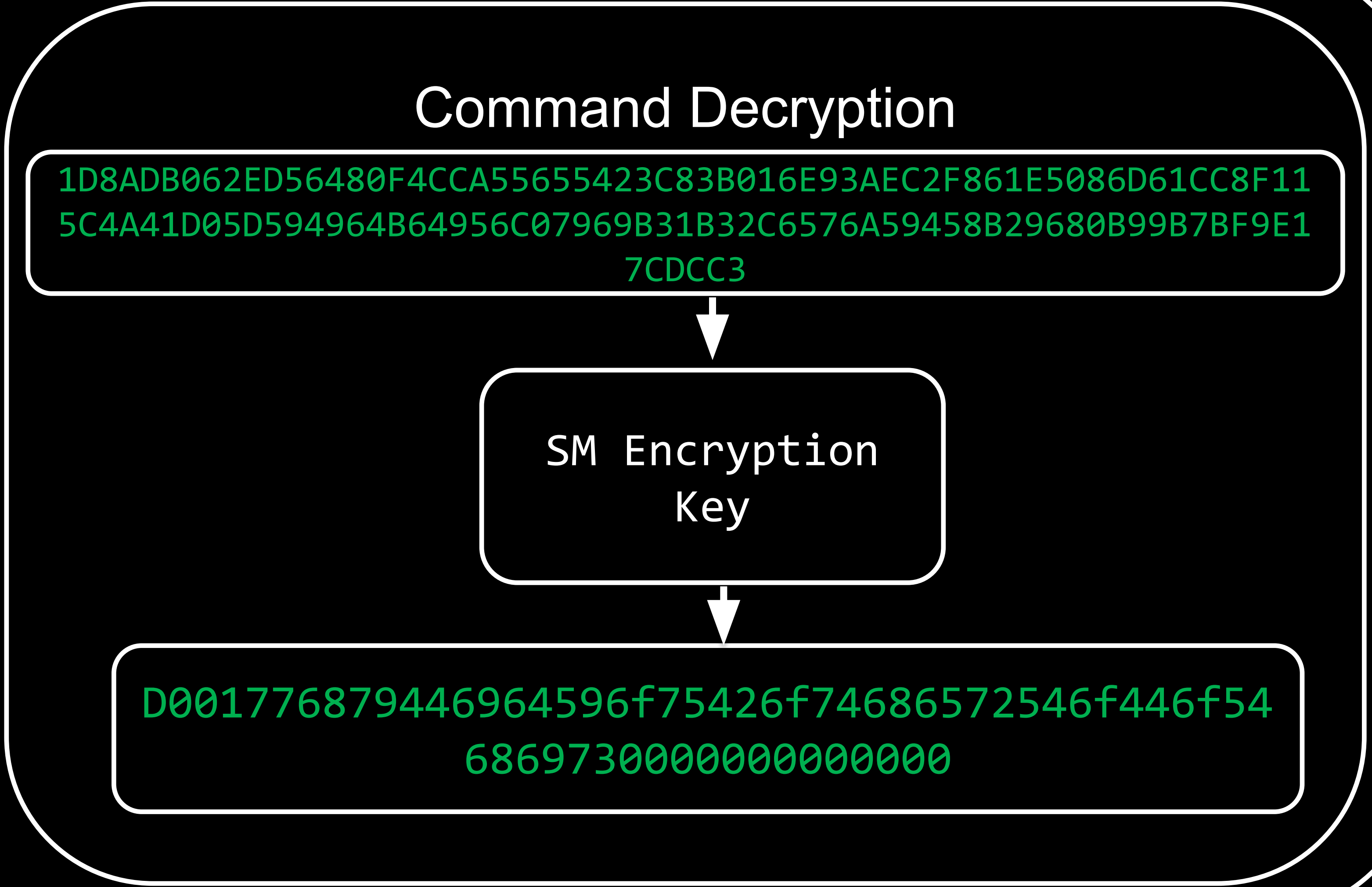
```
1D8ADB062ED56480F4CCA55655423C83B016E93AEC2F861E5086D61CC8F11
5C4A41D05D594964B64956C07969B31B32C6576A59458B29680B99B7BF9E1
7CDCC3
```

```
0A0085401D8ADB062ED56480F4CCA55655423C83B016E93AEC2F861E5086D61CC8F1
15C4A41D05D594964B64956C07969B31B32C6576A59458B29680B99B7BF9E17CDCC3
990290008E08BB4B96E7B80C42B69000FE4B
```

```
85 [40]
1D8ADB062ED56480F4CCA5565
5423C83B016E93AEC2F861E50
86D61CC8F115C4A41D05D5949
64B64956C07969B31B32C6576
A59458B29680B99B7BF9E17CD
CC3

99 [02]
9000

8E [08]
BB4B96E7B80C42B6
```



## Command Decryption

```
1D8ADB062ED56480F4CCA55655423C83B016E93AEC2F861E5086D61CC8F11
5C4A41D05D594964B64956C07969B31B32C6576A59458B29680B99B7BF9E1
7CDCC3
```

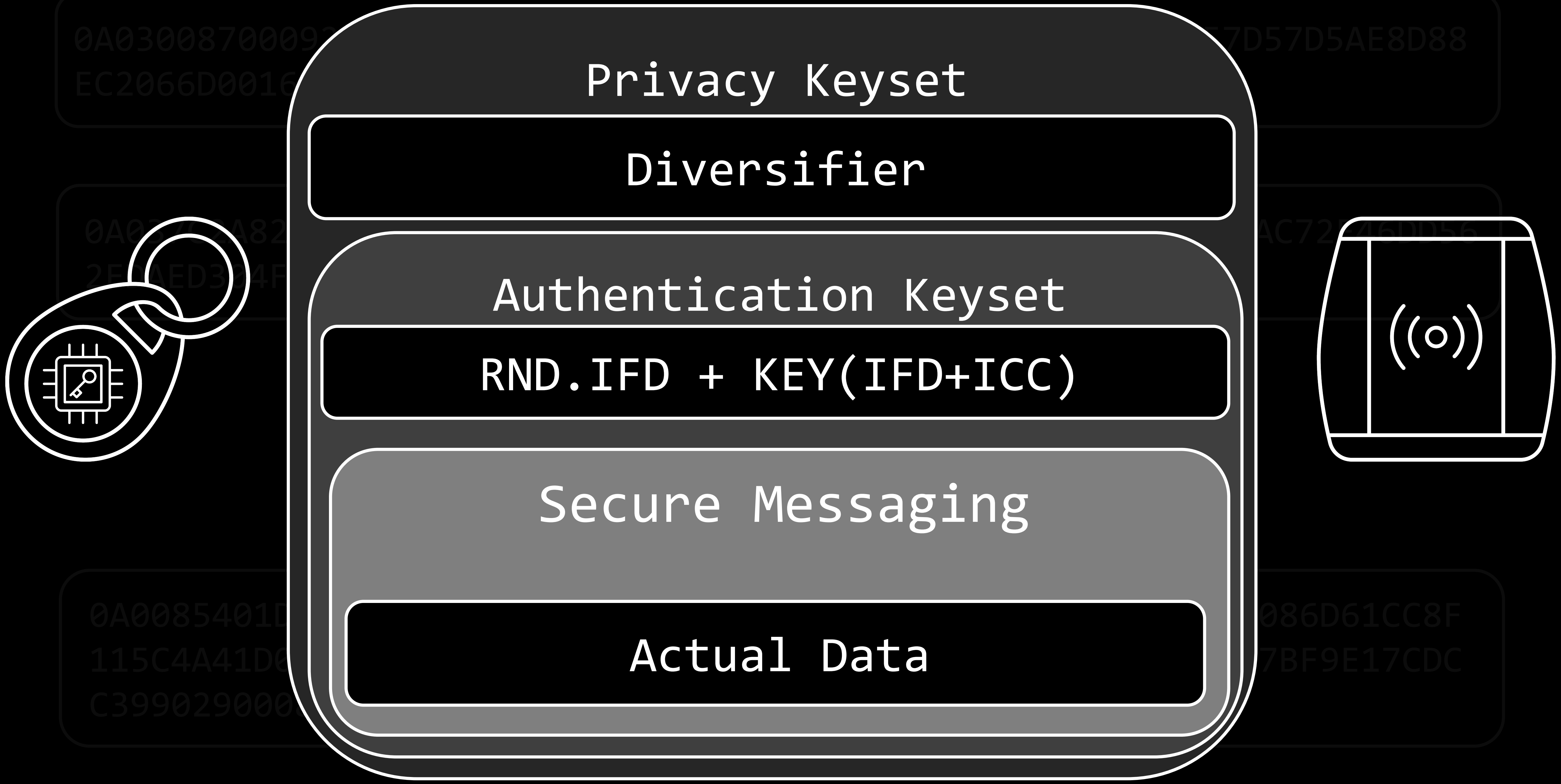
SM Encryption Key

```
D00177687944696459 6f75426f74686572546f446f54
686973000000000000
```

```
0A0085401D8ADB062ED56480F4CCA55655423C83B016E93AEC2F861E5086D61CC8F1
15C4A41D05D594964B64956C07969B31B32C6576A59458B29680B99B7BF9E17CDCC3
990290008E08BB4B96E7B80C42B69000FE4B
```

```
D0 [01]    = ASN1 Tag for Object
776879446964596f75426f74686572546f446f54686973

000000000000    = Padding
```



Privacy Keyset

Diversifier

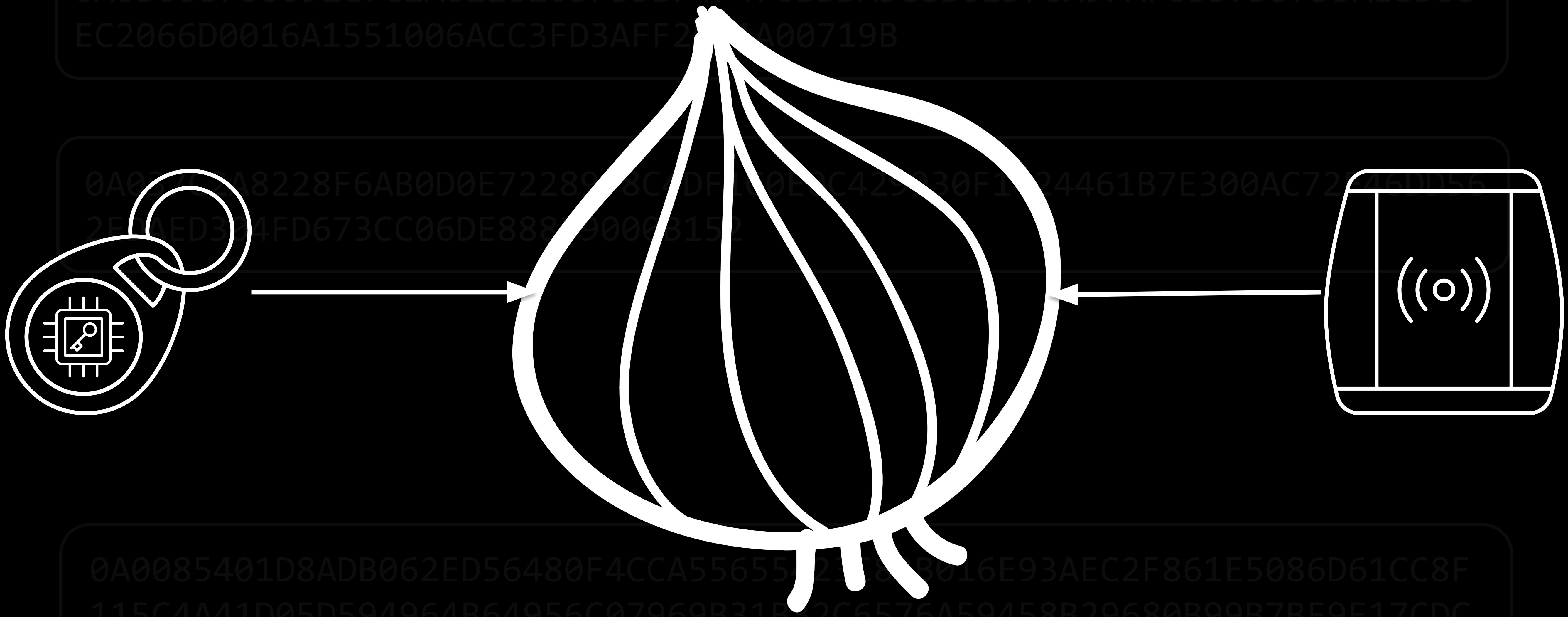
Authentication Keyset

RND.IFD + KEY(IFD+ICC)

Secure Messaging

Actual Data

```
0A03008700092C7C2A8228203FB3BF4F476BBDA5C8B01D76A9FAF6557D57D5AE8D88
EC2066D0016A1551006ACC3FD3AFF2[illegible]A00719B
```



```
0A0[illegible]A8228F6AB0D0E72289[illegible]8C4DF[illegible]0E[illegible]C429[illegible]30F1[illegible]24461B7E300AC72[illegible]6DD56
2F[illegible]AED3[illegible]4FD673CC06DE888[illegible]9000B152
```

```
0A0085401D8ADB062ED56480F4CCA55655[illegible]2[illegible]8[illegible]B016E93AEC2F861E5086D61CC8F
115C4A41D05D594964B64956C07969B31B[illegible]2C6576A59458B29680B99B7BF9E17CDC
C3990290008E08BB4B96E7B80C42B69000FE4B
```

# Now, on to Iceman

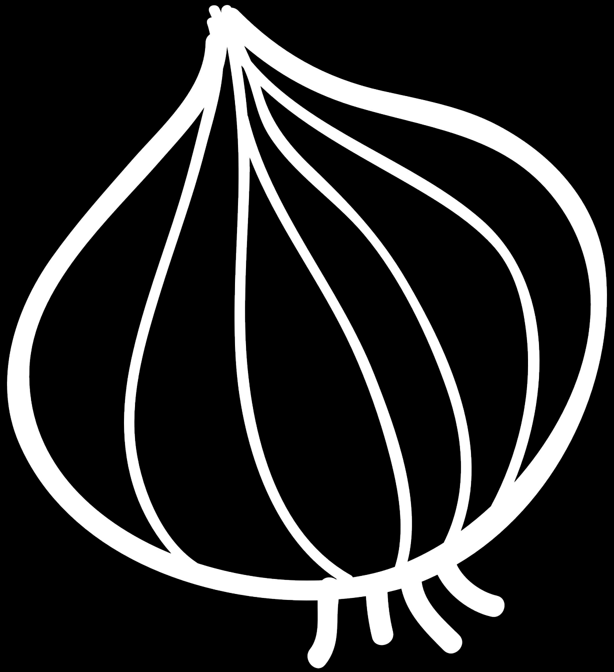
# Secure Information Object - SIO

A SIO has following properties:

- Data container
- It can be stored everywhere
- Independent of the media carrier
- Encrypted and Signed Payload
- Diversified keys
- Variable sized

# Secure Information Object - SIO

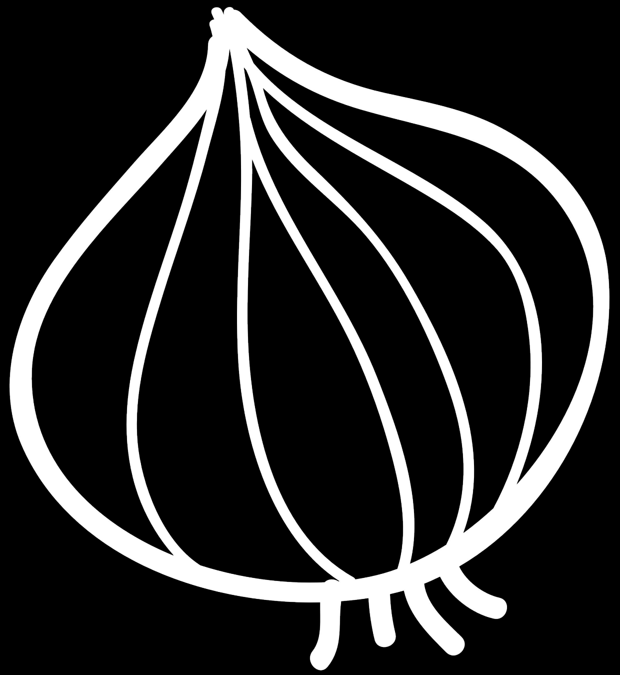
```
30328105018AFB0954A5020500A60881010
10403030008A7178515A52FA14117068249
A73879F3BB084C43194148FB7DA9020500
```



# Secure Information Object - SIO

More bytes?!?!

```
30328105018AFB0954A5020500A60881010
10403030008A7178515A42FA14117069449
A73879F3BB084C434BD048FB7DA9020500
```



# Secure Information Object - SIO

```
[=] ---------------- ASN1 TLV -----------------
[=]  -- 30 [32] 'SEQUENCE'
[=]    -- 81 [05] 'elem'
[=]        00: 01 8A FB 09 54
[=]    -- A5 [02] '[5]'
[=]        -- 05 [00] 'NULL'
[=]    -- A6 [08] 'elem'
[=]        -- 81 [01] 'elem'
[=]            00: 01
[=]        -- 04 [03] 'OCTET STRING'  hex: '03 00 08'
[=]    -- A7 [17] 'elem'
[=]        -- 85 [15] 'elem'
[=]            00: A5 2F A1 41 17 06 82 49 A7 38 79 F3 BB 08 4C 43
[=]            10: 19 41 48 FB 7D
[=]    -- A9 [02] 'elem'
[=]        -- 05 [00] 'NULL'
```

```
30328105018AF
B0954A5020500
A608810101040
3030008A71785
15A52FA141170
68249A73879F3
BB084C4319414
8FB7DA9020500
```

# Secure Information Object - SIO

```
[=] ----------------- ASN1 TLV ------------------
[=]  -- 30 [32] 'SEQUENCE'
[=]    -- 81 [05] 'elem'
[=]        00: 01 8A FB 09 54
[=]    -- A5 [02] '[5]'
[=]        -- 05 [00] 'NULL'
[=]    -- A6 [08] 'elem'
[=]        -- 81 [01] 'elem'
[=]            00: 01
[=]        -- 04 [03] 'OCTET STRING'  hex: '03 00 08'
[=]    -- A7 [17] 'elem'
[=]        -- 85 [15] 'elem'
[=]            00: A5 2F A1 41 17 06 82 49 A7 38 79 F3 BB 08 4C 43
[=]            10: 19 41 48 FB 7D
[=]    -- A9 [02] 'elem'
[=]        -- 05 [00] 'NULL'
```

```
30328105018AF
B0954A5020500
A608810101040
3030008A71785
15A52FA141170
68249A73879F3
BB084C4319414
8FB7DA9020500
```

# Secure Information Object - SIO

## Let’s break it down!

# Secure Information Object - SIO

```
[=] ----------------- ASN1 TLV ------------------
[=]  -- 30 [32] 'SEQUENCE'
[=]    -- 81 [05] 'elem'
[=]        00: 01 8A FB 09 54
[=]    -- A5 [02] '[5]'
[=]        -- 05 [00] 'NULL'
[=]    -- A6 [08] 'elem'
[=]        -- 81 [01] 'elem'
[=]            00: 01
[=]        -- 04 [03] 'OCTET STRING'  hex: '03 00 08'
[=]    -- A7 [17] 'elem'
[=]        -- 85 [15] 'elem'
[=]            00: A5 2F A1 41 17 06 82 49 A7 38 79 F3 BB 08 4C 43
[=]            10: 19 41 48 FB 7D
[=]    -- A9 [02] 'elem'
[=]        -- 05 [00] 'NULL'
```

```
30328105018AF
B0954A5020500
A608810101040
3030008A71785
15A52FA141170
68249A73879F3
BB084C4319414
8FB7DA9020500
```

# Secure Information Object - SIO

```
[=] ---------------- ASN1 TLV -----------------
[=]  -- 30 [32] 'SEQUENCE'
[=]    -- 81 [05] 'elem'
[=]        00: 01 8A FB 09 54
[=]    -- A5 [02] '[5]'
[=]        -- 05 [00] 'NULL'
[=]    -- A6 [08] 'elem'
[=]        -- 81 [01] 'elem'
[=]            00: 01
[=]        -- 04 [03] 'OCTET STRING'  hex: '03 00 08'
[=]    -- A7 [17] 'elem'
[=]        -- 85 [15] 'elem'
[=]            00: A5 2F A1 41 17 06 82 49 A7 38 79 F3 BB 08 4C 43
[=]            10: 19 41 48 FB 7D
[=]    -- A9 [02] 'elem'
[=]        -- 05 [00] 'NULL'
```

Relative OID
018AFB0954

# Secure Information Object - SIO

```
[=] ---------------- ASN1 TLV -----------------
[=]  -- 30 [32] 'SEQUENCE'
[=]    -- 81 [05] 'elem'
[=]       00: 01 8A FB 09 54
[=]    -- A5 [02] '[5]'
[=]       -- 05 [00] 'NULL'
[=]    -- A6 [08] 'elem'
[=]       -- 81 [01] 'elem'
[=]           00: 01
[=]       -- 04 [03] 'OCTET STRING'  hex: '03 00 08'
[=]    -- A7 [17] 'elem'
[=]       -- 85 [15] 'elem'
[=]           00: A5 2F A1 41 17 06 82 49 A7 38 79 F3 BB 08 4C 43
[=]           10: 19 41 48 FB 7D
[=]    -- A9 [02] 'elem'
[=]       -- 05 [00] 'NULL'
```

Relative OID
018AFB0954

Key Reference ID
01

# Secure Information Object - SIO

```
[=] ---------------- ASN1 TLV -----------------
[=]  -- 30 [32] 'SEQUENCE'
[=]    -- 81 [05] 'elem'
[=]       00: 01 8A FB 09 54
[=]    -- A5 [02] '[5]'
[=]       -- 05 [00] 'NULL'
[=]    -- A6 [08] 'elem'
[=]       -- 81 [01] 'elem'
[=]           00: 01
[=]       -- 04 [03] 'OCTET STRING'  hex: '03 00 08'
[=]    -- A7 [17] 'elem'
[=]       -- 85 [15] 'elem'
[=]           00: A5 2F A1 41 17 06 82 49 A7 38 79 F3 BB 08 4C 43
[=]           10: 19 41 48 FB 7D
[=]    -- A9 [02] 'elem'
[=]       -- 05 [00] 'NULL'
```

Relative OID
018AFB0954
Key Reference ID
01
Crypto
03 00 08

# Secure Information Object - SIO

```
[=] ---------------- ASN1 TLV -----------------
[=]  -- 30 [32] 'SEQUENCE'
[=]    -- 81 [05] 'elem'
[=]       00: 01 8A FB 09 54
[=]    -- A5 [02] '[5]'
[=]       -- 05 [00] 'NULL'
[=]    -- A6 [08] 'elem'
[=]       -- 81 [01] 'elem'
[=]          00: 01
[=]       -- 04 [03] 'OCTET STRING'  hex: '03 00 08'
[=]    -- A7 [17] 'elem'
[=]       -- 85 [15] 'elem'
[=]          00: A5 2F A1 41 17 06 82 49 A7 38 79 F3 BB 08 4C 43
[=]          10: 19 41 48 FB 7D
[=]    -- A9 [02] 'elem'
[=]       -- 05 [00] 'NULL'
```

```
Relative OID
018AFB0954
Key Reference ID
01
Crypto
03 00 08
PACS Payload
A4 2F A1 41 17
06 94 49 A7 38
79 F3 BB 08 4C
43 4B D0 48 FB
7D
```

black hat ASIA 2025

# Secure Information Object - SIO

```
Relative OID
01 8A FB 09 54
Key Reference ID
01
Crypto
03 00 08
PACS Payload
A5 2F A1 41 17 06 82 49 A7 38 79
F3 BB 08 4C 43 19 41 48 FB 7D
```

# Secure Information Object - SIO

Relative OID

```
01 8A FB 09 54
```

Key Reference ID

```
01
```

Crypto

```
03 00 08
```

PACS Payload

```
A5 2F A1 41 17 06 82 49 A7 38 79
F3 BB 08 4C 43 19 41 48 FB 7D
```

Every SIO belongs to a root OID

```
2B0601040181E43801010204
```

Relative OID is added to it

```
2B0601040181E43801010204018AFB0954
```

black hat ASIA 2025

# Secure Information Object - SIO

```
Relative OID
01 8A FB 09 54
Key Reference ID
01
Crypto
03 00 08
PACS Payload
A5 2F A1 41 17 06 82 49 A7 38 79
F3 BB 08 4C 43 19 41 48 FB 7D
```

# Secure Information Object - SIO

```
Relative OID
01 8A FB 09 54
Key Reference ID
01
Crypto
03 00 08
PACS Payload
A5 2F A1 41 17 06 82 49 A7 38 79
F3 BB 08 4C 43 19 41 48 FB 7D
```

Key Reference ID indicates if the SIO is

```
- Standard keyed  01
- Elite keyed     00
- Custom keyed    ??
```

This SIO uses the standard key

# Secure Information Object - SIO

```
Relative OID
018AFB0954
Key Reference ID
01
Crypto
03 00 08
PACS Payload
A5 2F A1 41 17 06 82 49 A7 38 79
F3 BB 08 4C 43 19 41 48 FB 7D
```

# Secure Information Object - SIO

Relative OID

```
01 8A FB 09 54
```

Key Reference ID

```
01
```

Crypto

```
03 00 08
```

PACS Payload

```
A5 2F A1 41 17 06 82 49 A7 38 79
F3 BB 08 4C 43 19 41 48 FB 7D
```

A SIO can use two different cryptos

| | |
|---|---|
| - EAX | 03 00 08 |
| - EAX´ Prime | 03 00 09 |

This SIO uses EAX

# Secure Information Object - SIO

```
Relative OID
01 8A FB 09 54
Key Reference ID
01
Crypto
03 00 08
PACS Payload
A5 2F A1 41 17 06 82 49 A7 38 79
F3 BB 08 4C 43 19 41 48 FB 7D
```

```
PACS Payload contains two parts

A5 2F A1 41 17 06 82 49 A7 38 79
F3 BB 08 4C 43 19 41 48 FB 7D
```

# Secure Information Object - SIO

PACS encrypted payload

XX bytes

```
A5 2F A1 41 17 06 82 49 A7 38 79
F3 BB 08 4C 43 19 41 48 FB 7D
```

PACS Signature

16 bytes

```
A5 2F A1 41 17 06 82 49 A7 38 79
F3 BB 08 4C 43 19 41 48 FB 7D
```

# In order to decrypt the payload

# In order to decrypt the payload

You need a key

# In order to decrypt the payload

You need a key

And every SIO uses a diversified key

# Key Diversification Function - KDF

Behind the scenes

HMAC with SHA1

Feed with a specially crafted 48 byte input

Outputs a 16 byte key

# Key Diversification Function - KDF

Behind the scenes

Remember that HMAC generates a 20 byte hash

*For us developing in a memory unsafe environment*

# You got the diversified key,  encrypted payload…

## You got the diversified key, encrypted payload…

Now what?????

## You got the diversified key, encrypted payload…

# Time to look at Next layer

## You got the diversified key, encrypted payload…

# The Crypto algorithms

# Authenticated Encryption With Associated Data - AEAD

Encryption and Signature in one go

Behind the scenes: AES and OMAC

Two different AEAD cryptographic algorithms is used

## Authenticated Encryption With Associated Data - AEAD

- EAX
- EAX' Prime

# Authenticated Encryption With Associated Data - AEAD

EAX

1. https://www.cs.ucdavis.edu/~rogaway/papers/eax.pdf
2. AES, EBC, CMAC
3. X byte encryption bytes
4. 16 bytes signature

# Authenticated Encryption With Associated Data - AEAD

EAX' Prime

i. ANSI C12.22-2012

   https://tiny.cc/jeee001

ii. AES, CBC, CMAC

iii. X byte encryption bytes

iv. X bytes signature ( standard 4 bytes )

## Authenticated Encryption With Associated Data - AEAD

Luckily

HID uses the Bouncy Castle C# implementation

# Authenticated Encryption With Associated Data - AEAD

*Which is open source*

https://github.com/bcgit/bc-csharp/

## Authenticated Encryption With Associated Data - AEAD

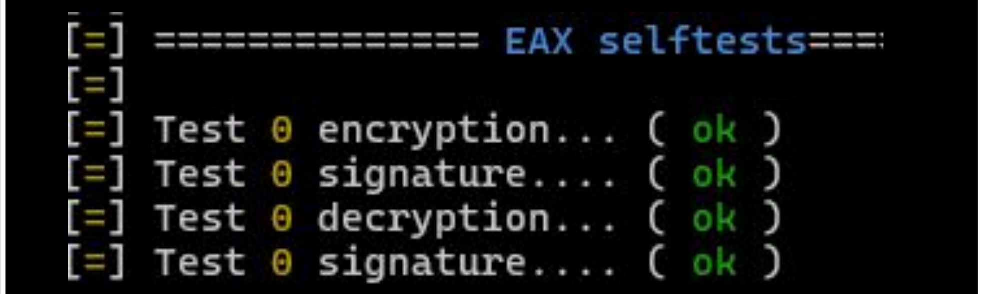
but

I needed a C implementation

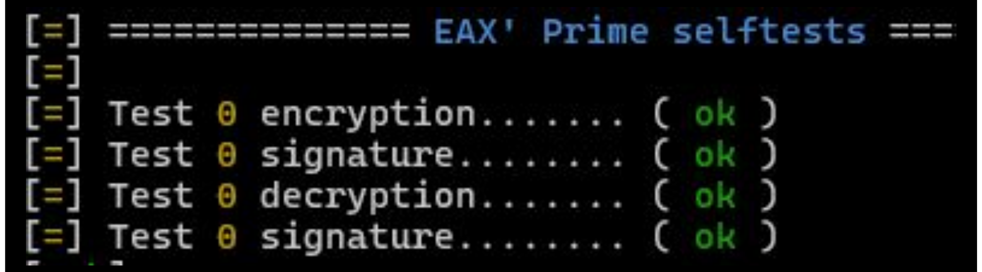
This took 2 weeks

# Authenticated Encryption With Associated Data - AEAD

## getting test vectors…

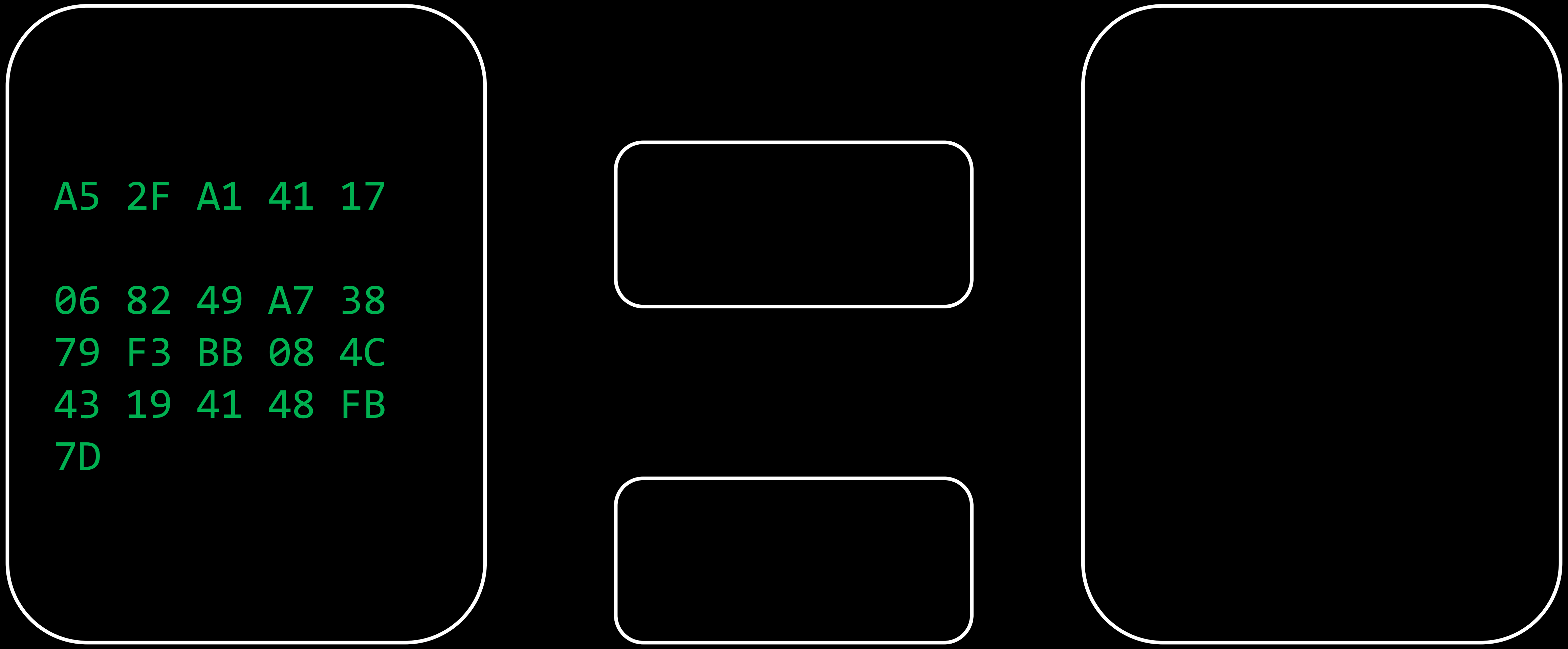


```
[=] ============== EAX selftests===
[=]
[=] Test 0 encryption... ( ok )
[=] Test 0 signature.... ( ok )
[=] Test 0 decryption... ( ok )
[=] Test 0 signature.... ( ok )
```



```
[=] ============== EAX' Prime selftests ===
[=]
[=] Test 0 encryption....... ( ok )
[=] Test 0 signature........ ( ok )
[=] Test 0 decryption....... ( ok )
[=] Test 0 signature........ ( ok )
```

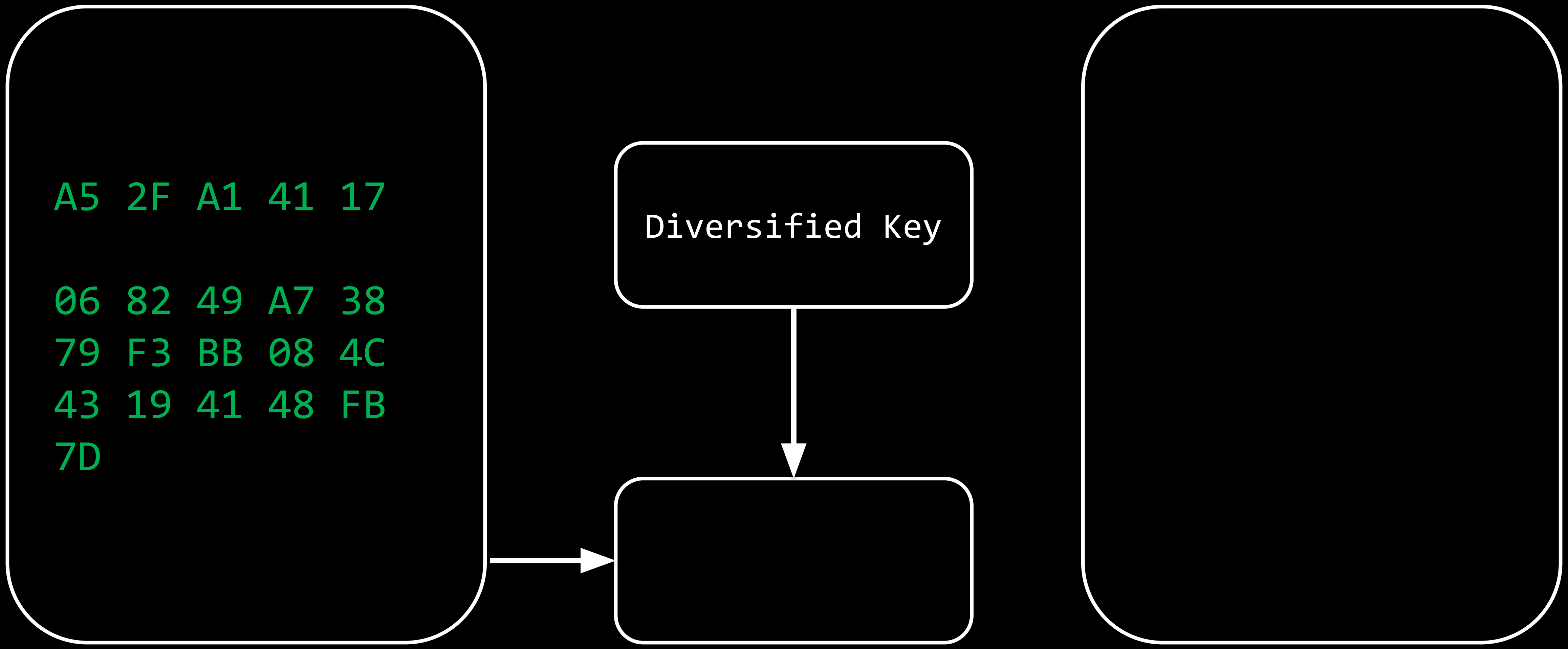
# Decrypt and Verify SIO



```
A5 2F A1 41 17

06 82 49 A7 38
79 F3 BB 08 4C
43 19 41 48 FB
7D
```

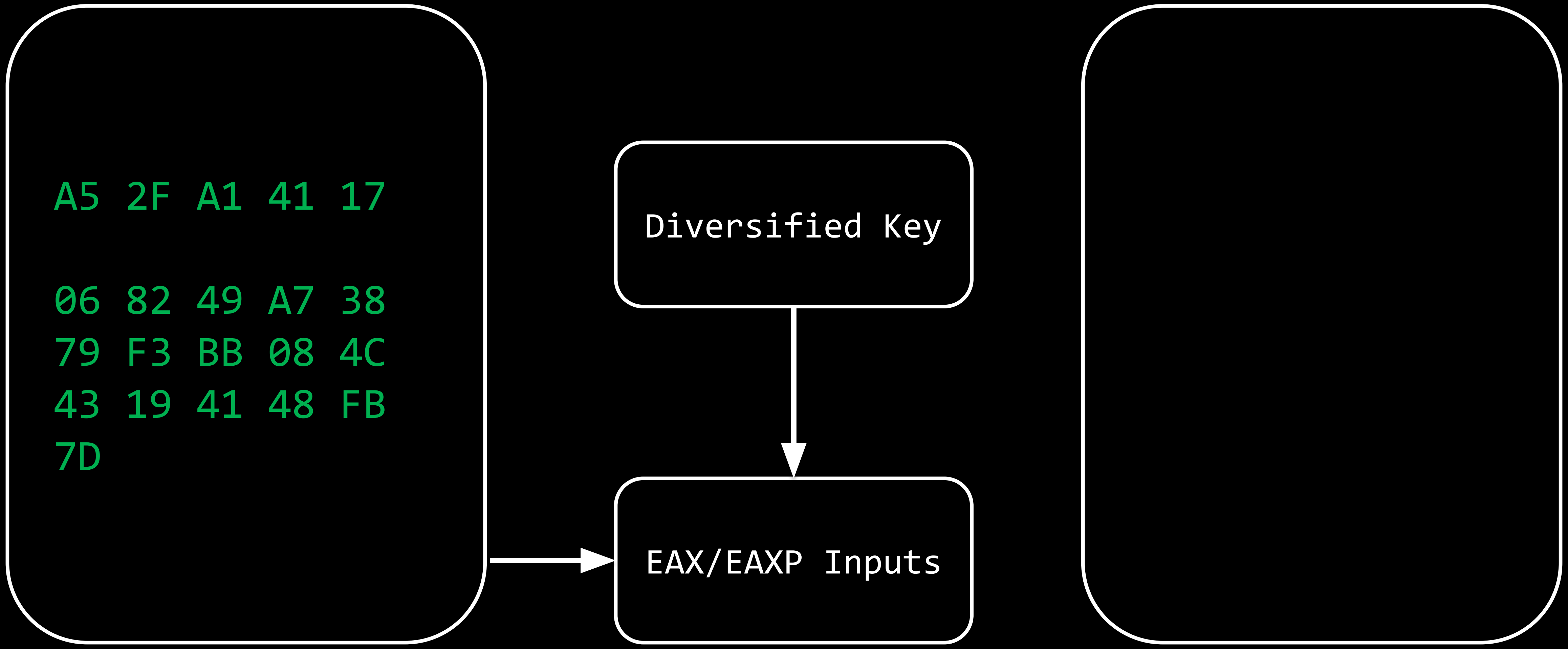
# Decrypt and Verify SIO



```
A5 2F A1 41 17

06 82 49 A7 38
79 F3 BB 08 4C
43 19 41 48 FB
7D
```

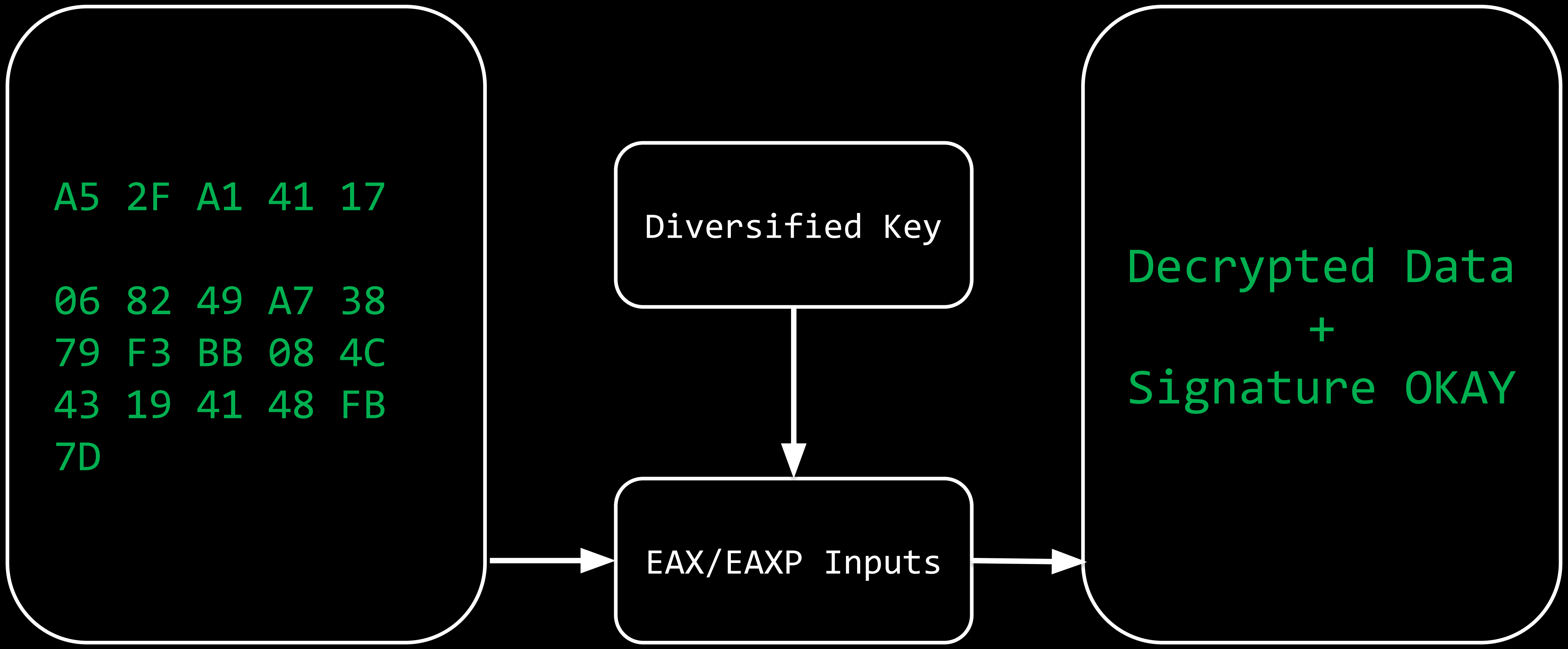
# Decrypt and Verify SIO



```
A5 2F A1 41 17

06 82 49 A7 38
79 F3 BB 08 4C
43 19 41 48 FB
7D
```

# Decrypt and Verify SIO



```
A5 2F A1 41 17

06 82 49 A7 38
79 F3 BB 08 4C
43 19 41 48 FB
7D
```

# You decrypted the PACS payload…

Time to look at
Next layer

# Padded PACS Wiegand Format

Wiegand format padded with NN bits in the end.

nn - Number of padded zeros in the end
xx - PACS Payload

# Padded PACS Wiegand Format

Wiegand format padded with NN bits in the end.

nn - Number of padded zeros in the end
xx - PACS Payload

Example: H10301
26 bit format

nn xx xx xx xx
06 1B 7D 00 40

# Padded PACS Wiegand Format

Number of shifts: 06

Hex to bin: 1B 7D 00 40 - 0001 1011 0111 1101 0000 0000 0100 0000

# Padded PACS Wiegand Format

Number of shifts: 06

Hex to bin: 1B 7D 00 40 - 0001 1011 0111 1101 0000 0000 0100 0000

# Padded PACS Wiegand Format

Number of shifts: 06

Hex to bin: 1B 7D 00 40 - 0001 1011 0111 1101 0000 0000 0100 0000

Shift to right 1 times: 0001 1011 0111 1101 0000 0000 0100 000

# Padded PACS Wiegand Format

Number of shifts: 06

Hex to bin: 1B 7D 00 40 - 0001 1011 0111 1101 0000 0000 0100 0000

Shift to right 2 times: 0001 1011 0111 1101 0000 0000 0100 00

# Padded PACS Wiegand Format

Number of shifts: 06

Hex to bin: 1B 7D 00 40 - 0001 1011 0111 1101 0000 0000 0100 0000

Shift to right 3 times: 0001 1011 0111 1101 0000 0000 0100 0

# Padded PACS Wiegand Format

Number of shifts: 06

Hex to bin: 1B 7D 00 40 - 0001 1011 0111 1101 0000 0000 0100 0000

Shift to right 4 times: 0001 1011 0111 1101 0000 0000 0100

# Padded PACS Wiegand Format

Number of shifts: 06

Hex to bin: 1B 7D 00 40 - 0001 1011 0111 1101 0000 0000 0100 0000

Shift to right 5 times: 0001 1011 0111 1101 0000 0000 010

# Padded PACS Wiegand Format

Number of shifts: 06

Hex to bin: 1B 7D 00 40 - 0001 1011 0111 1101 0000 0000 0100 0000

Shift to right 6 times: 0001 1011 0111 1101 0000 0000 01

# Padded PACS Wiegand Format

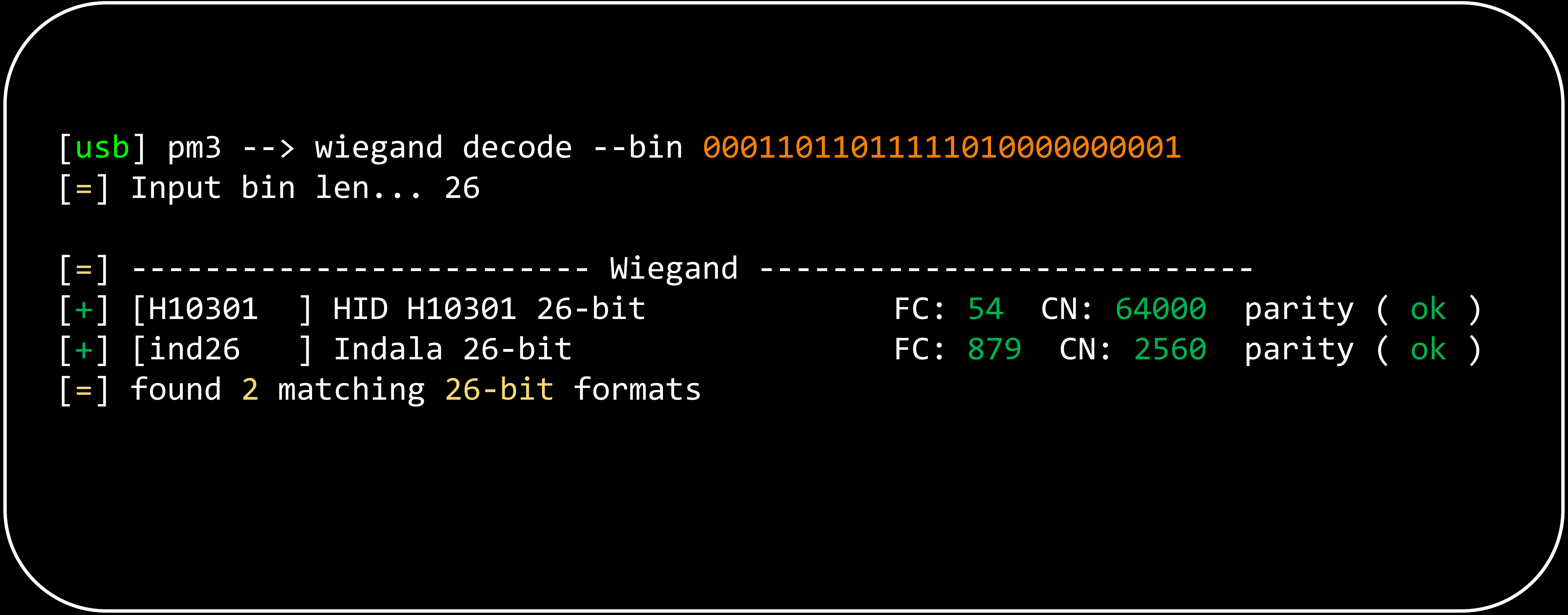
Number of shifts: 06

Hex to bin: 1B 7D 00 40 - 0001 1011 0111 1101 0000 0000 0100 0000

Shift to right 6 times: 0001 1011 0111 1101 0000 0000 01

Put the binary into a wiegand decoder

# Padded PACS Wiegand Format



```
[usb] pm3 --> wiegand decode --bin 00011011011111010000000001
[=] Input bin len... 26

[=] ------------------------- Wiegand ---------------------------
[+] [H10301  ] HID H10301 26-bit             FC: 54  CN: 64000  parity ( ok )
[+] [ind26   ] Indala 26-bit                 FC: 879  CN: 2560  parity ( ok )
[=] found 2 matching 26-bit formats
```

# Padded PACS Wiegand Format

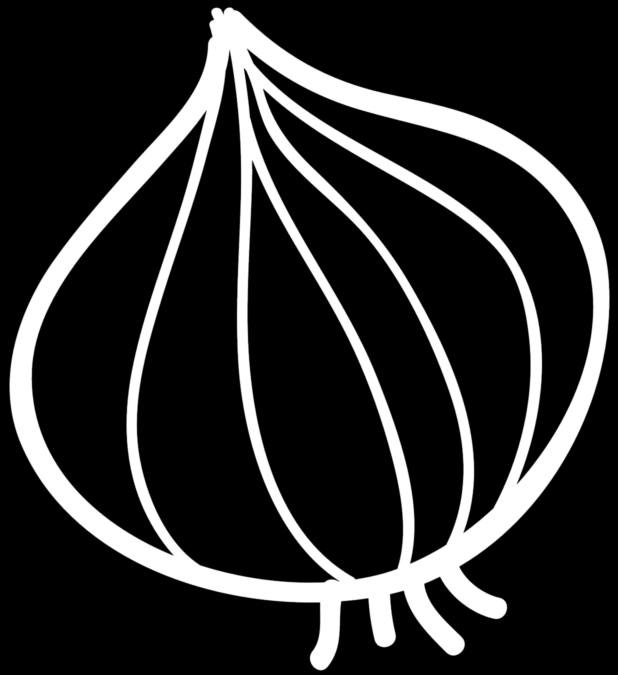
H10301 - 26 bit format

nn xx xx xx xx
06 1B 7D 00 40

Decoded, Decrypted, PACS Payload expressed as Wiegand Format

| | |
|---|---|
| Facility Code (FC) | 54 |
| Card Number (CN) | 64000 |

# That is the peeled onion



# Verdict?

- Yeah, this system is pretty secure
  - They’ve clearly put a lot of thought into the system, and done a lot to improve the security compared to other devices
- This talk isn’t saying that things are broken
- Systems need independent testing
- Vendors should embrace these types of research

# Thank you!

Review how systems work

Evaluate these systems beyond the specification sheet

Report actual findings to vendors