Relayed payWave transaction trace

This section presents an example trace from our relay, when relaying the payWave qVDSC protocol, with timings and the hex of each message. We also include a break down of each message explaining its meaning. Each of the digits of the credit card number of the card used has been replaced with X.

```
Run time: 548ms total, 247ms to send GPO and get the answer back

2014-09-15 14:10:05.394 | NetworkTask  | Sending SELECT message to wake up
card.
2014-09-15 14:10:05.476 | MainActivity | Card responds:
6F378407A0000000031010A52C500A5649534120444542495 49F38189F66049F02069F03069F
1A0295055F2A029A039C019F37045F2D02656E9000
which parses as:
  6F | len:37    File Control Information (FCI) Template
      84 | len:7    DF Name: A0000000031010
      A5 | len:2C    Proprietary Information
          50 | len:10    Application Label: 56495341204445424954
        9F38 | len:18    Processing Options Data Object List (PDOL)
            9F66 | len:04   Card Production Life Cycle
            9F02 | len:06   Amount, Authorised (Numeric)
            9F03 | len:06   Amount, Other (Numeric)
            9F1A | len:02   Terminal Country Code
              95 | len:05   Terminal Verification Results
            5F2A | len:02   Transaction Currency Code
              9A | len:03   Transaction Date00A4040007A000000003101000
              9C | len:01   Transaction Type
            9F37 | len:04   Unpredictable Number
        5F2D | len:2    Language Preference: 656E

--First message received from terminal at 14:10:08.186
2014-09-15 14:10:08.186 | PaymentService | Hex received from reader:
00A404000E325041592E5359532E444446303100
which parses as: SELECT PAY.SYS.DDF01

2014-09-15 14:10:08.191 | EmulatorApplet | Sending cache response to reader:
6F20840E325041592E5359532E4444463031A50EBF0C0B61094F07A00000000310109000
which parses as:
  6F | len:20    File Control Information (FCI) Template
      84 | len:14    DF Name: 325041592E5359532E4444463031
      A5 | len:0E    Proprietary Information
        BF0C | len:0B    File Control Information (FCI) Issuer Discretionary
         Data
              61 | len:09    Directory Entry
              4F | len:7    Application Identifier (AID): A0000000031010
```

```
2014-09-15 14:10:08.210 | PaymentService | Hex received from reader:
00A4040007A000000003101000
which parses as: SELECT A0000000031010

2014-09-15 14:10:08.217 | EmulatorApplet | Sending cache response to reader:
6F378407A0000000031010A52C500A5649534120444542495495 49F38189F66049F02069F03069F
1A0295055F2A029A039C019F37045F2D02656E9000
which parses as above.

2014-09-15 14:10:08.252 | PaymentService | Hex received from reader :
80A800002383213220400000000000030000000000000826000000000008261409150033 8F
507800
which parses as:
    Card Production Life Cycle     32-20-40-00
    Amount, Authorised (Numeric)   000000000030
    Amount, Other (Numeric)        000000000000
    Terminal Country Code          0826
    Terminal Verification Results  0000000000
    Transaction Currency Code      0826
    Transaction Date               140915
    Transaction Type               00
    Unpredictable Number           338F5078

2014-09-15 14:10:08.255 | EmulatorApplet | Sending GPO command over relay
2014-09-15 14:10:08.498 | NetworkTaskTCP | len : 199
2014-09-15 14:10:08.506 | NetworkTaskTCP | Total message send time = 247ms
2014-09-15 14:10:08.556 | EmulatorApplet | Returning response from card :
7781C29F4B81804D8EC3F85EB28D9C8828E2238BFE8F922F89D08DEDA061DE7270CF6EB01510
9D58DC58B34706CED0BFA24A28ED3E6AE0B2908617D34199B0A3BD298187376F639F65203C84
EEE7BC60B4D14F649E67C62162CAF53045E8D5A2A99E39589483A28DF24941C6AF486FEEBA0A
8C6DB33978309EFF87FFF9984C9DECDFDCE6728DB19404100203009F1007060A0A0390000057
13XXXXXXXXXXXXXXXXD16042015140000001001F820220009F360200579F26083501E6BD0985
62889F6C0210009000
which parses as:
  77 | len:81    Response Message Template Format 2
    9F4B | len:128    Signed Dynamic Application Data (SDAD): 4D8EC3F85EB28D
    9C8828E2238BFE8F922F89D08DEDA061DE7270CF6EB015109D58DC58B34706CED0BFA24A
    28ED3E6AE0B2908617D34199B0A3BD298187376F639F65203C84EEE7BC60B4D14F649E67
    C62162CAF53045E8D5A2A99E39589483A28DF24941C6AF486FEEBA0A8C6DB33978309EFF
    87FFF9984C9DECDFDCE6728DB1
      94 | len:4    Application File Locator: 10020300
    9F10 | len:7    Issuer Application Data (IAD): 060A0A03900000
      57 | len:19    Track 2 Equivalent Data: XXXXXXXXXXXXXXXXD1604201514000
      0001001F
```

```
      82 | len:2    Application Interchange Profile: 2000
    9F36 | len:2    Application Transaction Counter: 0057
    9F26 | len:8    Application Cryptogram: 3501E6BD09856288
    9F6C | len:2    Card Transaction Qualifiers (CTQ): 1000

2014-09-15 14:10:08.526 | EmulatorApplet | Reading card nonce on a separate
thread, and storing it for later.
2014-09-15 14:10:08.541 | EmulatorApplet | Received card nonce : 9E90BD37


2014-09-15 14:10:08.625 | PaymentService | Hex received from reader : 00B202
1400
which parses as: READ RECORD 0214

2014-09-15 14:10:08.635 | EmulatorApplet | Sending cached resp. to terminal:
2014-09-15 14:10:08.661 | EmulatorApplet | Returning response from the cache:
7081C08F01079081906103C2C80BF24F3E7117BCF60F29B2DF92EFBF52E4AAA6F27FC0A13BE2
2EE638806C77F08FDC1F80717DC79D9B0D1F1FC137F648E537DC2A36DAD9B3F367189F35B958
3AFE400B6D72D2362F31C3AD3510FB20C890FFC2C8B43B2389E36877C6C6E4C7BFD7D3BABB12
04CF440EC9E9FB6D855EFEF4C6E105A0F46A732CAD8644924AED8A97614E36EED4C0EE19BBB2
54922488C9DC1A7E668C6867F5937F2A69729D1120E3D2954DBBC4C935A10A06857FB8F63E72
CB9F3201039000
which parses as:
  70 | len:81    Record Template
      8F | len:1    Certification Authority Public Key Index: 07
      90 | len:144  Issuer Public Key Certificate: 6103C2C80BF24F3E7117BCF60
      F29B2DF92EFBF52E4AAA6F27FC0A13BE22EE638806C77F08FDC1F80717DC79D9B0D1F1
      FC137F648E537DC2A36DAD9B3F367189F35B9583AFE400B6D72D2362F31C3AD3510FB2
      0C890FFC2C8B43B2389E36877C6C6E4C7BFD7D3BABB1204CF440EC9E9FB6D855EFEF4C
      6E105A0F46A732CAD8644924AED8A97614E36EED4C0EE19BBB254
      92 | len:36   Issuer Public Key Remainder: 88C9DC1A7E668C6867F5937F2A6
      9729D1120E3D2954DBBC4C935A10A06857FB8F63E72CB
    9F32 | len:1    Issuer Public Key Exponent: 03

2014-09-15 14:10:08.706 | PaymentService | Msg from reader : 00B2031400
which parses as: READ RECORD 0314

2014-09-15 14:10:08.715 | EmulatorApplet | Sending cached resp. to terminal:
2014-09-15 14:10:08.730 | EmulatorApplet | Returning response from card :
7081D19F468190B04DCF375EB59A6F941757E8BBC926C95EA748381A6F0CCCFEF7415A76CCB3
D424F801AFA5A3624D4C6694BD2281A70CED813AF297D72374F3CE2D8343FC9B3DDEBEA1A553
B0D2BA896CA134785334F61ACF3CA6EB10061A694B97A281C50C11A5D242AD492118D644C85E
AB2F44AC445659282A4AAB132E84A3C52F5D9AC9F6EE8E57CE8C7595A3C71FF422DEED59049F
4701039F481A75F342106927017D05443C3F53B310F08A69C382B72B3ACEC1DB5A08XXXXXXXX
XXXXXXXX5F3401005F24031604309F6905019E90BD379000
```

```
which parses as:
  70 | len:81    Record Template
    9F46 | len:144    ICC Public Key Cert: B04DCF375EB59A6F941757E8BBC926C95
    EA748381A6F0CCCFEF7415A76CCB3D424F801AFA5A3624D4C6694BD2281A70CED813AF29
    7D72374F3CE2D8343FC9B3DDEBEA1A553B0D2BA896CA134785334F61ACF3CA6EB10061A6
    94B97A281C50C11A5D242AD492118D644C85EAB2F44AC445659282A4AAB132E84A3C52F5
    D9AC9F6EE8E57CE8C7595A3C71FF422DEED5904
    9F47 | len:1    ICC Public Key Expo: 03
    9F48 | len:26   ICC Public Key Remainder: 75F342106927017D05443C3F53B310
    F08A69C382B72B3ACEC1DB
      5A | len:8  Application Primary Account Number (PAN): XXXXXXXXXXXXXXXX
    5F34 | len:1  (PAN) Sequence Number: 00
    5F24 | len:3  Application Expiration Date YYMMDD: 160430
    9F69 | len:5  Card Authentication Related Data: 019E90BD37

-- Final message sent back at 14:10:08.730
```