Formal models of bank cards for free

Fides Aarts, Joeri de Ruiter and Erik Poll

Digital Security, Radboud University Nijmegen

Introduction

- Active learning on bank cards
- Learn state machines of implementations
- Dutch, German, Swedish and UK debit and credit cards
  - All implementations of EMV standard

EMV

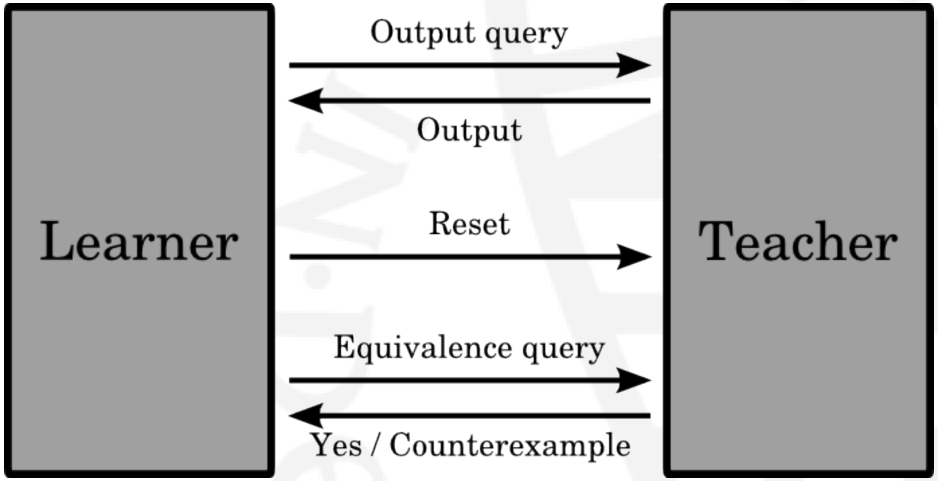
- Standard for payment cards
- Started in 1993 by EuroPay, MasterCard and Visa
- Over 1 billion cards in use
- Required for Single Euro Payments Area (SEPA)
- Over 700 pages of specifications
- EMV-CAP for online banking

EMV transaction

- Initialisation
- Cardholder verification
  - Offline PIN
- Card authentication
  - SDA / DDA / CDA
- Transaction
  - Online / offline
  - Confirmed by cryptogram (TC / AAC / ARQC)

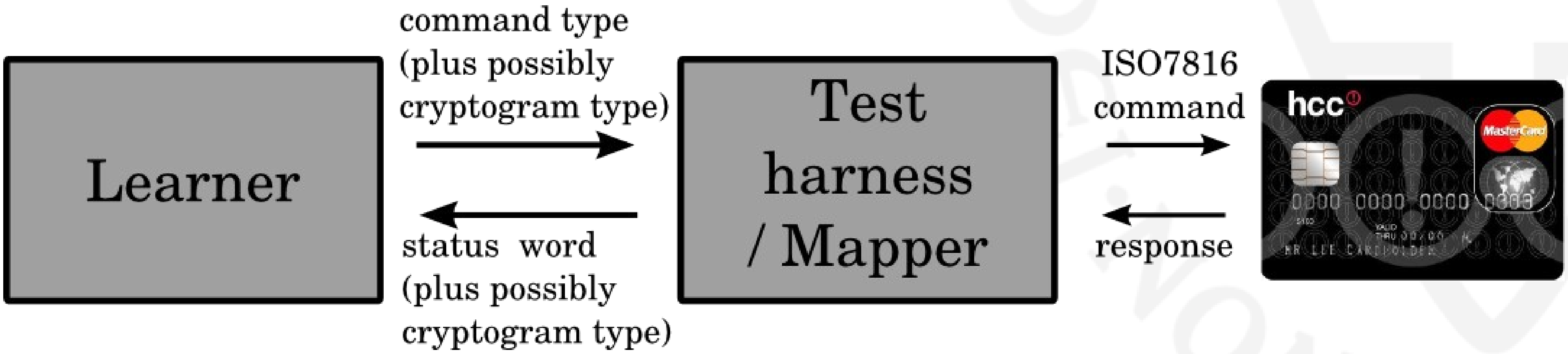
Learning

- LearnLib used
  - Implementation of adapted L* algorithm
- Deterministic Mealy machine M = $(I,O,Q,q^0,\delta,\lambda)$
- Equivalence queries approximated
  - Random (1000 traces of length 10-50)
  - W-Method



Learning

- Custom test harness for EMV smartcards
  - In total 15 different commands
  - Input symbols: commands
  - Output symbols: status words (optionally with cryptogram type)



Learner

command type (plus possibly cryptogram type)

status word (plus possibly cryptogram type)

Test harness / Mapper

ISO7816 command

response

Test harness

- Java
- Around 300 lines of code
- Standard library for communication with smartcards
- Separate method for each input symbol
- Parameters fixed
  - Random number
  - PIN code
- Variations of instructions
- Bank's secret key unknown

Commands

- SELECT
- GET PROCESSING OPTIONS
  - Correct / incorrect parameters
- GET DATA
  - Existing / non-existing data
- READ RECORD
  - Existing / non-existing records

Initialisation

- VERIFY

Cardholder verification

- INTERNAL AUTHENTICATE

Card authentication

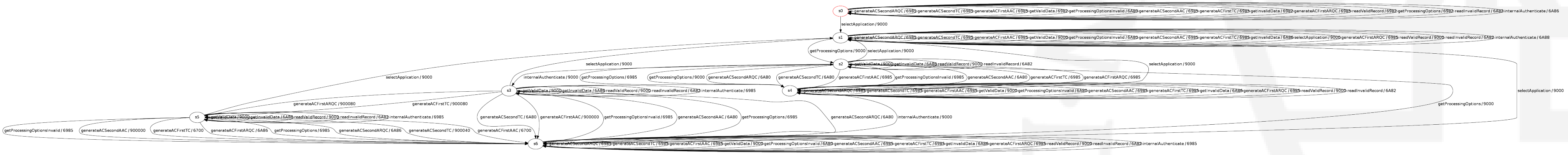
- GENERATE AC
  - 6 variations

Transaction

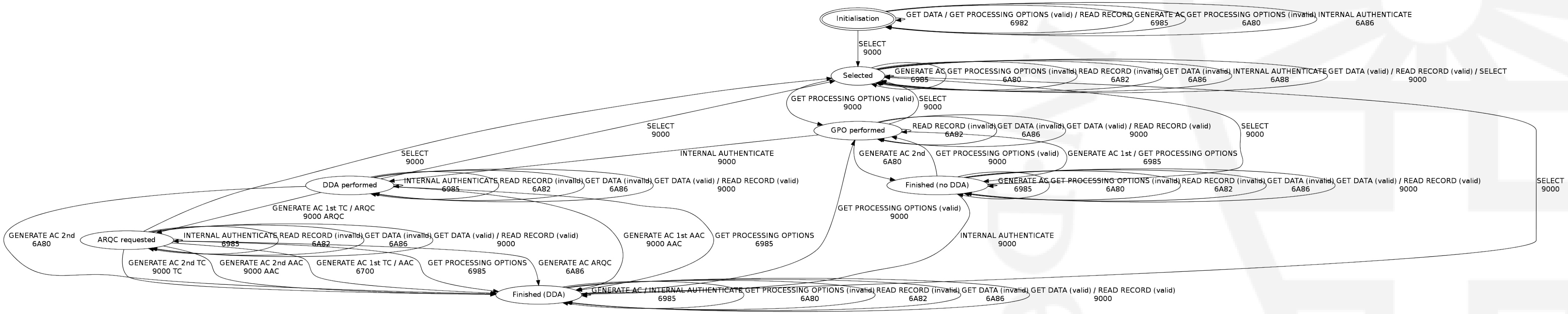
Results

- Learned 33 models for 16 cards
- Between 855 and 1695 membership queries
- Less than 20 minutes to construct final hypothesis
- 4 to 8 states learned
- Most cards did not follow state machine specified by MasterCard
- No security problems found

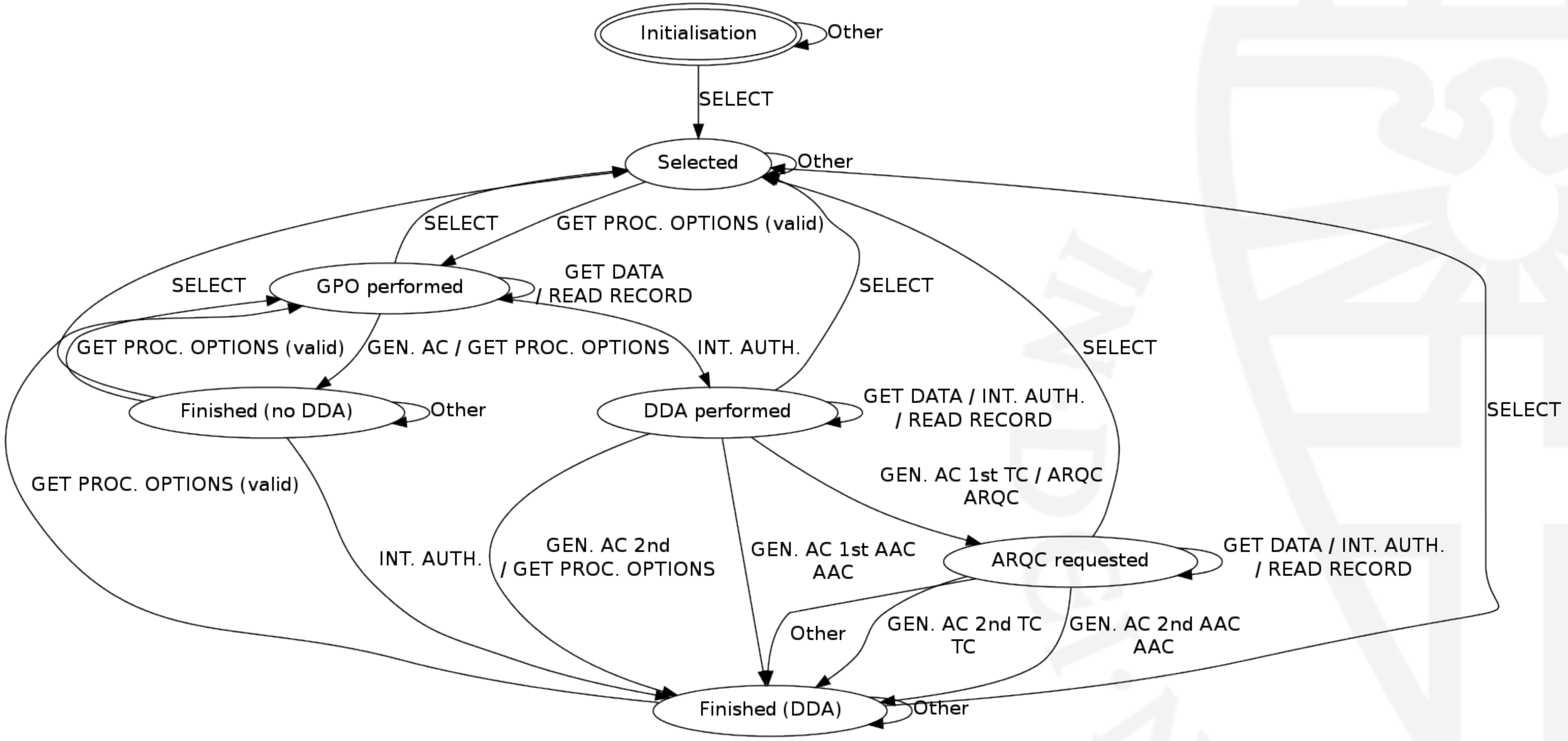
Results


s0
generateACSecondARQC / 6985
generateACSecondTC / 6985
generateACFirstAAC / 6985
getValidData / 6982
getProcessingOptionsInvalid / 6A80
generateACSecondAAC / 6985
generateACFirstTC / 6985
getInvalidData / 6982
generateACFirstARQC / 6985
readValidRecord / 6982
getProcessingOptions / 6982
readInvalidRecord / 6A82
internalAuthenticate / 6A86
selectApplication / 9000
s1
generateACSecondARQC / 6985
generateACSecondTC / 6985
generateACFirstAAC / 6985
getValidData / 9000
getProcessingOptionsInvalid / 6A80
generateACSecondAAC / 6985
generateACFirstTC / 6985
getInvalidData / 6A86
selectApplication / 9000
generateACFirstARQC / 6985
readValidRecord / 9000
readInvalidRecord / 6A82
internalAuthenticate / 6A88
getProcessingOptions / 9000
selectApplication / 9000
selectApplication / 9000
s2
getValidData / 9000
getInvalidData / 6A86
readValidRecord / 9000
readInvalidRecord / 6A82
selectApplication / 9000
selectApplication / 9000
selectApplication / 9000
internalAuthenticate / 9000
getProcessingOptions / 6985
getProcessingOptions / 9000
generateACSecondARQC / 6A80
generateACSecondTC / 6A80
generateACFirstAAC / 6985
getProcessingOptionsInvalid / 6985
generateACSecondAAC / 6A80
generateACFirstTC / 6985
generateACFirstARQC / 6985
s3
getValidData / 9000
getInvalidData / 6A86
readValidRecord / 9000
readInvalidRecord / 6A82
internalAuthenticate / 6985
s4
generateACSecondARQC / 6985
generateACSecondTC / 6985
generateACFirstAAC / 6985
getValidData / 9000
getProcessingOptionsInvalid / 6A80
generateACSecondAAC / 6985
generateACFirstTC / 6985
getInvalidData / 6A86
generateACFirstARQC / 6985
readValidRecord / 9000
readInvalidRecord / 6A82
getProcessingOptions / 9000
generateACFirstARQC / 900080
generateACFirstTC / 900080
s5
getValidData / 9000
getInvalidData / 6A86
readValidRecord / 9000
readInvalidRecord / 6A82
internalAuthenticate / 6985
generateACSecondTC / 6A80
generateACFirstAAC / 900000
getProcessingOptionsInvalid / 6985
generateACSecondAAC / 6A80
getProcessingOptions / 6985
generateACSecondARQC / 6A80
internalAuthenticate / 9000
getProcessingOptionsInvalid / 6985
generateACSecondAAC / 900000
generateACFirstTC / 6700
generateACFirstARQC / 6A86
getProcessingOptions / 6985
generateACSecondARQC / 6A86
generateACSecondTC / 900040
generateACFirstAAC / 6700
s6
generateACSecondARQC / 6985
generateACSecondTC / 6985
generateACFirstAAC / 6985
getValidData / 9000
getProcessingOptionsInvalid / 6A80
generateACSecondAAC / 6985
generateACFirstTC / 6985
getInvalidData / 6A86
generateACFirstARQC / 6985
readValidRecord / 9000
readInvalidRecord / 6A82
internalAuthenticate / 6985

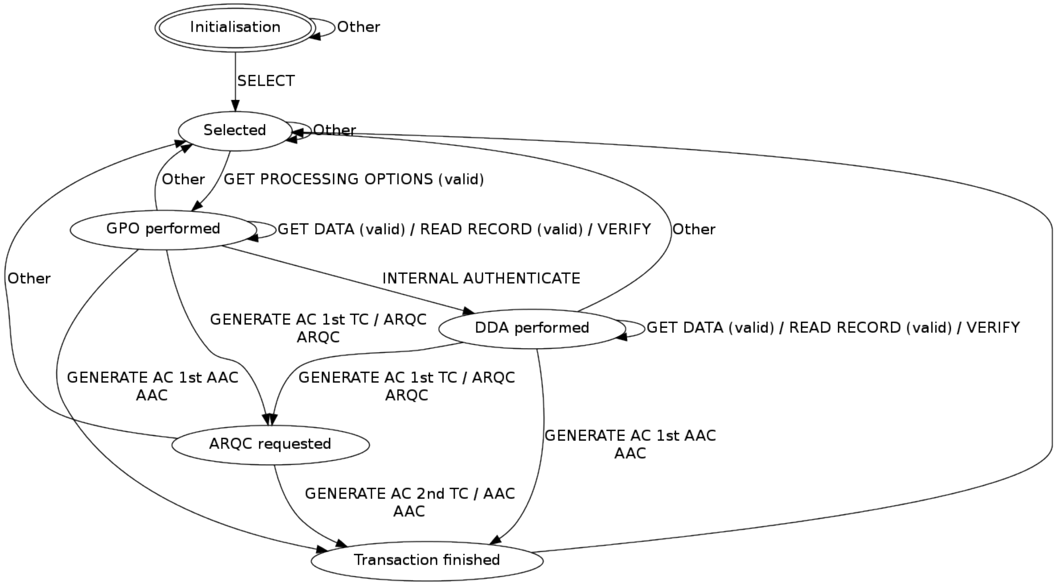
Results


Initialisation
GET DATA / GET PROCESSING OPTIONS (valid) / READ RECORD
6982
GENERATE AC
6985
GET PROCESSING OPTIONS (invalid)
6A80
INTERNAL AUTHENTICATE
6A86
SELECT
9000
Selected
GENERATE AC
6985
GET PROCESSING OPTIONS (invalid)
6A80
READ RECORD (invalid)
6A82
GET DATA (invalid)
6A86
INTERNAL AUTHENTICATE
6A88
GET DATA (valid) / READ RECORD (valid) / SELECT
9000
GET PROCESSING OPTIONS (valid)
9000
SELECT
9000
GPO performed
READ RECORD (invalid)
6A82
GET DATA (invalid)
6A86
GET DATA (valid) / READ RECORD (valid)
9000
SELECT
9000
SELECT
9000
SELECT
9000
INTERNAL AUTHENTICATE
9000
GENERATE AC 2nd
6A80
GET PROCESSING OPTIONS (valid)
9000
GENERATE AC 1st / GET PROCESSING OPTIONS
6985
DDA performed
INTERNAL AUTHENTICATE
6985
READ RECORD (invalid)
6A82
GET DATA (invalid)
6A86
GET DATA (valid) / READ RECORD (valid)
9000
Finished (no DDA)
GENERATE AC
6985
GET PROCESSING OPTIONS (invalid)
6A80
READ RECORD (invalid)
6A82
GET DATA (invalid)
6A86
GET DATA (valid) / READ RECORD (valid)
9000
SELECT
9000
GENERATE AC 1st TC / ARQC
9000 ARQC
GET PROCESSING OPTIONS (valid)
9000
GENERATE AC 2nd
6A80
ARQC requested
INTERNAL AUTHENTICATE
6985
READ RECORD (invalid)
6A82
GET DATA (invalid)
6A86
GET DATA (valid) / READ RECORD (valid)
9000
GENERATE AC 1st AAC
9000 AAC
GET PROCESSING OPTIONS
6985
INTERNAL AUTHENTICATE
9000
GENERATE AC 2nd TC
9000 TC
GENERATE AC 2nd AAC
9000 AAC
GENERATE AC 1st TC / AAC
6700
GET PROCESSING OPTIONS
6985
GENERATE AC ARQC
6A86
Finished (DDA)
GENERATE AC / INTERNAL AUTHENTICATE
6985
GET PROCESSING OPTIONS (invalid)
6A80
READ RECORD (invalid)
6A82
GET DATA (invalid)
6A86
GET DATA (valid) / READ RECORD (valid)
9000

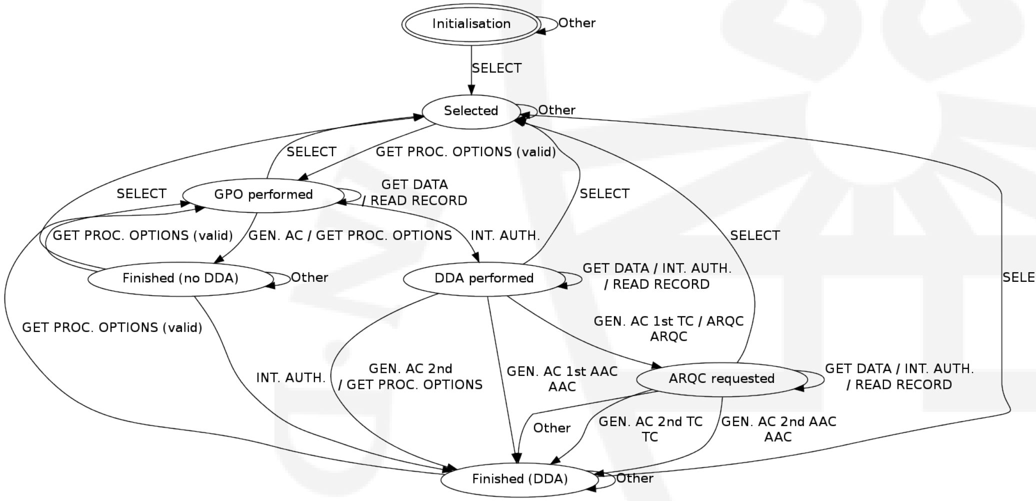
Results


Initialisation
Other
SELECT
Selected
Other
SELECT
GET PROC. OPTIONS (valid)
SELECT
GPO performed
GET DATA
/ READ RECORD
SELECT
SELECT
GET PROC. OPTIONS (valid)
GEN. AC / GET PROC. OPTIONS
INT. AUTH.
SELECT
Finished (no DDA)
Other
DDA performed
GET DATA / INT. AUTH.
/ READ RECORD
SELECT
GET PROC. OPTIONS (valid)
GEN. AC 1st TC / ARQC
ARQC
INT. AUTH.
GEN. AC 2nd
/ GET PROC. OPTIONS
GEN. AC 1st AAC
AAC
ARQC requested
GET DATA / INT. AUTH.
/ READ RECORD
Other
GEN. AC 2nd TC
TC
GEN. AC 2nd AAC
AAC
Finished (DDA)
Other

Maestro cards

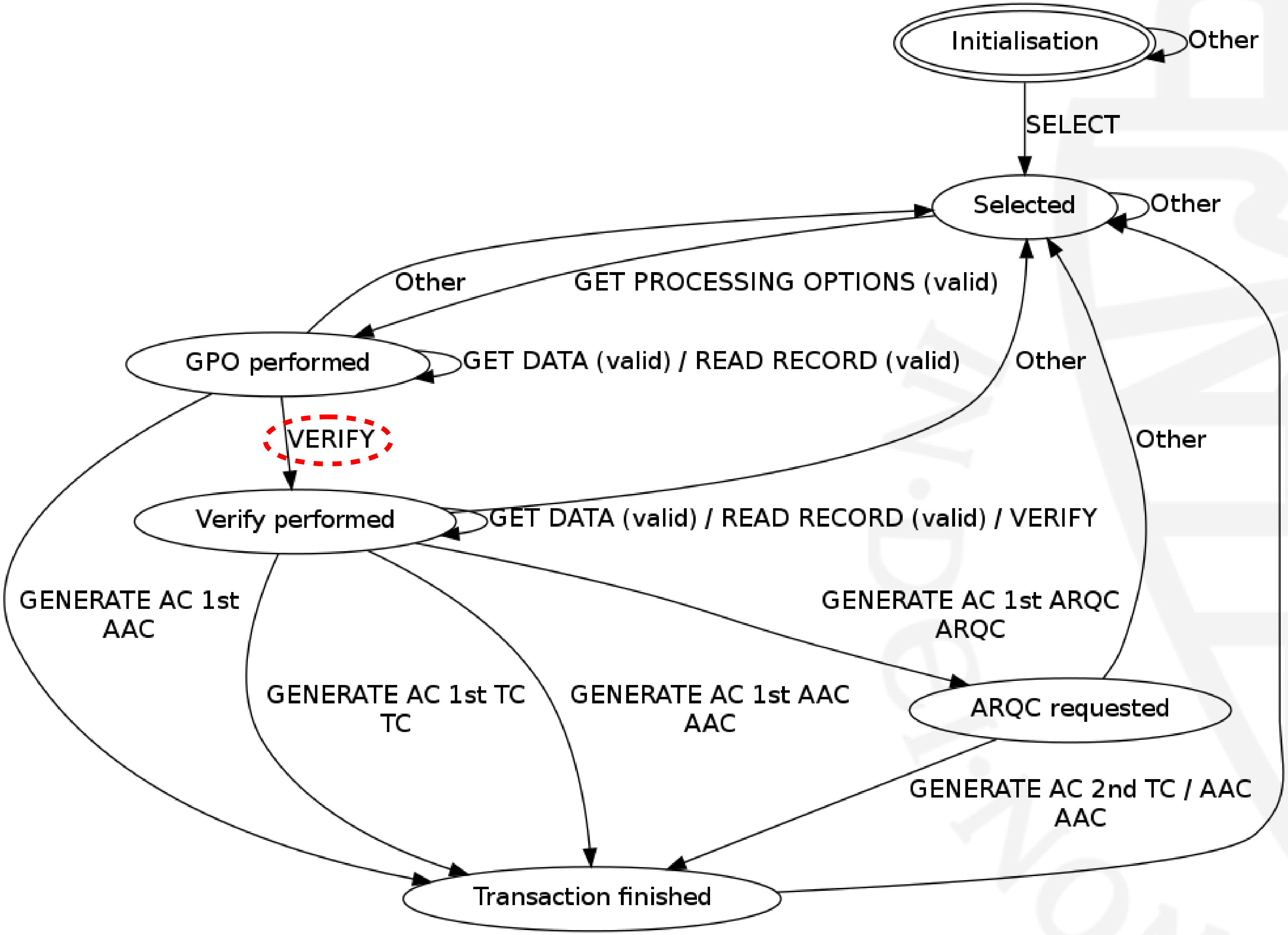


Rabobank Maestro

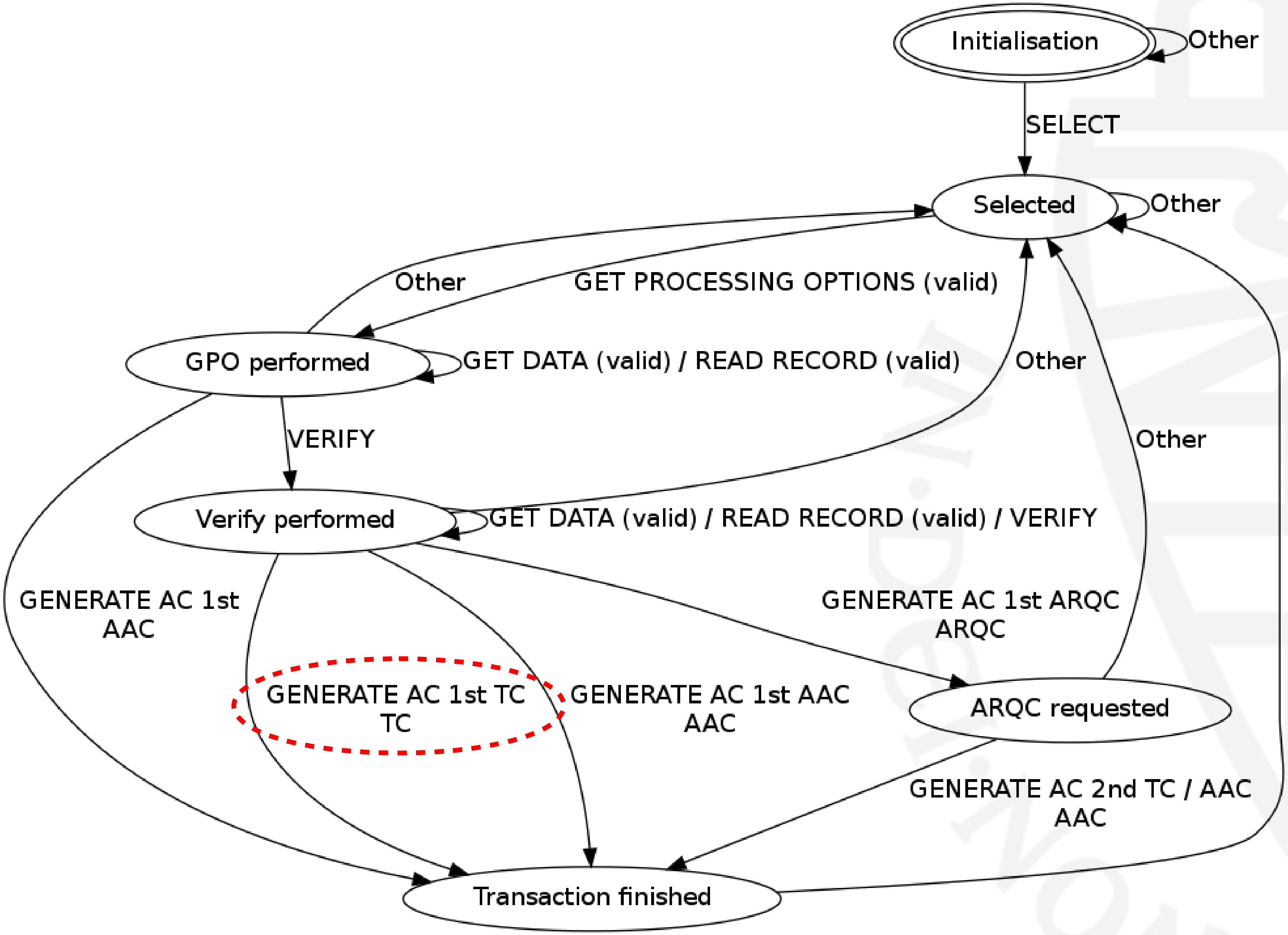


Volksbank Maestro

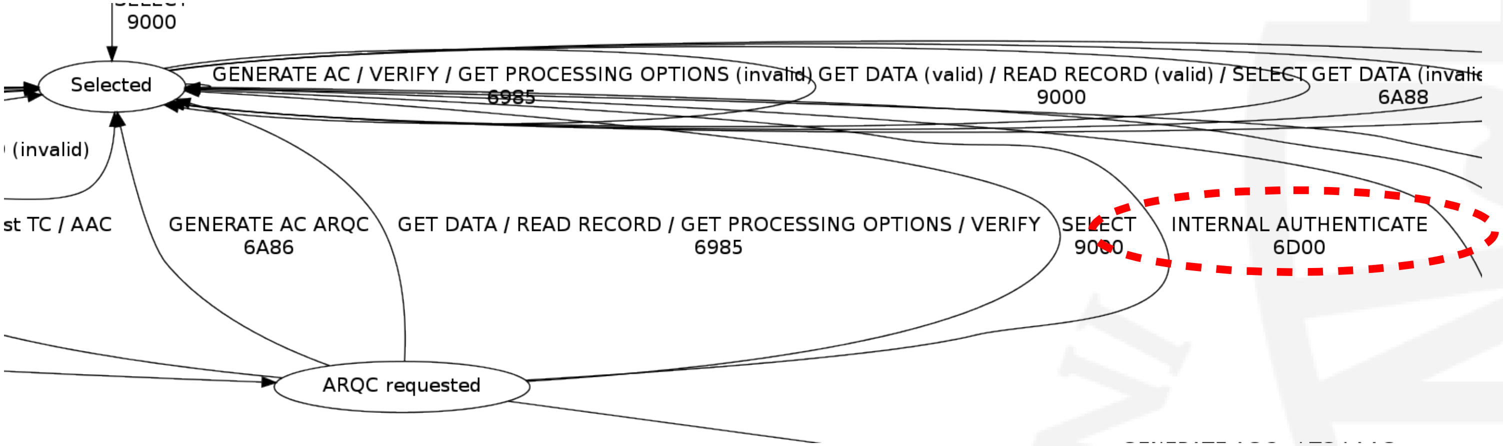
EMV-CAP

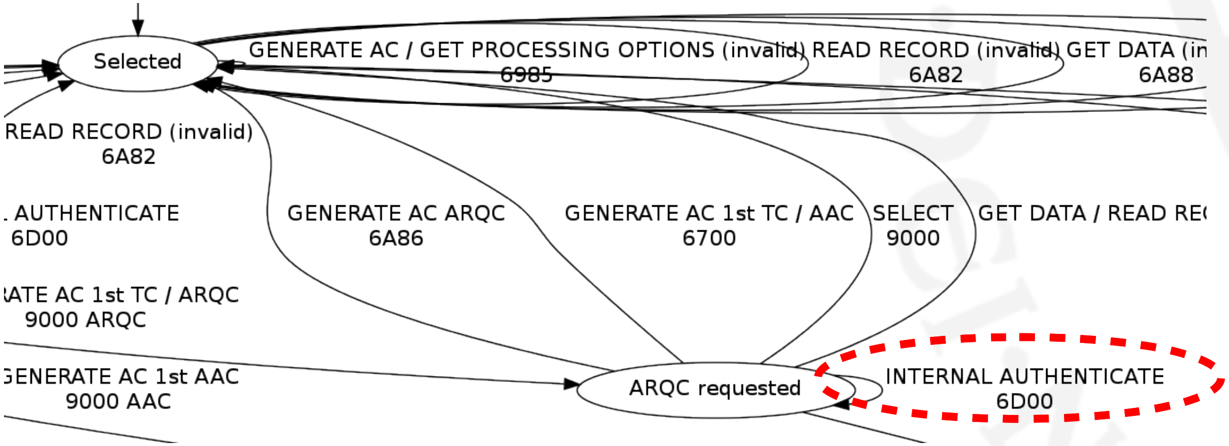

Initialisation
Other
SELECT
Selected
Other
Other
GET PROCESSING OPTIONS (valid)
GPO performed
GET DATA (valid) / READ RECORD (valid)
Other
VERIFY
Other
Verify performed
GET DATA (valid) / READ RECORD (valid) / VERIFY
GENERATE AC 1st
AAC
GENERATE AC 1st ARQC
ARQC
GENERATE AC 1st TC
TC
GENERATE AC 1st AAC
AAC
ARQC requested
GENERATE AC 2nd TC / AAC
AAC
Transaction finished

EMV-CAP

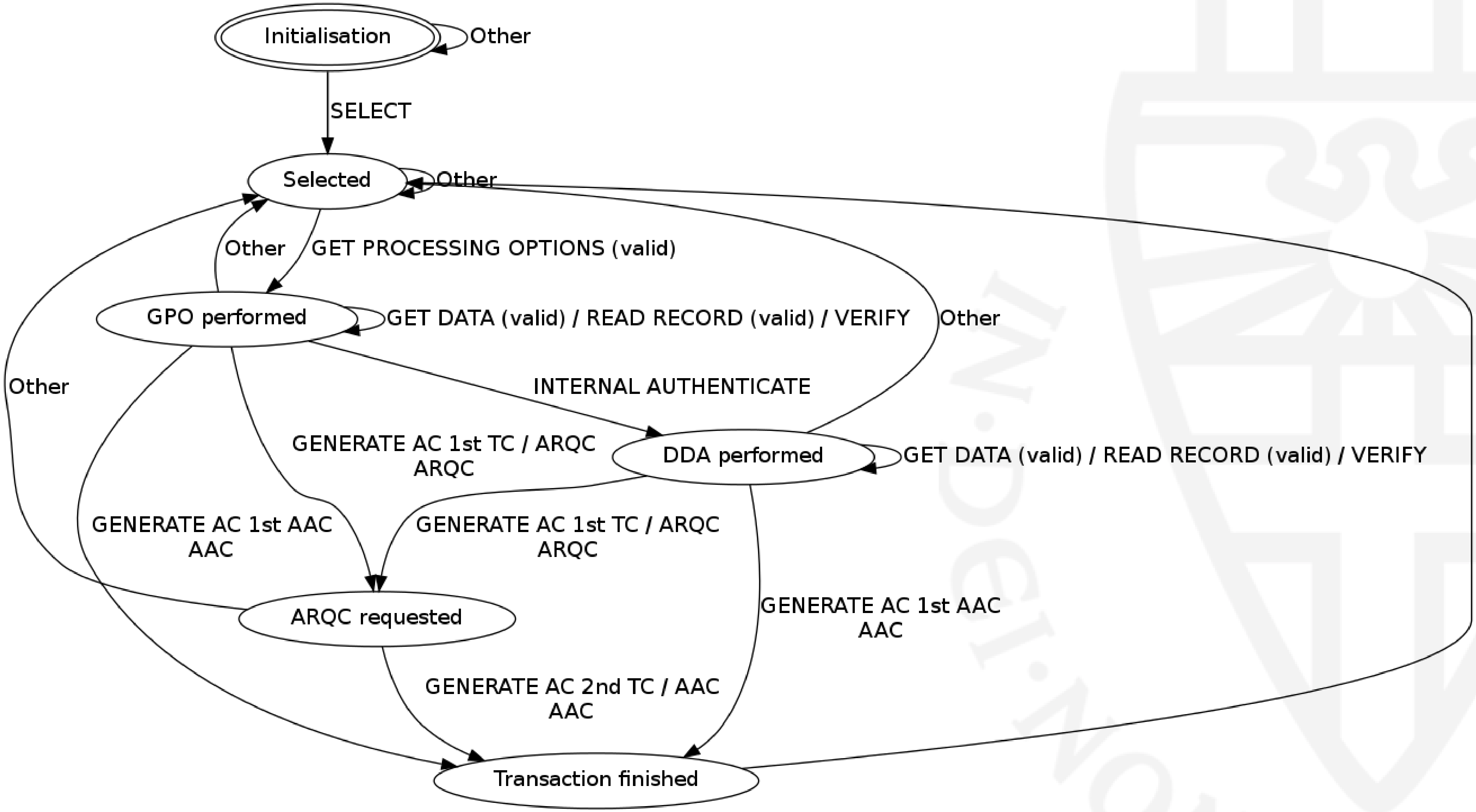

Initialisation
Other
SELECT
Selected
Other
Other
GET PROCESSING OPTIONS (valid)
GPO performed
GET DATA (valid) / READ RECORD (valid)
Other
VERIFY
Other
Verify performed
GET DATA (valid) / READ RECORD (valid) / VERIFY
GENERATE AC 1st
AAC
GENERATE AC 1st ARQC
ARQC
GENERATE AC 1st TC
TC
GENERATE AC 1st AAC
AAC
ARQC requested
GENERATE AC 2nd TC / AAC
AAC
Transaction finished

Error handling

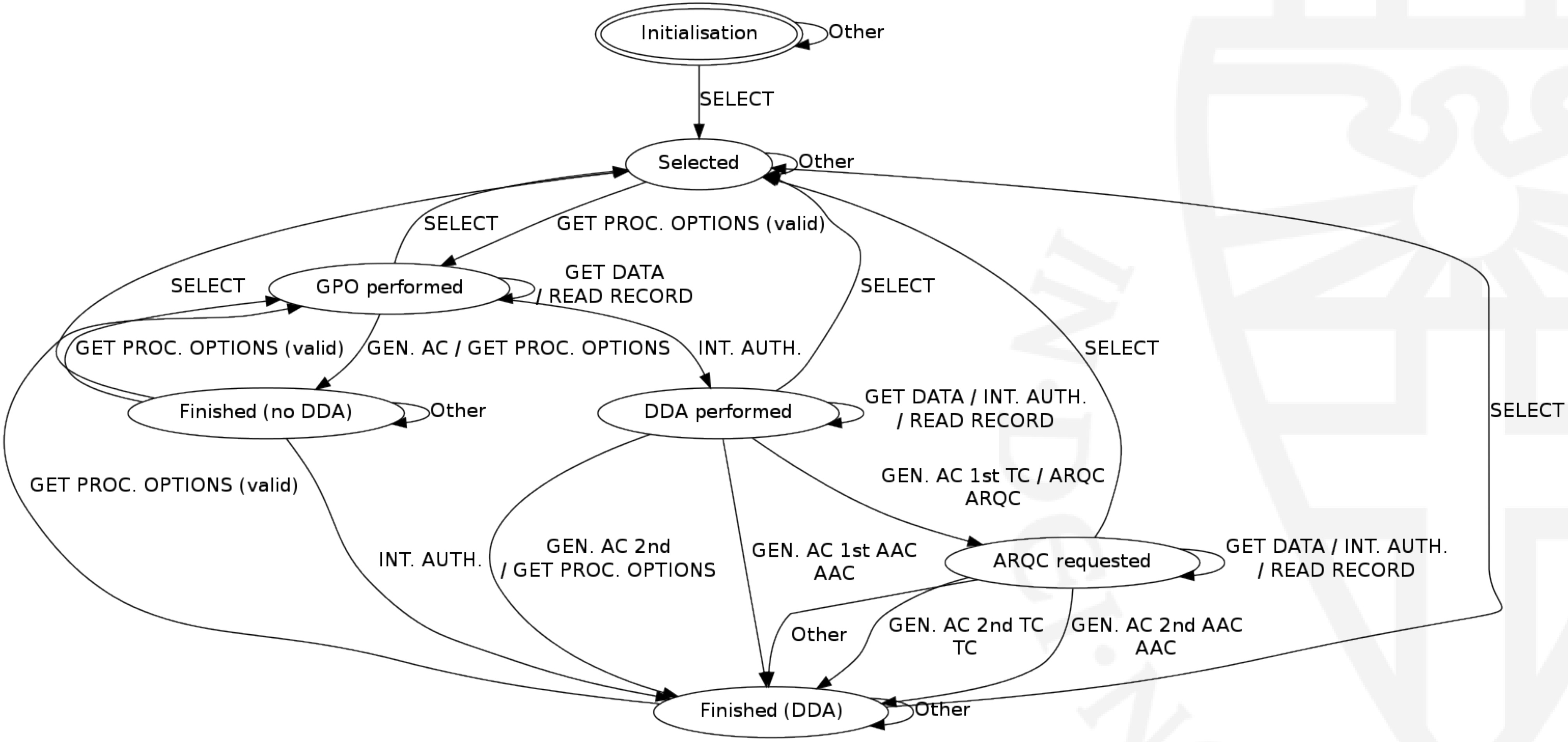

9000
Selected
GENERATE AC / VERIFY / GET PROCESSING OPTIONS (invalid)
6985
GET DATA (valid) / READ RECORD (valid) / SELECT
9000
GET DATA (invalid
6A88
(invalid)
st TC / AAC
GENERATE AC ARQC
6A86
GET DATA / READ RECORD / GET PROCESSING OPTIONS / VERIFY
6985
SELECT
9000
INTERNAL AUTHENTICATE
6D00
ARQC requested



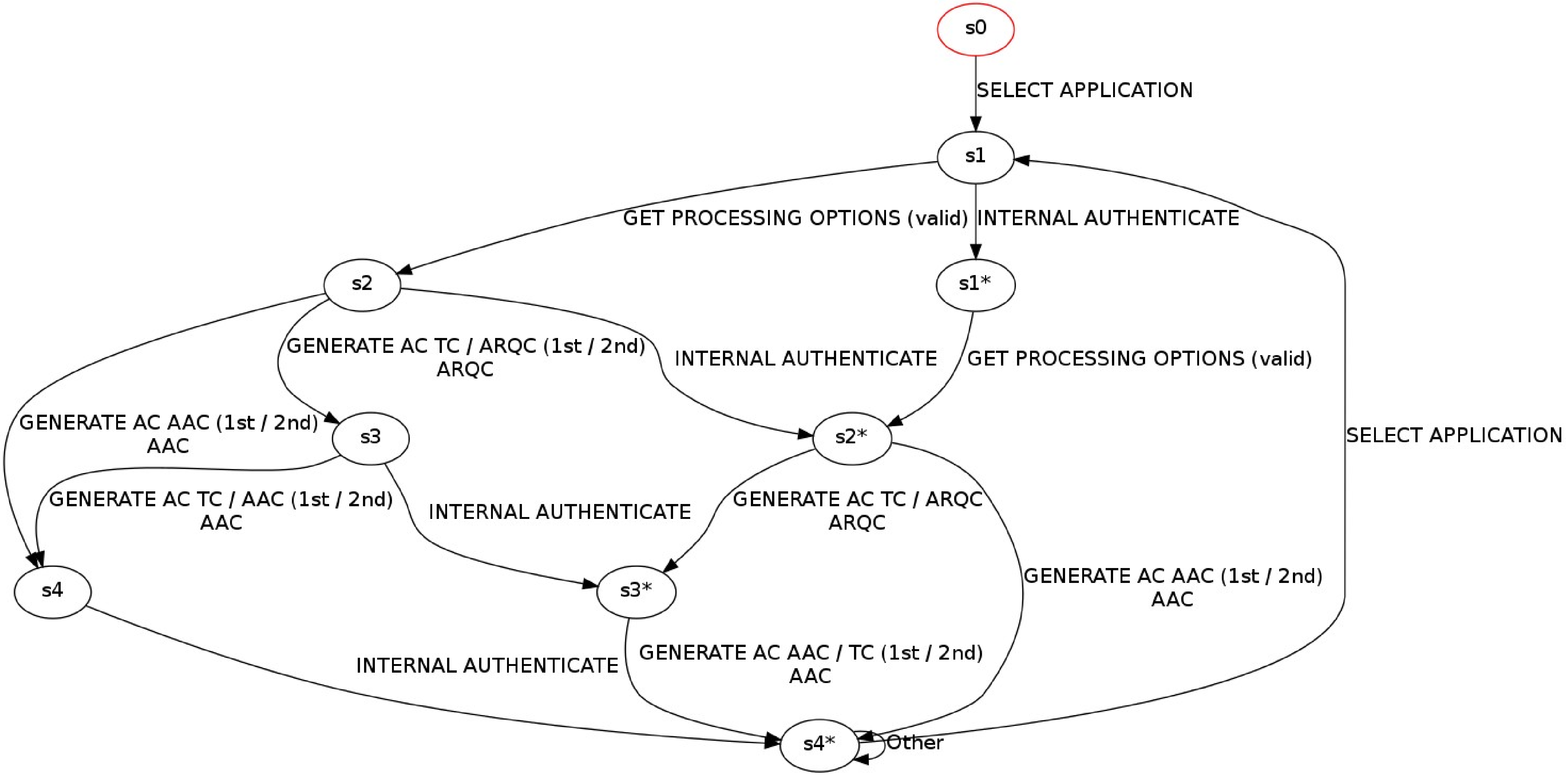
Data authentication



Data authentication



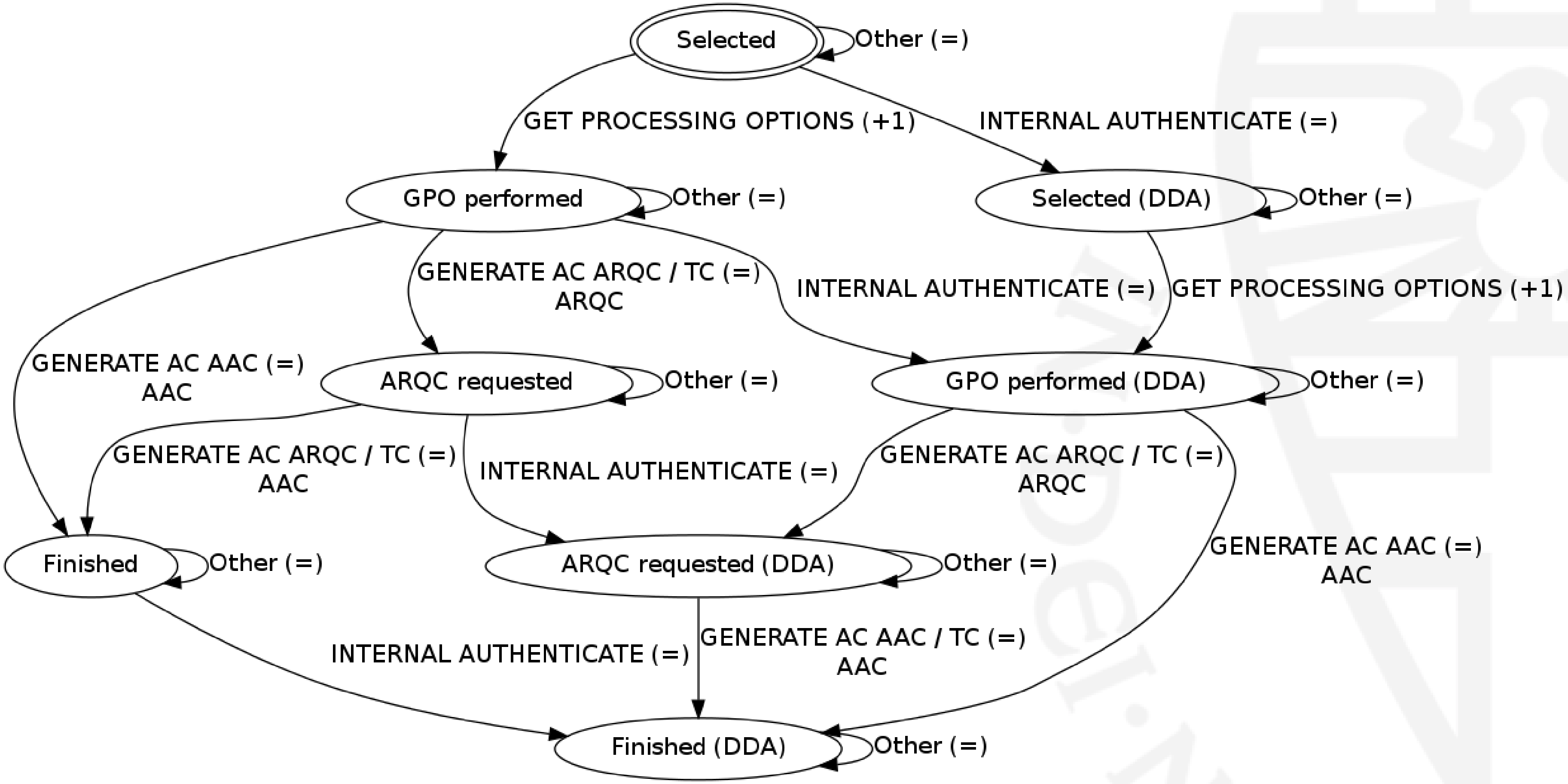
Data authentication


s0
SELECT APPLICATION
s1
GET PROCESSING OPTIONS (valid)
INTERNAL AUTHENTICATE
s2
s1*
GENERATE AC TC / ARQC (1st / 2nd)
ARQC
INTERNAL AUTHENTICATE
GET PROCESSING OPTIONS (valid)
GENERATE AC AAC (1st / 2nd)
AAC
s3
s2*
SELECT APPLICATION
GENERATE AC TC / AAC (1st / 2nd)
AAC
INTERNAL AUTHENTICATE
GENERATE AC TC / ARQC
ARQC
s4
s3*
GENERATE AC AAC (1st / 2nd)
AAC
INTERNAL AUTHENTICATE
GENERATE AC AAC / TC (1st / 2nd)
AAC
s4*
Other

Learning the ATC

- Application Transaction Counter
- Possible for card supporting GET DATA for ATC
- Added a mapper around test harness
  - Request ATC before and after every command

Result


Selected
Other (=)
GET PROCESSING OPTIONS (+1)
INTERNAL AUTHENTICATE (=)
GPO performed
Other (=)
Selected (DDA)
Other (=)
GENERATE AC ARQC / TC (=)
ARQC
INTERNAL AUTHENTICATE (=)
GET PROCESSING OPTIONS (+1)
GENERATE AC AAC (=)
AAC
ARQC requested
Other (=)
GPO performed (DDA)
Other (=)
GENERATE AC ARQC / TC (=)
AAC
INTERNAL AUTHENTICATE (=)
GENERATE AC ARQC / TC (=)
ARQC
Finished
Other (=)
ARQC requested (DDA)
Other (=)
GENERATE AC AAC (=)
AAC
INTERNAL AUTHENTICATE (=)
GENERATE AC AAC / TC (=)
AAC
Finished (DDA)
Other (=)

Using these diagrams

- Reverse engineering
  - Manual inspection of correctness and security
- Fuzzing or model-based testing
  - Use as basis for automated fuzz testing
- Formal verification
  - Use as basis for model checking

Conclusion

- Obtained useful models for EMV cards
- Gives insight in different design decisions
- Helpful in security or compliance evaluations
- Most cards did not follow state machine specified by MasterCard
- Applicable for any smartcard application

Conclusion

- Obtained useful models for EMV cards
- Gives insight in different design decisions
- Helpful in security or compliance evaluations
- Most cards did not follow state machine specified by MasterCard
- Applicable for any smartcard application

Thanks for your attention!