ISO/IEC 24727-2
Generic Card Interface

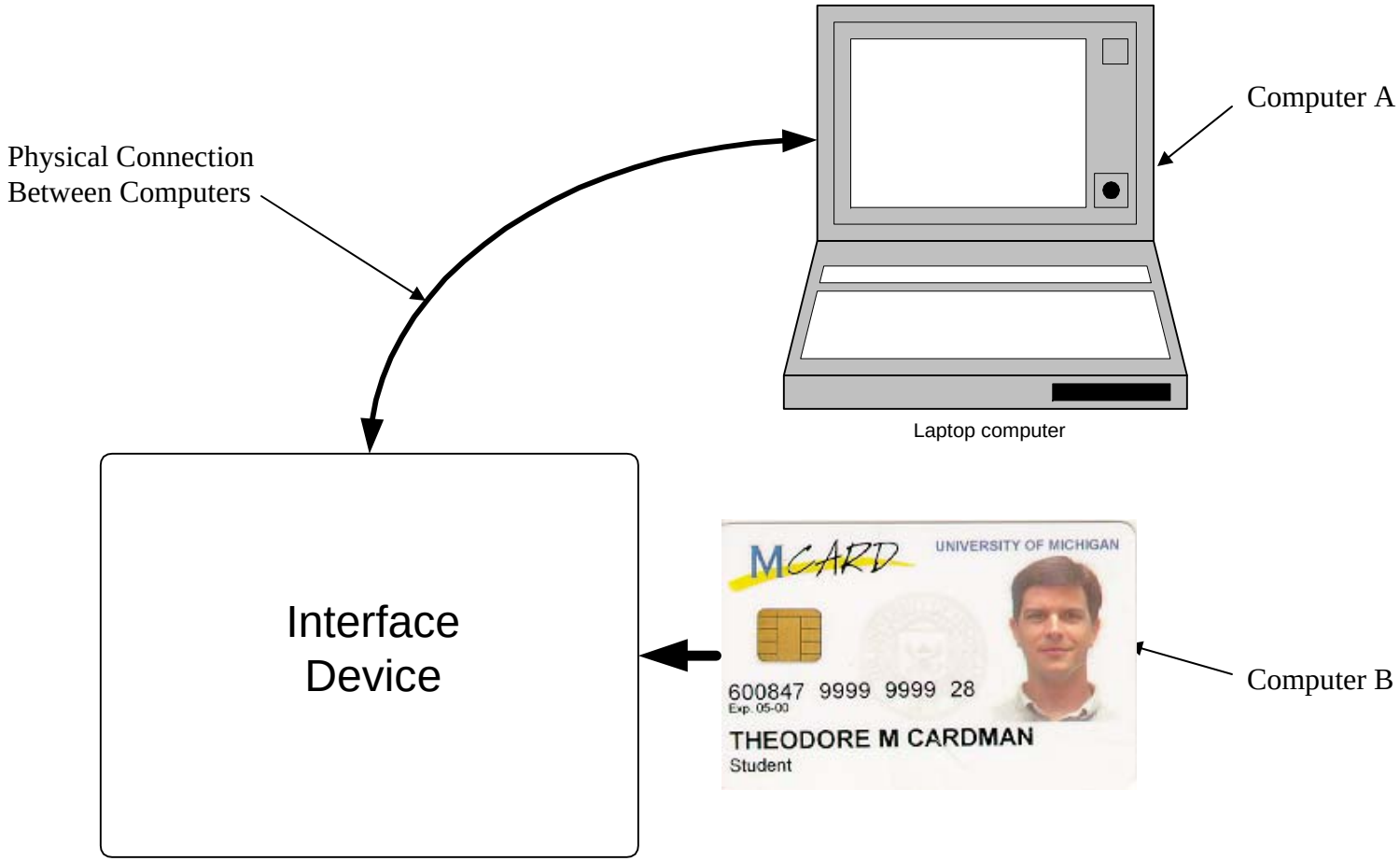
How Can 24727 Be Used?
A Value Proposition

- Architecting for evolution: an identity abstraction
  - Service Access Layer Interface for Identity (SALII)
- Discoverable, manageable, securable tokens
  - Baked-in support for multi-credential & -issuer tokens
- Token and service interoperability at two levels
  - Low-level GCI (Generic Card Interface), high level SALII
- Software-defined adaptation of applications to tokens
  - Procedural Elements & Data Model Registry
- An architecture for a secure smart card/token reader
  - Plumb the stack with authenticated, secure sessions
- Authenticate the token, the subject, and applications
  - With crypto protocols, biometrics, PINs and passwords

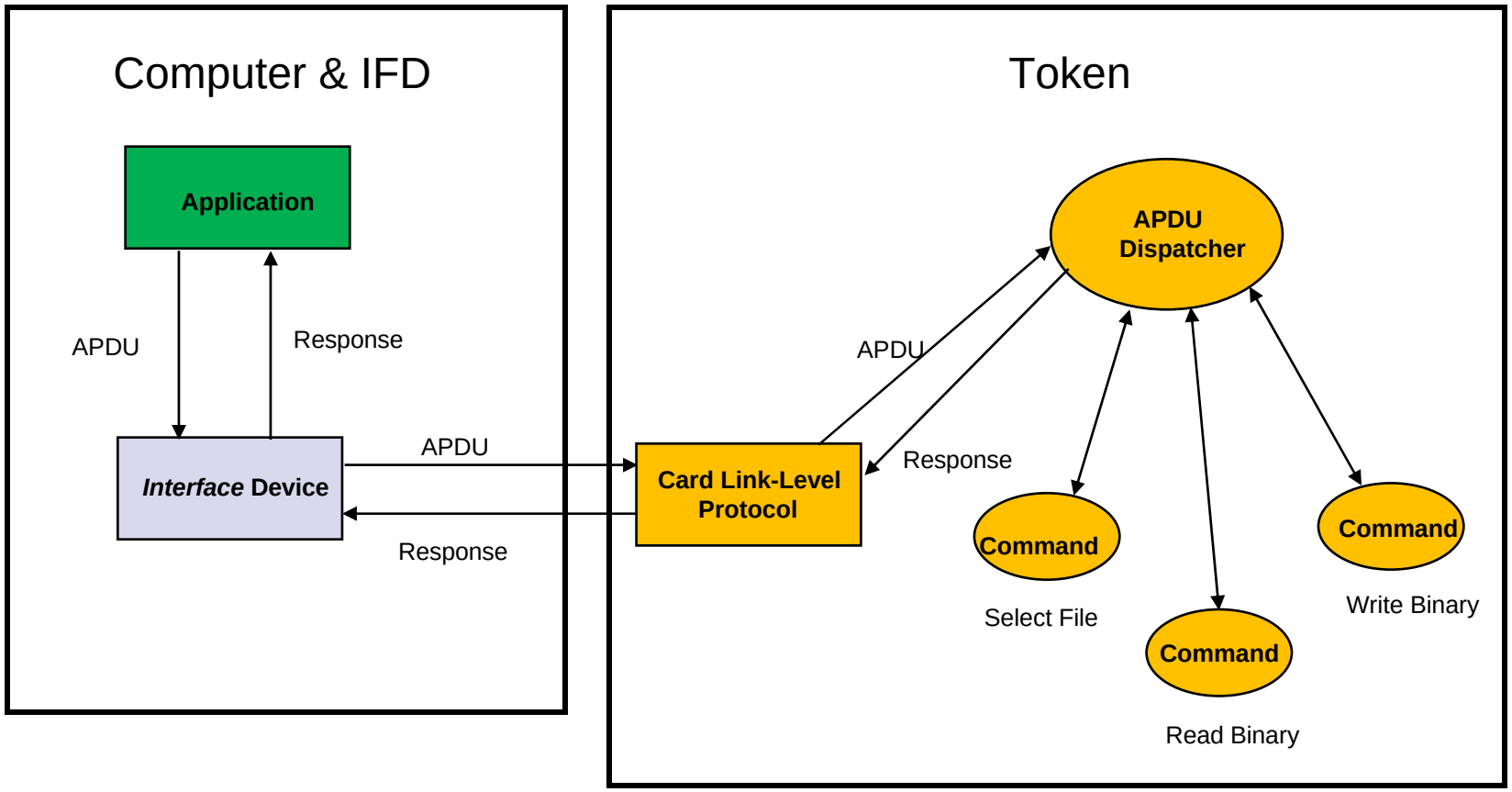
Presentation Objectives

- Review the standard capabilities of tokens
- Review application operations
- Review the goals of the GCI
- Review the APDUs of the GCI
- Review GCI bootstrapping
- Review GCI to proprietary APDU mapping

A Generic Token Application Configuration



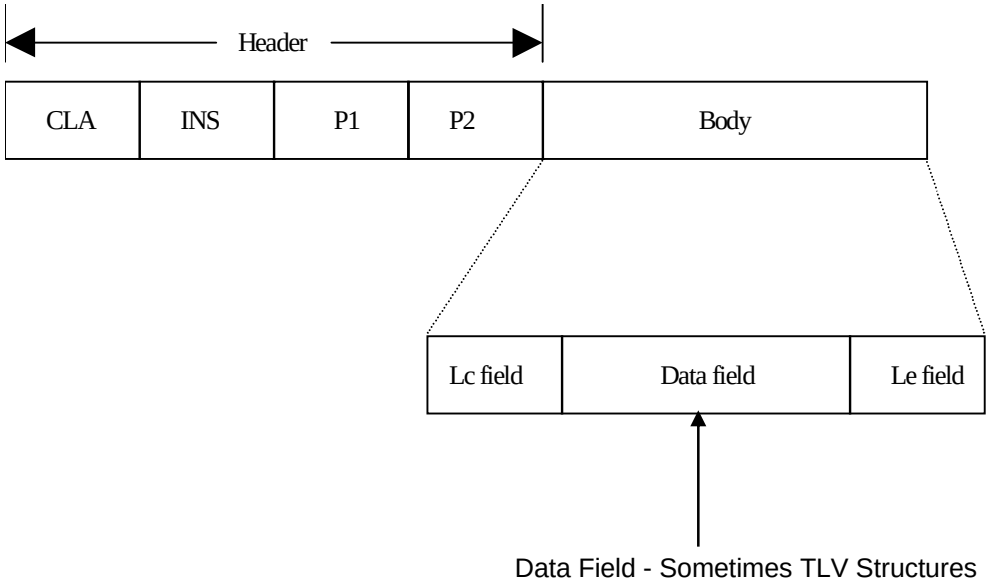
Standard Application Communications Architecture



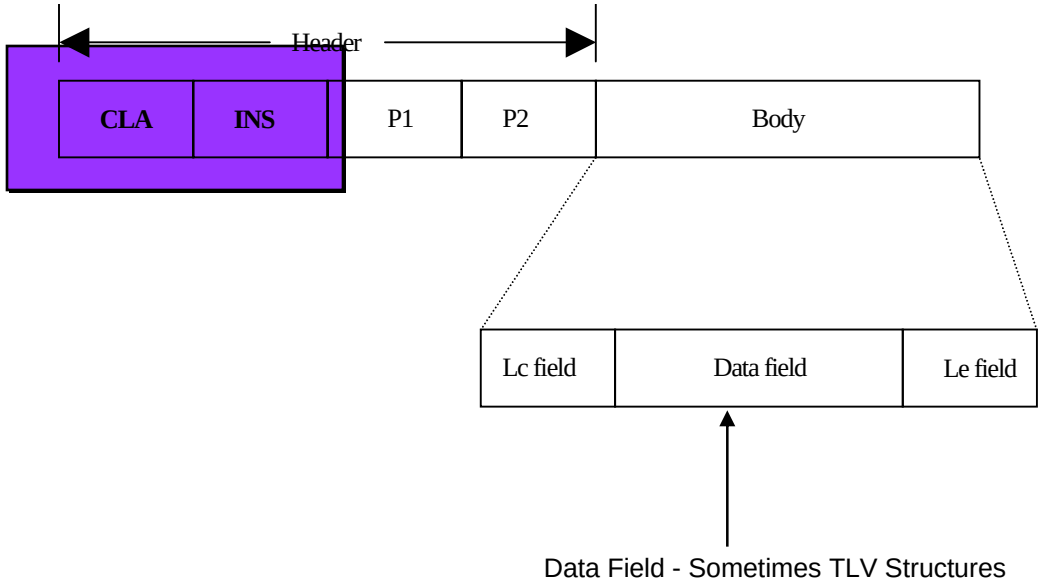
Two Primary Smart Card Protocols

- T = 0
  - Half-duplex
  - Byte oriented (I.e. error detection done on a byte basis)
  - Mixes card control with communication protocol
  - Most cards speak (at least) T = 0
- T = 1
  - Half-duplex
  - Block oriented
  - More efficient (higher speed)
  - Better “layer isolation” e.g can support secure messaging

T = 0 Command APDU Structure



CLA & INS Parameters



Usually Thought of As

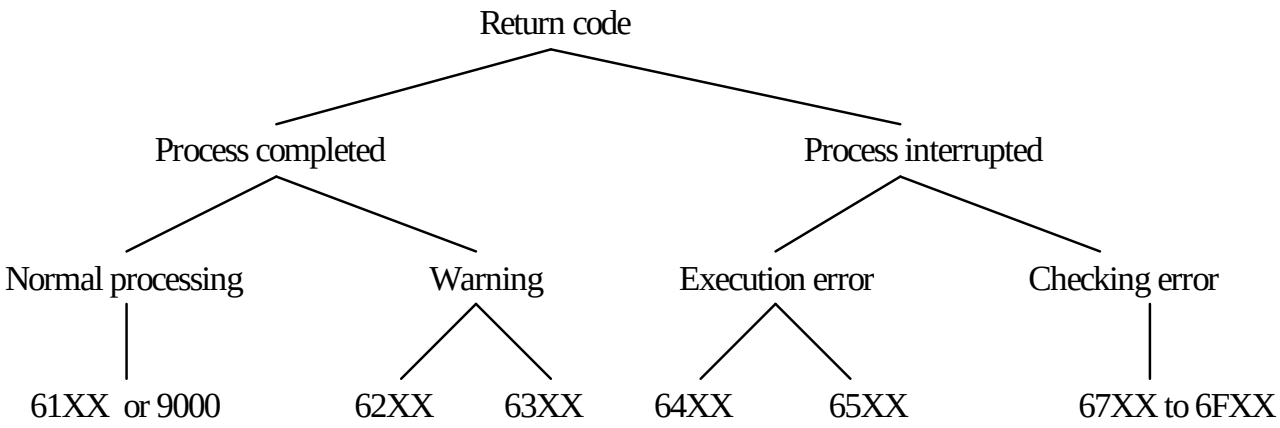
- CLAss
  - Generally says where the definition of this command is found.
- INStruction
  - Generally defines a specific command within a CLAss grouping

CLA Instruction Set Definitions

- 0X — ISO/IEC 7816-4 instructions (files and security)
- 10 to 7F — Reserved for future use
- 8X or 9X — ISO/IEC 7816-4 instructions
- AX — Application and/or vendor-specific instructions
- B0 to CF — ISO/IEC 7816-4 instructions
- D0 to FE — Application and/or vendor-specific instructions
- FF — Reserved for protocol type selection

T = 0 Response APDU Structure

Status Code Structure



T = 1 Block Structure

Prologue Field			Information Field	Epilogue Field
Node Address NAD	Protocol Control Byte PCB	Length LEN	APDU Data Length	Error Detection LRC/CRC
1 byte	1 byte	1 byte	0 to 254 bytes	1 or 2 bytes

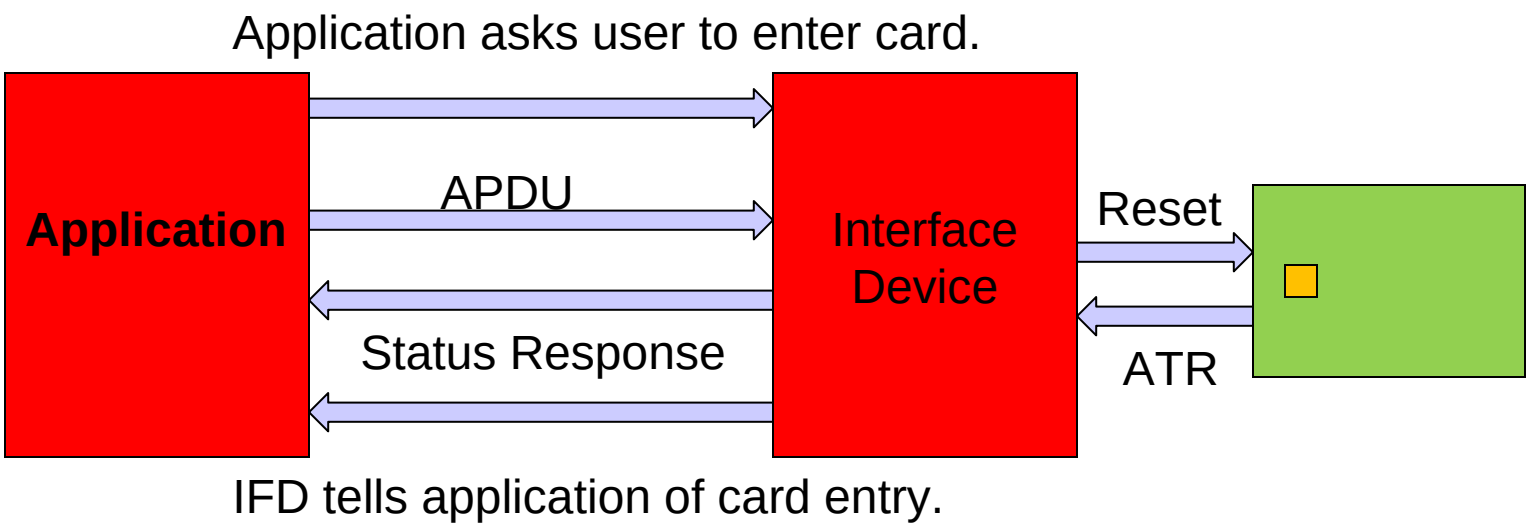
T = 1 Block Types

- Information Block
  - Conveys information to/from reader-side & card-side applications
- Receive Ready Block
  - Conveys ACKs & NAKs
- Supervisory Block
  - Conveys protocol control information

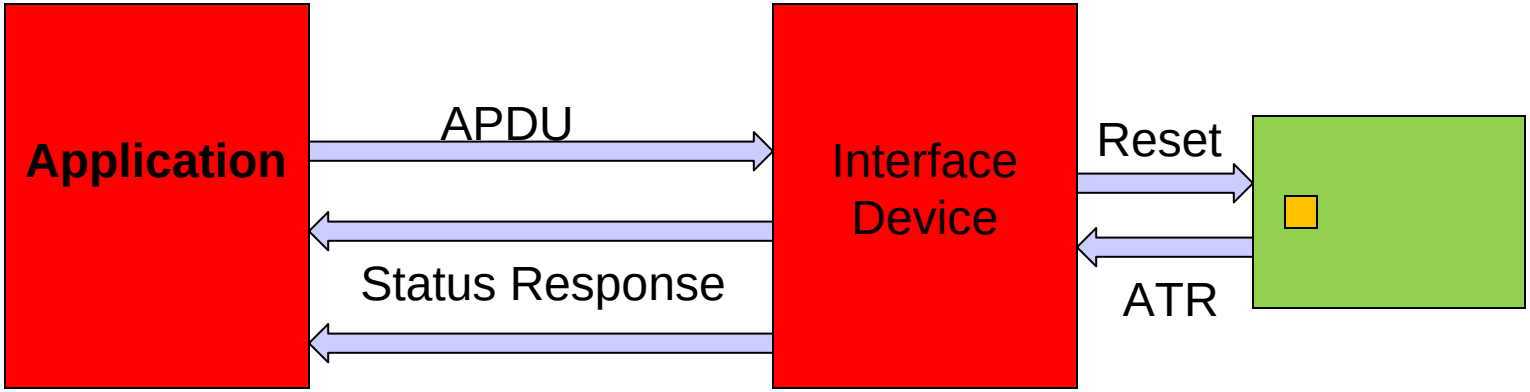
TLV Structures

- Format defined in ISO 7816-4
- TLV - Tag Length Value
- Tag - gives a name to the value contained in the structure
- Length - number of bytes stored in the structure
- Value - the actual number
- Two flavors - “Simple TLV” and “BER-TLV”
- Simple TLV - 1-byte Tag; 1-3 byte Length; 0-64K byte value.
- BER-TLV - defined in ISO/IEC 8825

Application starts the process

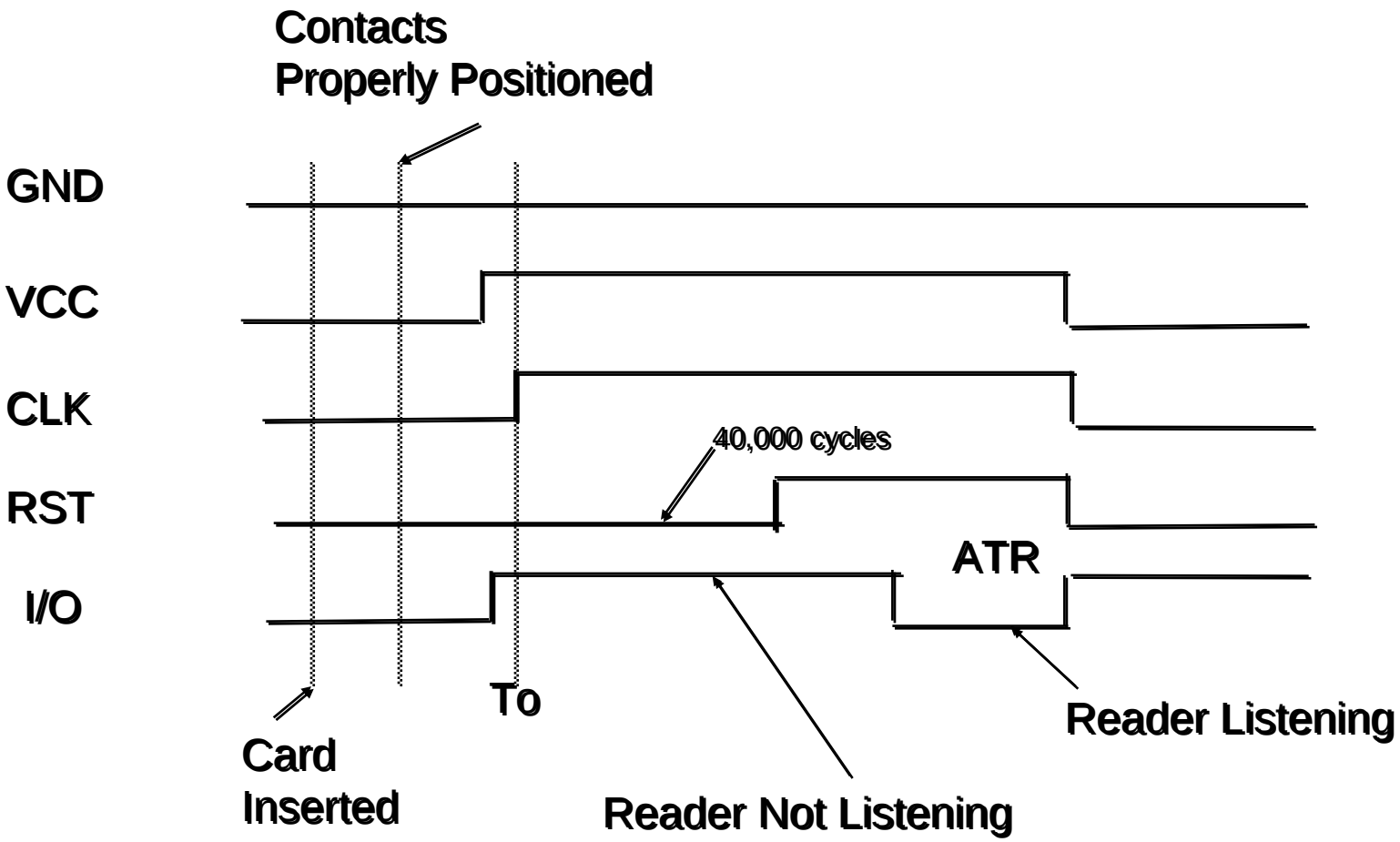


User (Token) starts the process



IFD tells application of card entry.

Power Up Sequence



Answer To Reset

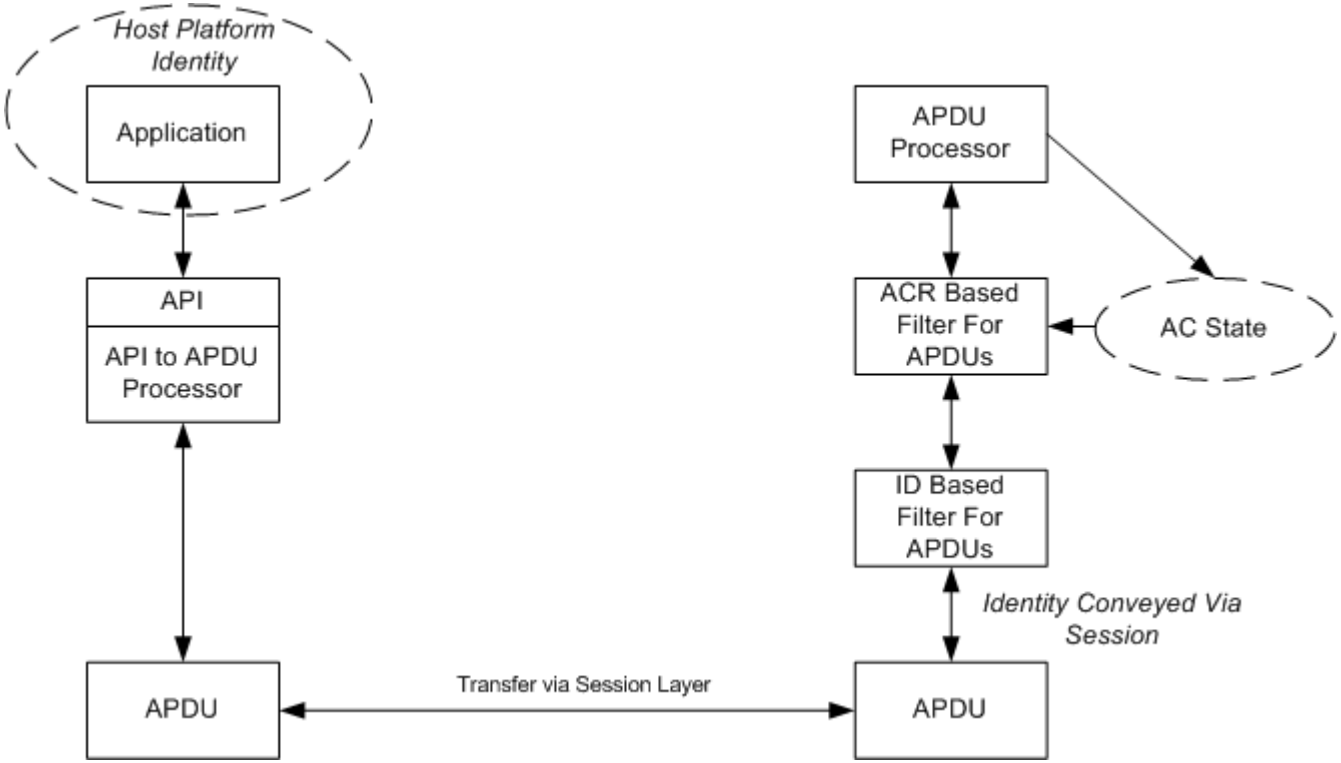
- TS Mandatory initial character

- T0 Indicator for presence of interface characters
- TA_1 Global, codes F1 and D1
- TB_1 Global, codes 11 and Pl1
- TC_1 Global, code N
- TD_1 Codes Y_2 and T
- TA_2 Specific
- TB_2 Global, code Pl2
- TC_2 Specific
- TD_2 Codes Y_3 and T
- TA_3 TA_i, TB_i, and Tc_i are specific
- [el]TD_i Codes Y_{i+1} and T
- T1 (Maximum of 15 characters)
- [el]TK
- TCK Optional check character

TS Special Character

- Conveys bit “sense” between reader and card
- Conveys “big endian” vs “little endian” byte ordering between reader and card

The ISO/IEC 24727 Paradigm



API to APDU Conversion

- Requires a well defined API (ISO/IEC 24727-3)
- Requires a well defined APDU set (ISO/IEC 24727-2)

AND – to build working systems

- Requires a means to map the well defined APDU set to proprietary APDU sets

ISO/IEC 24727-2: Generic Card Interface

- Intermediate language between client-application API and card specific command sets
- Extracts a name-to-data-object map or map URL from the physical ICC that enables Parts 3 and 4 to use this intermediate language
- Extracts a translation script or script URL from the physical ICC that maps the intermediate language to the actual capabilities of the physical ICC
- Expressed as ISO/IEC 7816-4, -8 and -9 APDUs.
- Allows for integration and use of cards presenting proprietary command sets.

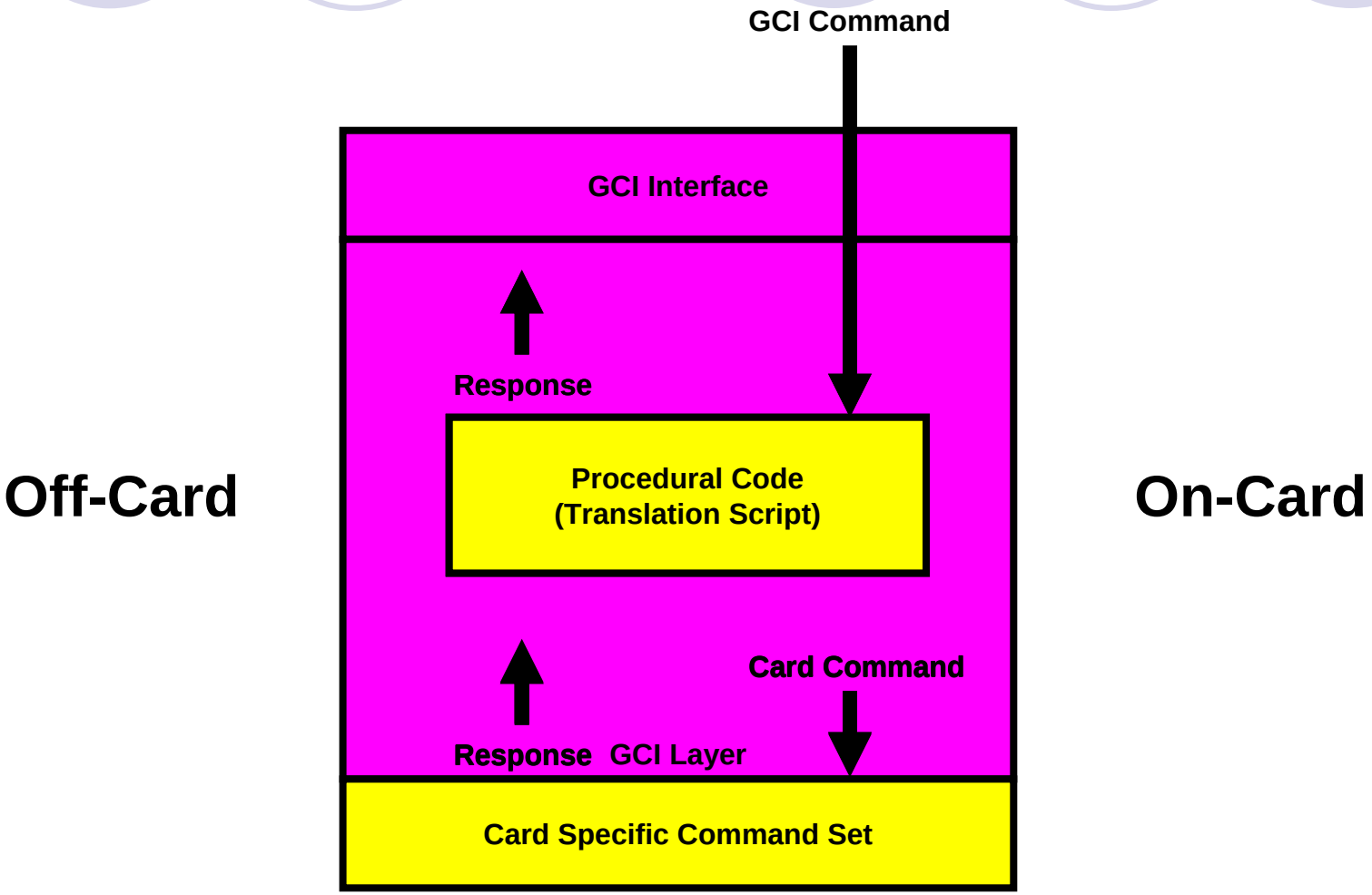
GCI APDUs

- SELECT
- READ BINARY
- UPDATE BINARY
- GET DATA
- PUT DATA
- GENERATE ASYMMETRIC KEY PAIR
- VERIFY
- CHANGE REFERENCE DATA
- GET CHALLENGE
- INTERNAL AUTHENTICATE
- EXTERNAL AUTHENTICATE
- MUTUAL AUTHENTICATE
- GENERAL AUTHENTICATE
- PERFORM SECURITY OPERATION
  - COMPUTE DIGITAL SIGNATURE
  - HASH
  - VERIFY CERTIFICATE
  - ENCIPHER
  - DECIPHER
- MANAGE SECURITY ENVIRONMENT
- CREATE FILE
- DELETE FILE
- ACTIVATE FILE
- DEACTIVATE FILE
- RESET RETRY COUNTER
- GET RESPONSE

IFD Commands Conveyed via APDUs

- COLD RESET
- WARM RESET
- DEACTIVATE CONTACTS
- DEACTIVATE CONTACTS AND EJECT
- SELECT PROCEDURAL ELEMENT
- GET DATA
- PUT DATA
- LIST READERS

GCI Layer


GCI Command
GCI Interface
Response
Off-Card
Procedural Code
(Translation Script)
On-Card
Card Command
Response
GCI Layer
Card Specific Command Set

CCD Data Objects

Symbol	Tag	Description
PRO	‘80’	Profile of ISO/IEC 24727-2 with which this CCD complies
SAID	‘A0’	Sequence of application identifiers or card-applications
LANG	‘A1’	Procedural element description template
LANG-URL	‘5F50’	URL of the code that performs the translation
CIA-PROFILES	‘81’	CIA profiles present on the generic card interface
CIA-PROFILES-AUTOMATIC	‘82’	CIA profiles present on the generic card interface
DIGITAL-SIGNATURE-ON-CODE	‘5F3D’	Digital signature information for procedural element
IF-PROFILE	‘83’	Profile of ISO/IEC 24727-3 interface

ACD Data Objects

Symbol	Tag	Description
LANG	‘A1’	Procedural element description template
LANG-URL	‘5F50’	URL of code that performs the translation
SERVICE-DESCRIPTION	‘7F66’	Description of the services supported by the card-application
SERVICE-DESCRIPTION-LOCATION	‘7F67’	URL of a description of the services supported by the card-application
DIGITAL-SIGNATURE-ON-CODE	‘5F3D’	Digital signature information for procedural element

Alpha Card-application

- AID – ‘E8 28 81 C1 17 02’
- Alpha card-application is either present and selectable on the GCI or is emulated by or through the Service Access Layer (i.e. ISO/IEC 24727-3 layer)
- Alpha card-application defines a shared context for a collection of card-applications
- Alpha card-application contains differential-identities with global scope

QUESTIONS?

William MacGregor, NIST
William.macgregor@nist.gov