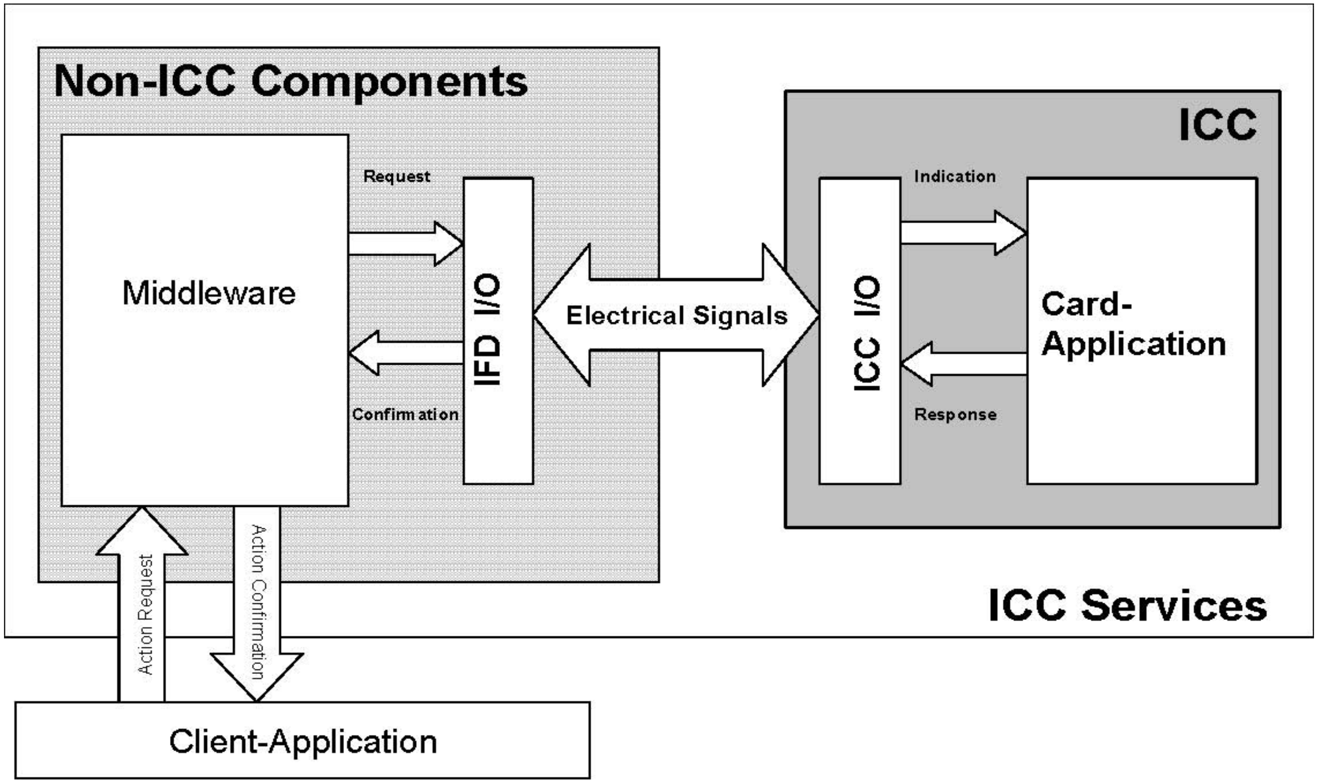
NIST
National Institute of
Standards and Technology

ISO/IEC 24727 Architecture

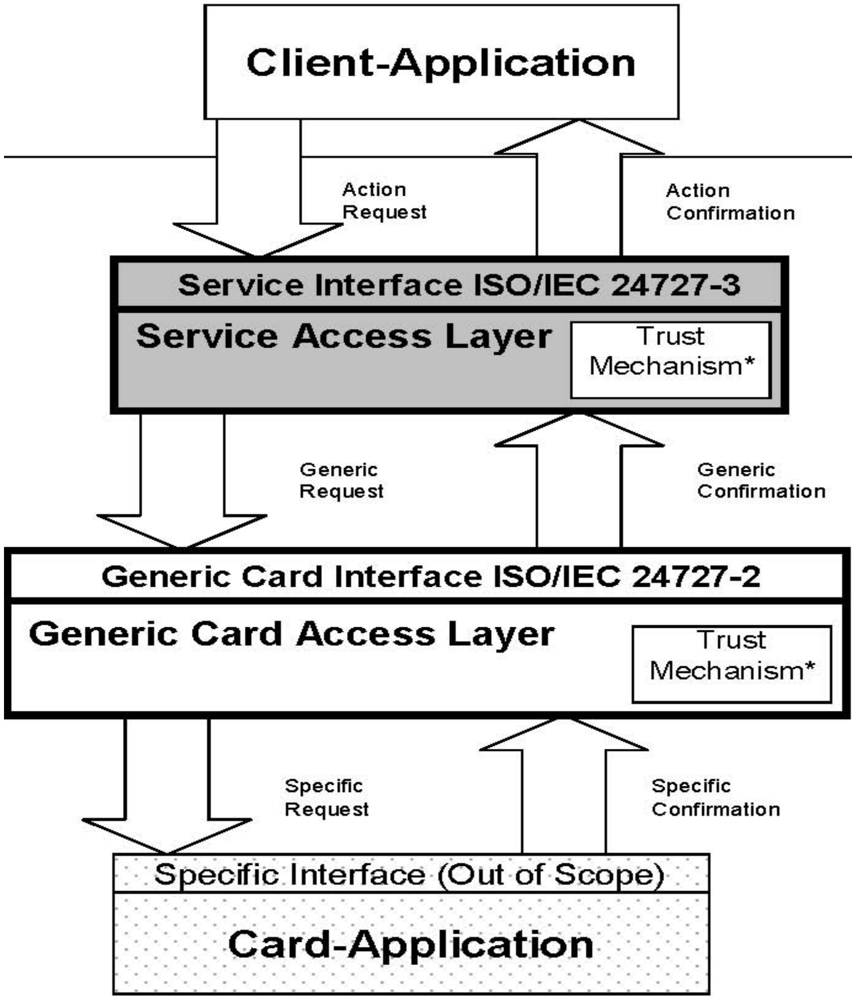
Session Objectives

- View ISO/IEC 24727-1 as requirements
- Consider the Architecture elements for subsequent ISO/IEC 24727 parts
- Consider the mechanisms to be used
- Consider the central features for exploration in subsequent parts

ISO/IEC 24727 Physical Architecture



ISO/IEC 24727 Logical Architecture



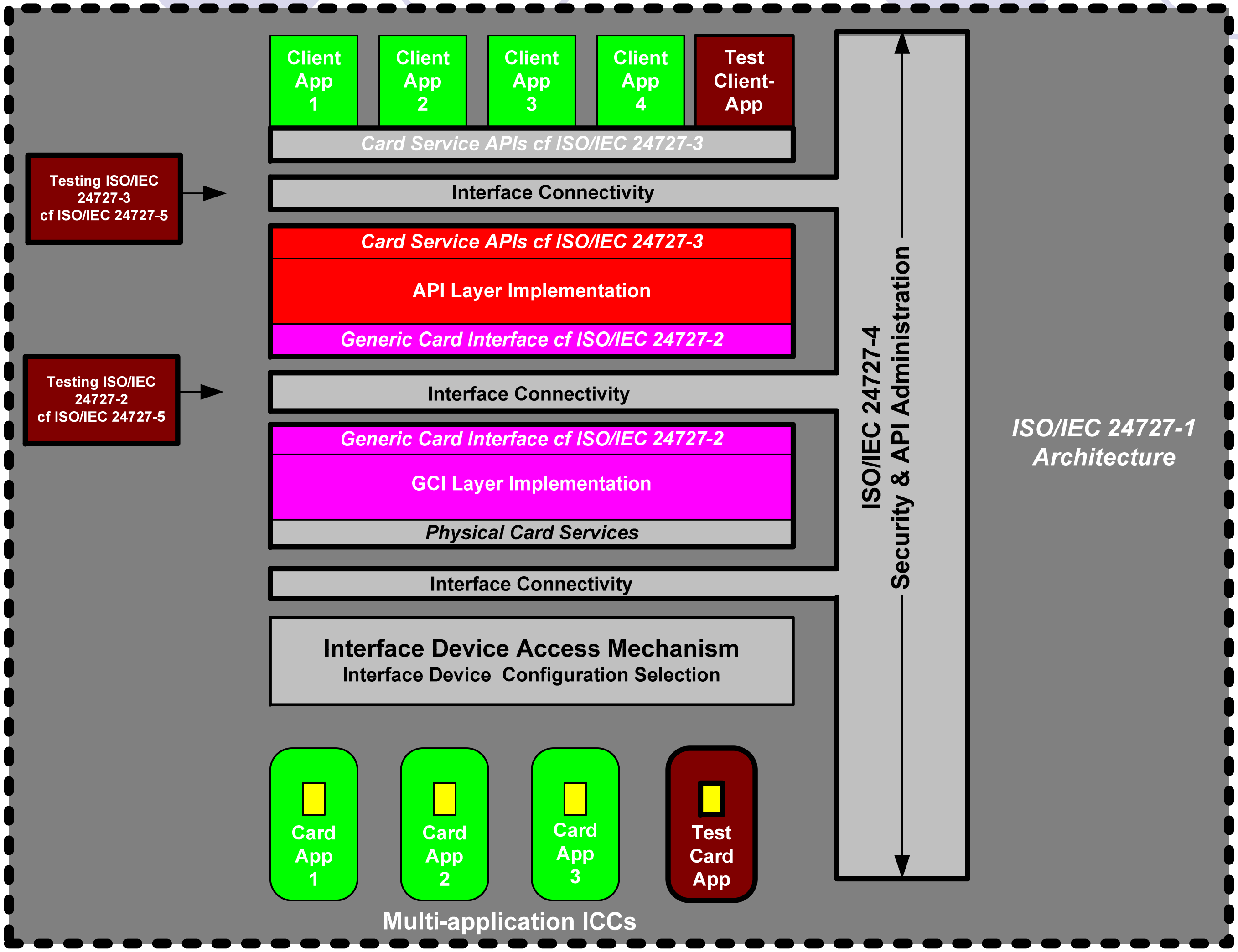
Expansion of Scope

- ISO/IEC 24727-4 was independently balloted as a New Work Item
- It expanded the scope of ISO/IEC 24727 to:
  - Include end-to-end security
  - Include connectivity
  - Include secure messaging
  - Include stack configuration and use
  - Include interface device (IFD) interface

Second Expansion of Scope

- Development of ISO/IEC 24727-3 identified the standardization of authentication protocols as essential for long-term interoperability.
- The ISO amendment process was deemed too unwieldy to support the evolution of authentication protocols.
- ISO/IEC 24727-6 was independently balloted as a new work item to establish a standard for a registry for authentication protocols.

ISO/IEC 24727: A Standard in 6 Parts



Client App 1

Client App 2

Client App 3

Client App 4

Test Client-App

Card Service APIs cf ISO/IEC 24727-3

Testing ISO/IEC 24727-3 cf ISO/IEC 24727-5

Interface Connectivity

Card Service APIs cf ISO/IEC 24727-3

API Layer Implementation

Generic Card Interface cf ISO/IEC 24727-2

Testing ISO/IEC 24727-2 cf ISO/IEC 24727-5

Interface Connectivity

Generic Card Interface cf ISO/IEC 24727-2

GCI Layer Implementation

Physical Card Services

Interface Connectivity

Interface Device Access Mechanism

Interface Device Configuration Selection

Card App 1

Card App 2

Card App 3

Test Card App

Multi-application ICCs

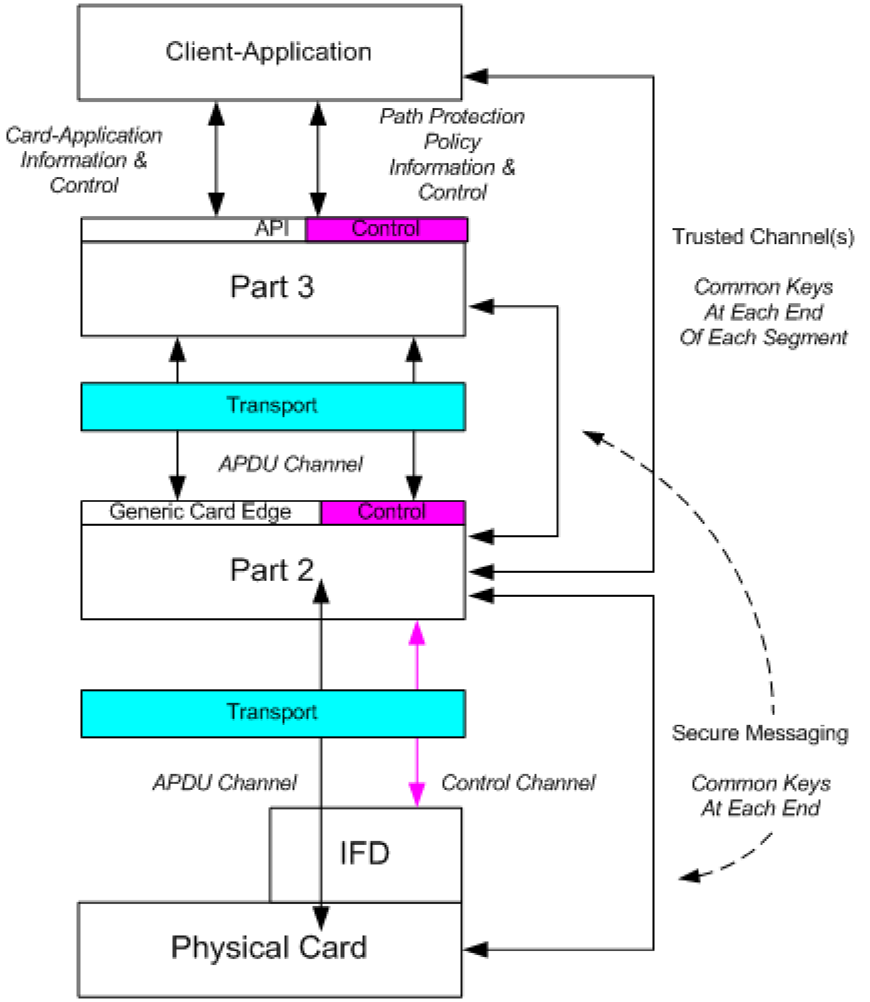
ISO/IEC 24727-4

Security & API Administration

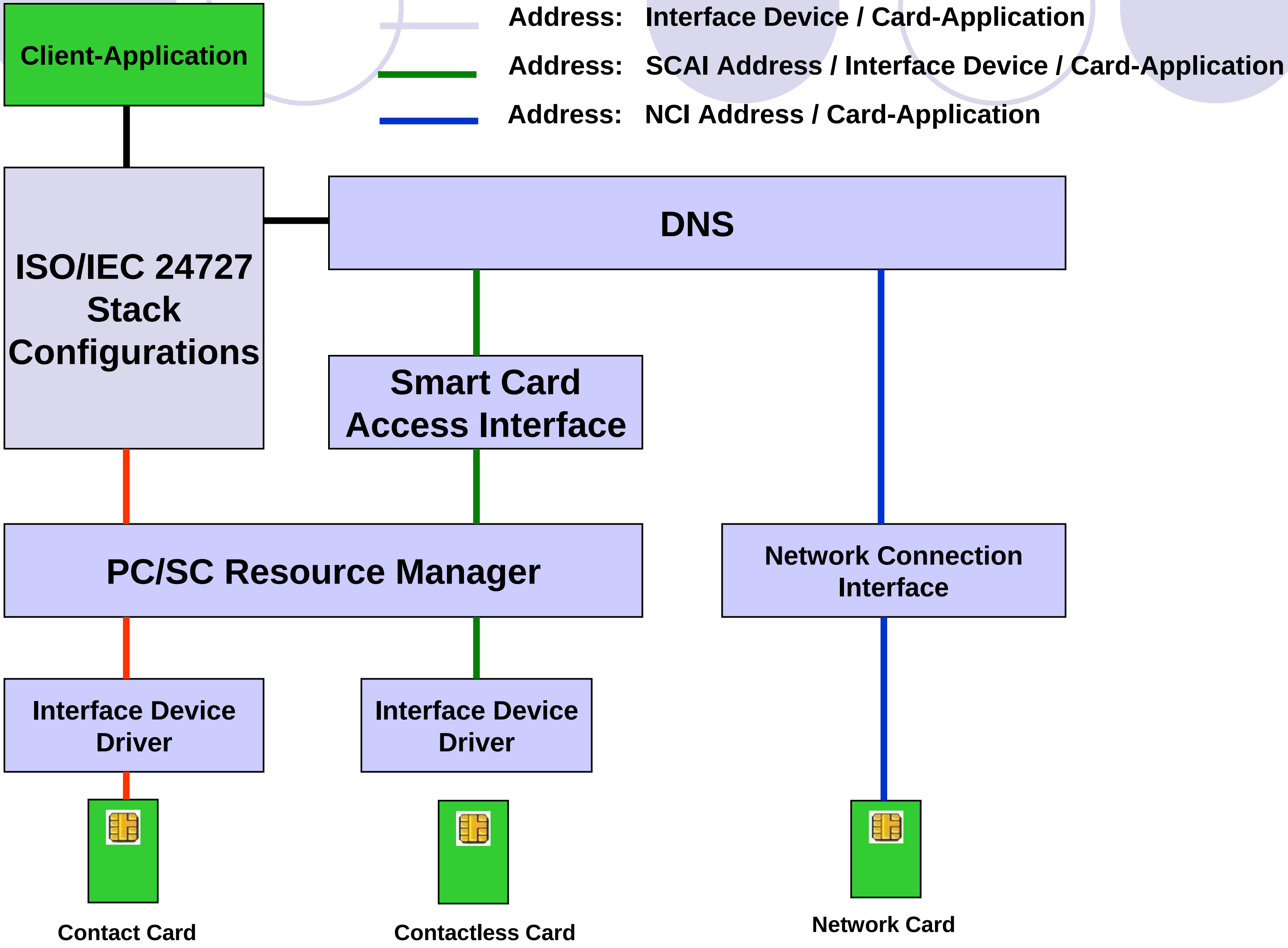
ISO/IEC 24727-1 Architecture

- Application
- Part 1 - Architecture
- Part 2 - Generic Card Interface
- Part 3 - Application Programming Interface
- Part 4 - API Adminstration
- Part 5 - Testing
- Part 6 – Register Auth Protocols

Stack Architecture Overview



ISO/IEC 24727-4: Path Environment



🟪 Address: Interface Device / Card-Application

🟩 Address: SCAI Address / Interface Device / Card-Application

🟦 Address: NCI Address / Card-Application

Client-Application

ISO/IEC 24727 Stack Configurations

DNS

Smart Card Access Interface

PC/SC Resource Manager

Network Connection Interface

Interface Device Driver

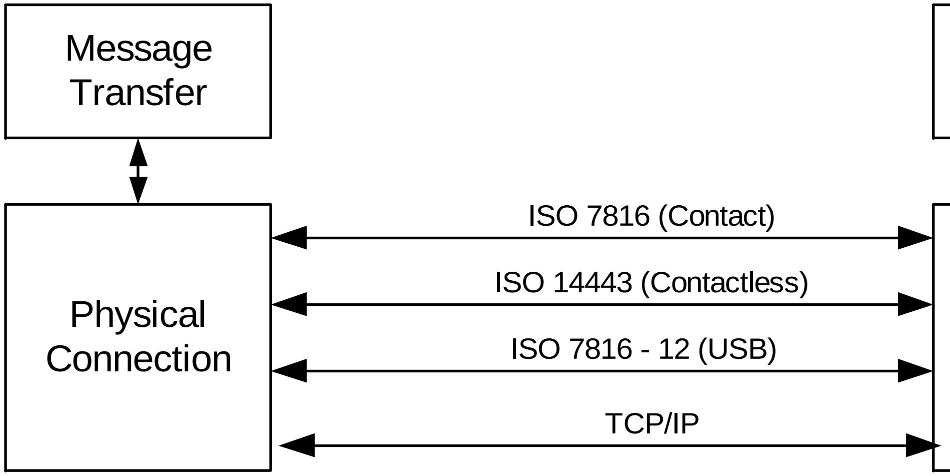
Interface Device Driver

Contact Card

Contactless Card

Network Card

Physical Connectivity

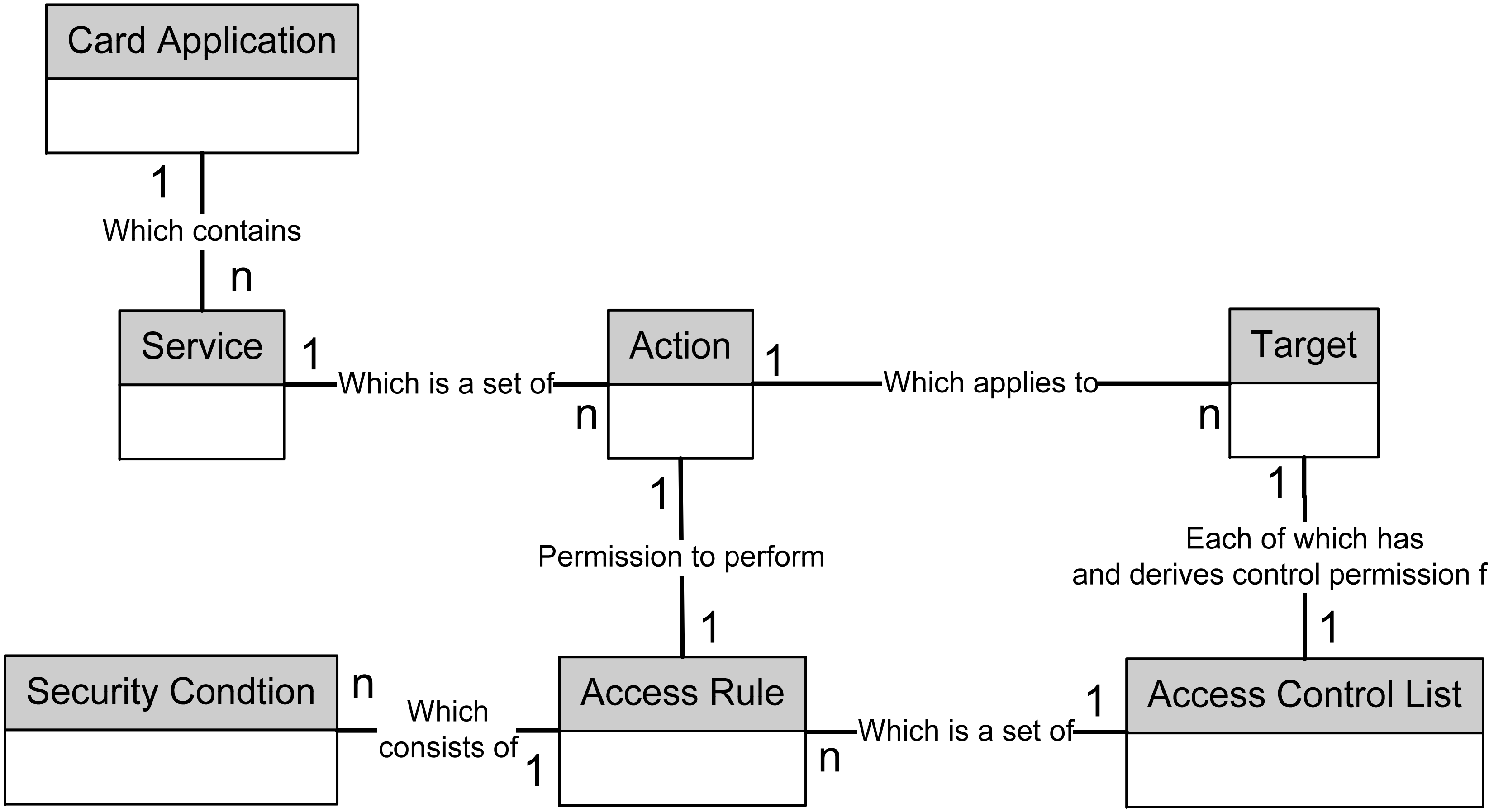


Transfer via Physical Layer

Two Security Environments

- On-card
  - Authenticating identities of cards, cardholders, and computers to each other.
  - Aimed at protecting access to on-card information and resources
    - Commands
    - Files
- Off-card
  - Computer and/or network security infrastructures
  - Aimed at establishing security across a wide area
  - Use smart cards as a component in these infrastructures

ISO/IEC 24727-3: Basic Entity Relationships



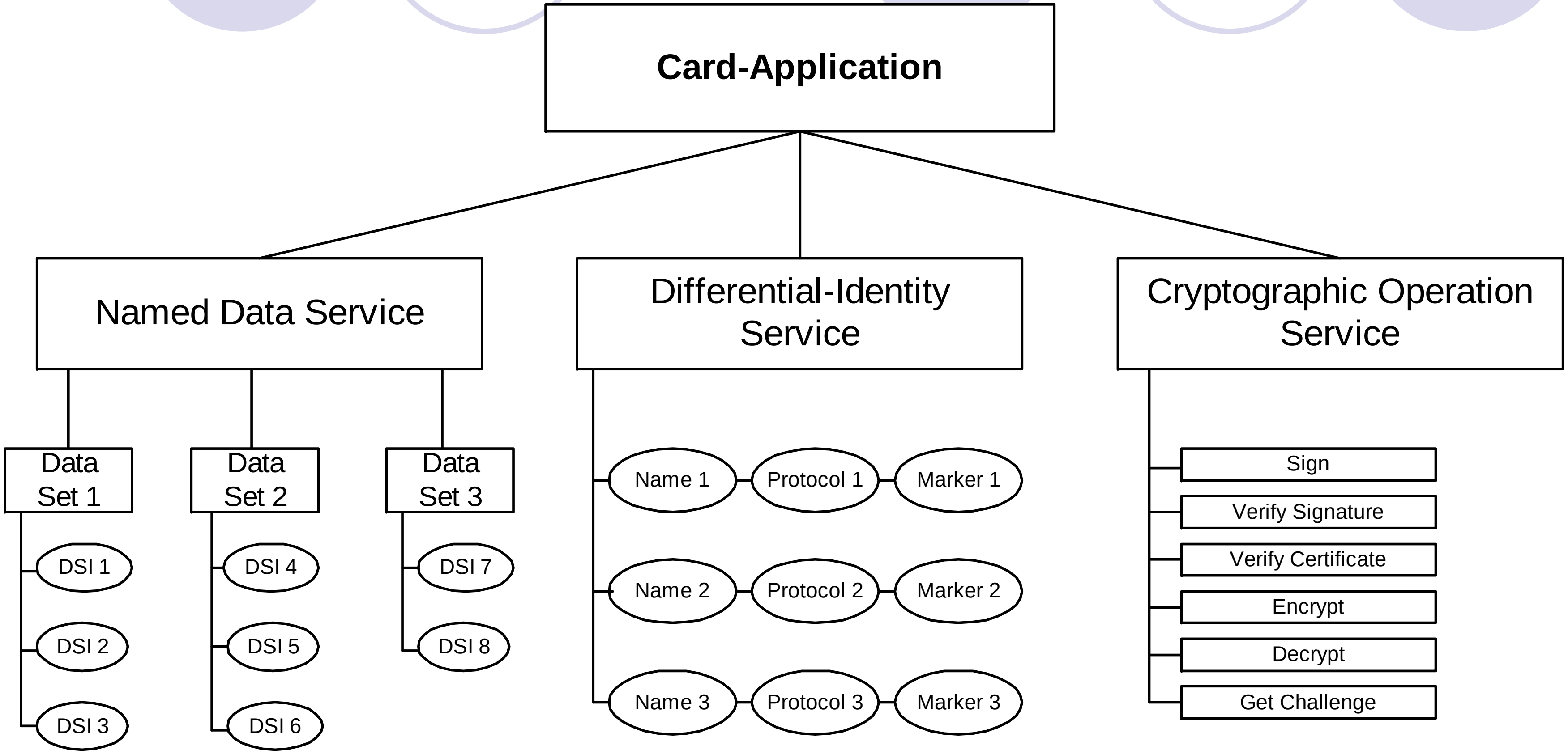
Common Infrastructure Semantics

- Card-application uniquely identifiable across a network environment
- Client-application to card-application “path” uniquely identifiable
- Mapping between client-application & card-application name spaces
- Security state establishment through differential-identity
- Information storage / retrieval through named data service
- Information and process protection via access control lists

Common IAS Semantics

- Data-Set
  - Client-application named set of information with common security characteristics
- Data Structure for Interoperability (DSI)
  - Client-application named quantum of information stored in data-set
- Differential-Identity
  - Mapping of client-application named entities to card-application “marked” entities allowing authentication via standard protocols
- Cryptographic Services
  - Protected Sign, VerifySignature, Encipher, & Decipher procedures

Generic IAS Card-Application



Authentication Protocol: an example

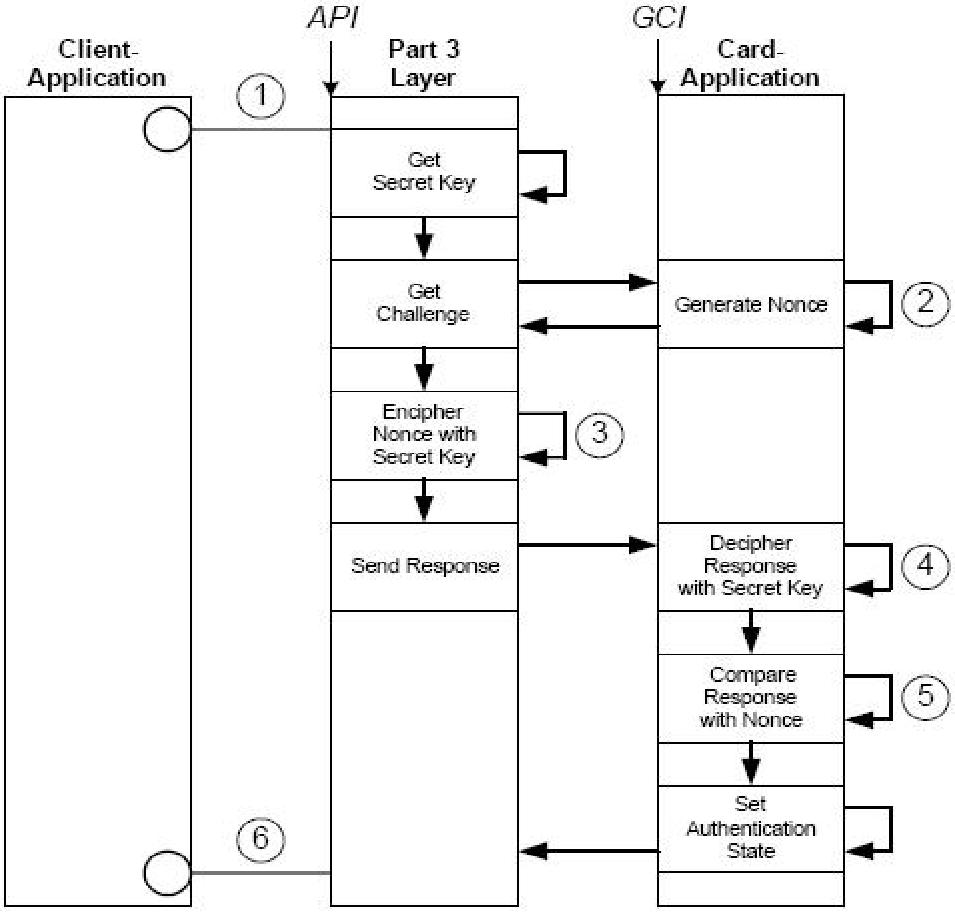


Figure A.5 — Symmetric External Authenticate

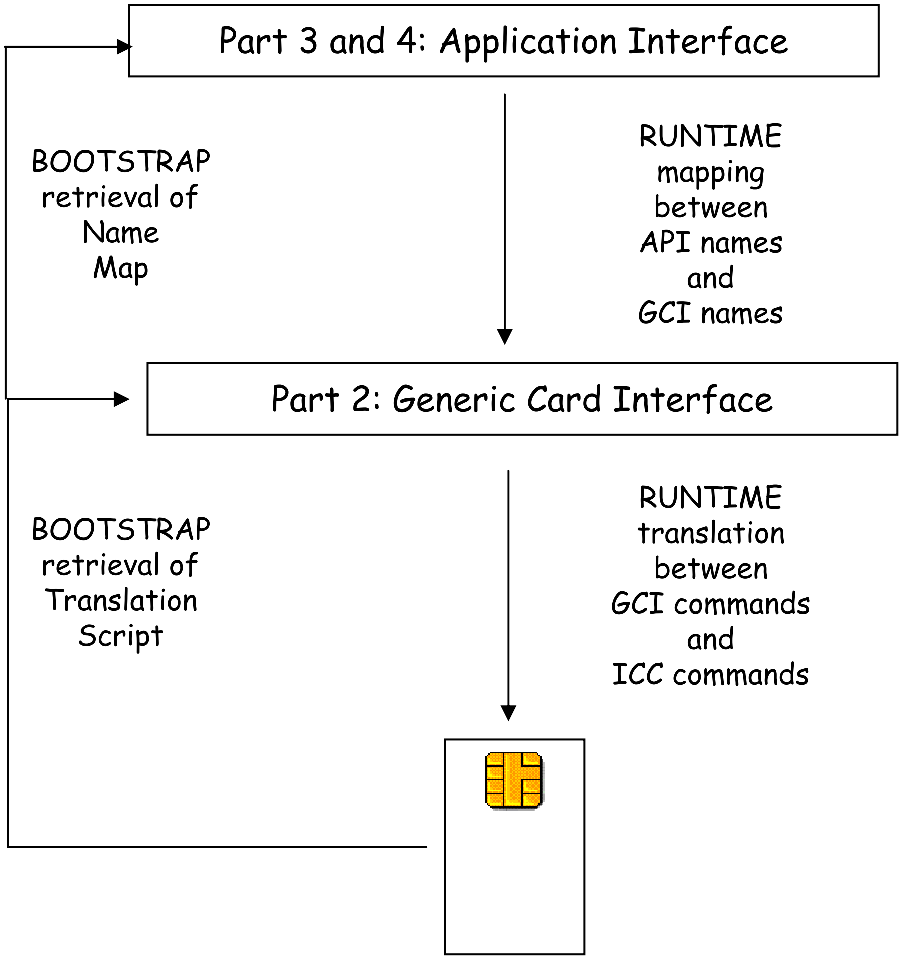
```
MarkerAP007 ::= SEQUENCE {

 encryptionAlgorithm
                  AlgorithmIDParameters,
 hashAlgorithm
                  AlgorithmIDParameters,
 keySize            INTEGER,
 secretKey          OCTET STRING,
 nonceSize          INTEGER

}
```

Discoverability Concepts

- Client-Application “discovers” the semantic content of the card-application through the Part 3 API
    - Differential-identity information
    - Data-set information
    - Request fulfillment facilities (Sign, etc.)
    - Security state requirements
- Part 3 Layer creates and retrieves a mapping structure (CIA) between Part 3 concepts and Part 2 mechanisms
- Part 3 Layer creates and retrieves the Card Capability Description
- Part 3 Layer creates and retrieves the Application Capability Description

Discoverability Mechanisms

- Discovery Mechanisms
  - Card Capability Description
  - Application Capability Description
  - Interoperability Registry (CIA)
- APDU Mapping
  - Part 2 APDU set defines basic command set
  - Proprietary APDUs may be mapped (procedurally and/or descriptively)



Part 3 and 4: Application Interface

BOOTSTRAP retrieval of Name Map

RUNTIME mapping between API names and GCI names

Part 2: Generic Card Interface

BOOTSTRAP retrieval of Translation Script

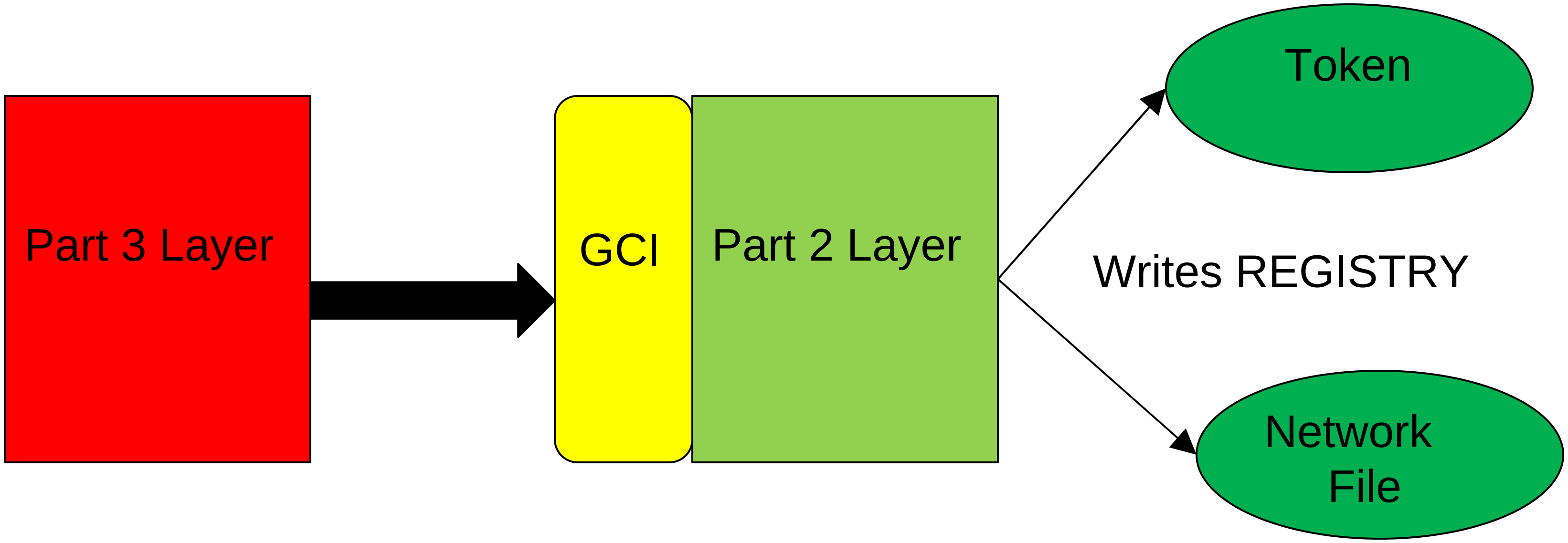
RUNTIME translation between GCI commands and ICC commands

Client-application level discovery

- Through the ISO/IEC 24727-3 API, a client-application can learn:
  - What card-applications are on a card.
  - What differential-identities can be authenticated.
  - What data-sets are available in each card-application.
  - What DSI's are available in each data-set.
  - What security state must be established to access a data-set.

Implementation level discovery

The Registry (CIA)



Implementation level discovery

- A Part 3 Layer writes a mapping (The CIA) of its use of the Part 2 Interface
- Mapping via The CIA conveys:
  - How are Data Sets mapped to the GCI?
    - Files or Data Objects?
  - How are DSI’s mapped to the GCI?
    - Files or Data Objects
  - What are the ACLs for a specific card-application?
  - What is the mapping of client-application names to Tags?
  - What is the mapping of differential-identity names to key references?

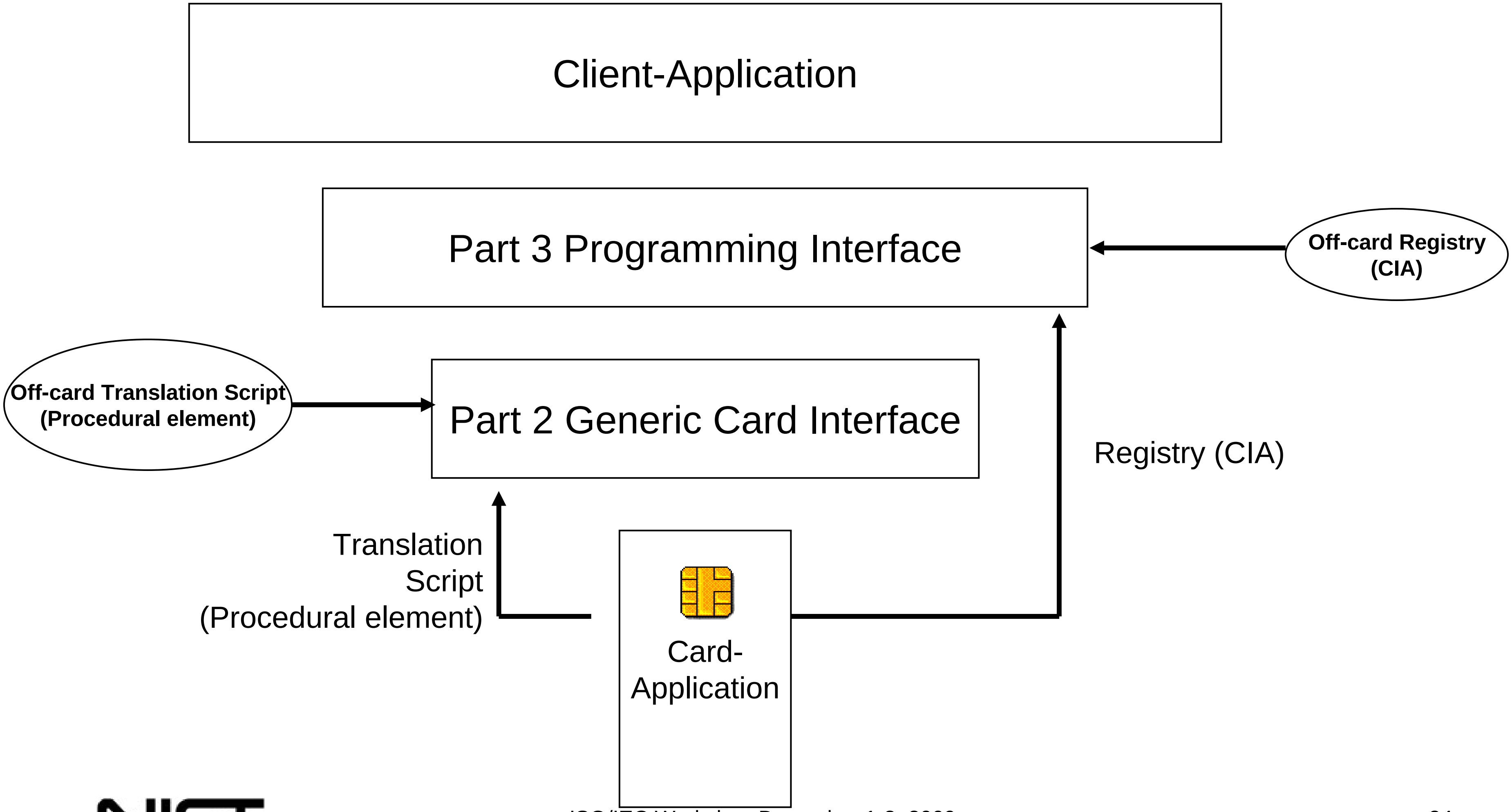
Extensibility

- *Part 3 API Provides Card-Application Administration Service*
- Administration of Card-Applications
  - CardApplicationList to show available card-applications
  - Create new card-applications
  - Delete existing card-application
- Administration of Services (e.g. add new, executable code)
  - CardApplicationServiceList – to show available card-application services
  - Create a new service in a card-application
  - Delete an existing service from a card-application
  - Load executable code to effect a new service
  - ExecuteAction is a generic API command for allowing a client-application to make new requests that are provided in new services

Backward Compatibility

- Translation Script (Procedural element)
  - Translation scripts may be found on-card or off-card
  - They may be created (off-card) for legacy tokens
  - Translation scripts may make semantic as well as procedural translations, allowing use of legacy concepts
- Cryptographic Information Application (CIA)
  - The CIA is a registry that may be found on-card or off-card.
  - It may be created (off-card) to describe a family of legacy cards

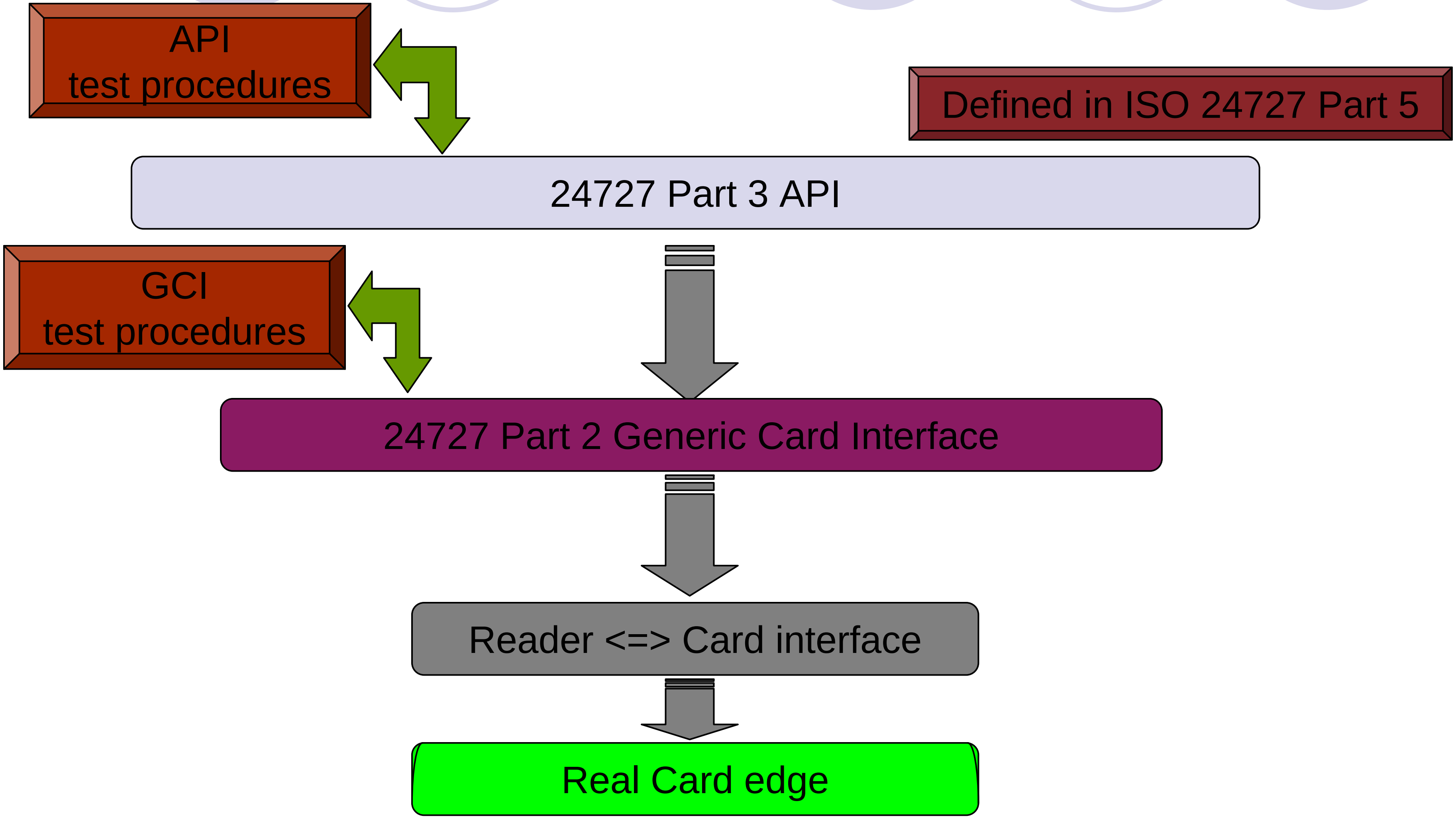
Backward Compatibility Mechanisms



Conformance Testing

- Behavioral testing
  - Functional testing
  - Tests based on requirements (what the product should or should not do according to the specification)
  - Allows, in principle, to do the tests in total ignorance of how the object under test is constructed

Interface Test Architecture


API
test procedures
Defined in ISO 24727 Part 5
24727 Part 3 API
GCI
test procedures
24727 Part 2 Generic Card Interface
Reader <=> Card interface
Real Card edge

Flexible Stack Configurations

- Loyal Stack
- Remote ICC Stack
- ICC Resident Stack
- Opaque ICC Stack
- Remote Loyal Stack
- Full Network Stack

QUESTIONS?