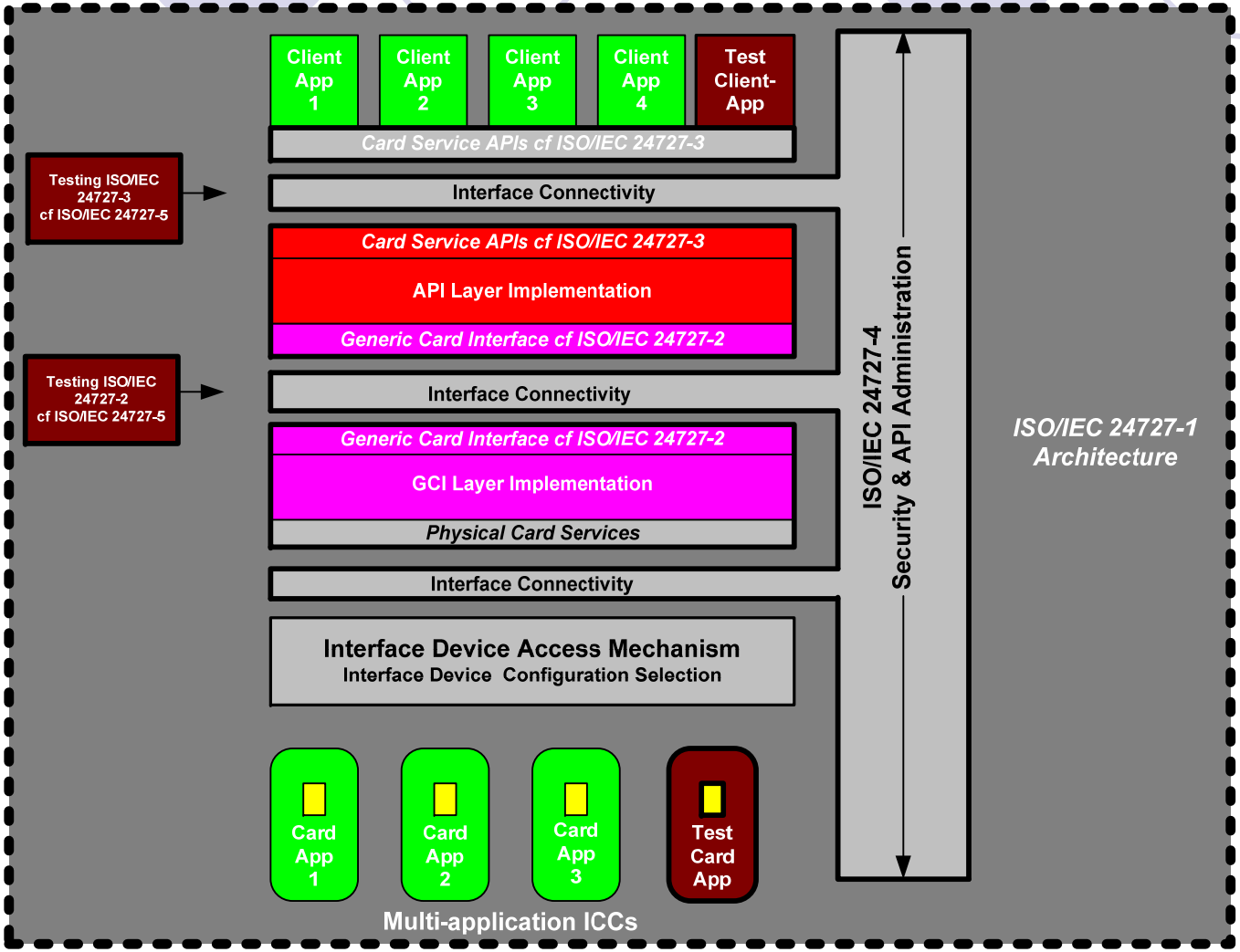
ISO/IEC 24727
Vocabulary and Semantics

ISO/IEC 24727: A Standard in 6 Parts



- 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

ISO/IEC 24727 Vocabulary

- *Interoperable* – independent implementations are interchangeable
- *Client-application* – processing software needing access to one or more card-applications
- *Card-application* – uniquely addressable set of functionalities on an ICC that provide data storage and computations services to a client-application

ISO/IEC 24727 Vocabulary

- *Interface* – point at which independent and often unrelated systems meet and act on or communicate with each other
- *Middleware* – software that connects two otherwise separate applications
- *Translation code* – procedural software that transforms commands on the generic card interface to commands implemented on an integrated circuit card

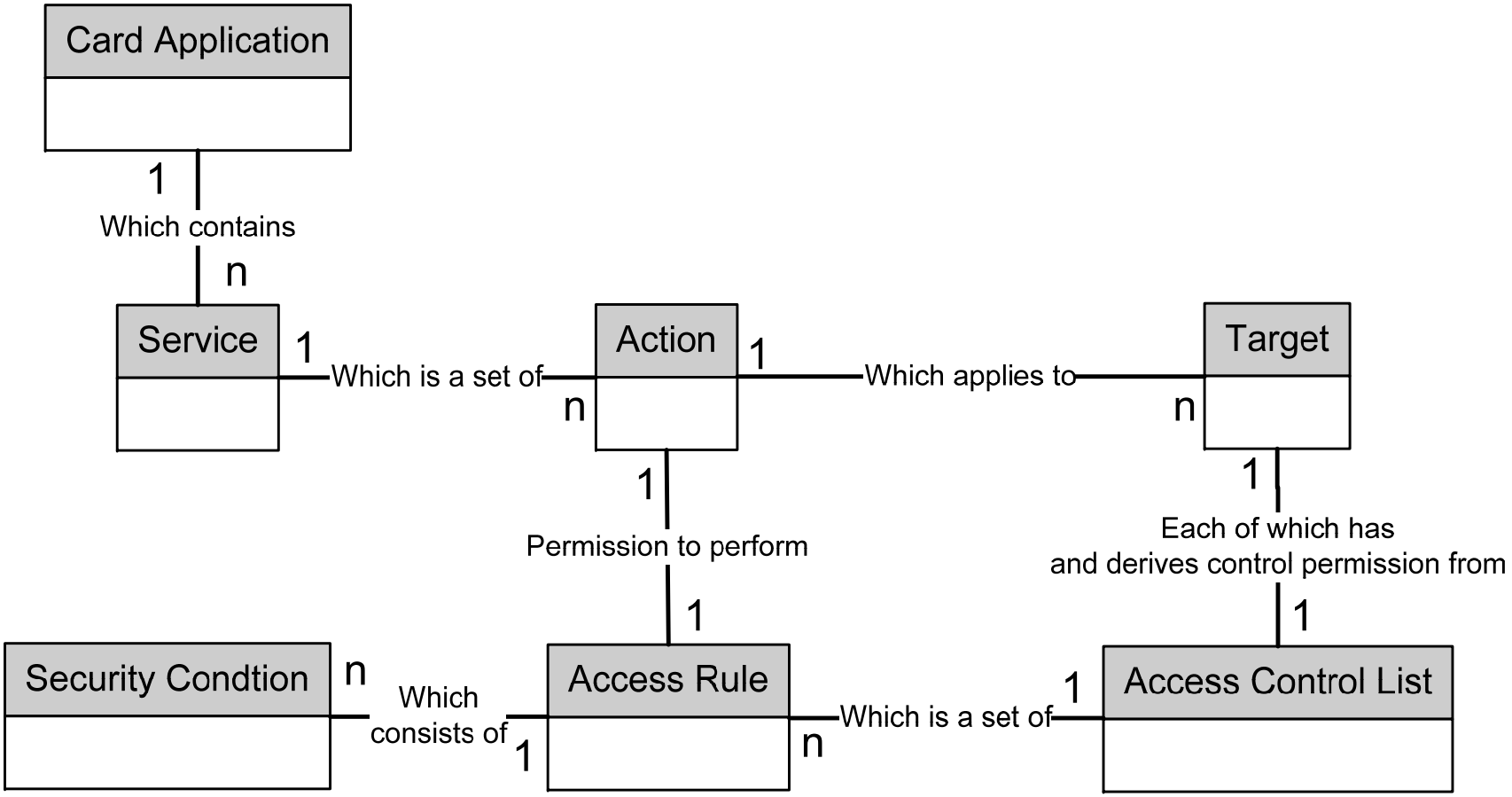
ISO/IEC 24727 Vocabulary

- *ISO/IEC 24727 protocol stack* – series of processing components connected by communication channels that connect a client-application to a card-application
- *Component* – executable code comprising a processing layer accessed with ISO/IEC 24727 defined application programming interfaces
- *Authentication* – process of assessing a level of confidence in identity or identification

ISO/IEC 24727 Vocabulary

- *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 – a storage mechanism for certificates
- *Differential-Identity* – set of information comprised of a name, a marker and an authentication protocol
- *Cryptographic Services* - Protected Sign, VerifySignature, Encipher, & Decipher procedures invoked through a specific differential-identity

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

Stack Architecture Overview