ISO/IEC 24727-4
API Administration

Presentation Objectives

- Review stack architectures
- Review security considerations
- Review connectivity considerations
- Review administration
- Review network operations

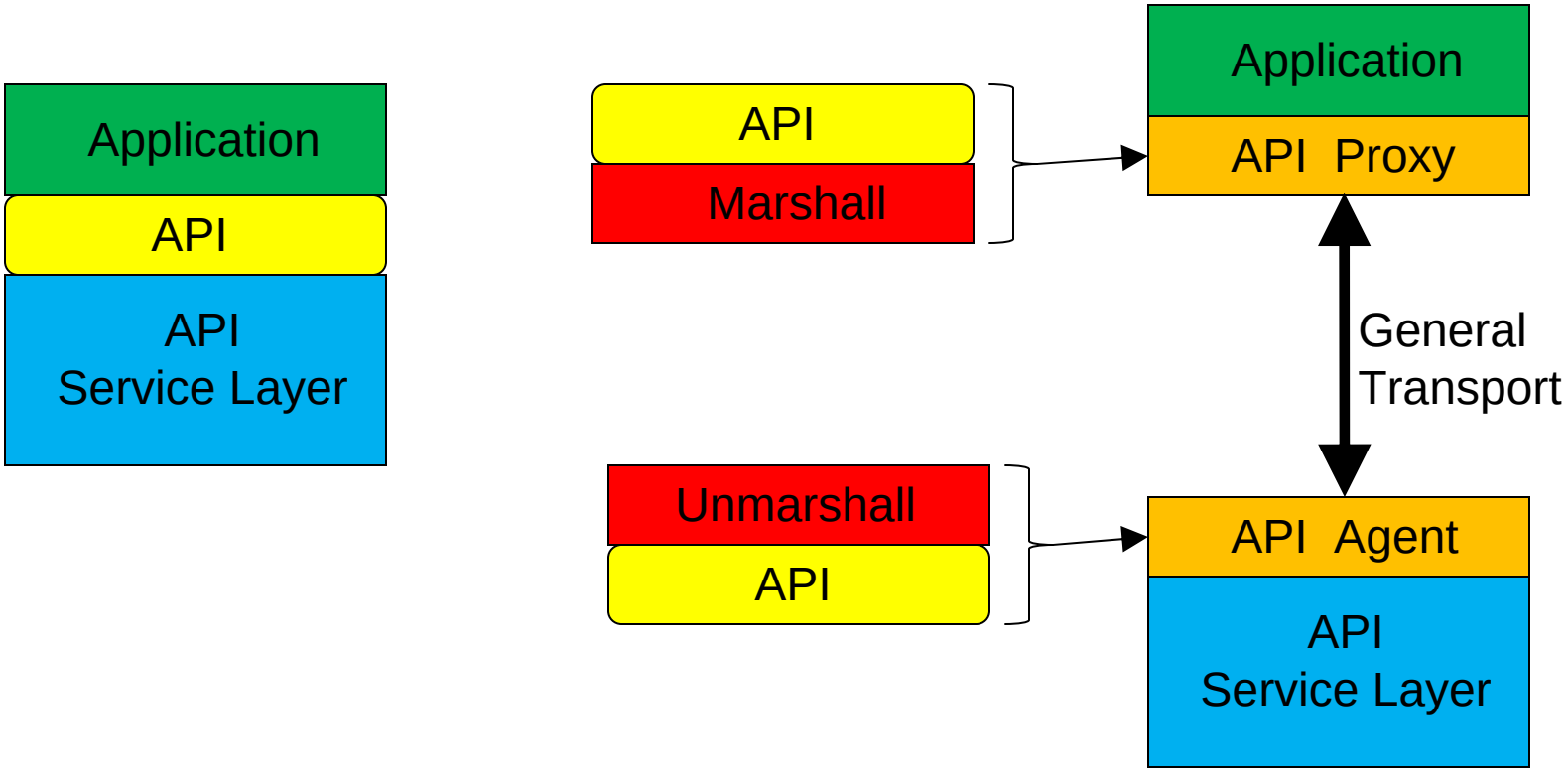
An expansion of scope

- 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

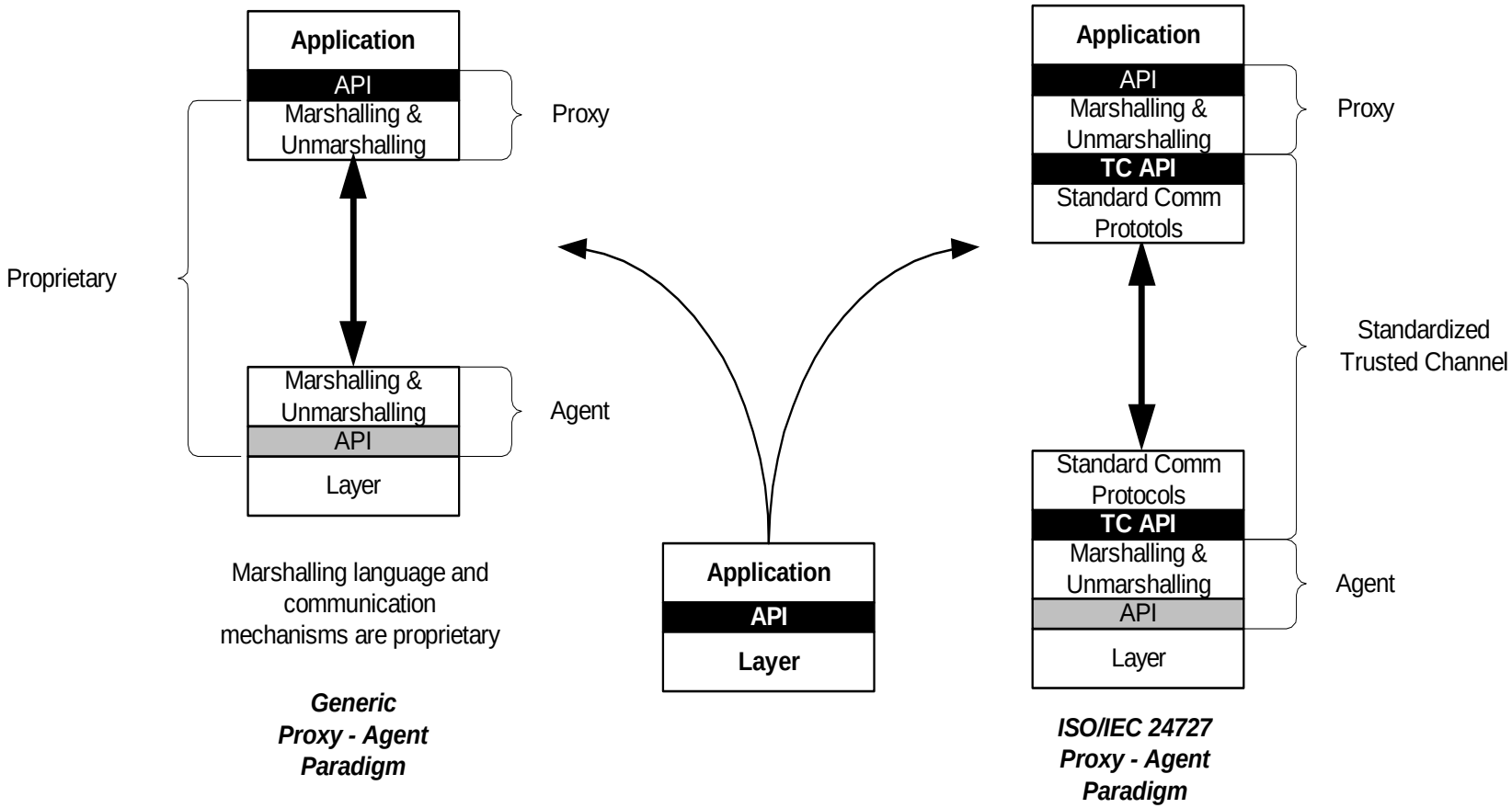
Purpose

- Stack Configuration
  - What is the utility of different stacks?
- Security Characteristics
  - What security can be achieved with each stack?
- Token Connection
  - How is the client-application to card-application connection made in each stack?

Proxy and Agent Architecture



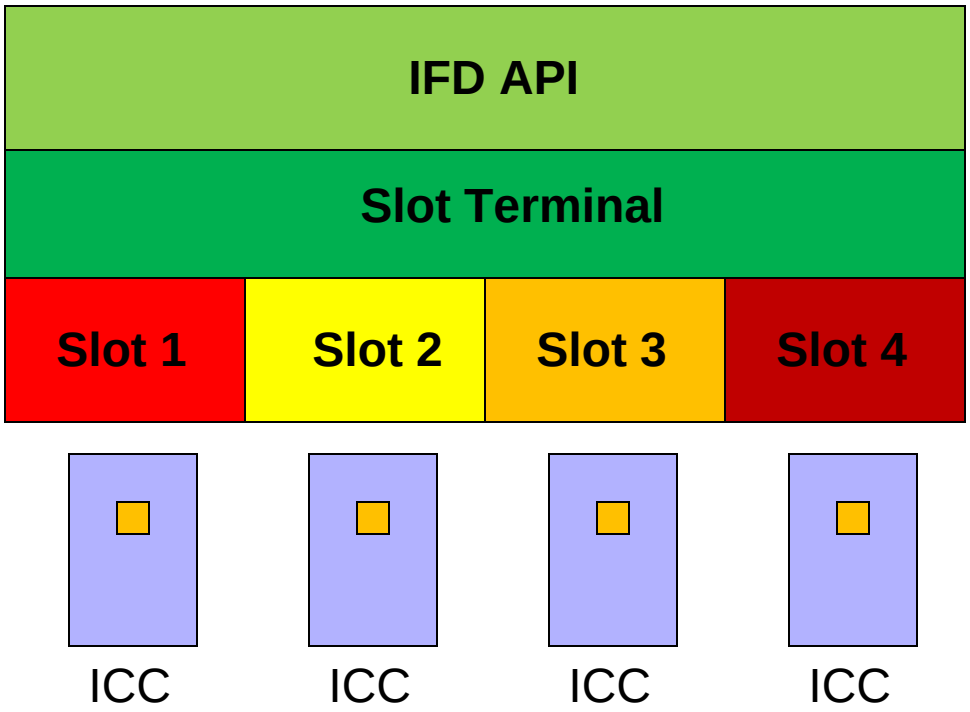
Proxy-Agents via Trusted Channel



Trusted Channel API

API Function	Functional Description
TC_API_Open	This function initiates the handshake through which the client and server orientation is established between the two ends of the channel and through which the security characteristics of the channel are established.
TC_API_Close	This function terminates the trusted-channel.
TC_API_Write	This function transfers a message through the trusted-channel to the terminus point at the other end of the trusted-channel.
TC_API_Read	This function accepts a message from the trusted-channel.
TC_API_Reset	This function flushes any pending messages in the trusted-channel and re-initializes the trusted-channel.
TC_API_GetStatus	This function retrieves the current status of the trusted-channel, including the status of any pending messages in the trusted-channel.

IFD API


IFD API
Slot Terminal
Slot 1
Slot 2
Slot 3
Slot 4
ICC
ICC
ICC
ICC

Interface Device (IFD) API
(Slot Terminal Related Requests)

- EstablishContext
- ReleaseContext
- ListIFDs
- GetIFDCapabilities
- GetStatus
- Wait
- Cancel
- ControlIFD

Interface Device (IFD) API
(Slot Related Requests)

- Connect
- Disconnect
- BeginTransaction
- EndTransaction
- Transmit

Interface Device (IFD) API
(User Related Requests)

- VerifyUser
- ModifyVerificationData
- Output

ASN.1 Representations

- ASN.1 is a formal language
- ISO/IEC 24727 uses ASN.1 to specify the interface requests in ISO/IEC 24727-3 & 4
- An ASN.1 representation of each request allows the interoperable implementation of a general PROXY-AGENT mechanism
- ASN.1 is also used to specify authentication protocols

Granularity of stack security

Path Protection Policy Class	
End-to-end	a single key or key set shall be used to secure the channel between the client-application and the card-application
Segmented	different keys or key sets shall be used to secure the various segments of the channel between the client-application and the card-application
Agnostic	no specification is given for the security characteristics of the channel between the client-application and the card-application; the strength or weakness of the security characteristics of the channel is immaterial.

Path protection policy categories

- *Intrinsic* - result of platform + channel default facets
- *Protected* - confidentiality + data integrity
- *Source-authenticated* - card-application authentication + Protected
- *Mutually-authenticated* - card-application authentication + Source-authenticated + Protected

Characteristics and Mechanisms

- confidential – eavesdropping prevented across the specific channel segment (mechanisms)
  - confidential-trusted-channel
  - loyal-platform
  - loyal-channel

- data integrity – data integrity maintained across the specific channel segment (mechanisms)
  - MAC-trusted-channel
  - loyal-platform
  - loyal-channel

- source integrity – authentication of differential-identity used to access information (mechanisms)
  - client-application authentication (internal-auth)
  - client-application authentication (external-auth)

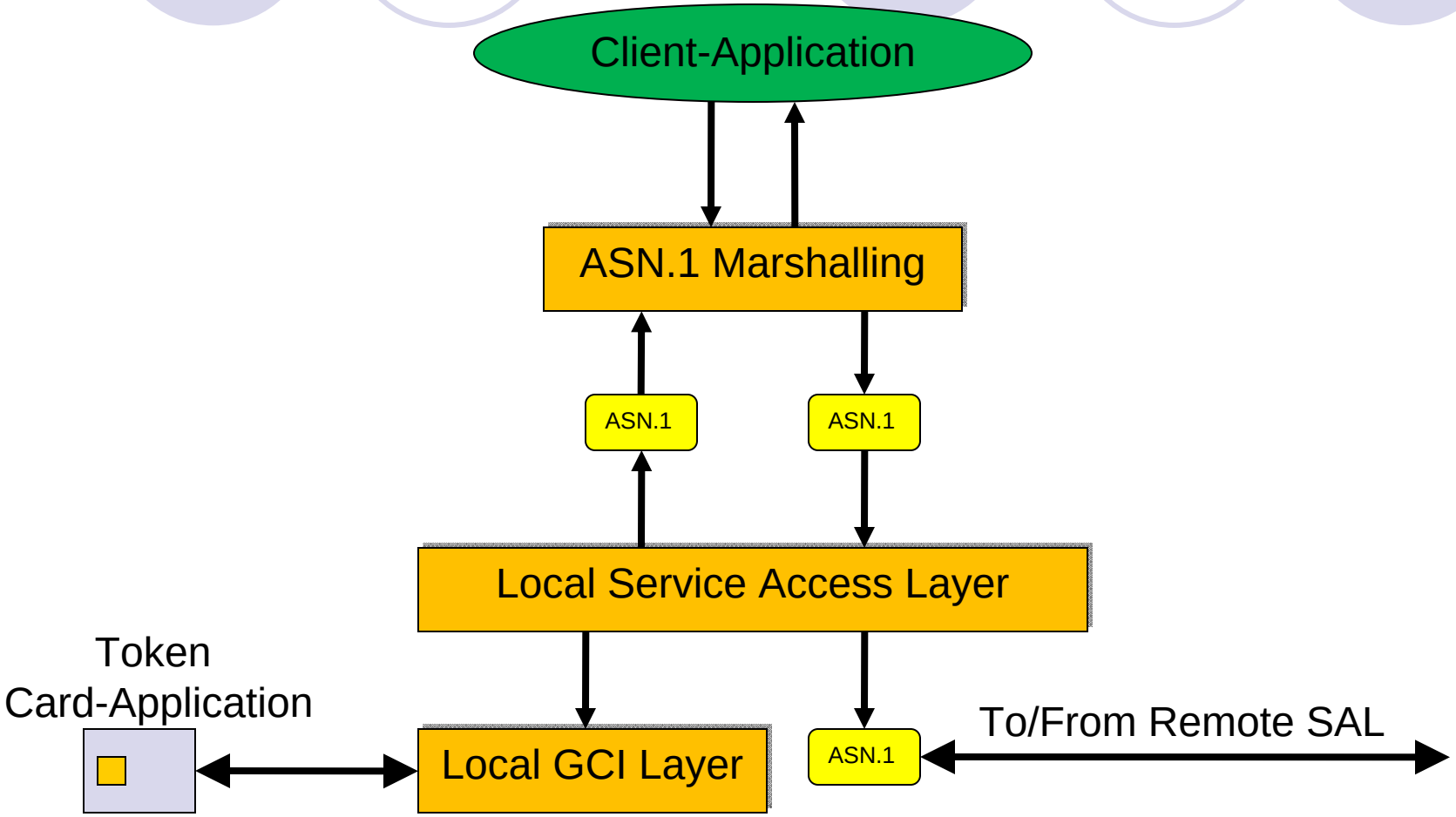
Most stringent security characteristics

Stack Configuration	Protected	Client Source	Mutual Auth
Loyal	End-to-end	End-to-end	End-to-end
Full-network	Segmented	Segmented	Segmented
Opaque-ICC	Segmented	Segmented	Segmented
Remote-loyal	Segmented	Segmented	Segmented
ICC-resident	End-to-end	End-to-end	Segmented
Remote-ICC	End-to-end	End-to-end	Segmented

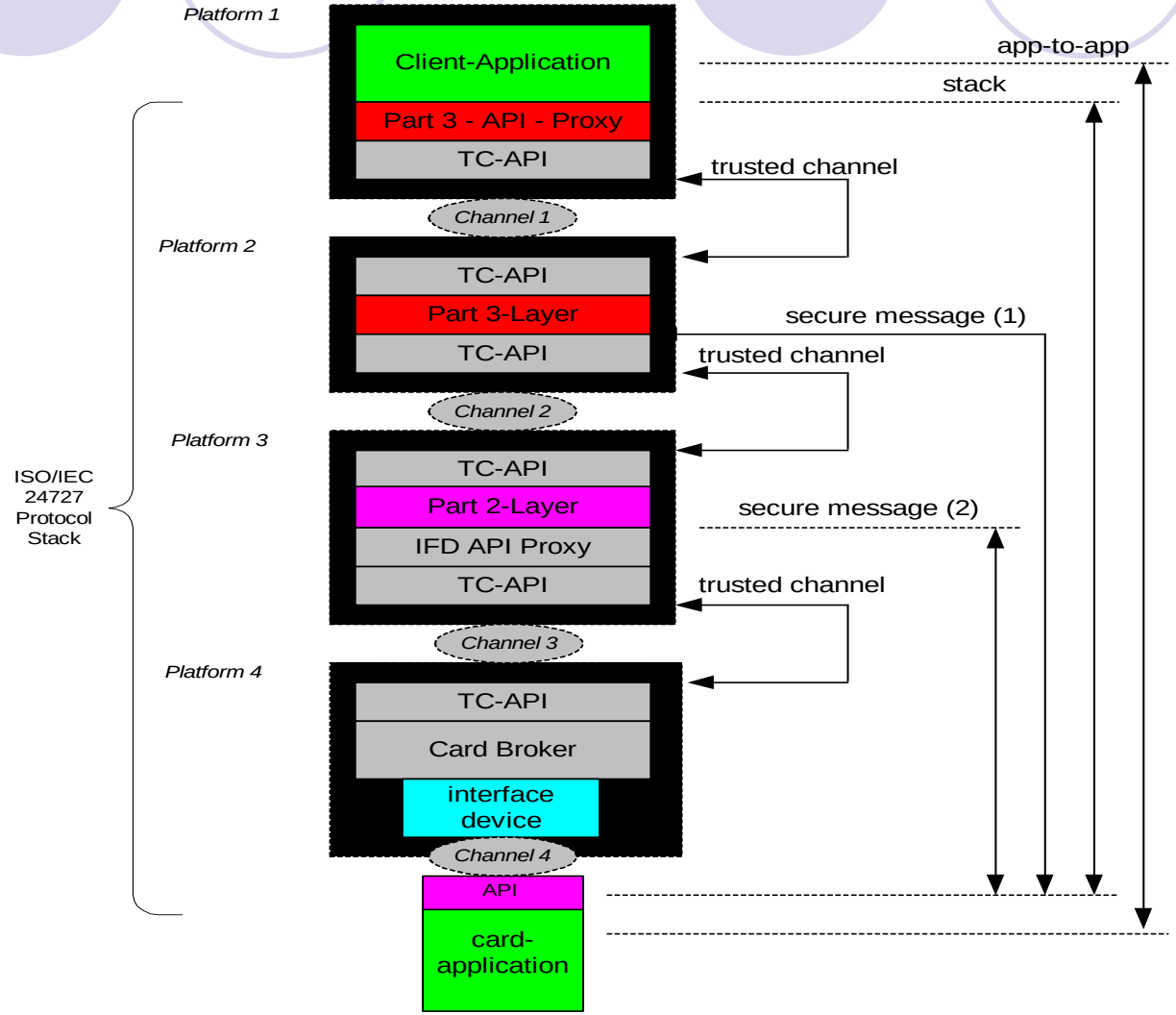
Flexible Stack Configurations

- ISO/IEC 24727 Generic Stack
- Loyal Stack
- Remote ICC Stack
- ICC Resident Stack
- Opaque ICC Stack
- Remote Loyal Stack
- Full Network Stack

Accessing SAM & Remote ICC Stack

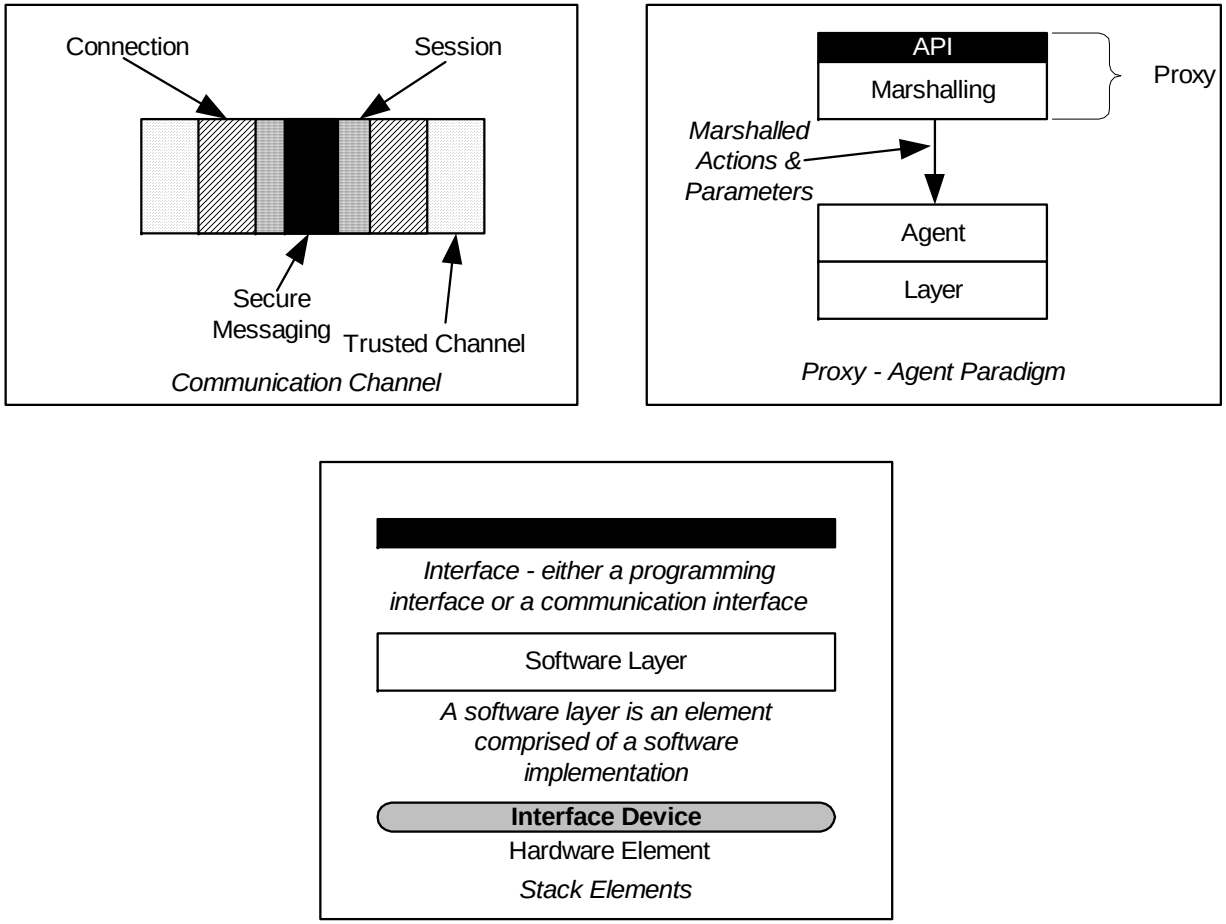


ISO/IEC 24727 Generic Stack

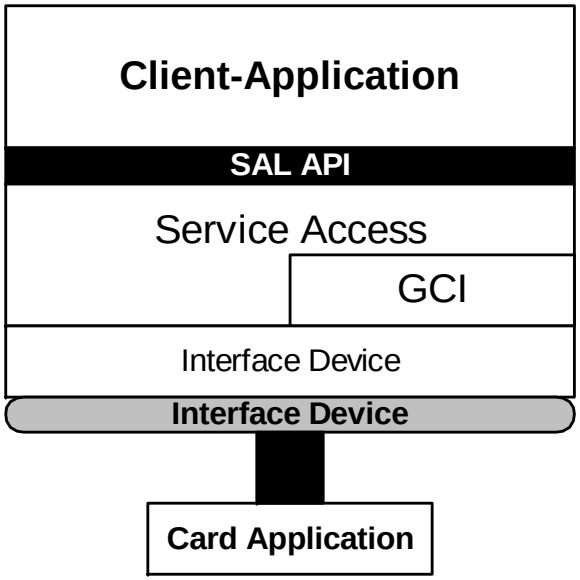


Stack Legend

Figure Legend



Loyal Stack



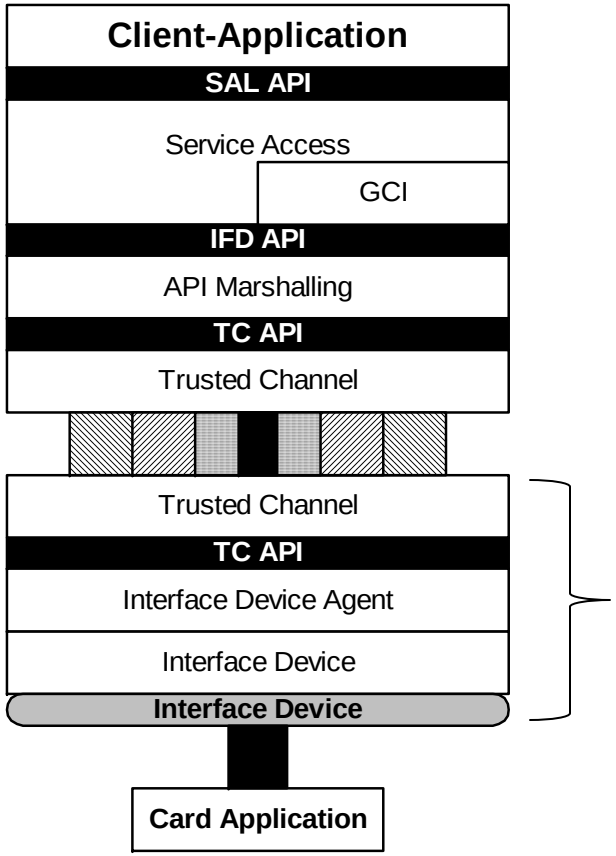
Stack Configuration

The most common current smart card stack configuration

Two interoperability points:

- at the SAL API
- at the card-application

Remote ICC Stack

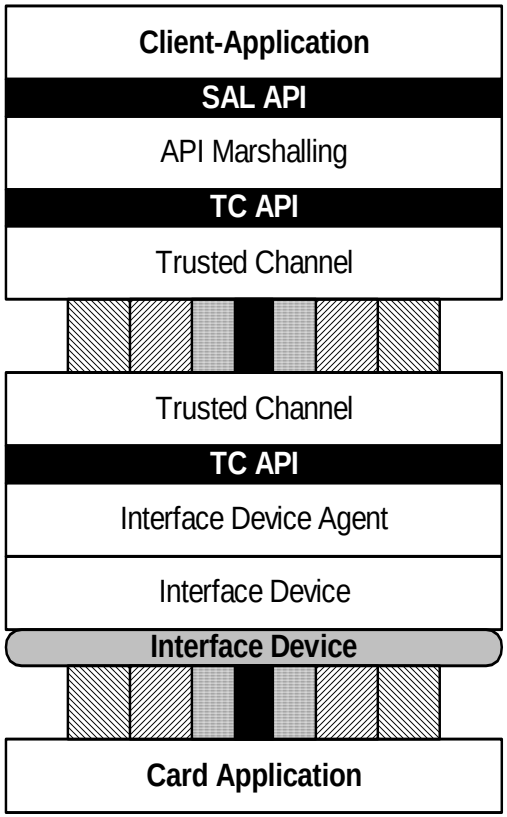


Stack Configuration

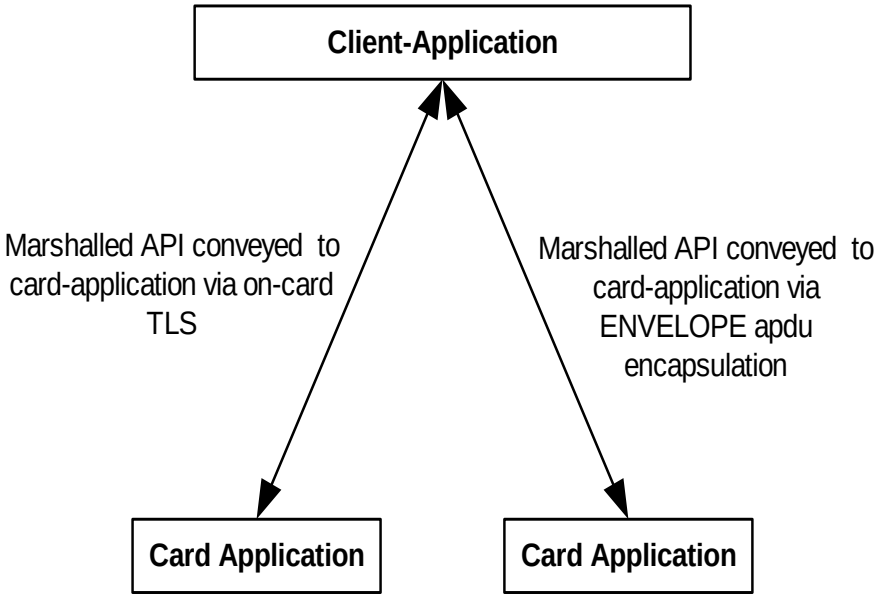
This configuration closely matches a GlobalPlatform remote configuration

Remote platform can be adversary

ICC Resident Stack

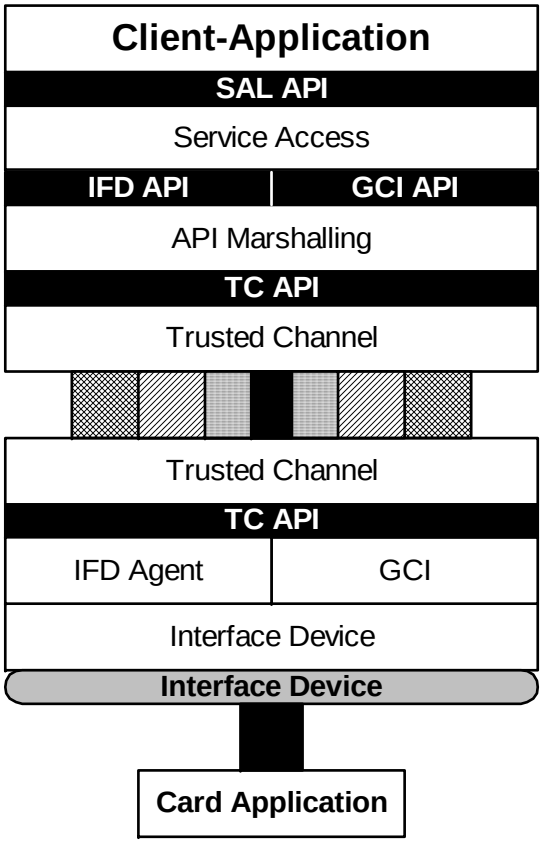


Stack Configuration



Two path mechanisms between client-application and card-application

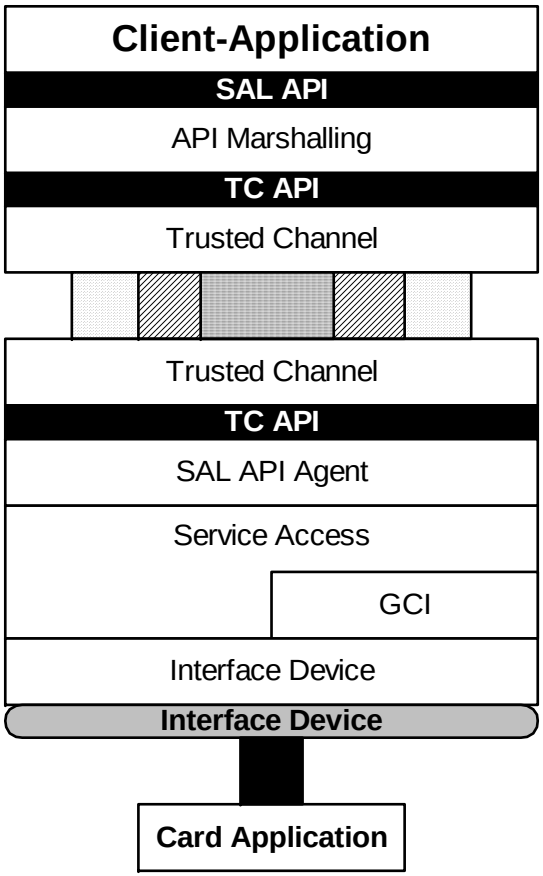
Opaque ICC Stack



Stack Configuration

This configuration supports a POS Terminal based on a GCI interface

Remote Loyal Stack

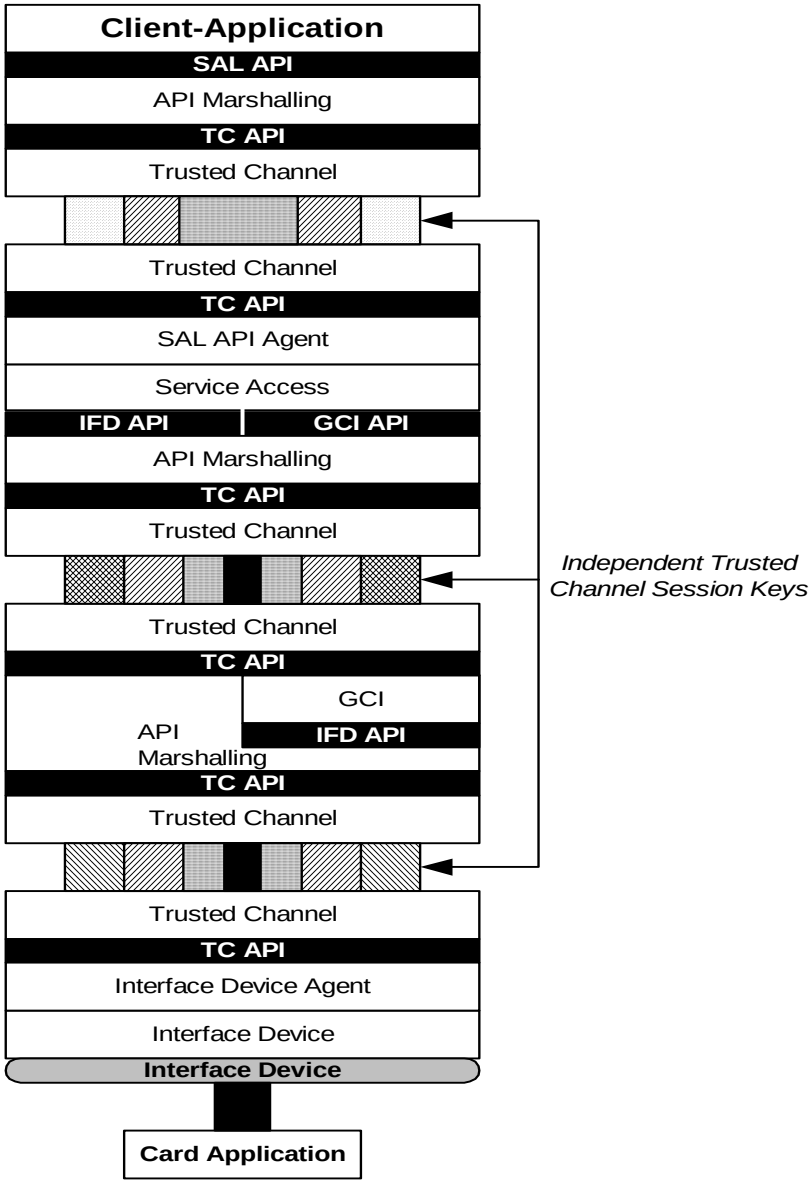


Stack Configuration

This stack configuration supports a very
High level terminal architecture
e.g. a cell-phone application serving
As an IAS service provider

Full Network Stack

A configuration aimed at testing



Stack Configuration

QUESTIONS?