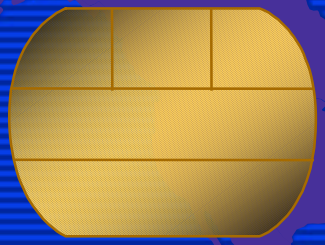
Open Platform Development



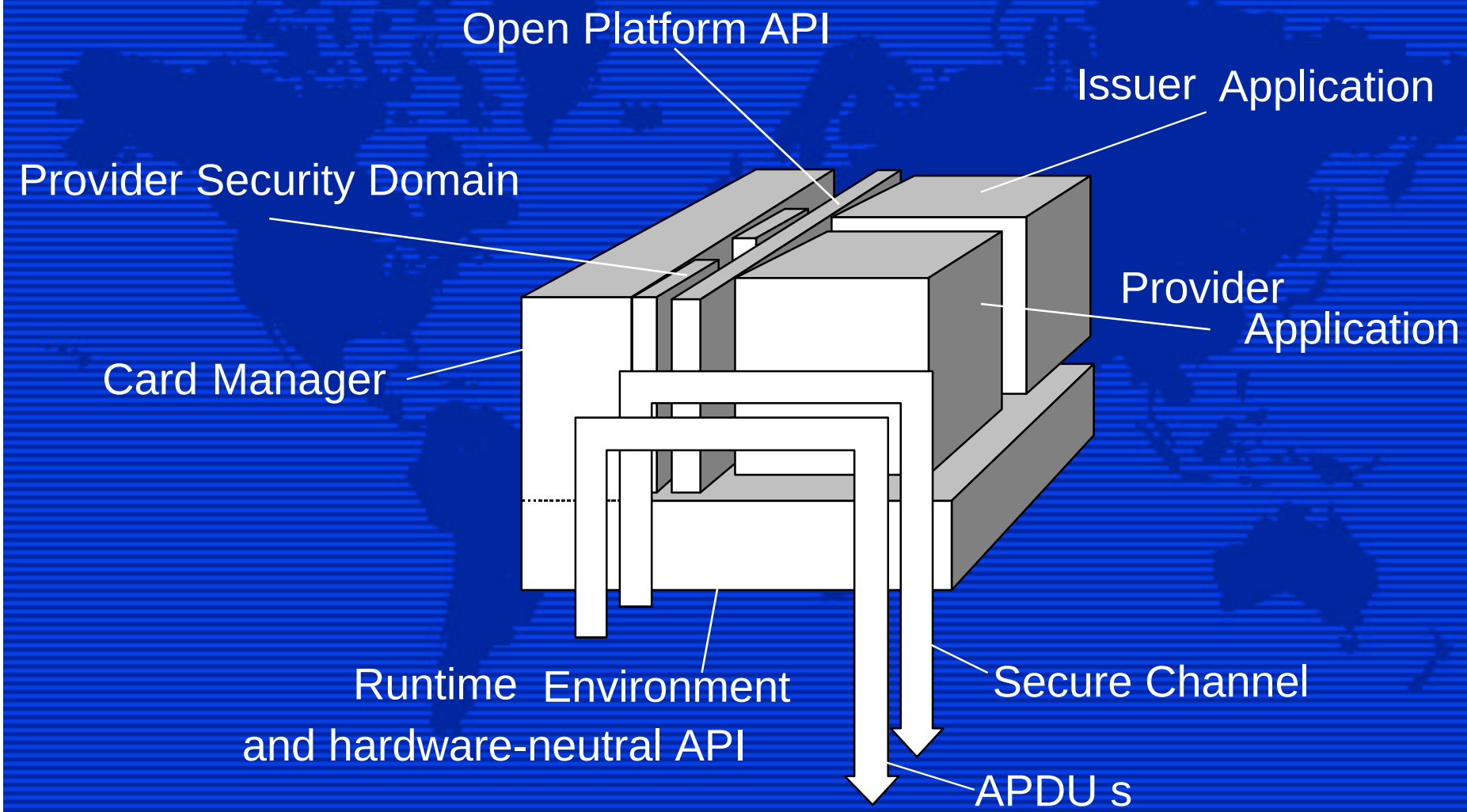
THE OPEN PLATFORM PROTECTION PROFILE (OP3) TAKING THE COMMON CRITERIA TO THE OUTER LIMITS

Marc Kekicheff,
Forough Kashef,
David Brewer

Introduction

- Open Platform is a cross industry standard for multi-application reconfigurable smart cards
- OP may be viewed as an extension to JavaCard™ / Windows for Smart Card[R]
- OP3 is essential to prove trustworthiness worldwide
- OP3 follows SCSUG example and use CC
- Not without many challenges

The Open Platform Specification



OP Configurations

	OP Functionality				Cryptographic Support	
Configuration/ Feature Set	Card Manager	Security Domains	Delegated Management	DAP Verification	DES	RSA
Configuration 1a	X				X	
Configuration 1b	X	X			X	
Configuration 1b*	X	X		X	X	
Configuration 2a	X	X	X		X	X
Configuration 2b	X	X	X	X	X	X

Provides Secure Channel and Global PIN services to applications

Security Assumptions

VISA

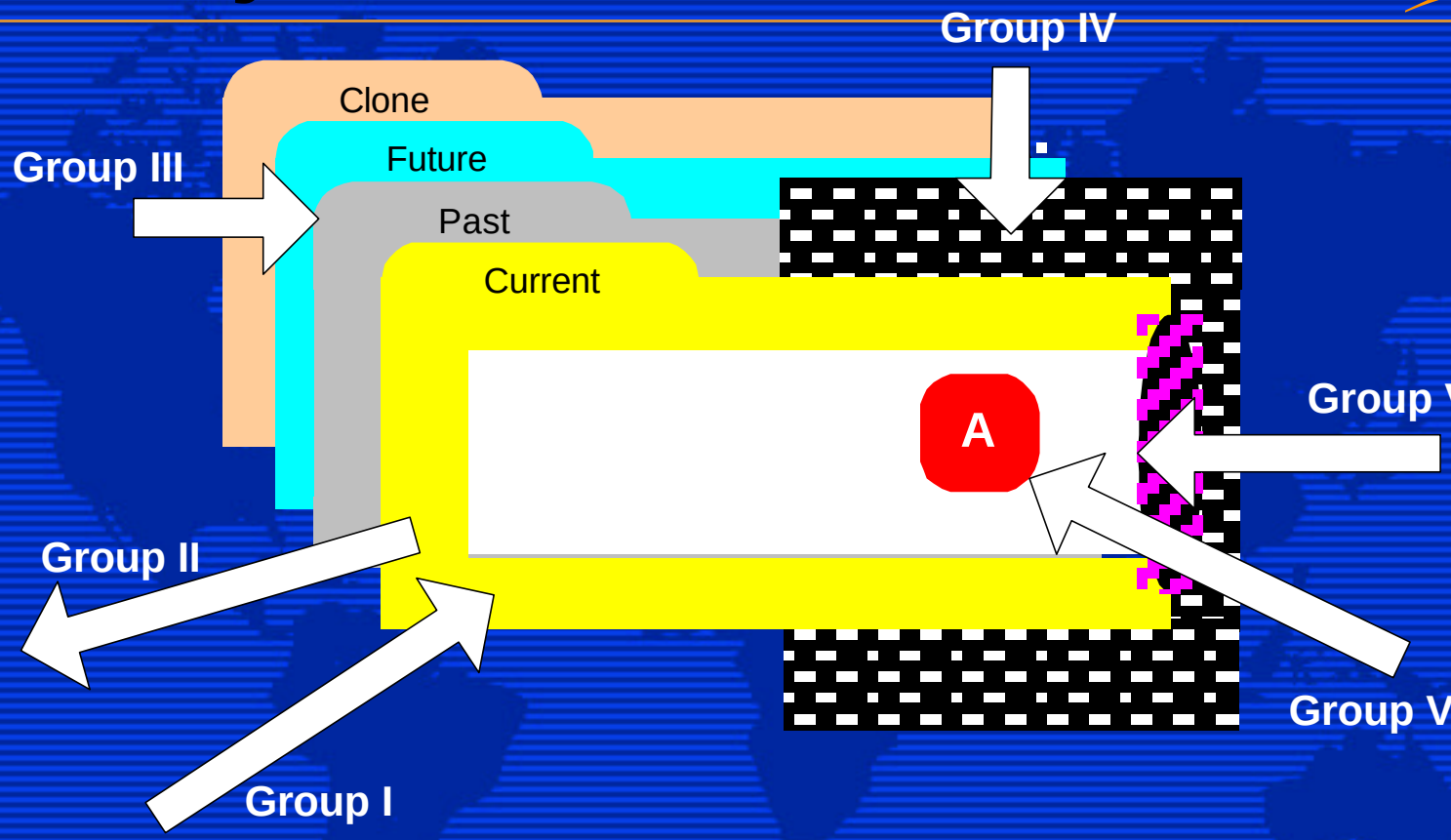
- OP merely a component
- Need to trust
  - back-office systems
  - cryptographic key management
  - byte code verification
  - card/chip operating environment (COE)
- Assumptions expose vulnerabilities that OP cannot protect itself against

The COE Assumption

VISA

- Tamper resistant
- Resistant to DPA, etc.
- Facilitates OP recovery
- Reports exceptions to OP
- Prevents bypass, etc. of OP security
- Enforces applet separation
- Provides object re-use

Security Threats



KEY

IC

RTE/OP/applications

CAD, incuding power etc

A Post issuance downloaded application

Card - CAD interface

Security Functions

- Extensive access control rules (discretionary and mandatory)
- Intrusion detection, Secure recovery
- Cryptography
  - host-card authentication, key confidentiality, message authentication, message encryption, MAC chaining
  - receipt generation and token verification

The Open Platform Profile (OP3)

- Usual structure
- In-line application notes and rationale statements
- Appendices on COE and applications
- Bags of refinement, lots of iterations

The TSF shall perform **delegated management receipt generation** in accordance with a specified cryptographic algorithm **(3-DES)** and cryptographic key **of double key length** that meet the following: **ANSI X9.52, FIPS 46/3 and OP Specification, paragraphs 7.9.2, 7.9.4, 7.9.5, 11.1, 11.1.3, 12.1.2.3, 13.9, 13.9.1, 13.9.2 and 13.9.3**. FCS_COP.1+7.1

Optional Components

- 2 categories choice of function or implementation detail
- Tried families of PPs - 10 profiles! Or a complex single document
- Packages work much better
  - Basic package +
  - Delegated Management
  - DAP Verification
  - Global PIN
- Selections for implementation choices

COE Specification (1)

- How do you deal with the COE?
  - Reference a PP (e.g. SCSUG-SCPP)?
  - Incorporate all the detail?
  - Provide a specification?
- Specification wins:
  - Including COE detail increases costs
  - Don’t have to track changes in other PPs
  - Don’t have to deal with the RTE API for applets

COE Specification (2)

- The COE specification:
  - COE assumption --> security objectives
  - Min TSFs necessary to meet objectives
  - Map to SCSUG-SCPP threats
- Need to ensure evaluators test the validity of the COE assumption
- Use an integration PP to do this

The OP API

VISA

- Similar to COE challenge
- Augment the COE assumption:
  - Can't load/remove an application without proper authority
  - Authenticity/integrity of code verified on loading
- Invite direct reference to OP3
- Advice on who to invoke OP services using FIA_UAU etc, but security API components would be better

Other Observations

- Some CC components cover initiation of a service but not its termination
- Need to link OP and COE functions, e.g COE passes application exceptions to OP to lock application or card
- Both handled by application notes

Conclusions

VISA

- OP3 has stretched CC to the limits
- But OP Spec successfully recast
- Security APIs would ease the task
- Business benefits
  - MRA
  - separate evaluations possible
  - reconfigurable smart cards