

The GlobalPlatform Card Security Requirements Specification

Dr. David Brewer (Gamma Secure Systems Limited)

Marc Kekicheff (GlobalPlatform) &

*dbrewer@gammasl.co.uk
www.gammasl.co.uk*

*kekichef@globalplatform.org
www.globalplatform.org*

Agenda

Introduction

Card Security Requirements Specification

Security Function Requirements

Off-card Policies

Operational Risk Management

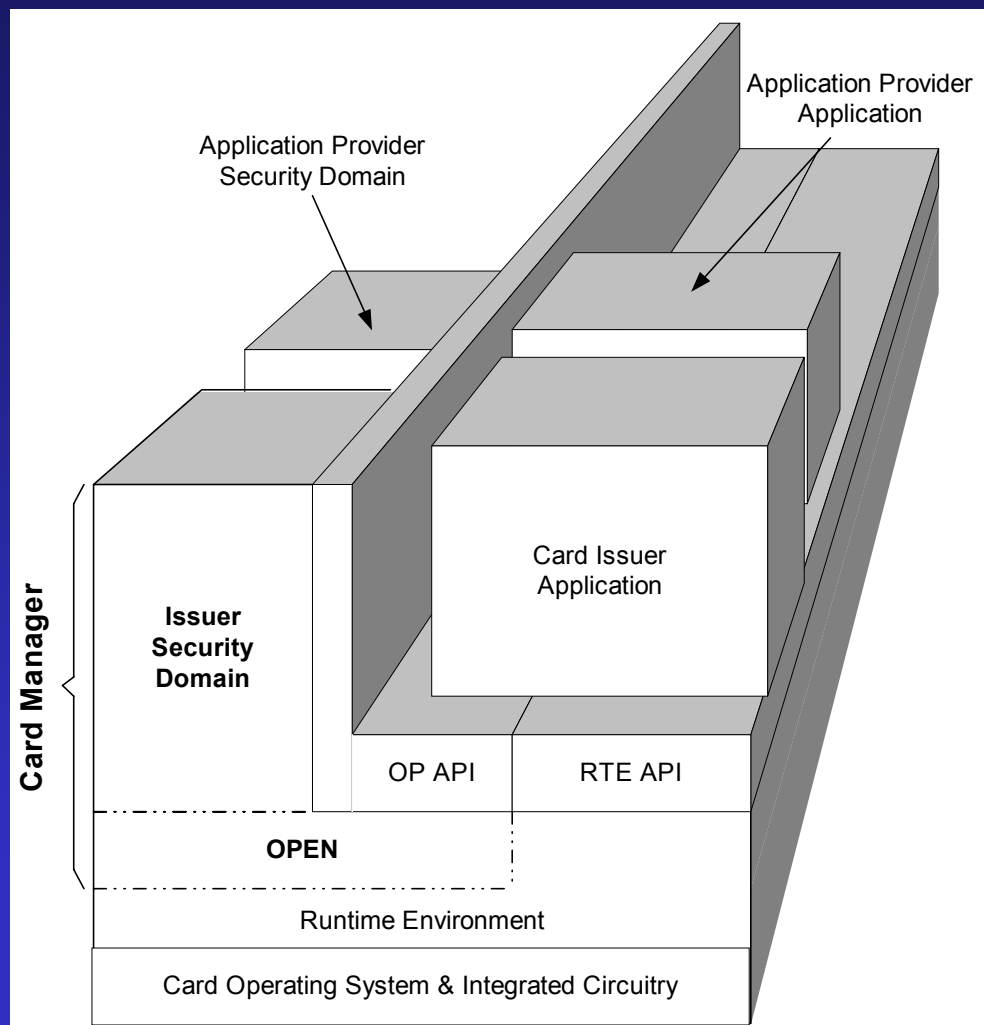
Summary

Introduction

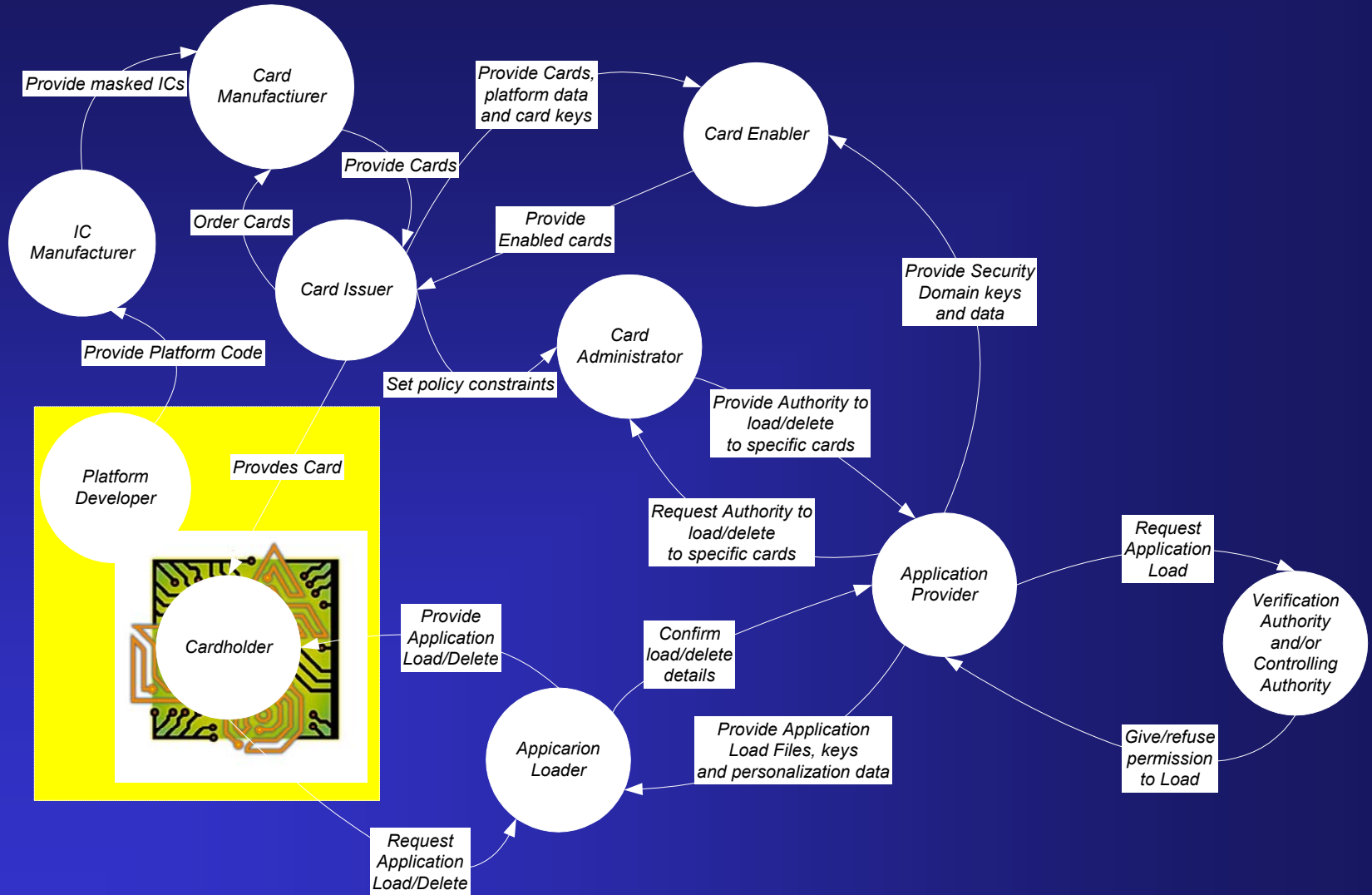
Note: you can download the Card Security Requirements Specification (CSRS) from:

www.globalplatform.org/specifications2.asp

The GlobalPlatform Smart Card

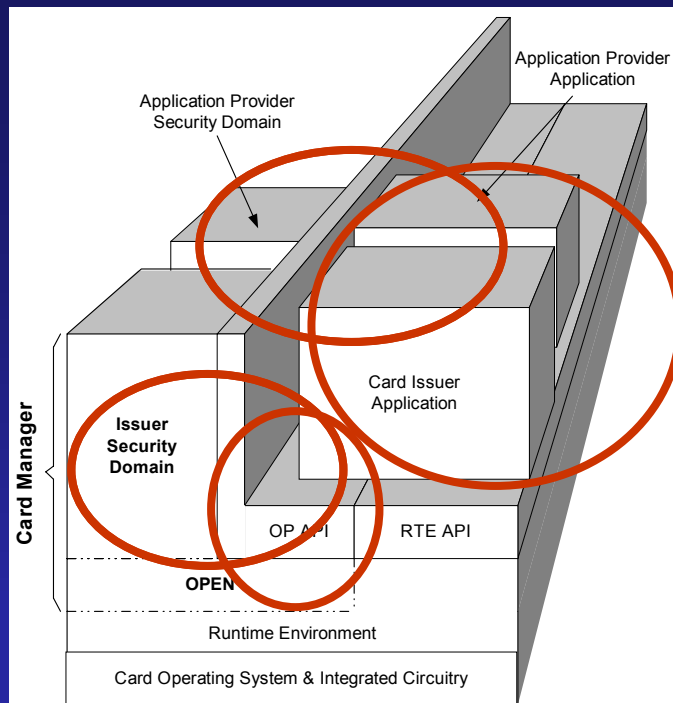


Actors and Roles



Users

- Card Administrator
- Security Domain User
- Application
- Cardholder
- Unknown (GETDATA)



Packages

37 functional packages:

1. Core

2.7 ISD Packages

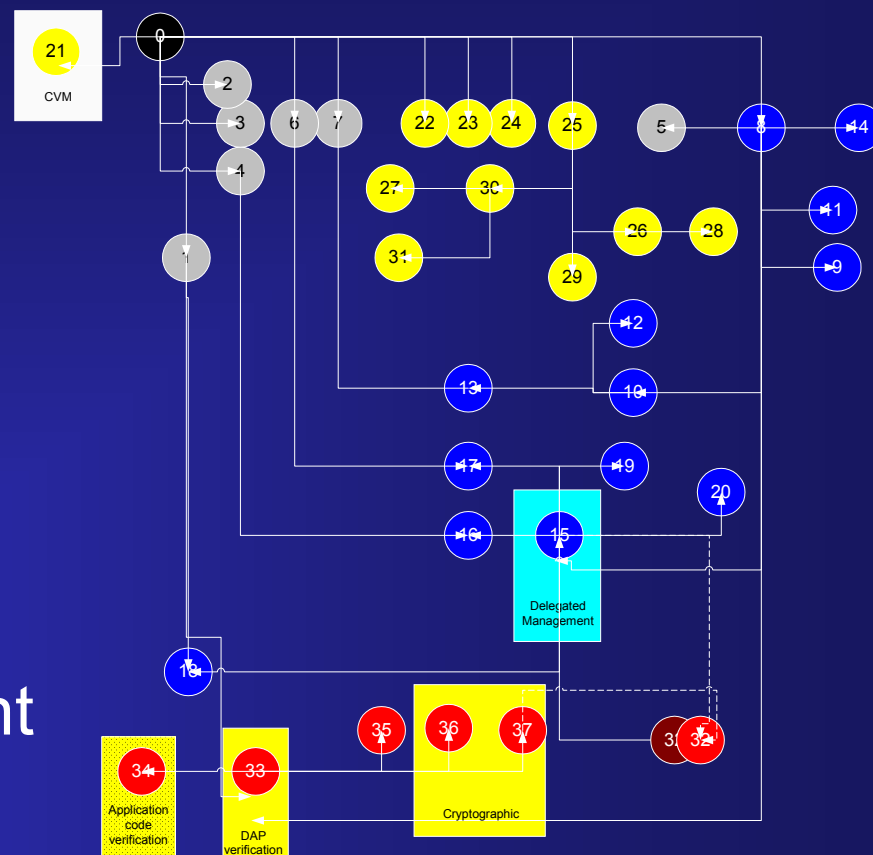
3.13 SD Packages

4.11 SCP Packages

5.6 others

Allows card configuration to be tailored to suit business/risk environment

Causes problems with PPs



Card Security Requirements Specification

Card Security Requirements Specification

Scope includes IC, OS, RTE and GP

Security features comply with the Card Specification, SCSUG, SSVG & JCSPP

Assets enumerated in detail (data dictionary)

Threats (based on SCSUG augmented to cover OP3)

No objectives or assumptions, just policies

Covers all possible card configurations

Semiformal definition of security functions

Security Function Requirements

Function Tables (Access Control)

Usual stuff: users, subjects, objects, attributes, operations, Y/N outcome

Users(s):	Unknown user		
Subject(s):	Security Domain		
Precondition:	A Security Domain shall be the currently SELECTED Application, but a Secure Channel Session is not in progress.		
Short Form:	Unknown_user and command_syntax_OK	Link backs(s):	Table 5-22: The Secure Channel Security Feature (Security Policy)

Security Precondition

(FDP_ACF.1/SCSUG) Security attribute based access control

The TSF shall enforce the (assignment) *access control SFP* to objects based on (assignment) *security attributes, named groups of security attributes*. FDP_ACC.1.1 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: (assignment) *rules governing access among controlled subjects and cont.*

FDP_ACF.1.2 The TSF following addition *authorize access* subjects to objects *that explicitly den*

Operation(s)	Object(s)	Security Attribute(s)	Rule(s)
N		N/a	A GPCS general error condition shall not exist for the COMMAND

Group 6	Security Domain Access Security Feature	
	FDP_ACC.1, FDP_ACF.1, FMT_MOF.1, FMT_MSA.2, FMT_MTD.1, FMT_MTD.3, FDP_ACC.2**	P.DATA_ACC, P.FILE_STR, T.ACCESS, T.BRUTE-FORCE, T.FIRST_USE, T.FLT_INS, T.INV_INP, T.LINK, T.LNK_ATT, T.UA_LOAD

The request is authorized.
This table links to Table 5-14: Other Card Management Functions in order to perform the
Security Post
tion(s)
of APDU response message is E-card entity.

Function Tables (e.g. APDU Commands)

No users or subjects, just operations and objects – access controls decision already made

Function can still fail

<p>Precondition: The Issuer Security Domain Access Security Feature (Table B), or the Token Verification Security Feature shall have authorized the request.</p> <p><u>This table forms part of the Core Package.</u></p>			
<p>Short Form: Request_authorized</p>		<p>Link back(s):</p> <ul style="list-style-type: none"> ❑ Table 5-2: The Issuer Security Domain Access Security Feature (Table B) ❑ Table 5-9: The Token Verification Security Feature 	
Operation(s)	Object(s)	Security Attribute(s)	Rule(s)
<p>INSTALL [FOR INSTALLABLE] ⁸¹</p>	APPLICATION	GP REGISTRY, GP REGISTRY [ASSOCIATED SD], SD [AID]	(The COMMAND [DATA: EXECUTABLE LOAD FILE AID] shall exist in GP REGISTRY) <u>and</u> (the COMMAND [DATA: APPLICATION AID] shall not yet exist in the GP REGISTRY) <u>and</u> (the resource requirements for the APPLICATION installation shall be available) <u>and</u> (the COMMAND [DATA: INSTALL PARAMETERS] resource requirements when present shall be available ⁸²).
<p>INSTALL [FOR MAKE SELECTABLE] ⁸³</p>	APPLICATION	GPREGISTRY, GP REGISTRY [APPLICATION LIFE CYCLE STATE]	(The COMMAND [DATA: APPLICATION AID] shall exist in GP REGISTRY) <u>and</u> (the GP REGISTRY [APPLICATION LIFE CYCLE STATE] shall be INSTALLED).
<p>Result (rule evaluates to true):</p>		<p>The requested operation is performed successfully (i.e. without error).</p> <p>The GP REGISTRY is updated accordingly.</p> <p>If a receipt is required, this table links to Table 5-10: The Receipt Generation Security Feature.</p>	
<p>Result (rule evaluates to false):</p>		<p>The requested function fails. The appropriate GPCS error APDU response message is returned to the requesting off-card entity.</p> <p>This table links to Table 5-45: The Failure Management Security Feature to rollback the failed function.</p>	

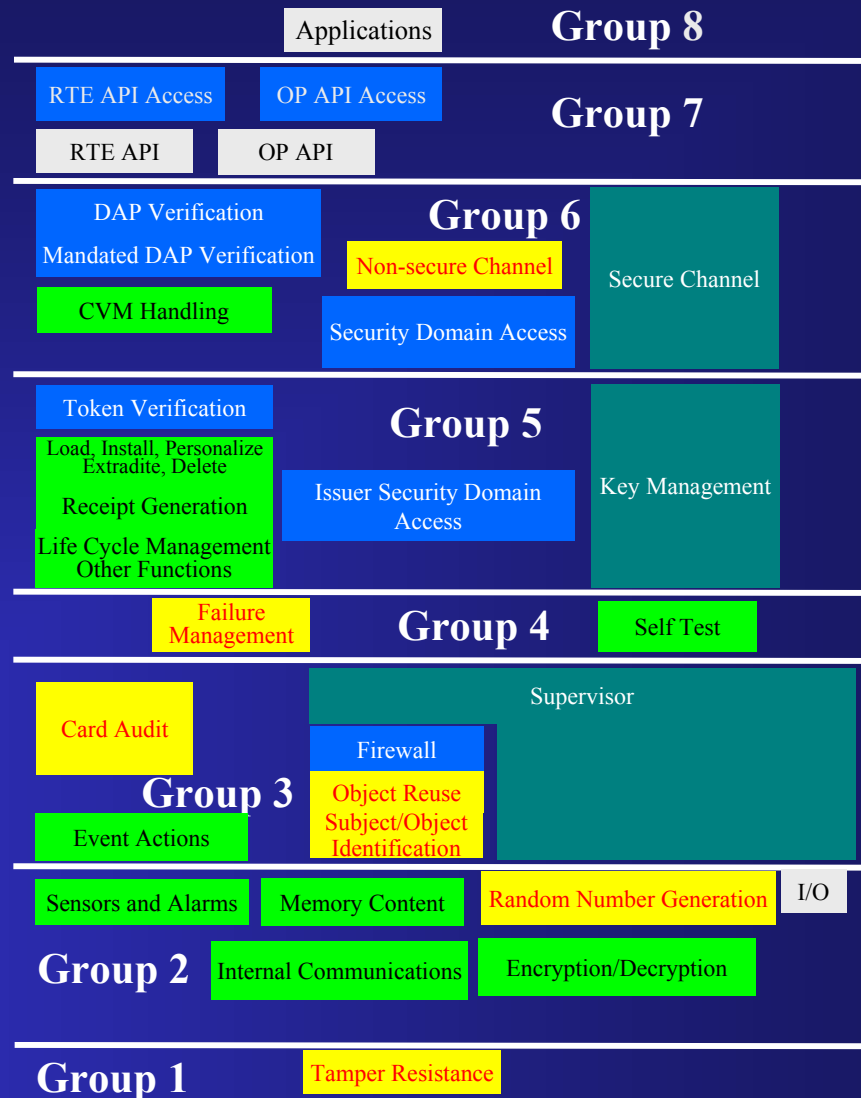
Table 5-5: The Card Content Management Security Feature (Install and make selectable)

Function Tables (Transformation functions)

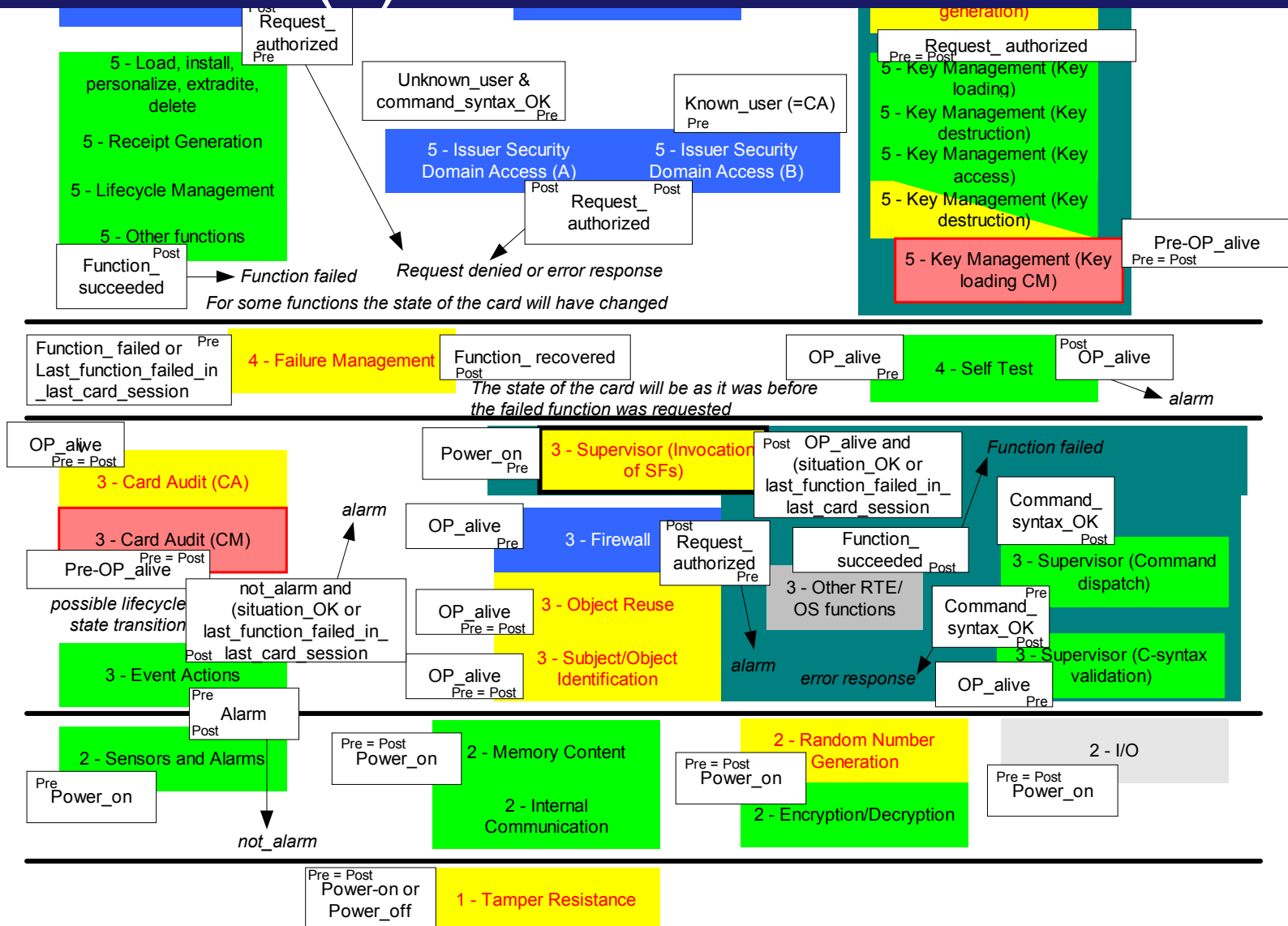
Failure modes are general (power failure, programming exceptions etc) and are dealt with by other tables

<p>Precondition: The service is being called in attempt to open a Secure Channel Session for the Card Administrator or a particular Security Domain User.</p> <p><u>This table forms part of the Core Package.</u></p>		
<p>Short Form: Known_user Link backs(s): Table 5-23: The Secure Channel Security Feature (Secure Channel Initiation)</p>		
Operation(s)	Input Object(s)	Output Object(s)
Generate	Key [SCP Static] ¹⁰² , DATA [DERIVATION DATA]	Unique Key [SCP Session: S-ENC], Key [SCP Session: S-MAC] ¹⁰³ generated in accordance with GPCS ref <i>d</i> .
<p>Table 5-13: The Key Management Security Feature (Key Generation Services)</p>		

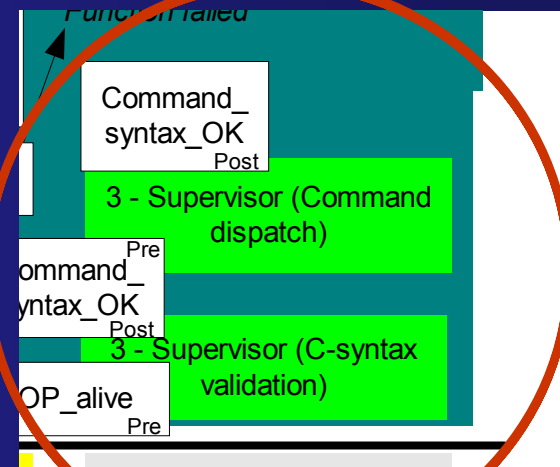
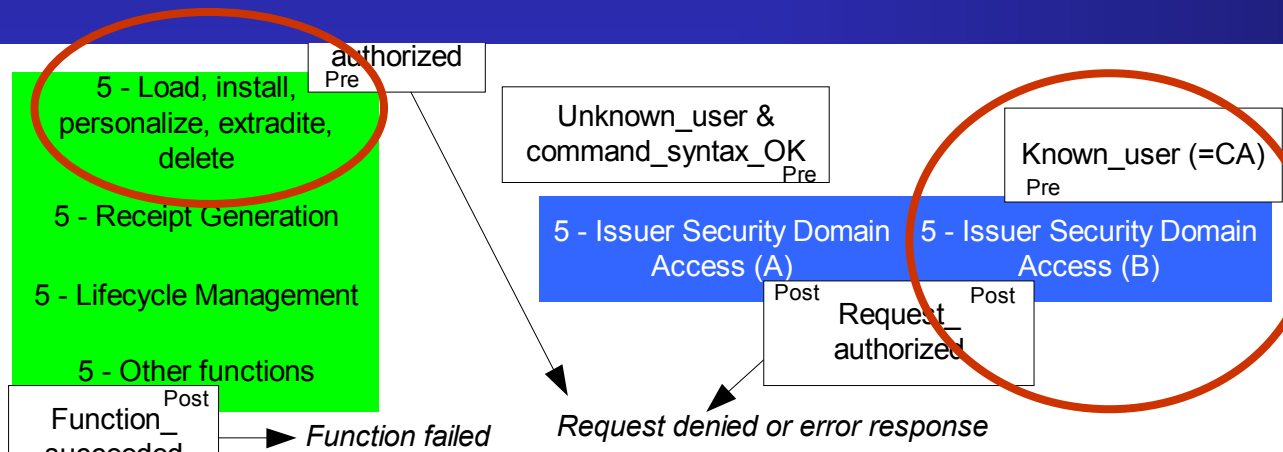
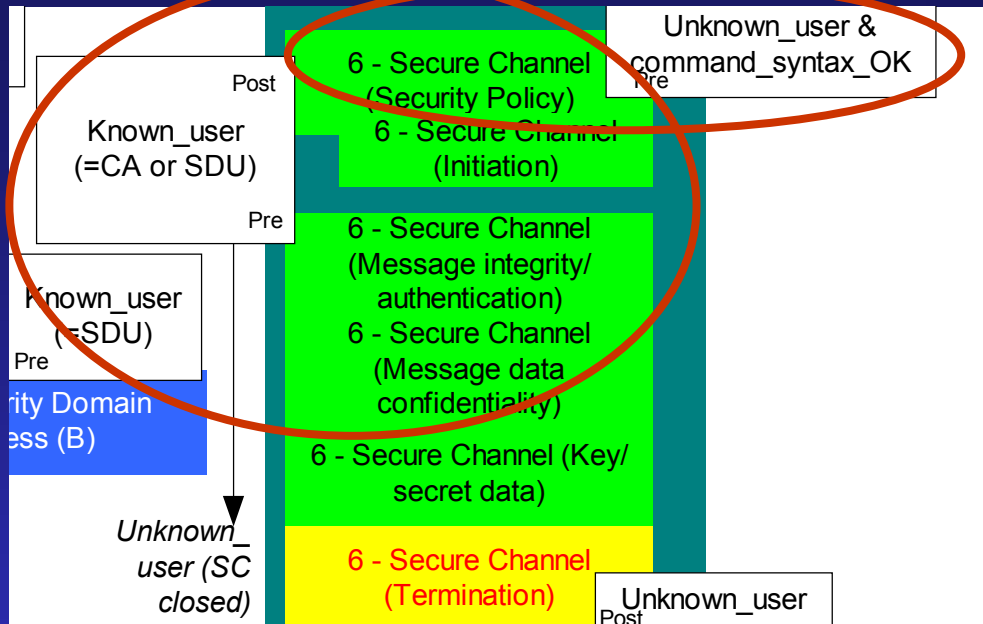
Security Architecture



The Detail (2)



Install [for Install] Example



Failure Management

Bad APDU Commands, or insufficient privilege

- Request denied, error response

Request authorised

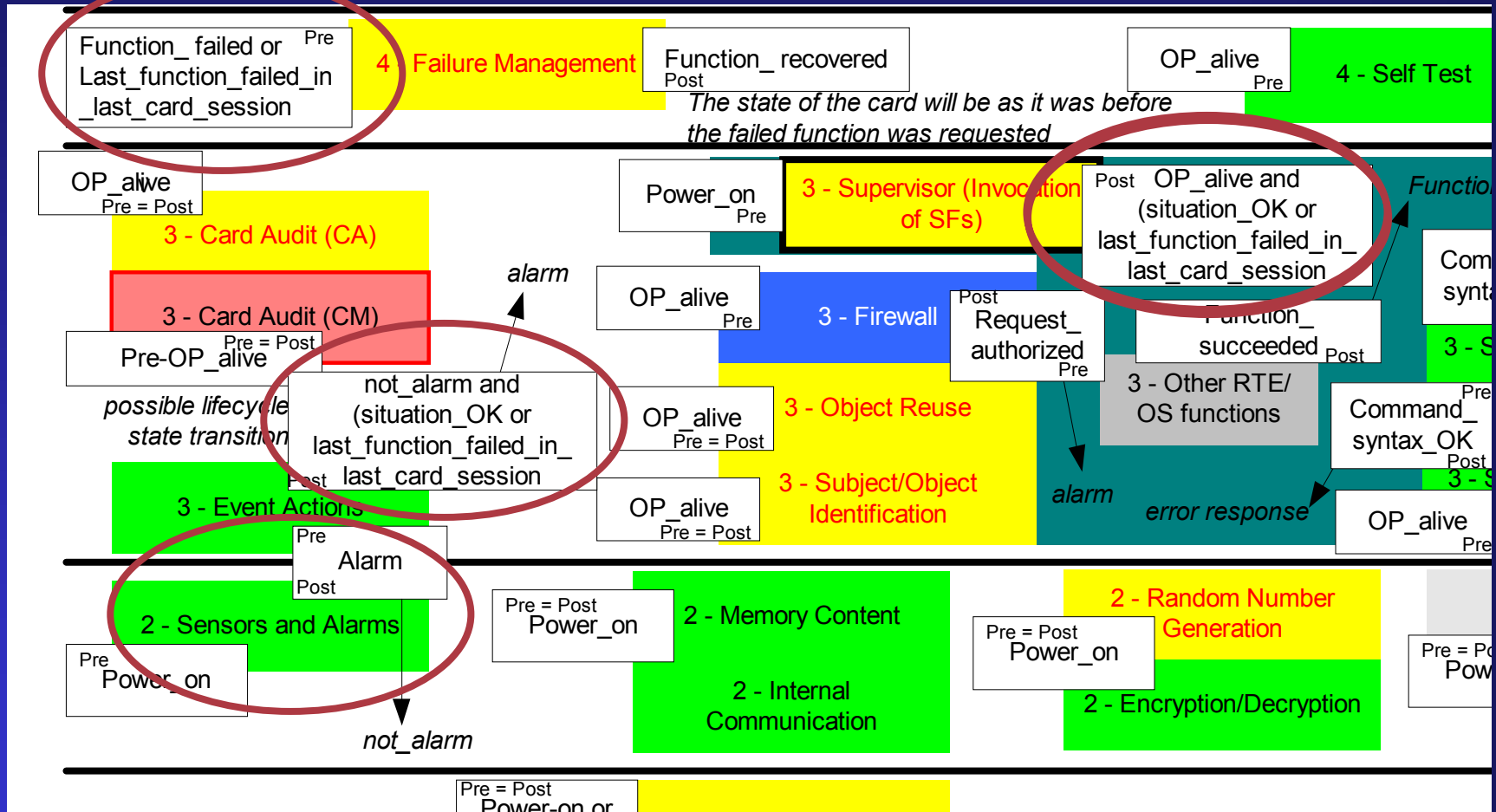
- Function failed or function succeeded

Alarm conditions

- Raised by Event Actions, Firewall, Failure Management, Sensors&Alarms, Applications

Event Actions is re-entrant

Power Failure Example



Summary

Three types of table

- Access control
- Regular functions (e.g. ADPU commands)
- Transformation functions

All mapped to SFRs, threats & policies in SC PPs

Dynamics handled by the pre/post conditions

Easy navigation via hyperlinks in CSRS

Tables act as autonomous processes

Could serve as the basis of a formal model

Off-card Policies

Policy

Policies define off-card requirements and select optional on-card functionality:

4.2.1 The P.ROLES Policy

When an off-card entity selects the Issuer Security Domain and is successfully authenticated, the off-card entity shall act on the authority of the Card Administrator (who is, for the majority of the card's Life Cycle, the Card Issuer, see 3.1).

When an off-card entity selects a Security Domain and is successfully authenticated, the off-card entity shall act on the authority of the Security Domain User (being the Application Provider, Controlling Authority, or Verification Authority) who owns the Security Domain concerned.

This policy fragment states what has to happen off-card

Alternative Policy Statements

Some CSRS policies have alternatives:

4.3.4 The P.APPLICATION_CODE_VERIFICATION Policy

Alternative policy statement 1: Byte code verification, or any other form of Application Code Verification is not required.

Alternative policy statement 2: Byte code verification and other forms of Application Code Verification is a requirement and shall always be carried out successfully prior to Application Load File on-card installation. This shall take place off-card. Application Code Verification shall at least include the algorithms necessary to establish that the Application would pass all omitted runtime checks.

Alternative policy statement 3: Byte code verification and other forms of Application Code Verification is a requirement and shall always be carried out successfully prior to Application Load File on-card installation. This shall take place off card **and shall be confirmed by using a Security Domain with Mandated DAP Verification privilege**. Application Code Verification shall at least include the algorithms necessary to establish that the Application would pass all omitted runtime checks.

Alternative policy statement 4: Byte code verification and other forms of Application Code Verification is a requirement and shall always be carried out successfully prior to Application Load File on-card installation. **This shall take place on-card**. Application Code Verification shall at least include the algorithms necessary to establish that the Application would pass all omitted runtime checks.

These reflect the different ways in which the card may be used, with on- and off-card requirements

Dependencies

Alternative policy statements require presence of particular functionality “packages”

Package G (DAP support): This package requires Package A (Card content loading extra Security Domains). It allows a Security Domain to have DAP Verification prevent the loading by the Card Administrator (or a privileged Application Provider) of associated with that Security Domain.

This configuration selection is predicated on the following security policies:

- ❑ Alternative 1, 2, or 3 of the [P.APPLICATION_CODE_VERIFICATION](#) Policy,
- ❑ Alternative 3 of the [P.LOAD_FILE_VERIFICATION](#) Policy.

Packages identify required security functionality

Security Feature) according to SCP01 or SCP02 Secure Channel Protocol.

This table forms part of the Core Package¹⁴¹, but some operations are package dependent.
The actual dependencies are given in the footnotes.

Extract from Table 5-23

Operational Risk Management

How Policy is Decided

Risk Assessment

- Some risks unacceptable to GP under any circumstance
- Others may be decided by actors involved:

	Inclusion in the card configuration of the Package containing the security features necessary to mitigate the risk
Unacceptable risk	Must be included
Acceptable risk	May be excluded

1. Significance of impact versus cost of protection
2. Time delay between:
 - » Event and its detection
 - » Detection and subsequent action
3. Who detects and who corrects
4. Exposures of the actors concerned
5. Who are the actors
6. What is their legal relationship

Examples

[X detects, Y corrects]

Case 1 Actor X is exposed but Y is not

Case 2 Actor Y is exposed but X is not

Case 3 Both actors are exposed

Case 4 Neither actor is exposed

CSRS also considers cases with three actors, and gives rules/guidance

Policies and Packages

The above statements are true IF the following condition is met:

- ❑ The actor performing the card management operation must be authenticated. The [P.SECURE_COMMUNICATION](#) Policy – alternative policy statement 1 enforces such rule.

GPCS provides a security feature called “Secure Channel Protocol” ([Package N](#) or [Package S](#)) to implement this [P.SECURE_COMMUNICATION](#) Policy. A Secure Channel Protocol provides a means of communication within a local

Users(s):	Actor A		
Subject(s):	Card Platform		
Precondition:	Card Platform is in a secure state		
Operation(s)	Object(s)	Security Property(ies)	Rule(s)
MANAGE	CARD CONTENT, CARD STATE	AUTHENTICITY CORRECTNESS and COMPLETENESS	(Actor A’s Authenticity shall be proven) <u>and</u> (Operation’s Correctness and Completeness may be requested)
Result (rule evaluates to true):	The operation is completed. The card’s contents and/or state are updated. Card Platform is in a secure state.		
Result (rule evaluates to false):	The operation is aborted. The card’s contents and/or state are unchanged. Card Platform is in a secure state.		

Table 4-1: Security Rule for Simple Case

Business Decisions

Before the cards can be ordered

- What is the purpose of the card base?
- What actors are going to be involved?
- What applications will be loaded now?
- What applications may be loaded in the future?

Need in place for operational risk management (e.g. Basel II):

- Assurance in the card technology
- Assurance that the off-card policies are met and continue to be met
- Ability to detect and react to incidents

Implies a combination of:

- The Common Criteria and ISO/IEC 17799 & BS 7799-2:2002

Summary

Captures all requirements from Card Spec + 4 PPs

Could be used to generate Security Targets and adds precision to the requirement

Business-led approach to risk assessment:

- Considers what actors are involved, time to detect, correct...
- Determines card configuration
- Determines off-card policies

Demands assurance in operational risk management