Book đọc đi kèm: - Book A

* Book B.

Chapter 1: general information

Chapter 2: model, the basic for architecture of the POS system.

Chapter 3: configuration.

Chapter 4: organization of kernel data.

Chapter 5: commands and responses

Chapter 6 and 7: processing

Chapter 8: security processing.

POS system: chỉ Reader và terminal.

Kernel chứa một set of functions cung cấp tất cả quá trình xử lý logic và data cần thiết để thực hiện giao dịch..

* Chức năng của Terminal:

Business logic để xác định transaction amount và transaction type: transaction amount thường thị sẽ được xác định trước giao dịch và là một con số cố định.

Online authorization và transaction logging:

Processing final outcome.

Phân tích nội dung của card: security check để xác nhận tính đúng đẵn và ủy quyền của data trong card.

Merchant input and display.

* Chức năng của reader:

Giao tiếp với card.

Tin nhắn led/audio, language, có thể bao gồm cả message. Selection of card application.

Complete interaction with card.

Quản lý data exchange giữa kernel và terminal: cho phép kernel gửi tagged data và yêu cầu từ terminal.

Xử lý outcome mang lại bởi kernel: kernel chỉ ra transaction sẽ approved offline, declined offline

Kernel activation

CVM selection,

Management of “no card response” timeout.

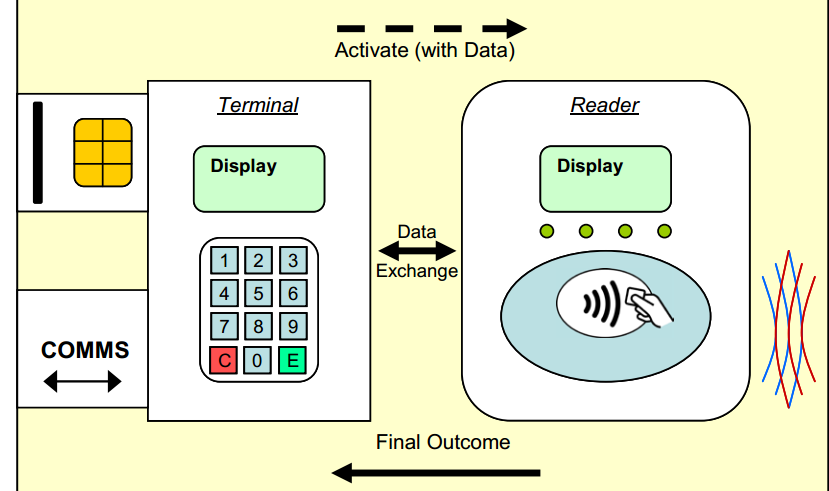
* Simple payment transaction

Require only the exchange of two signals:

ACT signal: để activate Reader, chứa các thông số như: transaction amount, transaction type. Trong một vài trường hợp thì không cần signal này nếu như reader được config là transaction automatically starts after previous transaction.

The OUT signal: bao gồm có các thông tin: approved, online request, declined, end of application. CVM được áp dụng cho terminal,

**READER and TERMINAL**

****

Cả reader hay terminal đều có display.

Câu hỏi: Reader database

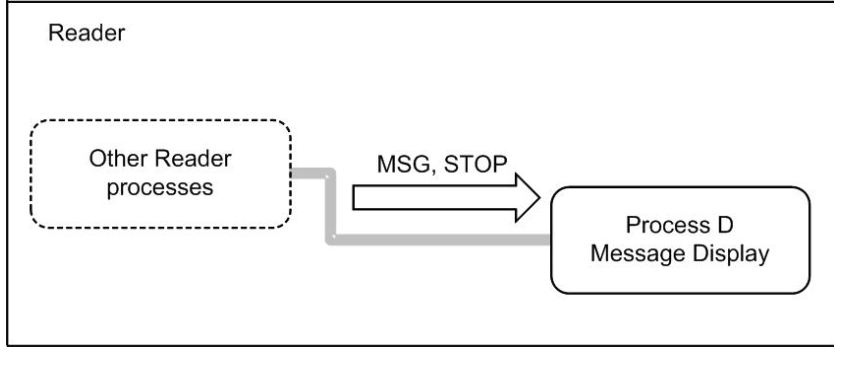
|  |  |
| --- | --- |
| Process M | Kiểm soát tổng thể và trình tự các quá trình. Configuration và activation, quá trình outcome. |
| Process D | User interface |
| Process S | Chọn ứng dụng của card. |
| Process P | Contactless interface |
| Process K | Giao tiếp với card một khi selection ok |

* Process P

Bao gồm reset field, polling, error indicator, removal procedure, collision detection,

* Process D

Quảng lý user interface request cụ thể là thông báo.



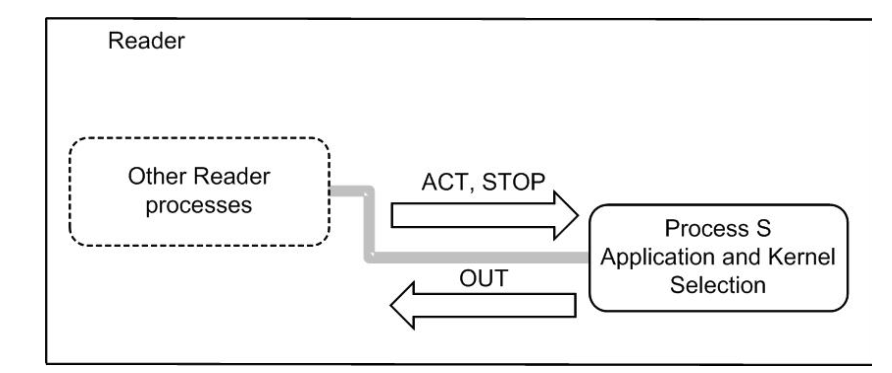
STOP signals sẽ clear display.

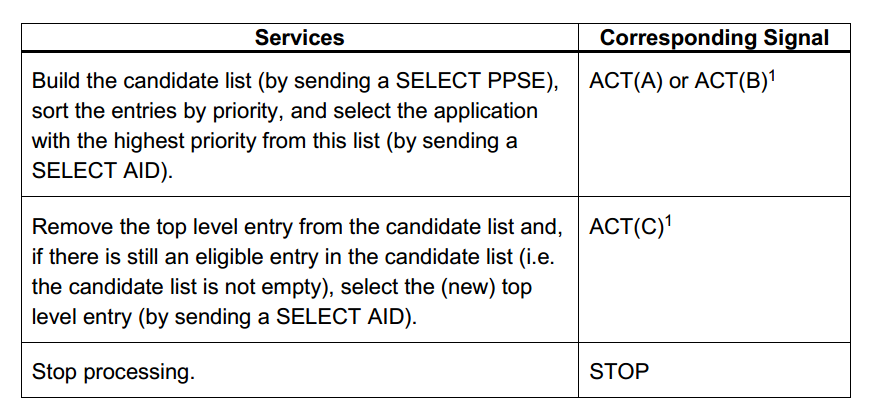
MSG, STOP signal sẽ không acknowledge.

User interface request data bao gồm: message indetifier (các message theo section 9.4 book A), language, balance hay amount .

* Process S

Quản lý việc chọn ứng dụng. Upon activation, ứng dụng được chọn sẽ chứa trong form của AID, kernel ID ở OUT signal





//\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Preprocessing

transaction bắt đầu với quá trình này

Mỗi reader combination {AID Kernel ID} sẽ chứa các thông tin CVM, limits, online/offline capability, contactless transaction limits.

Các giá trị này sẽ được kiểm chứng ở quá trình pre processing.

Nếu TTQ được config cho combination, nó sẽ được chỉnh sửa trong quá trình processing. Nếu như TTQ được config thì entry point reset byte 2, bit 8 và bit 7 ở copy of TTQ xuống 00b. (online cryptgram is not required và CVM not required. )

Nếu giá trị của Amount, Authorised =0 và Nếu zero amount allowed flag is present và zero amount allowed =0 thì set “ contactless application not allowed”.

* Terminal contactless transaction limit

Là maximum transaction amount mà trên mức này transaction sẽ không được thực hiện.

* Terminal CVM required limit

Master card introduced new rules for cardholder verification and receipt requirement. Với mức transaction amount nhỏ hơn mức này thì không cần phải có cardholder verification.

Chức năng này chỉ áp dụng cho mỗi CVM và quá trình xử lý biên lai. Không ảnh hưởng tới ủy quyền transaction online hay offline. Online authorization vẫn có thể được yêu cầu nếu terminal action analysis results trong một ARQC request to the card. (nếu card trả lại một ARQC đến TC request).

Terminal phải hỗ trợ NO CVM. Quá trình online transaction thấp hơn hay bằng terminal CVM required limit không yêu cầu một CVM.

* Terminal contactless floor limit

Transaction amount trên mức này sẽ được ủy quyền bởi nhà cấp phát.

Nếu như thấp hơn hoặc bằng mức này:

Transaction có thể đc ủy quyền offline nếu card chấp nhận (returns TC).

//\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* file within ICC

Files are seen from terminal. Mỗi nhánh của tree này được coi là: Application Definition File (ADF) hay Directory Definition File (DDF). ADF là entry point cho một hay nhiều AEF.

//\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* kernel state diagram

1. S1 idle

reader có thể được config như transaction tự bắt đầu dựa theo transaction trước đó ACT signal dung để activate reader, chứ các thông số transaction amount hay transaction type. Trong một vài trường hợp, ACT signal có thể không cần thiết và complete.

Khi reader nhận được act signal, nó sẽ activate the field và bắt đầu polling card. (terminal gửi ACT signal tới reader).

TLV là viết tắt của Tag, length, value.

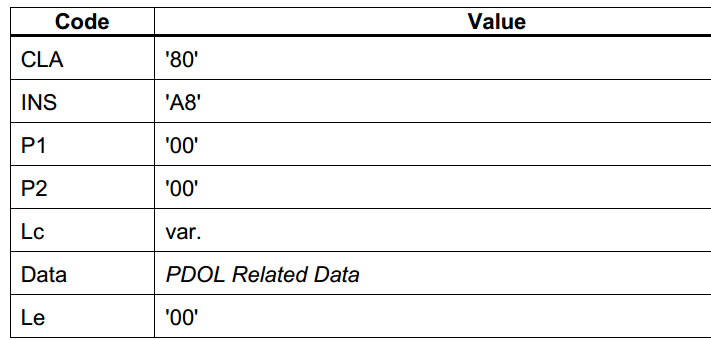
Processing Options Data Object List (PDOL)

(chứa một list terminal data object (tags và length) mà ICC cần cho quá trình GET PROCESSING OPTIONS command. ) được gửi từ PICC. Chẳng hạn như amount authorized, terminal capability, transaction type, DS request Operator ID.

Câu hỏi tags to read liên quan gì với pdol??

FCI template là byte string available ở trả lời của Select command. Tag: 6F.

Get Processing Options command khởi tạo transaction trong card.



PDOL chứa trong GPO command này. (PDOL là giá trị được trả về từ PICC trong khung trả lời của SELECT command). Nếu PDOL không chứa trong response to SELECT command thì data field sẽ k chứa gì.

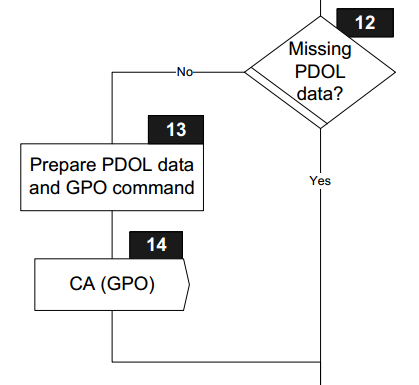
DF name ở tag 84. (của 6F) in select response.

DF name bắt buộc phải có.

Sau khi đã parse các transaction data trong act signal vào tlv database thì kernel khởi tạo unpredictable number.

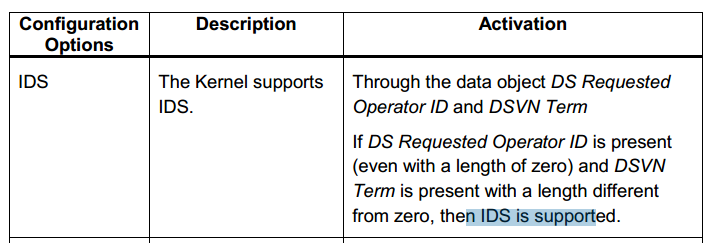
* Chú ý: signal và command là khác nhau.

Signal là giữa reader và terminal. Còn command là giữa reader và card.

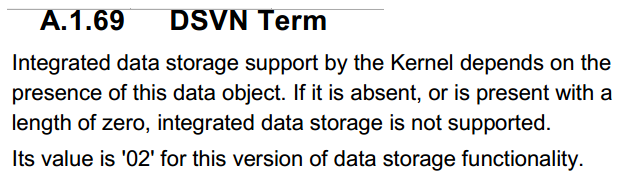


|  |
| --- |
| The parameter to the Signal is the command to be sent to the Card |

nghĩa là thông số trong CA signal này là GPO command.



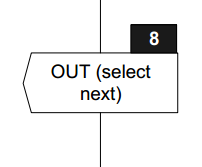
It is sent to the Card ở trong GPO command.



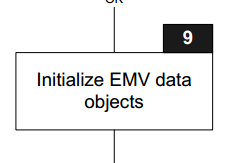
Any application identifier (AID, see 8.2.1.2) may be used as DF name.

* Chú ý: DF là dedicate file (file chuyên dụng).
* EF là elementary file.

Mỗi DF name phải unique trong card.



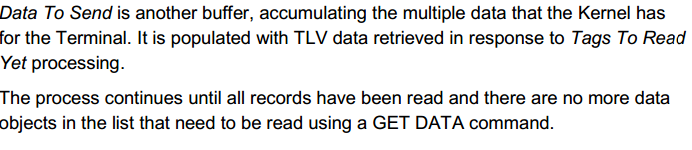
Add to list (GetTLV(tag of Error Indication), Discretionary Data)). Sau đó send Out signal (được gửi từ kernel).



Generate unpredictable number và lưu vào trong TLV database.

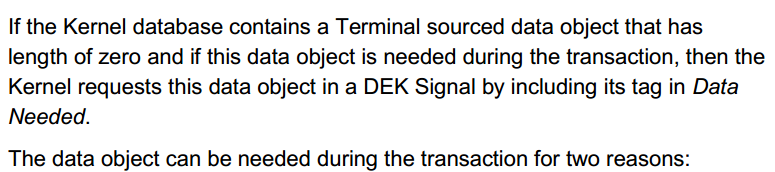
Terminal unpredictable number được gửi từ terminal đến card. (được tạo bởi terminal).

Data to send là một buffer khác. Chứa các list of data objects được gửi từ kernel to terminal trong DEK signal.



Data needed, kernel chứa buffer để tích lũy các tags mà kernel cần từ terminal.

Thông thường, kernel sử dụng DEK signal để yêu cầu data để hoàn thành transaction.



Tags to read:

|  |
| --- |
| List of tags indicating the data the Terminal has requested to be read. This data item is present if the Terminal wants any data back from the Card before the *Data Record*. |
| Nghĩa là: terminal sẽ gửi tags và length cho kernel, nó yêu cầu đọc mấy tags đó. |

Tags to Read yet:

Danh sách các tags và data mà kernel đã nhận được ở tags to read (được terminal gửi qua DET signal) để chuẩn bị chuyển đi. . nếu tag nào đã dc gửi từ kernel sẽ dc xóa đi.

Ban đầu mới vào, quá trình khởi tạo thì: add Tags to read -> Tags to read yet.

Trong phần request data: Nếu như data objects của (tags to read: value của nó là các tags mà terminal yêu cầu đọc) hiện diện ở Kernel database với value field set to zero, kernel gửi DEK signal để yêu cầu giá trị của tags to read. DF8112

**ĐƯỢC KERNEL GỬI ĐẾN TERMINAL QUA DEK signal.**

**Và terminal gửi qua kernel qua DET signal.**

**9F38 : PDOL được gửi từ card.**

Tags to write before gen ac:

Data terminal request to be sent to card.

Câu hỏi: Read and write là sao ta?

Write là cái terminal muốn gửi cho card.

Read là cái terminal muốn nhận. từ card.

Hai cái trên đều thông qua thg trung gian là kernel.

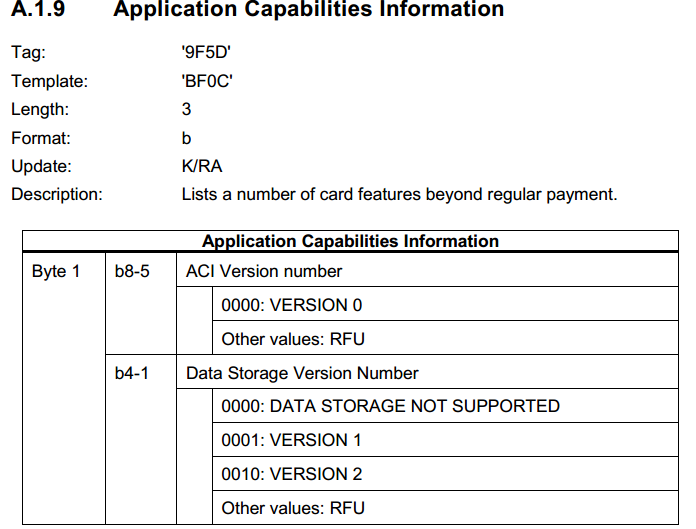
Amount, File Control Information

Câu hỏi: data needed, data to send liên hệ giữa kernel và reader bằng signal hay sao?

Through ACT hay DET signal, kernel có data object (tags to read) chứa các tags (và length) của data object được gửi cho terminal.

Application Capabilities information:

Chứa các card features dựa vào thanh toán thông thường. Chứa trong File Control Information Template.



Câu hỏi: TLV database là gì?

Kernel maintains a TLV database để lưu trữ tất cả TLV encoded data object.

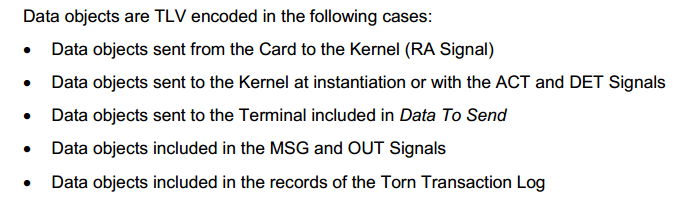
Nó là bản copy của bộ dữ liệu Kernel thích hợp với transaction type và AID. TLV database này được update trong quá trình transaction. Thông qua data from reader, terminal,

Đối tượng dữ liệu được nhận biết bởi kernel nếu tag được liệt kê ở Annex A.

Các data object are transaction related data objects sent to Kernel by terminal with ACT and DET signal.

* Chú ý: AID giống FID.

RA signal chứa R-APDU hoặc SW12. Dược trả lời từ card. Nếu SW12 khác 9000 chỉ ra rằng card không xử lý Generate AC command ở torn transaction.



CDA :



in CDA, the card generates a dynamic signature and an application cryptogram together.



9F5C: DS request operator: được nhận về ở PDOL. Nghĩa là card cần data của tag này.

9F5E: DS ID, TLV của DS ID được gửi về trong SELECT COMMAND response.

**TRẠNG THÁI 2**

Câu hỏi: timeout có giá trị là bao nhiêu?

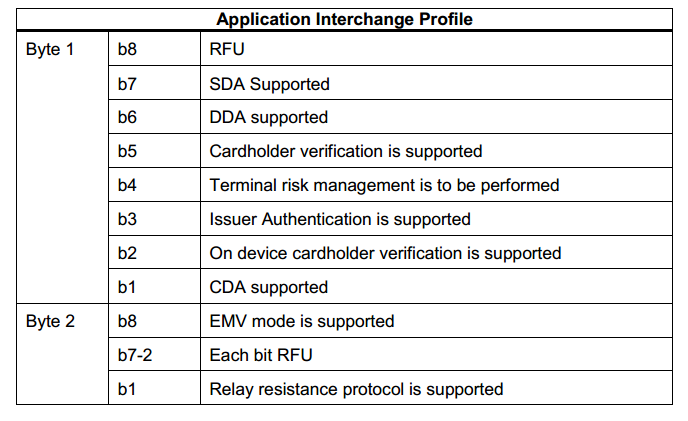
an RA Signal containing the R-APDU or SW12 returned by the Card,

tag 77: response message template format 2.

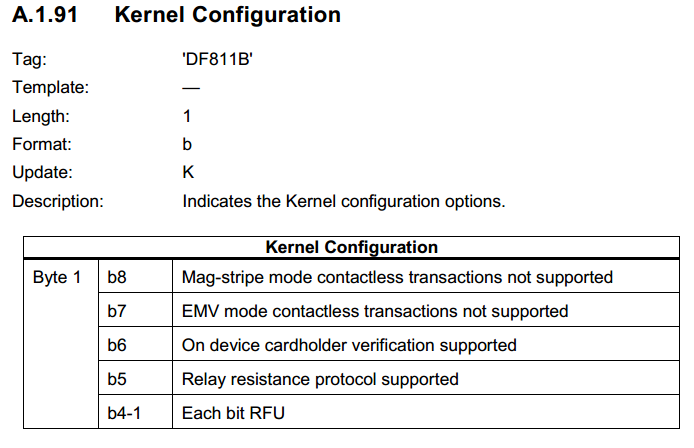
Isnotempty hay empty là kiểm tra giá trị của tag.

Not present hay present là tag đó có xuất hiện hay k

Tag 82: quy dinh xem emv mode có support hay k?



Kernel configuration k hỗ trợ stripe



**Chú ý: nếu bên kernel chưa nhận được PDOL từ card. Thì nó sẽ gửi tiếp select command cho card. (rơi vào trạng thái s2).**

**S3.34***Reader Contactless Transaction Limit* := *Reader Contactless Transaction Limit (No  
On-device CVM) (tag: DF8124)***S3.35***Reader Contactless Transaction Limit* := *Reader Contactless Transaction Limit (On  
device CVM) (tag: DF8125).*

Câu hỏi: hai cái trên nó nghĩa là no CVM hay CVM ở outcome parameter set.

CVM là viết tắt của cardholder verification method.

Câu hỏi: parsing and store là gì?

Câu hỏi: invalid response là sao??

RRP protocol:

Relay attack: the relay fast enough cho terminal không bị timeout. , criminals may run the risk of being caught if they have go around with an antenna or an NFC phone to connect with bankcards people keep in their pockets or handbags.

Sử dụng fraudulent terminal để thực hiện transaction. Trong khi giao dịch thực tế được chuyển tiếp thông qua một thẻ gian lận.

QUÁ TRÌNH:

Bit ở Application interchange profile được sử dụng thông báo reader là card hỗ trợ relay attack, bit ở kernel configuration sử dụng (kernel hỗ trợ).

Reader gửi một C- APDU (exchange relay resistance data) đến card với một số ngãu nhiên. Card trả lời cũng với một số ngẫu nhiên, timing estimates.

Nếu timing exceeds the maximum thì reader sẽ thử lại hai lần nữa.

Kết quả protocol này dựa vào CDA. The timings trả về bởi card ở exchange relay resistance data bao gồm trong signed dynamic application data (response of generate ac command).

Nếu transaction hoàn thanhf without CDA, additional data is included in the online message, issuer sẽ thực hiện check.

The transaction ok nếu như thời gian xử lý nằm trong thời gian cho phép.

Trạng thái 3 (continue)

Câu hỏi: Cái signal: L1RSP bao gồm cả transmission error, nó đều hiện là try again hay là lỗi (end application) Vậy thì gửi lại ở đâu?

CHỉ một trong 2 mode Stripe hay EMV mode hỗ trợ.

Trong trường hợp, k hỗ trợ hai mode emv và stripe, sẽ diễn ra invalid response.

User interface request data: error- other card.

Trạng thái: đợi Exchange relay resistance data command:

Nếu như bên kernel nhận được DET signal, nó sẽ quay trở lại trạng thái cũ. Đợi tiếp.

Khi mà nhận được RA signal thì nó mới xử lý tiếp.

Terminal verification results ở OUT DATA RECORD.

Trạng thái: 3, R1:

Câu hỏi: 

SFI: Short File Identifier.

SFI xuất hiện ở trong GPO response.

5 bit đầu tiên chỉ SFI.

Byte tiếp theo chỉ record number được đọc cho SFI đó.

Byte tiếp theo nữa chỉ last record number được đọc cho SFI đó. Nếu như last record number > 2nd byte thì all records ranging from second number và bao gồm cả byte thứ 3 sẽ được đọc cho SFI đó. Ví dụ: record number: 01, last record number la 04. READ RECORD command sẽ được gửi 4 lần.

DS Slot Availability tag: 9f5f ở trong khung GPO command response.

DS summary 1: tag 9F7D ở trong khung GPO command response.

DS Unpredictable Number: tag 9F7F cũng ở khung GPO command response.

*DS Slot Management Control tag* 9F6F

*DS ODS Card* 9F54 những cái trên đều chứa trong GPO response.