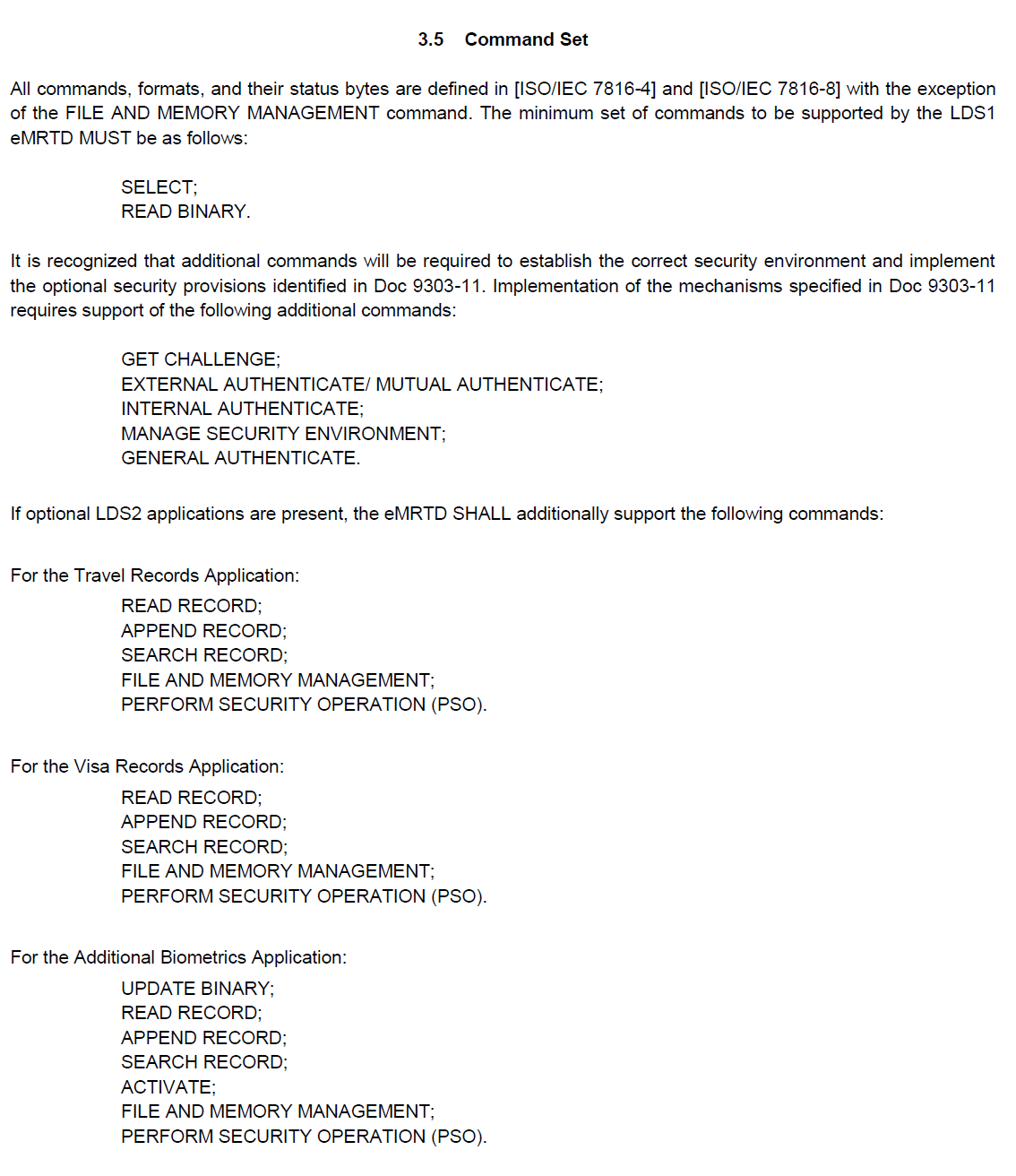
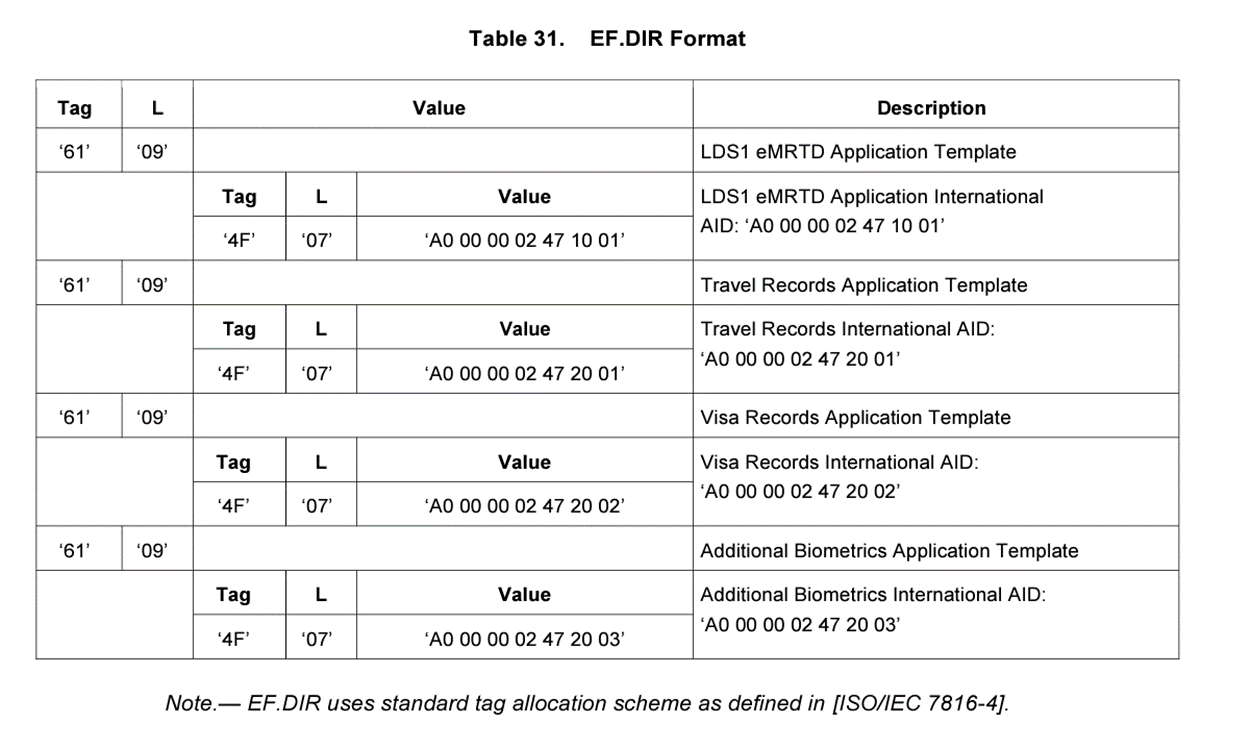


**Cấu trúc bộ nhớ của smartcard MRTD theo ICAO 9303**



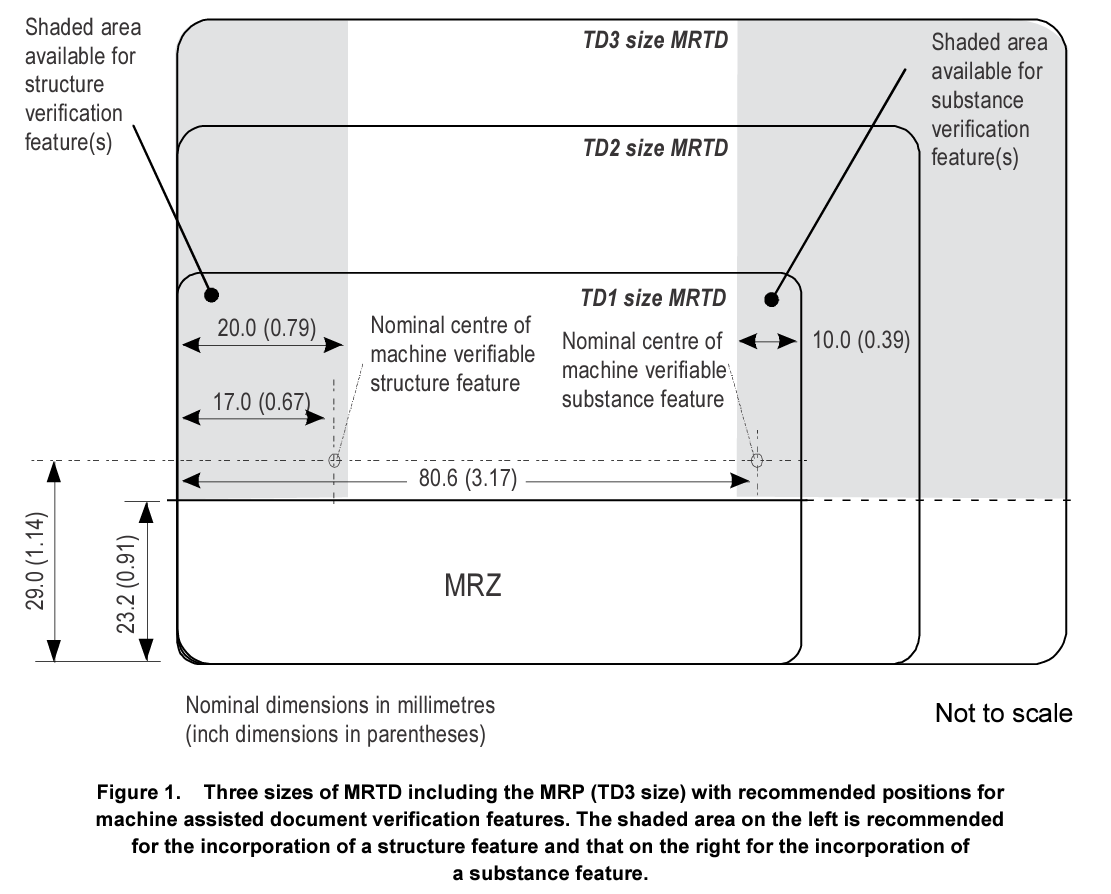


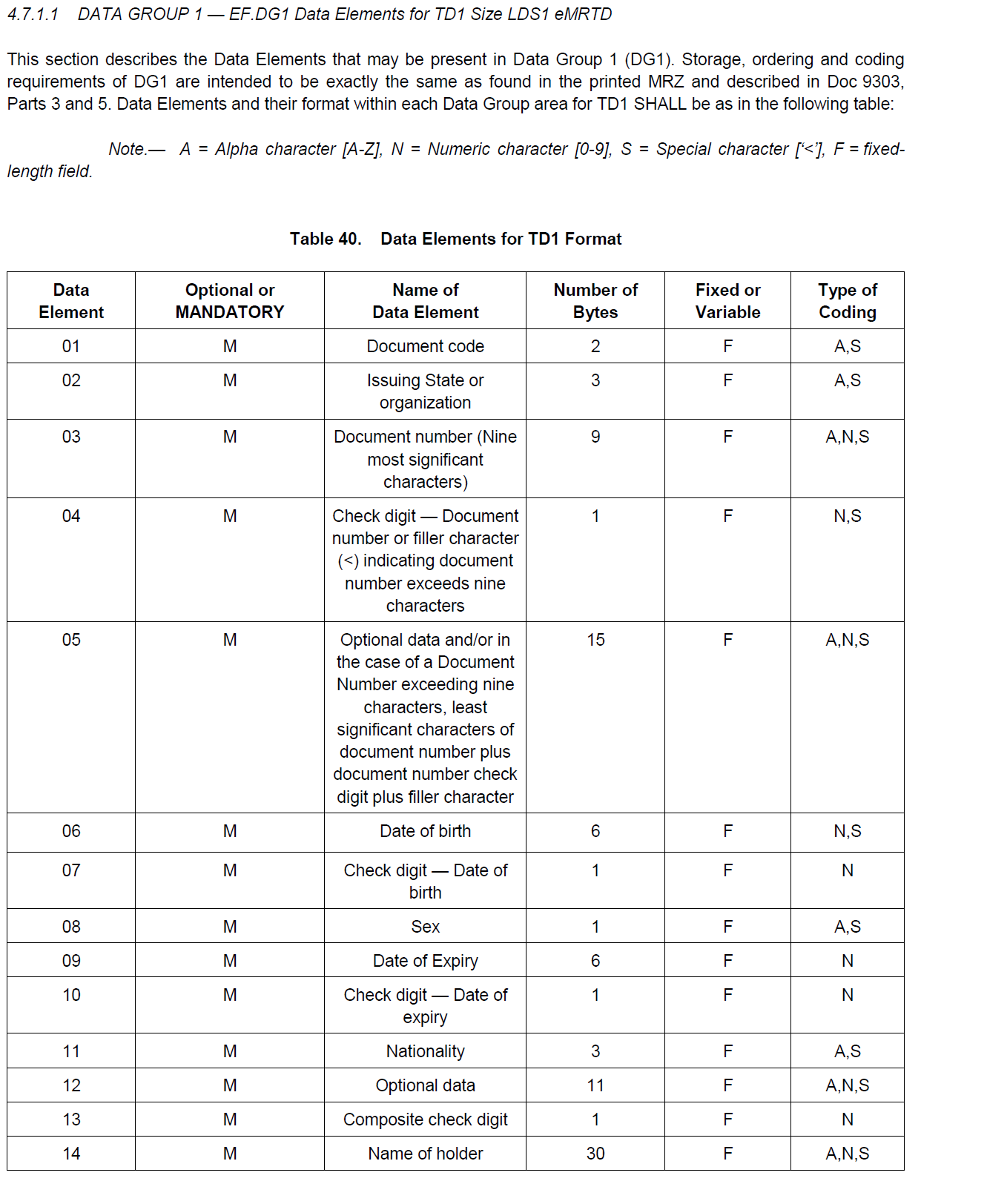
**AID tiêu chuẩn của các app trong ICAO9303**

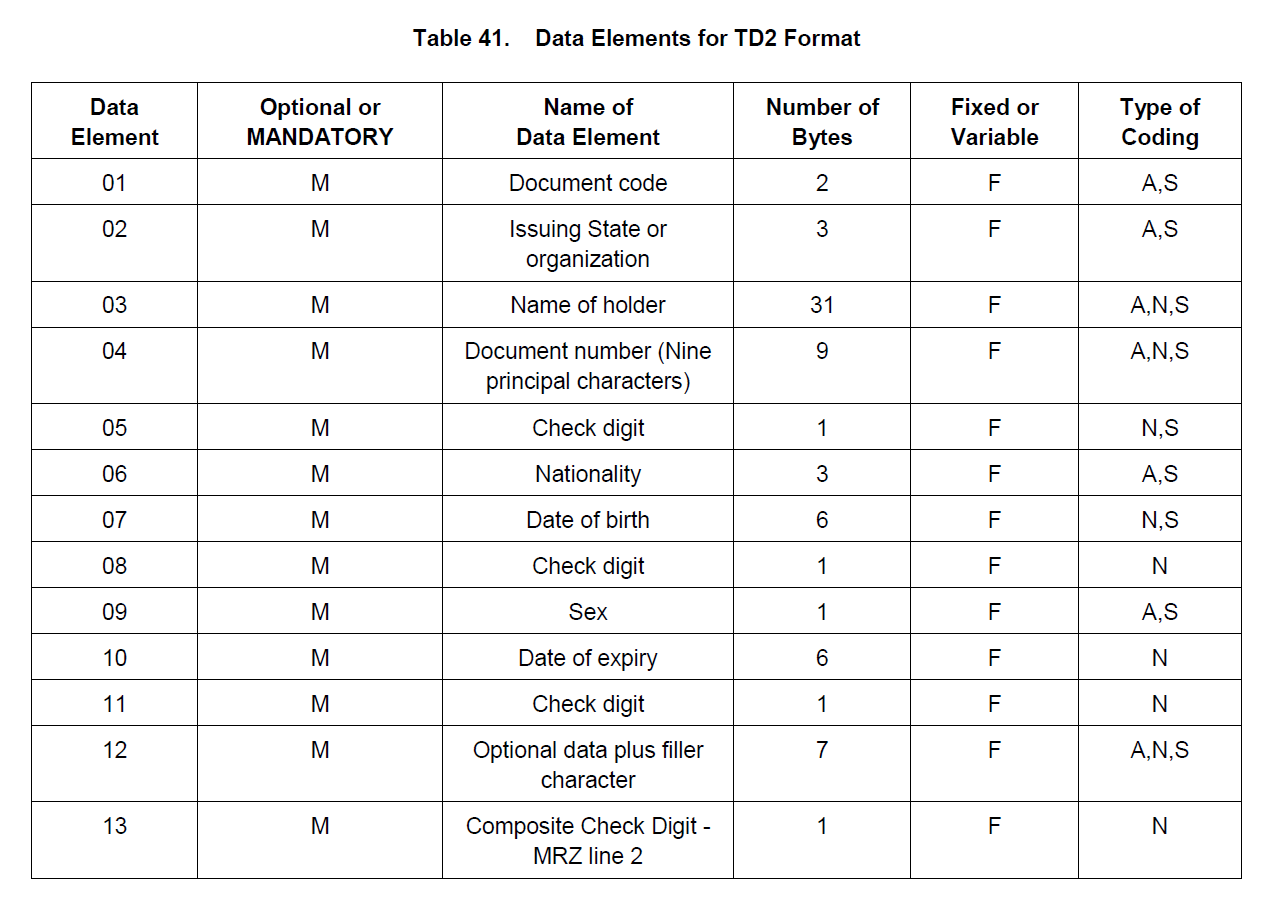
|  |  |
| --- | --- |
|  | The LDS1 eMRTD application is MANDATORY;  - The LDS1 eMRTD application SHALL consist of data recorded by the Issuing State or organization, Data Groups 1 through 16 together with the Document Security Object (EF.SOD);  - The Document Security Object (EF.SOD) within the LDS1 eMRTD application consists of the hash values as defined in Doc 9303-11 and Doc 9303-12 for the Data Groups in use, and is needed to validate the integrity of data created by the issuer and stored in the LDS1 eMRTD application. |

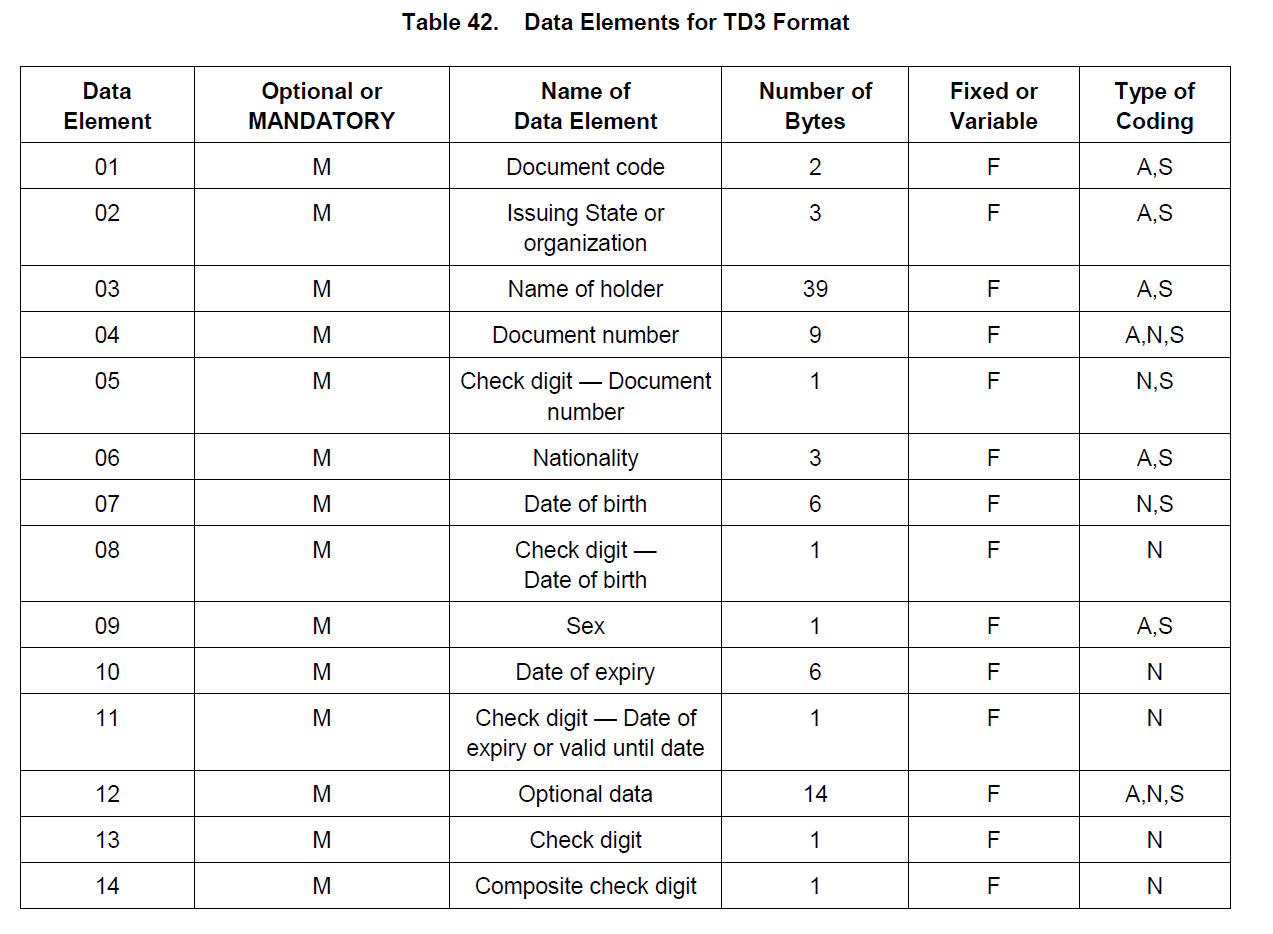
**Cấu trúc dữ liệu lưu trữ trong các EF file của eMRTD**

**(Tham khảo thêm chi tiết hơn ở** **ICAO9303\_Part 3 và Part 5 )**

****





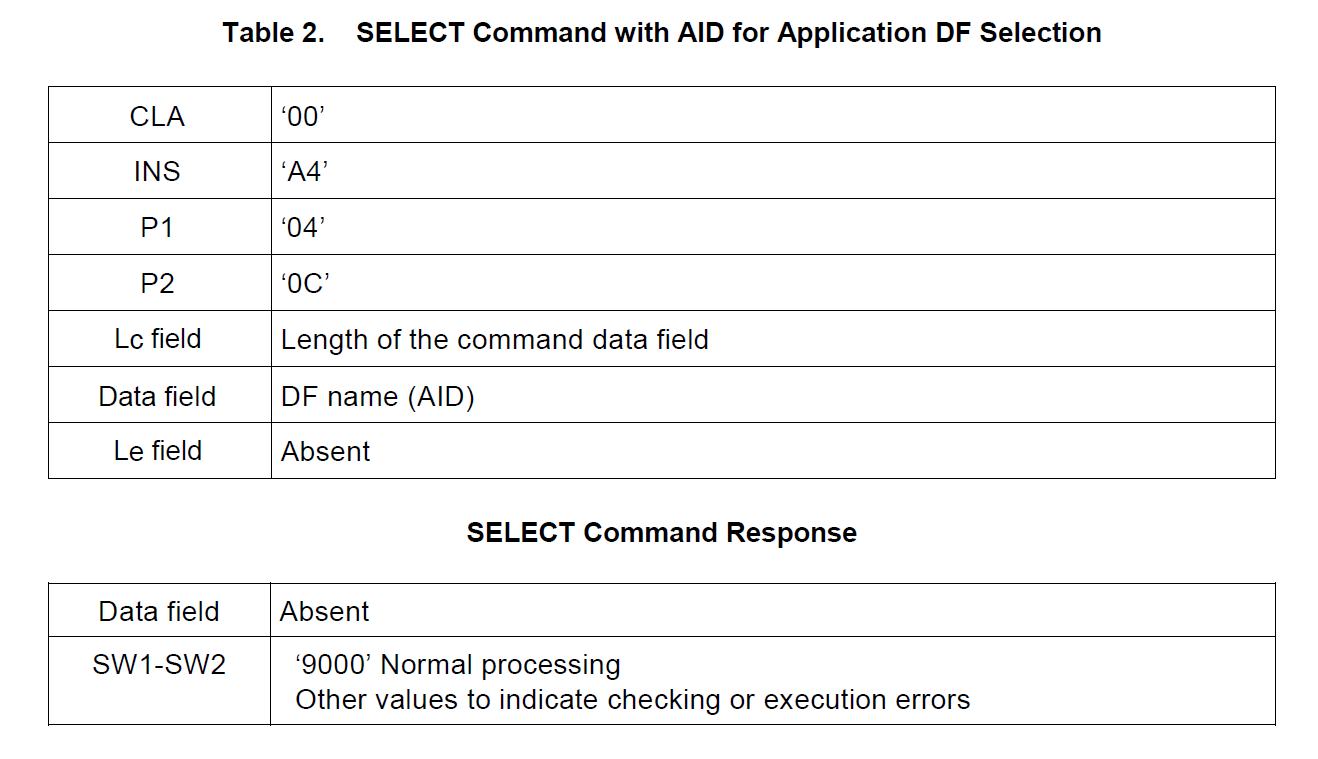


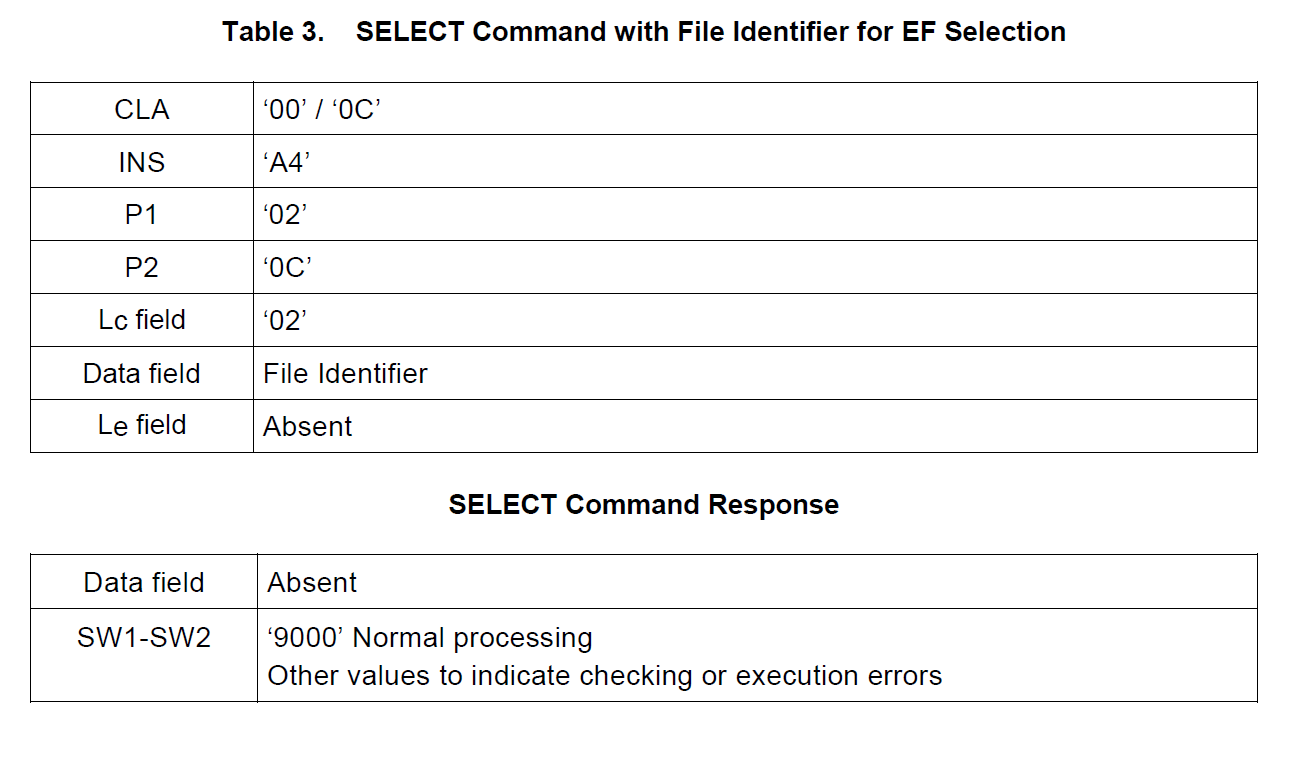
Qui định cụ thể về nội dung các trường dữ liệu (document code, issuing state…) được nêu chi tiết trong ICAO9303\_Part3.

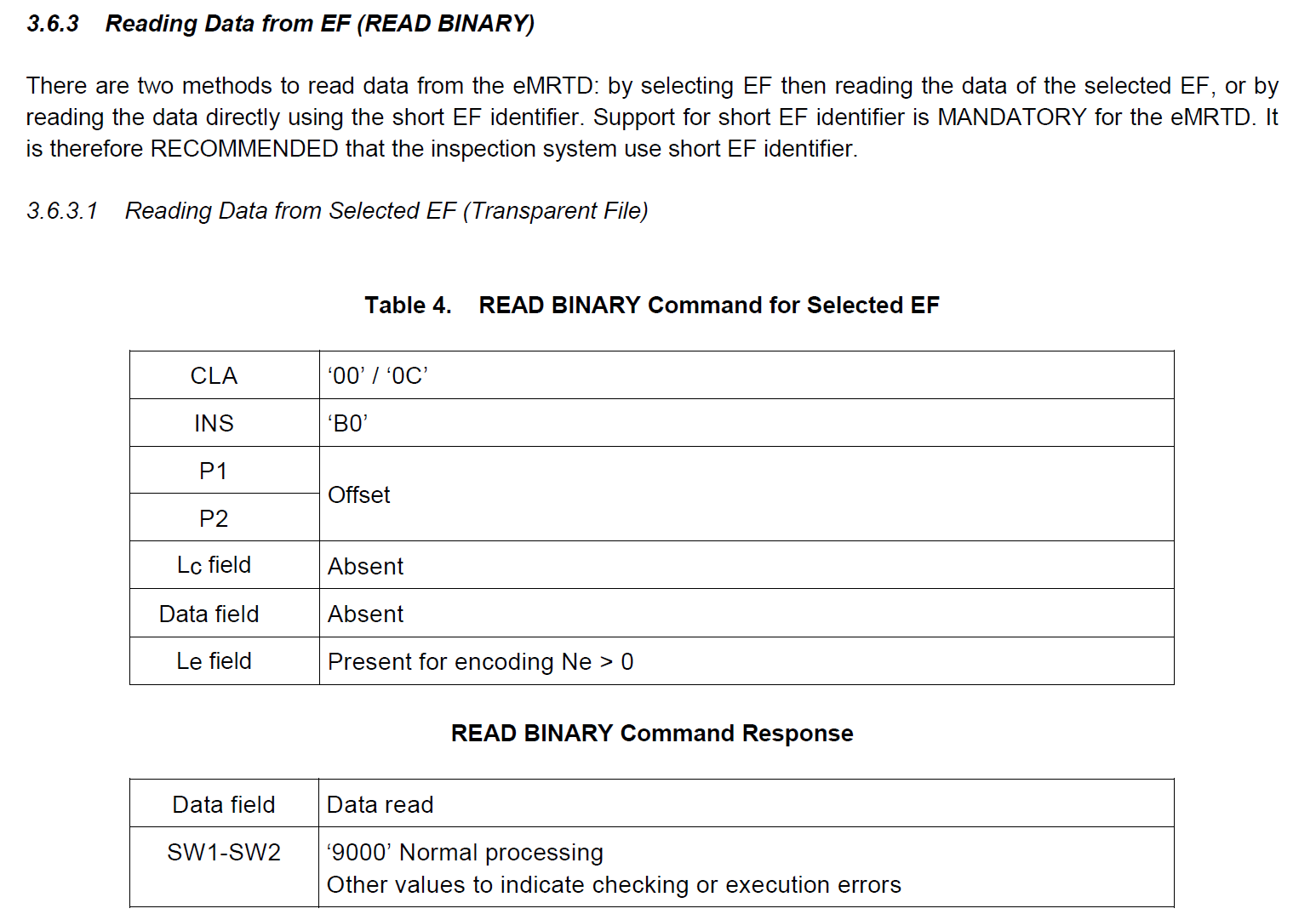
Tham khảo thêm chi tiết về cấu trúc dữ liệu của các EF.DG2 to 16 trong ICAO9303\_Part 10. Hiện tại, để phục vụ build app mô phỏng eMRTD ta sẽ quan tâm đến các một số thông tin cơ bản như trong EF.DG1 ở trên. Sau khi xong, nếu xét thấy cần thiết thì có thể phát triển thêm EF.DG2 (Encoded Identification Features - Face) và thêm EF.DG3 (Additional Identification Feature — Finger(s)).

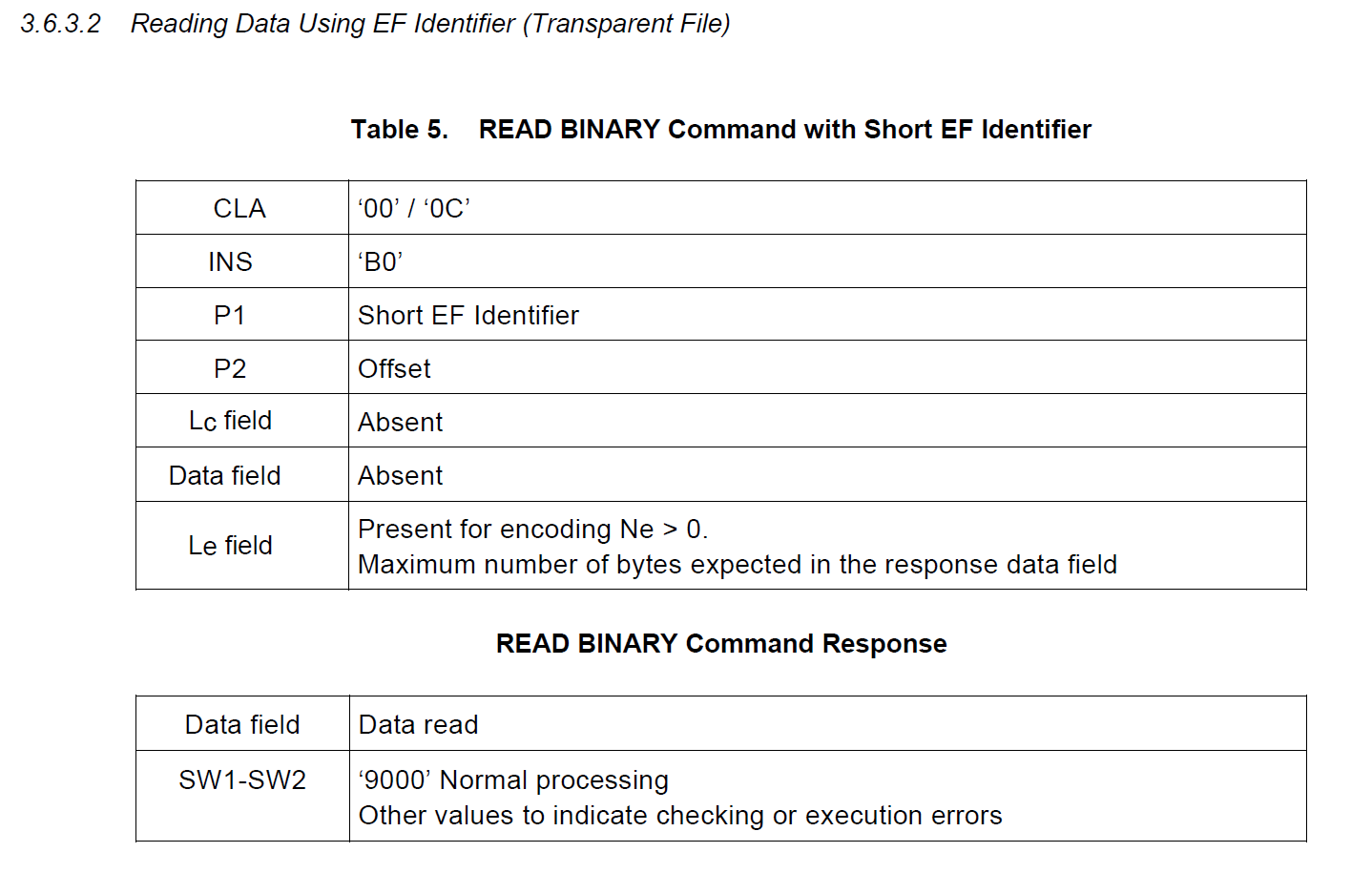
**Các bước để Reader đọc thông tin từ thẻ**

**(Đã được thực hiện trong reader app mà SW team đã build, confirm lại với SW team)**

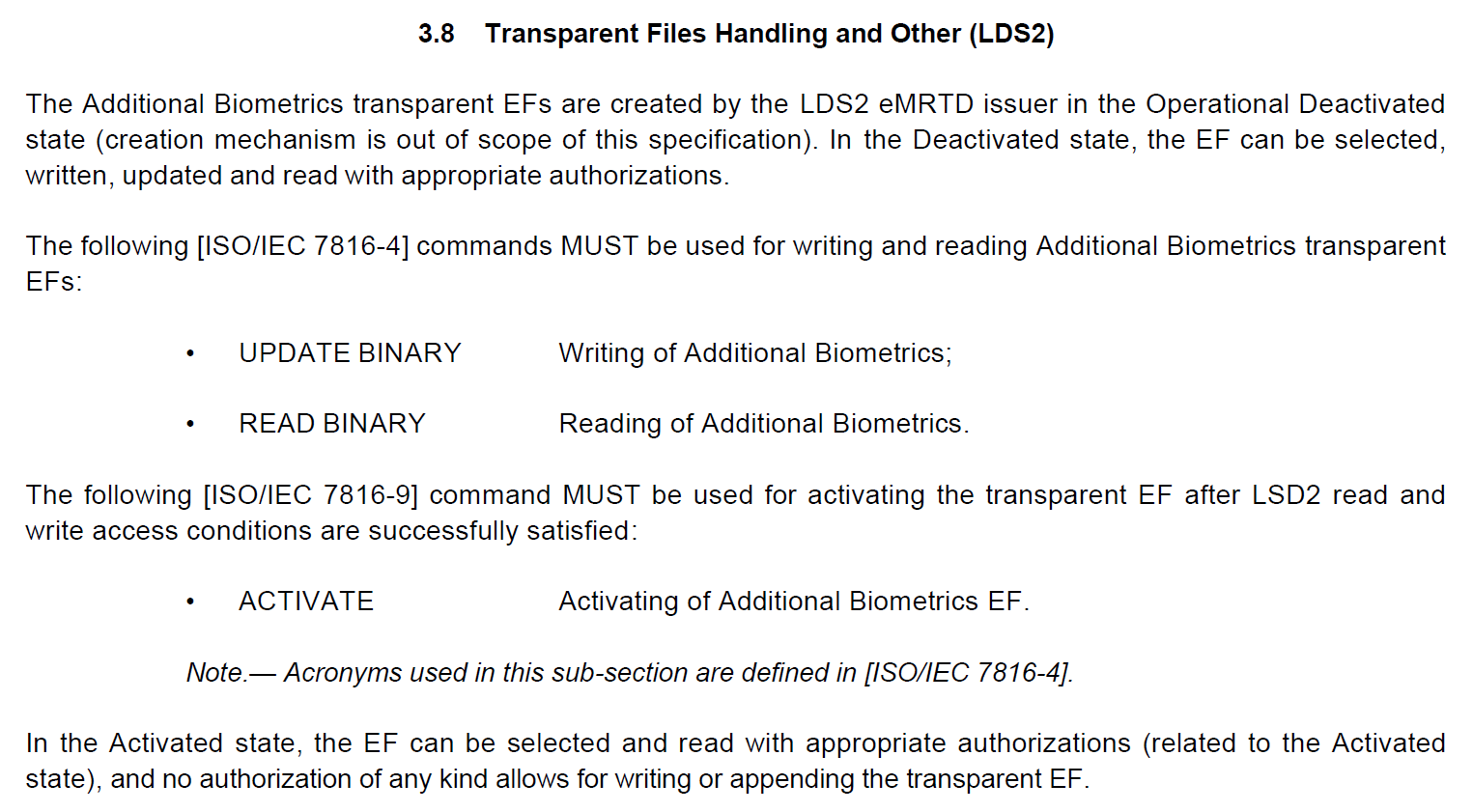




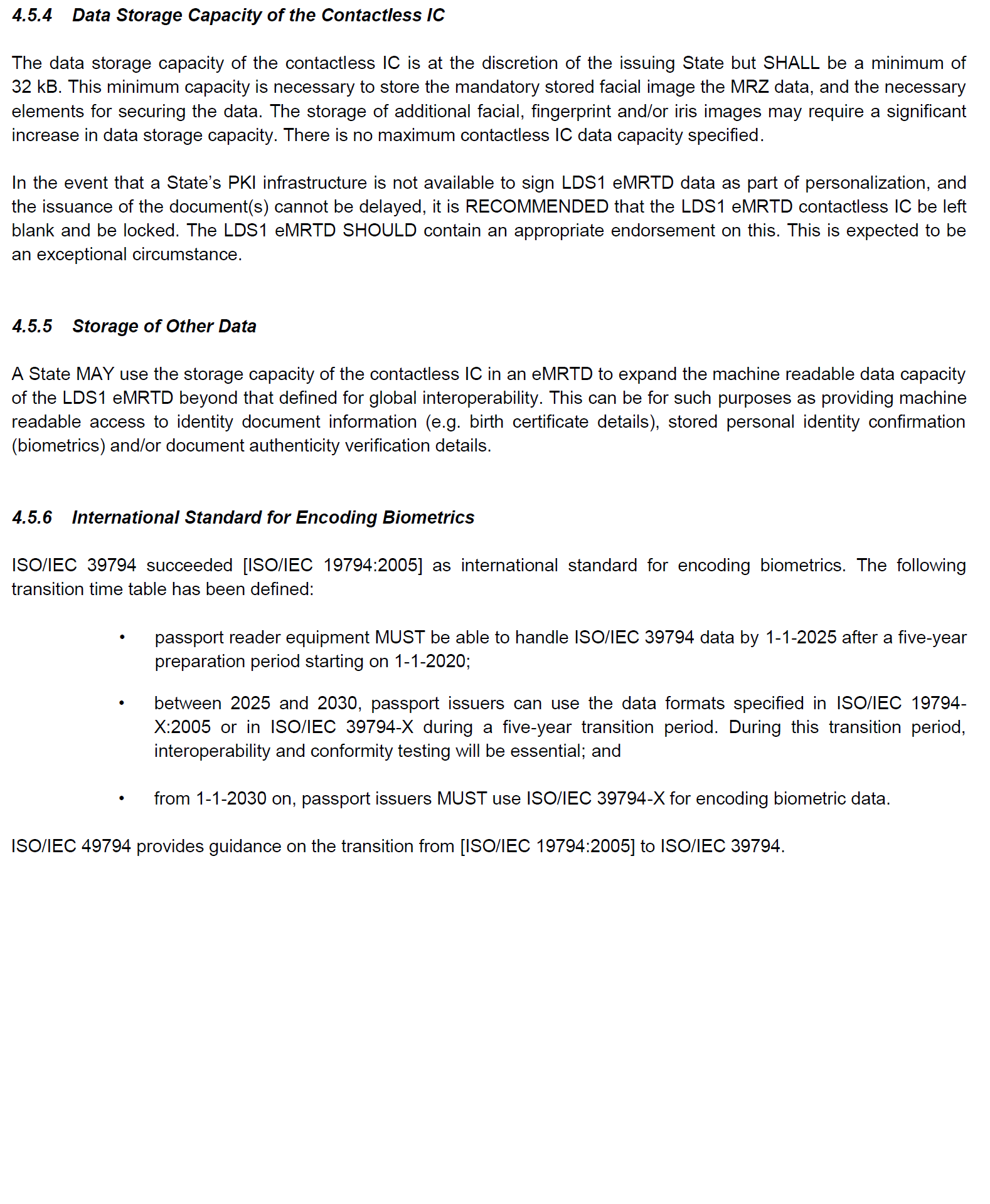




**Với LDs2**

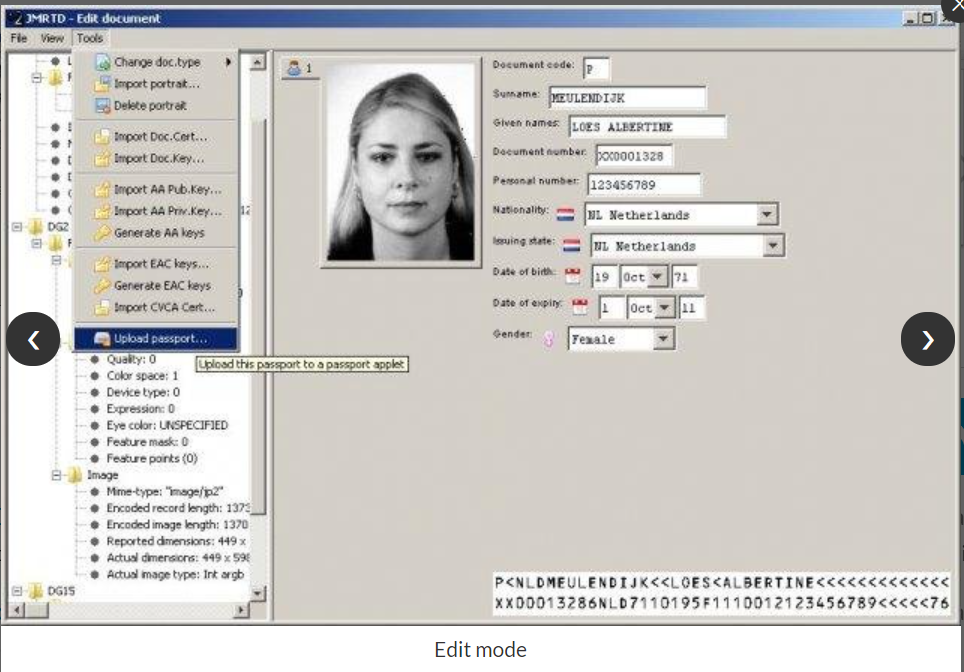


***- Có vẻ như lý do khiến Reader app do team SW build chưa thể đọc được ảnh trên CCCD gắn chip (dù data có được lưu ở*** EF.DG2 trên thẻ***) là do dữ liệu này nằm ở LDS2 và để truy cập cần có authentication với card issuer.***



Flow chart cho app mô phỏng eMRTD ta cần build

1. Start with UI để tạo mới (hoặc load ID doc đã lưu) (ví dụ)



2. Khi tạo mới xong hoặc đã sẵn sàng, active ID doc và lưu các dữ liệu cơ bản (chưa cần face, finger: sẽ lưu ở version sau) vào file text EF.DG1

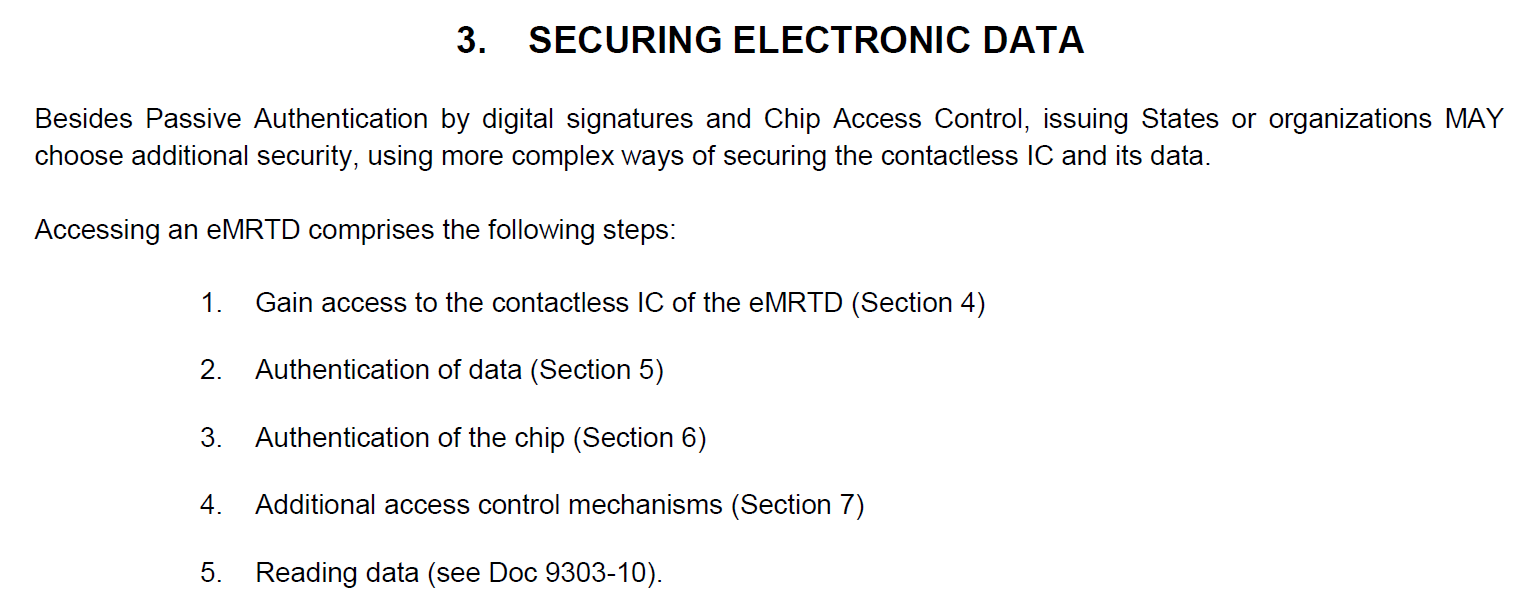
3. Active NFC Host-based card emulation mode (service) và chờ APDU từ card reader

4.Nhận APDU Select AID từ cardreader và hồi đáp APDU theo tiêu chuẩn

5.Nhận APDU Select File cho EF1.DG1 từ cardreader và hồi đáp APDU theo tiêu chuẩn

6.Nhận APDU READ BINARY cho EF1.DG1 từ cardreader và hồi đáp APDU với “data” đã lưu trong EF.DG1 trong bước 2 theo tiêu chuẩn.

7. Clean up, stop NFC Host-based card emulation mode (service) để tránh xung đột khi các app khác trong mobile có sử dụng NFC được khởi chạy, exit app.



At least one of BAC or PACE SHALL be supported by the eMRTD. PACE is REQUIRED for LDS2. PACE offers better

protection against eavesdropping than BAC (See also Appendix A ICAO9303\_part 11)

