TCVN TIÊU CHUẨN QUỐC GIA

TCVN 11167-11:2015
ISO/IEC 7816-11:2004

Xuất bản lần 1

THẺ DANH ĐỊNH - THẺ MẠCH TÍCH HỢP - PHẦN11: XÁC MINH CÁ NHÂN BẰNG PHƯƠNG PHÁP SINH TRẮC HỌC

Identification cards - Integrated circuit cards - Part 11: Personal verification through biometric methods

HÀ NỘI - 2015

Mục lục **Trang**

Lời nói đầu

TCVN 11167-11:2015 hoàn toàn tương đương với ISO/IEC 7816-11:2004.

TCVN 11167-11:2015 do Tiểu Ban kỹ thuật tiêu chuẩn quốc gia TCVN/JTC 1/SC 17 *"Thẻ nhận dạng"* biên soạn, Tổng cục Tiêu chuẩn Đo lường Chất lượng đề nghị, Bộ Khoa học và Công nghệ công bố.

Bộ tiêu chuẩn TCVN 11167 (ISO/IEC 7816) *Thẻ định danh – Thẻ mạch tích hợp* gồm các tiêu chuẩn sau:

- Phần 1: Thẻ tiếp xúc - Đặc tính vật lý;
- Phần 2: Thẻ tiếp xúc - Kích thước và vị trí tiếp xúc;
- Phần 3: Thẻ tiếp xúc - Giao diện điện và giao thức truyền;
- Phần 4: Tổ chức, an ninh và lệnh trao đổi;
- Phần 5: Đăng ký của bên cung cấp ứng dụng;
- Phần 6: Phần tử dữ liệu liên ngành trong trao đổi;
- Phần 7: Lệnh liên ngành đối với ngôn ngữ truy vấn thẻ có cấu trúc;
- Phần 8: Lệnh đối với hoạt động an ninh;
- Phần 9: Lệnh đối với quản lý thẻ;
- Phần 10: Tín hiệu điện và trả lời để thiết lập lại cho thẻ đồng bộ;
- Phần 11: Xác minh cá nhân bằng phương pháp sinh trắc học;
- Phần 12: Thẻ tiếp xúc - Thủ tục vận hành và giao diện điện tử USB;
- Phần 13: Lệnh đối với quản lý ứng dụng trong môi trường đa ứng dụng;
- Phần 15: Ứng dụng thông tin mã hóa.

Thẻ định danh - Thẻ mạch tích hợp - Phần 11: Xác minh cá nhân bằng phương pháp sinh trắc học

Identification cards – Integrated circuit cards – Part 11: Personal verification through biometric methods

1 Phạm vi áp dụng

Tiêu chuẩn này quy định các lệnh liên ngành liên quan tới an ninh được dùng đối với việc xác minh cá nhân bằng phương pháp sinh trắc học trong (các) thẻ mạch tích hợp. Tiêu chuẩn này cũng quy định cấu trúc dữ liệu và phương pháp truy nhập dữ liệu đối với việc sử dụng một thẻ như một phần mang dữ liệu tham chiếu sinh trắc học và/hoặc thiết bị thực hiện xác minh một sinh trắc học cá nhân (đối chiếu trên thẻ). Việc định danh cá nhân sử dụng phương pháp sinh trắc học không đề cập trong phạm vi của tiêu chuẩn này.

2 Tài liệu viện dẫn

Các tài liệu viện dẫn sau rất cần thiết cho việc áp dụng tiêu chuẩn này. Đối với các tài liệu viện dẫn ghi năm công bố thì áp dụng phiên bản được nêu. Đối với các tài liệu viện dẫn không ghi năm công bố thì áp dụng phiên bản mới nhất, bao gồm cả các sửa đổi, bổ sung (nếu có).

TCVN 11167-4:2015 (ISO/IEC 7816-4:2003) Thẻ định danh - Thẻ mạch tích hợp - Phần 4: Tổ chức, an ninh và lệnh trao đổi,

Bộ ISO/IEC 19785[1] Information technology - Common Biometric Exchange Framework Format (CBEFF) (*Công nghệ thông tin - Định dạng khuôn mẫu trao đổi sinh trắc học phổ biến (CBEFF)*)

3 Thuật ngữ và định nghĩa

Tiêu chuẩn này áp dụng các thuật ngữ và định nghĩa sau.

1 ISO/IEC CD 19785:2005 đã được xây dựng thành các tiêu chuẩn: ISO/IEC 19785-1:2015, ISO/IEC 19785-2:2006 và ISO/IEC 19785-3:2015

3.1

Dữ liệu sinh trắc học (biometric data)

Mã hóa dữ liệu một hay nhiều đặc trưng sử dụng trong xác minh sinh trắc học.

3.2

Thông tin sinh trắc học (biometric information)

Thông tin cần thiết bởi thế giới bên ngoài nhằm xây dựng việc xác minh dữ liệu.

3.3

Dữ liệu tham chiếu sinh trắc học (biometric reference data)

Dữ liệu lưu trữ trong thẻ với mục đích so sánh với dữ liệu xác minh sinh trắc học.

3.4

Xác minh sinh trắc học (biometric verification)

Quy trình xác minh bởi một so sánh một-một của dữ liệu xác minh sinh trắc học đối với dữ liệu tham chiếu sinh trắc học.

3.5

Dữ liệu xác minh sinh trắc học (biometric verification data)

Dữ liệu được thu thập trong quá trình một quy trình xác thực đối với việc so sánh với dữ liệu tham chiếu sinh trắc học.

3.6

Khuôn mẫu (template)

Được quy định trong TCVN 11167-4 (ISO/IEC 7816-4).

CẢNH BÁO Thuật ngữ "khuôn mẫu" có nghĩa: trường giá trị của một đối tượng dữ liệu được xây dựng. Nó không được nhầm lẫn với khuôn mẫu dữ liệu sinh trắc học được xử lý.

4 Thuật ngữ viết tắt

Tiêu chuẩn này áp dụng các thuật ngữ viết tắt sau.

Thuật ngữ	Tiếng Anh	Tiếng Việt
AID	Application Identifier	Mã định danh ứng dụng
AT	Authentication Template	Khuôn mẫu chứng thực
BER	Basic Encoding Rules	Quy tắc mã hóa cơ bản
BIT	Biometric Information Template	Khuôn mẫu thông tin sinh trắc học
BD	Biometric Data	Dữ liệu sinh trắc học (BD)
BDP	BD in proprietary format	BD theo định dạng độc quyền

Thuật ngữ	Tiếng Anh	Tiếng Việt
BDS	BD in standardized format	BD theo định dạng chuẩn
BDT	Biometric Data Template	Khuôn mẫu dữ liệu sinh trắc học
CCT	Cryptographic Checksum Template	Khuôn mẫu kiểm tra mã hóa
CRT	Control Reference Template	Khuôn mẫu tham chiếu kiểm soát
CT	Confidentiality Template	Khuôn mẫu bảo mật
DE	Data Element	Phần tử dữ liệu
DF	Dedicated File	Tệp tin chuyên dụng
DO	Data Object	Đối tượng dữ liệu
DST	Digital Signature Template	Khuôn mẫu chữ ký số
EFID	Elementary File ID	Mã định danh tệp tin cơ bản
FCI	File Control Information	Thông tin kiểm soát tệp tin
ID	Identifier	Mã định danh
L	Length	Độ dài
OID	Object Identifier	Mã định danh đối tượng
RD	Reference Data	Dữ liệu tham chiếu
SE	Security Environment	Môi trường an ninh
SM	Secure Messaging	Thông điệp an ninh
TLV	Tag-Length-Value	Giá trị-độ dài-thẻ
UQ	Usage Qualifier	Bộ định tính sử dụng
VIDO	Verification requirement Information Data Object	Đối tượng dữ liệu thông tin yêu cầu xác minh
VIT	Verification requirement Information Template	Khuôn mẫu thông tin yêu cầu xác minh

5 Lệnh đối với quy trình xác minh sinh trắc học

Các lệnh: thu hồi, xác minh và chứng thực được quy định trong TCVN 11167-4 (ISO/IEC 7816-4) được sử dụng để xác minh sinh trắc học. Dữ liệu sinh trắc học (ví dụ: đặc trưng khuôn mặt, hình dáng tai, vân tay, phổ giọng, âm tần, gõ phím) có thể cần bảo vệ chống lại việc làm lại hay trình bày dữ liệu xác minh từ dữ liệu sinh trắc học gốc (ví dụ: một dấu vân tay, một bức ảnh khuôn mặt). Một phương pháp để ngăn chặn loại tấn công này là gửi dữ liệu xác minh vào thẻ với một checksum mã hóa hay một chữ ký số áp dụng thông điệp an ninh

được quy định trong TCVN 11167-4 (ISO/IEC 7816-4). Tương tự, thông điệp an ninh có thể được sử dụng để đảm bảo tính xác thực của dữ liệu sinh trắc học lấy ra từ thẻ.

5.1 Lệnh truy xuất thông tin sinh trắc học

Các lệnh quy định trong TCVN 11167-4 (ISO/IEC 7816-4) trong các điều liên quan tới tham chiếu dữ liệu phải được sử dụng đối với lấy thông tin sinh trắc học.

5.2 Lệnh đối với quy trình xác minh sinh trắc học tĩnh

Lệnh được sử dụng cho một quá trình xác minh tĩnh (xem Phụ lục A) là lệnh VERIFY được quy định trong TCVN 11167-4 (ISO/IEC 7816-4). Các thông tin được truyền đạt là:

- Bộ nhận dạng tham chiếu sinh trắc học (hay bộ định tính dữ liệu tham khảo)
- Dữ liệu xác minh sinh trắc học.

Dữ liệu xác minh sinh trắc học có thể được mã hóa như các đối tượng dữ liệu BER-TLV (xem Bảng 2). Các byte CLA có thể chỉ ra rằng trường dữ liệu lệnh là BER-TLV được mã hóa (xem TCVN 11167-4 (ISO/IEC 7816-4)).

Nhằm kết hợp các lược đồ sinh trắc học, xâu chuỗi lệnh được quy định trong TCVN 11167-8 (ISO/IEC 7816-8) có thể được sử dụng.

5.3 Lệnh đối với quy trình xác minh sinh trắc học động

Để thừa nhận một phản ứng của người dùng được yêu cầu (xem Phụ lục A), lệnh GET CHALLENGE phải được sử dụng.

Loại thách thức trong quá trình xác minh sinh trắc học, ví dụ: một cụm từ cho âm tần hay một cụm từ dùng gõ phím, phụ thuộc vào các thuật toán sinh trắc học, có thể được quy định tại P1 của lệnh GET CHALLENGE (xem TCVN 11167-4 (ISO/IEC 7816-4)). Các thuật toán tương ứng có thể được lựa chọn thay đổi bằng cách sử dụng lệnh MANAGE SECURITY ENVIRONMENT (ví dụ: lựa chọn SET với CRT AT và bộ định tính sử dụng DO và thuật toán DO id trong trường dữ liệu).

Sau khi một lệnh GET CHALLENGE thành công, một lệnh EXTERNAL AUTHENTICATE được gửi vào thẻ. Trường dữ liệu lệnh truyền tải dữ liệu xác minh sinh trắc học có liên quan. Để mã hóa dữ liệu xác minh sinh trắc học, các nguyên tắc giống nhau áp dụng như đối với lệnh VERIFY, xem Điều 5.1.

6 Phần tử dữ liệu

6.1 Thông tin sinh trắc học

Khuôn mẫu thông tin sinh trắc học (BIT) cung cấp thông tin mô tả liên quan tới dữ liệu sinh trắc học tương ứng. Khuôn mẫu này được cung cấp bởi thẻ trong việc hồi đáp một lệnh nhận trước một quy trình xác minh. Bảng 1 quy định thông tin sinh trắc học về các DO.

Bảng 1 - Thông tin sinh trắc học của các DO

<table>
<tr><th>Thẻ</th><th>Độ dài</th><th colspan="5">Giá trị</th><th>Ưu tiên</th></tr>
<tr><td>'7F60'</td><td>Thay đổi</td><td colspan="5">Khuôn mẫu thông tin sinh trắc học (BIT)</td><td></td></tr>
<tr><td></td><td></td><td>Thẻ</td><td>Độ dài</td><td colspan="3">Giá trị</td><td></td></tr>
<tr><td></td><td></td><td>'80'</td><td>1</td><td colspan="3">Tham chiếu thuật toán đối với việc sử dụng trong lệnh VERIFY/EXT. AUTHENTICATE/MANAGE SE</td><td>Tùy chọn</td></tr>
<tr><td></td><td></td><td>'83'</td><td>1</td><td colspan="3">Bộ định tính dữ liệu tham chiếu đối với việc sử dụng lệnh VERIFY/EXT. AUTHENTICATE/MANAGE SE</td><td>Tùy chọn</td></tr>
<tr><td></td><td></td><td>'A0'</td><td>Thay đổi</td><td colspan="3">Thông tin sinh trắc học về các DO được quy định trong tiêu chuẩn này</td><td>Tùy chọn</td></tr>
<tr><td></td><td></td><td>

'06'
'41'
'42'

'4F'</td><td>

Thay đổi
Thay đổi
Thay đổi

Thay đổi</td><td colspan="3">Quyền phân bổ thẻ (xem TCVN 11167-6)
– Mã định danh đối tượng (OID)
– Thẩm quyền quốc gia (xem TCVN 11167-4)
– Bên phát hành (xem TCVN 11167-4)
– Mã định danh ứng dụng (AID), định danh ứng dụng và bên cung cấp (xem TCVN 11167-4)
Thẩm quyền phân bổ thẻ mặc định của cơ quan có thẩm quyền.</td><td>Một trong những DO này là bắt buộc nếu có 'A1'</td></tr>
<tr><td></td><td></td><td>'A1'</td><td>Thay đổi</td><td colspan="3">Thông tin sinh trắc học của các DO quy định bởi quyền phân bổ thẻ (định danh bắt buộc, xem bên trên) Cũng xem ví dụ trong Phụ lục C</td><td>Bắt buộc nếu không có 'A0'</td></tr>
<tr><td></td><td></td><td></td><td></td><td>Thẻ</td><td>Độ dài</td><td>Giá trị</td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td>

'8x'/'Ax'
'9x'/'Bx'</td><td>

Thay đổi
Thay đổi</td><td>Các DO đinh nghĩa bởi thẩm quyền phân bổ thẻ
... (nguyên thủy/nhân tạo)
... (nguyên thủy/nhân tạo)</td><td>

Phụ thuộc DO</td></tr>
</table>

CHÚ THÍCH Trong trường hợp thẻ không thực hiện quá trình xác minh, khuôn mẫu thông tin sinh trắc học cũng có thể chứa dữ liệu tham chiếu sinh trắc học (xem Bảng 3) và dữ liệu có thể tùy ý (thẻ '53' hoặc '73') ví dụ: để dữ liệu được chuyển giao cho một hệ thống dịch vụ, nếu xác minh là tích cực (xem Phụ lục C).

Nếu một số BIT Ưu tiên bên trong cùng một ứng dụng, thì chúng phải được nhóm lại như trong Bảng 2.

Bảng 2 - Khuôn mẫu nhóm BIT

Thẻ	Độ dài	Giá trị			Ưu tiên
'7F61'	Thay đổi	Khuôn mẫu nhóm BIT			
		Thẻ	**Độ dài**	**Giá trị**	
		'02'	Thay đổi	Số lượng các BIT trong nhóm	Bắt buộc
		'7F60'	Thay đổi	BIT 1	Theo điều kiện
				...	
		'7F60'	Thay đổi	BIT n	Theo điều kiện

Một khuôn mẫu nhóm BIT có thể được phục hồi, ví dụ: bởi

- Một lệnh GET DATA
- Đọc ra một tập tin trong DF, EFID tương ứng tìm thấy trong FCI, hoặc
- Đọc một mẫu SE (xem TCVN 11167-4), trong đó mẫu nhóm BIT được lưu trữ.

6.2 Dữ liệu sinh trắc học

Dữ liệu sinh trắc học (dữ liệu xác minh sinh trắc học, dữ liệu tham chiếu sinh trắc học) có thể được trình bày:

- như một tổ hợp các phần tử dữ liệu,
- trong một dữ liệu sinh trắc học DO được quy định trong TCVN 11167-6 (ISO/IEC 7816-6), hoặc
- như tổ hợp của các DO trong một mẫu dữ liệu sinh trắc học, xem Bảng 3.

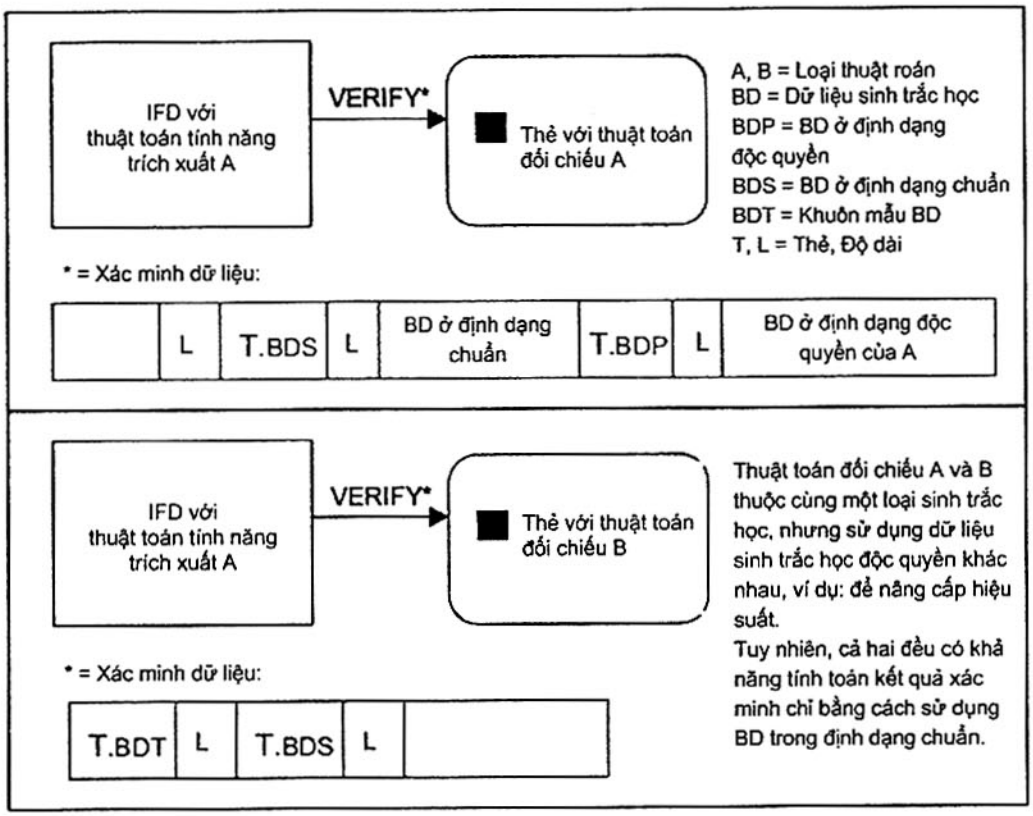
Bảng 3 - Dữ liệu sinh trắc học của các DO

Thẻ	Độ dài	Giá trị			Ưu tiên
'5F2E'	Thay đổi	Dữ liệu sinh trắc học			
'7F2E'	Thay đổi	Khuôn mẫu dữ liệu sinh trắc học			
		Thẻ	**Độ dài**	**Giá trị**	
		'5F2E'	Thay đổi	Dữ liệu sinh trắc học	Ít nhất một trong các DO được xem xét, nếu khuôn mẫu được dùng
		'81'/'A1'	Thay đổi	Dữ liệu sinh trắc học với định dạng chuẩn hóa (nguyên thủy/nhân tạo)	
		'82'/'A2'	Thay đổi	Dữ liệu sinh trắc học với định dạng độc quyền (nguyên thủy/nhân tạo)	

Như trình bày trong Bảng 3, dữ liệu sinh trắc học có thể được chia thành một phần với định dạng chuẩn và trong một phần với định dạng độc quyền, theo đó một phần với các định dạng

độc quyền có thể được sử dụng, ví dụ: để đạt được một hiệu suất tốt hơn. Việc sử dụng dữ liệu sinh trắc học với các định dạng chuẩn và độc quyền được trình bày trong Hình 1.

Cấu trúc và mã hóa dữ liệu sinh trắc học là loại sinh trắc học (ví dụ: đặc điểm khuôn mặt, dấu vân tay) phụ thuộc và nằm ngoài phạm vi của tiêu chuẩn này.



Hình 1 - Sử dụng dữ liệu sinh trắc học với cấu trúc độc quyền và chuẩn hóa

6.3 Thông tinh yêu cầu xác minh

6.3.1 Mục đích

Yêu cầu xác minh hiện nay được cung cấp bởi:

- Yêu cầu xác minh đối tượng dữ liệu thông tin VIDO (thẻ '96', định dạng ngắn), hoặc
- Yêu cầu xác minh thông tin mẫu VIT (thẻ 'A6', dạng dài).

VIDO hoặc VIT, nếu có, là một phần của thông tin thông số kiểm soát tập tin của DF tương ứng hoặc được lưu trữ trong một tập tin mở rộng FCI như được quy định trong TCVN 11167-4 (ISO/IEC 7816-4). VIDO và VIT chứa thông tin, trong đó cho biết dữ liệu tham khảo để chứng thực người dùng (ví dụ: mật khẩu và/hoặc dữ liệu sinh trắc học) là:

- Kích hoạt hay vô hiệu hóa và
- Có thể sử dụng hoặc không sử dụng được.

CHÚ THÍCH Thông thường các cờ kích hoạt/vô hiệu hóa dưới sự kiểm soát của chủ thẻ, cờ có thể sử dụng/không sử dụng dưới sự kiểm soát của bên cung cấp ứng dụng.

6.3.2 VIDO - định dạng ngắn

Byte đầu tiên của VIDO (xem Bảng 4) cho thấy bằng bản đồ bit mà các khóa (tức là dữ liệu tham chiếu để xác minh người dùng) được kích hoạt (bit đặt là 1) hay vô hiệu hóa (bit đặt là 0). Byte thứ hai chỉ ra bởi bản đồ bit mà các khóa sử dụng được (bit đặt là 1) hoặc không sử dụng được (bit đặt là 0). Mỗi byte sau đây là các tham chiếu khóa. Tham chiếu khóa đầu tiên tương ứng với bit b8 của các bản đồ bit, tham chiếu khóa thứ hai với bit b7 và tiếp tục. Số lượng tham chiếu khóa được đưa ra mặc nhiên bởi chiều dài của VIDO, ví dụ: khi L là nhỏ hơn hoặc bằng 10, số lượng tham chiếu khóa là L-2.

Bảng 4 - Cấu trúc VIDO

Thẻ VIDO	Độ dài	Cờ Bật/Tắt	Cờ Hữu dụng/ Vô dụng	Tham chiếu khóa	Tham chiếu khóa	...
'96'	Thay đổi	'xx'	'xx'	'xx'	'xx'	...

6.3.3 VIT - định dạng dài

Các VIT trình bày thông tin theo dạng dài, theo đó thông tin bổ sung có thể được cung cấp trong bộ định tính sử dụng DO. Các DO mà có thể xảy ra trong một VIT, được thể hiện trong Bảng 5.

Bảng 5 - Khuôn mẫu thông tin yêu cầu xác minh (VIT) và các DO nhúng

Thẻ	Độ dài	Giá trị		
'AB'	Thay đổi	Khuôn mẫu thông tin yêu cầu xác minh		
		Thẻ	Độ dài	Giá trị
		'90'	1	Cờ Bật/Tắt (Cờ DO)
		'95'	1	Bộ định tính sử dụng được quy định trong TCVN 11167-4 (ISO/IEC 7816-4)
		'83'	1	Tham chiếu khóa

Việc kích hoạt/vô hiệu hóa cờ DO là bắt buộc. Ít nhất mộttham chiếu khóa DO phải có mặt. Mỗi tham chiếu khóa DO có thể được bắt đầu bởi một bộ định tính sử dụng DO tương ứng. Nếu không thì bộ định tính sử dụng tương ứng với một khóa, thì việc sử dụng là mặc nhiên được biết đến. Trong ngữ cảnh này, một bộ định tính sử dụng đặt thành các giá trị 0, khóa tương ứng phải không được sử dụng.

CHÚ THÍCH Điều này không cần thiết để giới thiệu một VIT với một thẻ ứng dụng để lấy được bằng GET DATA, vì FCI hoặc các tập tin mở rộng FCI có thể luôn được đọc.

Phụ lục A

(tham khảo)

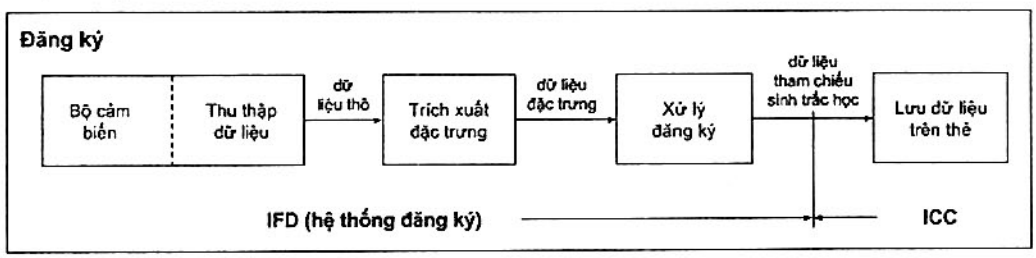
Quy trình xác minh sinh trắc học

A.1 Thuật ngữ viết tắt

Thuật ngữ	Tiếng Anh	Tiếng Việt
ICC	Integrated Circuit(s) Card	Thẻ mạch tích hợp
IFD	Interface Device	Thiết bị giao diện
OID	Object Identifier	Mã định danh đối tượng
SM	Secure Messaging	Thông điệp an ninh

A.2 Quy trình chọn lựa và quy trình xác minh

Lược đồ (giản thể) chung cho một quy trình chọn lựa được thể hiện trong Hình A.1.



Hình A.1 - Sơ đồ chung của quy trình chọn lựa

Cảm biến và mô-đun thu thập dữ liệu được coi là một đơn vị logic dù chúng có thể là các mô-đun riêng biệt. Dữ liệu thô thường được xử lý bên ngoài thẻ do kích thước đáng kể của dữ liệu thô.

Trong quá trình này, các đặc tính sinh trắc học được trích xuất và định dạng để sử dụng sau này. Trong quá trình chọn lựa hay ở giai đoạn sau, dữ liệu tham chiếu sinh trắc học có thể cùng với thông tin bổ sung được gửi theo một cách an toàn vào thẻ đối với việc lưu trữ và sử dụng tiếp theo.

Trong trường hợp đối chiếu trên thẻ, dữ liệu này không thể lấy ra sau khi lưu trữ. Trong trường hợp đối chiều ngoài thẻ, dữ liệu tham chiếu sinh trắc học có thể được lấy ra như là một phần của BIT. Dữ liệu tham chiếu sinh trắc học hoặc có thể toàn bộ BIT có thể được bảo đảm, ví dụ: bởi một chữ ký số. Ngoài việc truy cập với BIT có thể bị hạn chế, ví dụ: truy cập có thể chỉ sau khi thực hiện thành công một thủ tục xác thực.

Dữ liệu tham chiếu sinh trắc học có thể được lưu trữ trong thẻ:

- Trong giai đoạn cá nhân hóa thẻ, hoặc

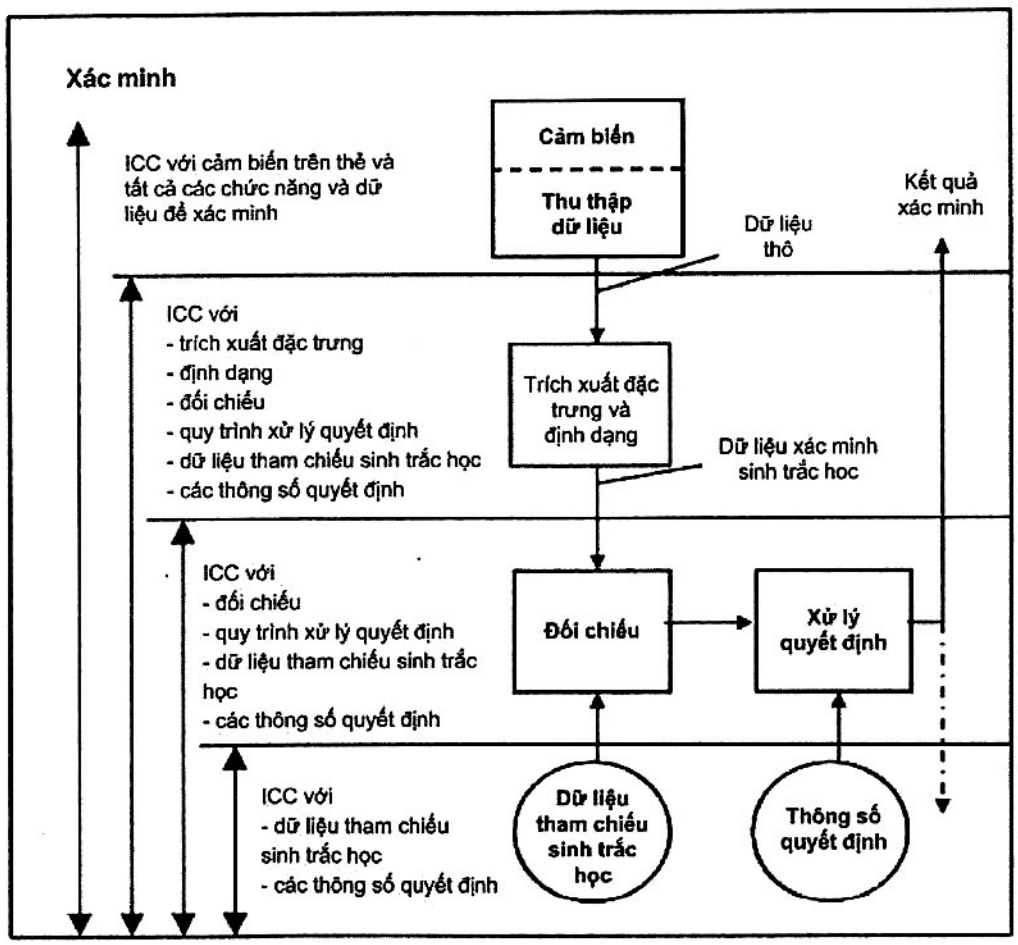
- Sau khi phát hành thẻ cho chủ thẻ.

Việc lưu trữ dữ liệu tham chiếu sau khi phát hành của thẻ cho chủ thẻ hoặc khi giao thẻ cho chủ thẻ được đề cập trong Phụ lục B.

Hình A.2 cho thấy một sơ đồ đơn giản cho một xác minh bao gồm các cấu hình sau:

- Với dữ liệu tham chiếu sinh trắc học và các thông số có thể được lưu trữ trong thẻ
- Với việc đối chiếu và xử lý quyết định trong thẻ
- Với tính năng trích xuất, định dạng, đối chiếu và xử lý quyết định trong thẻ
- Với một cảm biến trên thẻ và hiệu suất của quá trình xác minh toàn bộ trong thẻ.

Các cấu hình khác là có thể.



Hình A.2 - Sơ đồ chung của một quy trình xác minh

CHÚ THÍCH Các thông số quyết định thường bị ràng buộc để xử lý quyết định. Khi thẻ cung cấp dữ liệu tham chiếu sinh trắc học (có thể mã hóa bảo vệ) cho đối chiếu bên ngoài (trường hợp thấp nhất trong Hình A.2), các thông số quyết định có thể chỉ được thể hiên và lấy ra được (một cách an toàn), nếu chúng có chứa các thành phần cụ thể của người dùng.

A.3 Phân loại phương pháp xác minh sinh trắc học

Có tính đến trao đổi thông điệp khác nhau giữa thẻ và IFD, phân loại sau đây được sử dụng:

- Phương pháp xác minh sinh trắc học tĩnh:

  Một phương pháp xác minh sinh trắc học yêu cầu trình bày một đặc tính sinh lý (tức là tĩnh) của một cá nhân được xác thực (xem loại A) hay hiệu năng của một ghi danh, hành động được xác định trước (xem loại B).

- Phương pháp xác minh sinh trắc học động:

  Một phương pháp xác minh sinh trắc học yêu cầu một hành động động từ cá nhân được chứng thực (tức là một phản hồi của người dùng với một thách thức sinh trắc học, xem loại B).

Ví dụ về sinh trắc học loại A:

hình dạng tai
đặc điểm khuôn mặt
hình học ngón tay
vân tay
hình học tay
mống mắt
hình học cánh tay
võng mạc
mẫu mạch máu

CHÚ THÍCH Các loại sinh trắc học này chỉ có thể được dùng để xác minh tĩnh.

Ví dụ về sinh trắc học loại B:

gõ phím động
cử động môi
hình ảnh chữ ký
khẩu âm (âm tần)
động lực viết (chữ ký động)

CHÚ THÍCH Những loại sinh trắc học có thể được dùng để xác minh tĩnh hoặc xác minh năng động tùy thuộc vào cách sử dụng của các loại tương ứng.

Các đặc điểm chính của sinh trắc học loại A là:

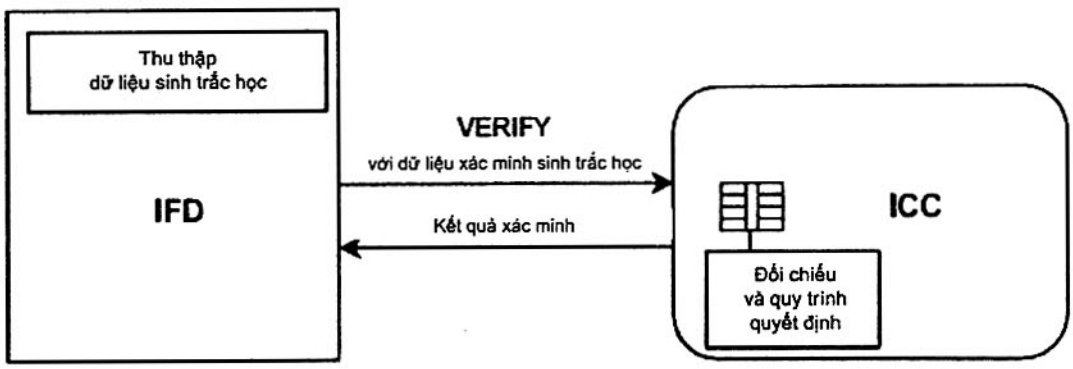
- Đơn nhất, không thể thay đổi được

- Có thể lựa chọn, nếu một số trường hợp cùng một loại tồn tại (ví dụ: ngón tay cái, ngón trỏ)
- Công khai, nếu các tính năng tương ứng (ví dụ: mặt, tai, vân tay) có thể được chụp hoặc đo bởi mọi mọi người, tức là những dữ liệu xác minh sinh trắc học tương ứng phải được trình bày với thẻ theo một cách xác thực (xem Phụ lục B, Hình B.4).

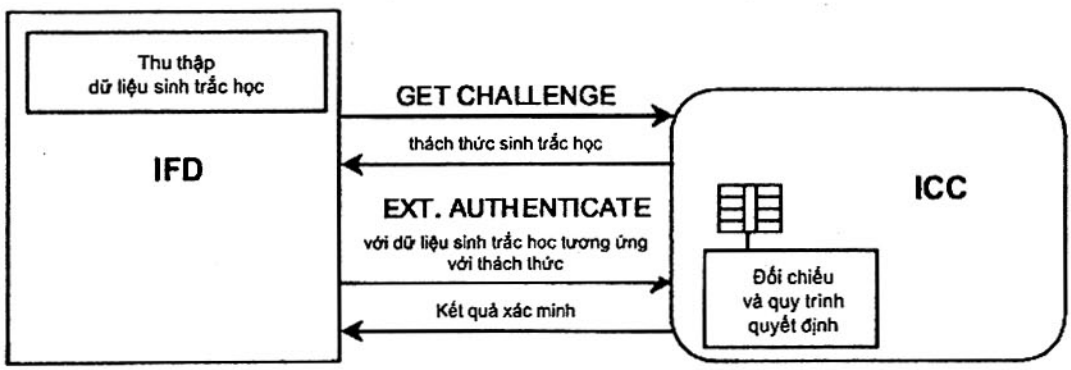
Các đặc điểm chính của sinh trắc học loại B là:

- Đơn nhất, nhưng điều chỉnh được
- Phụ thuộc thách thức, nếu việc xác minh động được sử dụng.

Hình A.3 và A.4 minh họa sự khác biệt giữa xác minh sinh trắc học tĩnh và động tại giao diện thẻ trong trường hợp đối chiếu và xử lý quyết định trên thẻ.



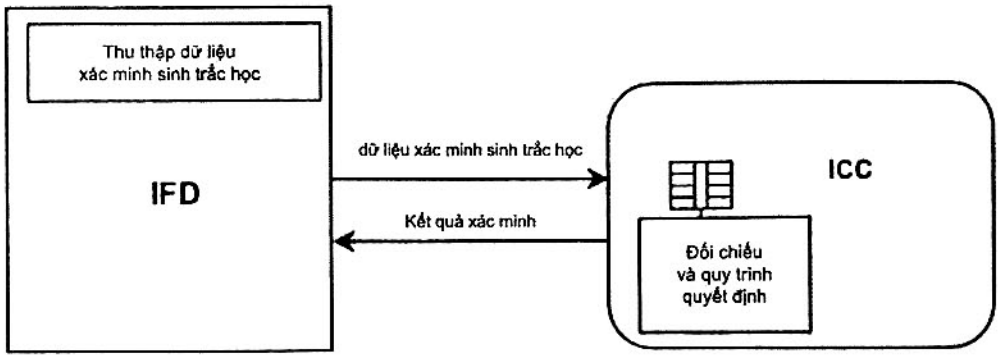
Hình A.3 - Lệnh đối với xác minh sinh trắc học tĩnh



Hình A.4 - Lệnh đối với xác minh sinh trắc học động

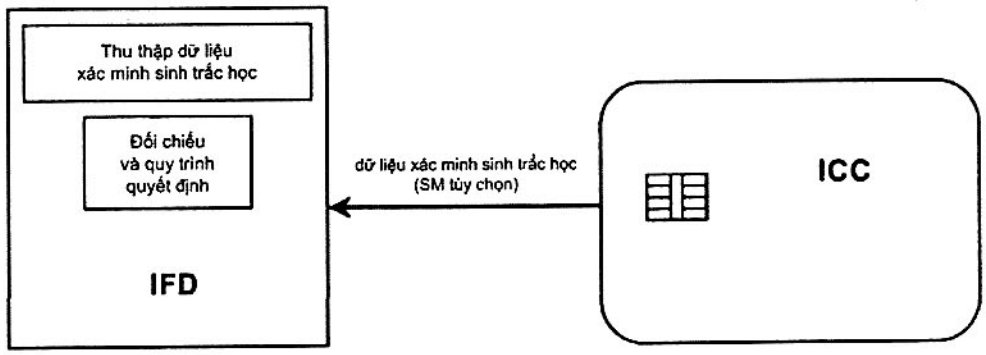
A.4 Lược đồ

Hình A.5 và A.6 minh họa một số kịch bản có liên quan tới xác minh sinh trắc học người dùng.

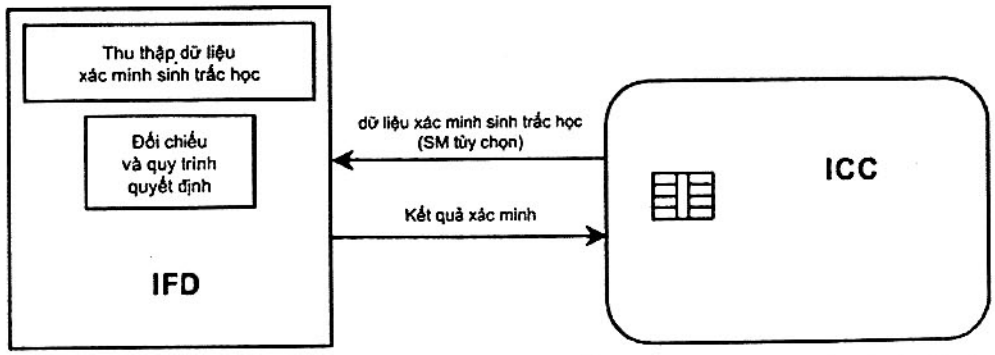


Kết quả của quá trình xác minh sinh trắc học sẽ thay đổi trạng thái an ninh thẻ. Nếu kết quả này cũng thay đổi trạng thái an ninh IFD thì sau đó nó cần được bảo vệ bằng thông điệp an ninh.

Hình A.5 - Lược đồ đối chiếu và quy trình quyết định trong thẻ



Điều kiện truy cập có thể được gắn vào dữ liệu tham chiếu sinh trắc học



Nếu kết quả của quá trình xác minh sinh trắc học thay đổi trạng thái an ninh thẻ thì nó cần được bảo vệ bằng thông điệp an ninh.

Hình A.6 - Lược đồ đối chiếu và quy trình quyết định ngoài thẻ

A.5 Truy hồi thông tin liên quan đối với quy trình xác minh sinh trắc học

Các IFD có thể cần thông tin liên quan đến quá trình xác minh. Danh sách sau đây gồm các mục thông tin có thể được yêu cầu bởi IFD:

- Loại sinh trắc học (ví dụ: dấu vân tay, đặc điểm khuôn mặt, ...)
- Sinh trắc học loại phụ, nếu thích hợp (ví dụ: ngón tay trỏ bên trái)
- Chỉ định dạng và loại định dạng dữ liệu sinh trắc học
- Tham chiếu thuật toán, nếu có và được sử dụng, ví dụ: trong lệnh MANAGE SECURITY ENVIRONMENT
- Mã định danh dữ liệu tham chiếu sinh trắc học (bộ định tính của dữ liệu tham chiếu trong lệnh VERIFY hoặc lệnh EXTERNAL AUTHENTICATE)
- Dữ liệu tùy ý, nếu có.

Phụ lục B

(tham khảo)

Ví dụ đối với việc lựa chọn và xác minh

B.1 Thuật ngữ viết tắt

Thuật ngữ	Tiếng Anh	Tiếng Việt
AID	Application Identifier	Mã định danh ứng dụng
AT	Authentication Template	Khuôn mẫu chứng thực
BIT	Biometric Information Template	Khuôn mẫu thông tin sinh trắc học
BT	Biometric Type	Loại sinh trắc học
CRT	Control Reference Template	Khuôn mẫu tham chiếu kiểm soát
DO	Data Object	Đối tượng dữ liệu
DST	Digital Signature Template	Khuôn mẫu chữ ký số
FCI	File Control Information	Thông tin kiểm soát tệp tin
FO	Format Owner	Chủ định dạng
FT	Format Type	Loại định dạng
ID	Identifier	Mã định danh
IFD	Interface Device	Thiết bị giao diện
OID	Object Identifier	Mã định danh đối tượng
RD	Reference Data	Dữ liệu tham chiếu
SM	Secure Messaging	Thông điệp an ninh
TAT	Tag allocation Authority Template	Khuôn mẫu thẩm quyền phân bổ thẻ
UQ	Usage Qualifier	Bộ định tính sử dụng
VIT	Verification Requirement Information Template	Khuôn mẫu thông tin yêu cầu xác minh
||	Concatenation	Kết hợp

B.2 Lựa chọn

Đối với ví dụ này, giả định rằng thẻ:

- là hoàn toàn cá nhân hóa, ngoại trừ việc lưu giữ dữ liệu tham chiếu sinh trắc học và khuôn mẫu thông tin sinh trắc học liên quan (điều này cũng bao gồm sự ưu tiên của một bản ghi sinh trắc học trong một tập tin khóa với các thuộc tính liên quan với dữ liệu tham

chiếu sinh trắc học, tức là bộ đếm thử lại với giá trị ban đầu, đặt lại mã với bộ đếm thử lại và giá trị ban đầu, các cờ với việc cho phép/vô hiệu hóa yêu cầu xác minh và khả năng thay đổi, ...)

- có xác minh mật khẩu nhằm bổ sung cho xác minh sinh trắc học.

Với lệnh CHANGE REFERENCE DATA, dữ liệu tham chiếu trắng được thay thế bằng dữ liệu tham chiếu người dùng được tính toán trong quá trình lựa chọn. Việc thi hành lệnh CHANGE REFERENCE DATA phải được ràng buộc với điều kiện an ninh, ví dụ: thiết lập trạng thái an ninh cần thiết sau khi hoàn thành thành công một thủ tục xác thực dựa trên mã hóa hay một mật khẩu được thể hiện thành công.

CHÚ THÍCH Các điều kiện an ninh cho lệnh CHANGE REFERENCE DATA, sau khi việc lựa chọn diễn ra, có thể khác nhau do các chính sách bảo mật của bên cung cấp ứng dụng (ví dụ: thay đổi dữ liệu tham chiếu không còn được phép sau khi ghi danh).

Sau khi dữ liệu tham chiếu sinh trắc học được lưu trữ, các Khuôn mẫu thông tin sinh trắc học BIT phải được lưu trữ, được sử dụng bởi IFD trong một quá trình xác minh trong ví dụ này. BIT được lưu trữ sau khi tất cả các loại và phân nhóm của tham chiếu sinh trắc học được lựa chọn.

Thông thường, một IFD (ví dụ: một máy tính, một thiết bị đầu cuối Internet công cộng hoặc một thiết bị đầu cuối tiền mặt) không được biết, cho dù thẻ đã trình bày:

- thuộc về một người dùng áp dụng sinh trắc học
- có một thuật toán sinh trắc học được hỗ trợ bởi các IFD
- loại sinh trắc học được sử dụng mà nó cần được cân nhắc
- giá trị mà tham chiếu khóa có liên quan (tức là bộ định tính dữ liệu tham khảo) có
- việc thực hiện các thông số thuật toán đối chiếu cụ thể phải được quan sát (ví dụ: giới hạn về số lượng chi tiết vụn vặt để được gửi trong dữ liệu xác minh).

Vì vậy các khuôn mẫu thông tin sinh trắc học cần cung cấp các thông tin như:

- bộ định tính dữ liệu tham chiếu sinh trắc học
- các OID của cơ quan cấp thẻ và việc định danh định dạng cho dữ liệu xác minh
- loại sinh trắc học và nhóm sinh trắc hoc được lựa chọn (ví dụ: ngón tay cái bên phải)
- các đối tượng dữ liệu khác, nếu có
- sự lặp lại của các DO tương ứng, nếu ví dụ: một sinh trắc học loại hai được lựa chọn.

Hình B.1 thể hiện các lệnh có thể được thực hiện theo cách này trong một quá trình lựa chọn.

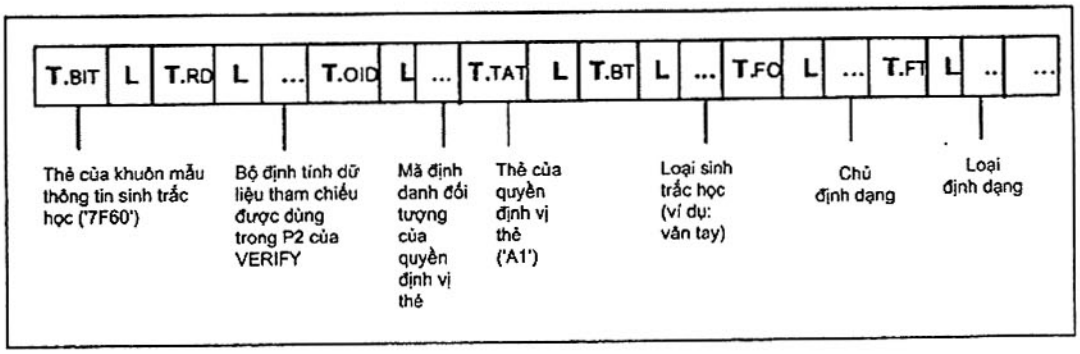
Lệnh / Hồi đáp	Ý nghĩa
VERIFY <mật khẩu> → **OK** ←	Thiết lập trạng thái ninh để lưu trữ các dữ liệu tham khảo sinh trắc học
CHANGE RD <dữ liệu tham chiếu sinh trắc học> → **OK** ←	Thay thế dữ liệu tham chiếu trống bằng dữ liệu tham chiếu sinh trắc học đã đăng ký
SELECT <ID tệp tin> → **OK** ←	Lựa chọn các tập tin cơ sở để lưu trữ khuôn mẫu thông tin sinh trắc học BIT (được lấy ra với lệnh GET DATA)
UPDATE BINARY <BIT> → **OK** ←	Lưu trữ khuôn mẫu thông tin sinh trắc học BIT

Hình B.1 - Lệnh đối với việc lựa chọn (ví dụ)

CHÚ THÍCH 1 Có thể có một sự cần thiết để bảo vệ việc chọn lựa thông điệp an ninh.

CHÚ THÍCH 2 Đối với thông tin lưu trữ và phục hồi cũng có các lệnh khác như mô tả trong TCVN 11167-4 (ISO/IEC 7816-4) có thể được sử dụng. Điều này cũng có hữu ích trong Hình B.4, B.6 và B.7.

Hình B.2 thể hiện BIT và các DO của nó.



Hình B.2 - Ví dụ về khuôn mẫu thông tin sinh trắc học (BIT), thẻ đánh dấu được ấn định bởi quyền ấn định thẻ được quy định

CHÚ THÍCH Các thẻ bên trong mẫu 'A1' được xác định thẩm quyền cấp thẻ được biểu thị.

B.3 Xác minh với một phương pháp sinh trắc học đơn lẻ

Quá trình xác minh bắt đầu với việc thu hồi các khuôn mẫu thông tin sinh trắc học, ví dụ: bằng cách áp dụng lệnh GET DATA. Nếu IFD hỗ trợ định dạng được yêu cầu cho dữ liệu xác minh sinh trắc học như được chỉ ra trong BIT và người dùng đã thể hiện đối tượng sinh trắc

học có liên quan, dữ liệu xác minh được được tính toán và chuyển tới thẻ bằng cách sử dụng lệnh VERIFY (xem Hình B.3).

Lệnh / Hồi đáp	Ý nghĩa
SELECT <AID> → **OK** ←	Lựa chọn ứng dụng với mã định danh ứng dụng (AID)
GET DATA <thẻ BIT> → Khuôn mẫu thông tin sinh trắc học ←	Truy thu khuôn mẫu thông tin sinh trắc học BIT
VERIFY <Dữ liệu xác minh sinh trắc học> → **OK** ←	Xác minh người dùng

Hình B.3 - Lệnh đối với xác thực không có thông điệp an ninh (ví dụ)

CHÚ THÍCH Nếu không có khuôn mẫu thông tin sinh trắc học là, nghĩa là trong ví dụ này là người dùng tương ứng sẽ không sử dụng sinh trắc học.

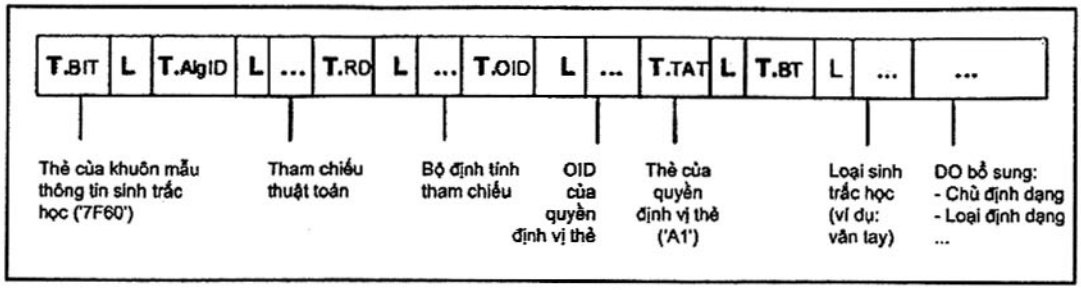
Nếu dữ liệu xác minh sinh trắc học được công khai (ví dụ: mặt, dấu vân tay, hình dạng tai), thì có một nhu cầu để bảo vệ chúng với thông điệp an ninh (xem Hình B.4).

Lệnh / Hồi đáp	Ý nghĩa
SELECT <AID> → **OK** ←	Lựa chọn ứng dụng với mã định danh ứng dụng (AID)
GET DATA <thẻ BIT> → Khuôn mẫu thông tin sinh trắc học ←	Truy thu khuôn mẫu thông tin sinh trắc học BIT
MANAGE SE <Tham chiếu khóa DO> → **OK** ←	Thiết lập CRT DST với khóa công khai đối với việc xác minh chứng nhận
VERIFY CERTIFICATE <chứng nhận> → **OK** ←	Xác minh chứng nhận phụ thuộc đơn vị sinh trắc học
GET CHALLENGE → số ngẫu nhiên ←	Yêu cầu một thách thức được sử dụng cho thông điệp an ninh
EXTERNAL AUTHENTICATE <chứng thực liên quan tới dữ liệu> → chứng thực liên quan tới dữ liệu ←	Chứng thực bên ngoài với việc thiết lập các khóa SM
VERIFY CERTIFICATE <chứng nhận> → **OK** ←	Xác minh người dùng với dữ liệu xác minh được bảo vệ SM; hồi đáp cũng có thể là SM được bảo vệ

Hình B.4 - Lệnh đối với xác minh thông điệp (ví dụ)

CHÚ THÍCH Thông điệp an ninh (SM) được nêu trong TCVN 11167-4 (ISO/IEC 7816-4).

Trong ví dụ này, quy trình xác minh bắt đầu với việc thu hồi khuôn mẫu thông tin yêu cầu xác minh (VIT) và khuôn mẫu thông tin sinh trác học tương ứng (BIT), trong đó có thể được lưu trữ, ví dụ: trong tệp tin mở rộng FCI (ID tệp tin mặc nhiên được biết đến). VIT chứa thông tin, dù việc xác minh sinh trắc học và/hoặc xác minh mật khẩu có sẵn và kích hoạt hay không có phép và bộ định tính tương ứng của dữ liệu tham chiếu (KeyRef) phải được sử dụng tại các giao diện thẻ. BIT trong ví dụ này (xem Hình B.5) chứa thông tin về tham chiếu thuật toán cụ thể thẻ (AlgID), bộ định tính của dữ liệu tham chiếu (KeyRef) và thông tin bổ sung như: loại sinh trắc học, chủ định dạng và kiểu định dạng.



Hình B.5 - Ví dụ về khuông mẫu thông tin sinh trắc học (BIT)

Nếu IFD và các thẻ được xem xét hỗ trợ các cơ chế tương tự và người dùng đã xem xét các đặc trưng sinh trắc học có liên quan, việc xác minh dữ liệu được tính toán và chuyển giao cho thẻ bằng cách sử dụng lệnh VERIFY trước đó bởi một lệnh MANAGE SECURITY ENVIRONMENT để chọn ra phương pháp xác nhận đặc biệt (xem Hình B.6).

Lệnh / Hồi đáp	Ý nghĩa
SELECT <ID tệp tin> → **OK** ←	Lựa chọn các tập tin mở rộng FCI
READ BINARY → VIT || BIT ←	Truy hồi khuôn mẫu thông tin yêu cầu xác minh VIT và khuôn mẫu thông tin sinh trắc học BIT
MANAGE SE <DO UQ || tham chiếu thuật toán DO Alg. || tham chiếu khóa DO> → **OK** ←	Thiết CRT AT với bộ định tính sử dụng UQ, tham chiếu thuật toán và tham chiếu khóa
VERIFY <dữ liệu sinh trắc học> → **OK** ←	Xác minh ngươi dùng

Hình B.6 - Lệnh đối với xác minh không cần thông điệp an ninh (ví dụ)

Khi xác minh sinh trắc học tĩnh cần thông tin từ thẻ trước khi xác minh, thông tin này có thể có mặt trong mẫu thông tin sinh trắc học.

B.4 Truy cập vào BIT trong trường hợp đối chiếu ngoài thẻ

BIT có thể kết hợp với các dữ liệu khác (ví dụ: dữ liệu giấy phép lái xe) có thể được bảo vệ ví dụ: bởi chữ ký của cơ quan cấp (ví dụ về việc bảo vệ dữ liệu xem Phụ lục D). Vì vậy BIT có thể được lấy ra bằng cách áp dụng một lệnh READ BINARY đơn giản, xem Hình B.7.

Lệnh / Hồi đáp	Ý nghĩa
SELECT <ID tệp tin> → **OK** ←	Lựa chọn các tập tin chứa khuôn mẫu thông tin sinh trắc học
READ BINARY → BIT ←	Các DO BIT có thể chứa khuôn mẫu thông điệp an ninh, ví dụ: để bảo đảm việc chứng thực dữ liệu tham chiếu sinh trắc học

Hình B.7 - Lệnh đối với truy hồi BIT (ví dụ)

Việc truy cập vào BIT thể bị hạn chế, tức là trước khi đọc một thủ tục chứng thực phải được thực hiện như trình bày Hình B.8.

Lệnh / Hồi đáp	Ý nghĩa
GET CHALLENGE → số ngẫu nhiên ←	Lấy một số ngẫu nhiên
EXT. AUTHENTICATE <chứng thực dữ liệu liên quan> → **OK** ←	Chứng thực các thực thể có quyền truy cập tới các BIT
READ BINARY → BIT ←	Đọc BIT

Hình B.8 - Lệnh đối với truy hồi các BIT sau khi thực hiện thủ tục xác minh (ví dụ)

Nếu BIT có được truyền, ví dụ: qua Internet, thì nó có thể là cần thiết để áp dụng thông điệp an ninh như trong Hình B.4 để cung cấp bảo mật và xác minh.

Phụ lục C

(tham khảo)

Đối tượng dữ liệu thông tin sinh trắc học

Phụ lục này trình bày các đối tượng dữ liệu thông tin sinh trắc học dựa trên Khung CBEFF, xem ISO/IEC 19785.

C.1 Thuật ngữ viết tắt

Thuật ngữ	Tiếng Anh	Tiếng Việt
BDB	Biometric Data Block	Khối dữ liệu sinh trắc học
BHT	Biometric Header Template	Khuôn mẫu tiêu đề sinh trắc học
BIT	Biometric Information Template	Khuôn mẫu thông tin sinh trắc học
CBEFF	Common Biometric Exchange Formats Framework	Khung định dạng trao đổi sinh trắc học phổ biến
DO	Data Object	Đối tượng dữ liệu
IBIA	International Biometric Industry Association	Hiệp hội công nghiệp sinh trắc học quốc tế
IC	Integrated Circuit(s)	Mạch tích hợp
MAC	Message Authentication Code	Mã chứng thực thông điệp
OID	Object Identifier	Mã định danh đối tượng
PID	Product Identifier	Mã định danh sản phẩm
SE	Security Environment	Môi trường an ninh
SMT	Secure Messaging Template	Khuôn mẫu thông điệp an ninh
TLV	Tag-Length-Value	Giá trị-độ dài-thẻ

C.2 Đối tượng dữ liệu thông tin sinh trắc học sử dụng trong trường hợp đối chiếu ngoài thẻ

C.2.1 Sử dụng một loại hoặc loại phụ sinh trắc học đơn lẻ

Trước một quá trình xác minh, thông tin có thể được lấy ra từ một thẻ thể hiện các chi tiết trực quan khi thực hiện quá trình xác minh. Các đối tượng dữ liệu có liên quan được trình bày trong Bảng C.1.

Bảng C.1 - Đối tượng dữ liệu thông tin sinh trắc học trong trường hợp đối chiếu ngoài thẻ

Thẻ	Độ dài	Giá trị					Ưu tiên
'7F60'	Thay đổi	Khuôn mẫu thông tin sinh trắc học (BIT)					
		Thẻ	**Độ dài**	**Giá trị**			
		'80'	1	Tham chiếu thuật toán đối với việc sử dụng trong lệnh VERIFY/EXT. AUTHENTICATE/MANAGE được quy định trong TCVN 11167-4 (ISO/IEC 7816-4); xem CHÚ THÍCH 5			Tùy chọn
		'83'	1	Bộ đinh tính dữ liệu tham chiếu đối với việc sử dụng trong lệnh VERIFY/EXT. AUTHENTICATE/MANAGE được quy định trong TCVN 11167-4 (ISO/IEC 7816-4)			Tùy chọn
		'06'	Thay đổi	OID của bộ tiêu chuẩn CBEFF, xem CHÚ THÍCH 6			Bắt buộc nếu không mặc định sử dụng
		'A1'	Thay đổi	Khuôn mẫu tiêu đề sinh trắc học (BHT) phù hợp với CBEFF			Bắt buộc
				Thẻ	**Độ dài**	**Giá trị**	
				'80'	2	Phiên bản tiêu đề bảo trợ (mặc định '0101')	Bắt buộc nếu không mặc định sử dụng
				'90'	Thay đổi	Chỉ mục, mã định danh đơn nhất được dùng đối với việc tham chiếu tập dữ liệu sinh trắc học này trong ngữ cảnh ứng dụng bên ngoài thẻ	Tùy chọn
				'81'	1-3	Loại sinh trắc học, xem Bảng C.2	Tùy chọn
				'82'	1	Loại phụ sinh trắc học, xem Bảng C.3	Tùy chọn, sử dụng chỉ với loại sinh trắc học
				'83'	7	Ngày tạo và thời gian của dữ liệu sinh trắc học (CCYMMDDhhmmss)	Tùy chọn
				'84'	Thay đổi	Bộ khởi tạo	Tùy chọn
				'85'	8	Thời gian hiệu lực (từ CCYYMMDD tới CCYYMMDD)	Tùy chọn

Thẻ	Độ dài	Giá trị					Ưu tiên
				'86'	2	Mã định danh sản phẩm (PID) tạo ra dữ liệu tham chiếu sinh trắc học, giá trị được gán bởi IBIA, xem: www.ibia.org	Tùy chọn
				'87'	2	Chỉ định dạng của dữ liệu xác minh sinh trắc học, giá trị được gán bởi IBIA, xem: www.ibia.org	Bắt buộc
				'88'	2	Loại định dạng của dữ liệu xác minh sinh trắc học, được quy định bởi chỉ định dạng	Bắt buộc
				'91'/'B1'	Thay đổi	Thông số thuật toán đối chiếu sinh trắc học (nguyên thủy/nhân tạo), xem CHÚ THÍCH 2 và 7.	Tùy chọn

CHÚ THÍCH 1 Chỉ có những đối tượng dữ liệu từ CBEFF được trình bày có liên quan với đối chiếu trên thẻ.

CHÚ THÍCH 2 Đối tượng dữ liệu bổ sung không được trình bày trong cấu trúc CBEFF chính.

CHÚ THÍCH 3 Trong Bảng C.1 các khối dữ liệu sinh trắc học được quy định trong ISO/IEC 19785 không được trình bày, khi dữ liệu tham chiếu sinh trắc học được lưu giữ riêng trong thẻ và không có trong BIT này, và dữ liệu xác minh sinh trắc học phải được trình bày bằng lệnh VERIFY.

CHÚ THÍCH 4 Trong Bảng C.1 không dữ liệu nào được trình bày, khi thường truy cập vào một dữ liệu, nếu được sử dụng bởi các ứng dụng, được cấp sau khi hoàn thành công việc xác minh sinh trắc học. dữ liệu có thể được lấy ra bằng cách sử dụng lệnh truy cập như GET DATA hoặc READ BINARY.

CHÚ THÍCH 5 Thế giới bên ngoài (như: IFD) dùng chỉ định dạng/loại định dạng để xác định cấu trúc cần thiết cho dữ liệu xác minh. Thuật toán đối chiếu trong thẻ được đề cập trong tham chiếu thuật toán.

CHÚ THÍCH 6 Nếu các phiên bản ISO của CBEFF (ISO/IEC 19785) được sử dụng, thì các OID của bộ tiêu chuẩn ISO có liên quan (ISO/IEC JTC1/SC37) là giá trị mặc định, tức là DO với thẻ '06' có thể là để trống. Nếu các OID đề cập đến NISTIR 6529, thì OID của Bộ ghi đối tượng an toàn máy tính (CSOR) tại NIST{joint-iso-itu-t (2) country (16) us (840) organization (1) gov (101) csor (3)} được sử dụng (mã 16 của OID: "608648016503").

CHÚ THÍCH 7 DO này cung cấp bất kỳ thông số đặc biệt của một việc thực hiện thuật toán đối chiếu trên thẻ, ví dụ: số lượng tối đa của các điểm dự kiến trong dữ liệu xác minh sinh trắc học xác minh. Nội dung của DO này được xác định bởi chỉ định dạng.

Bảng C.2 - Loại sinh trắc học được quy định trong ISO/IEC 19785

Tên loại sinh trắc học	Giá trị
Không có thông tin được đưa ra	'00'
Nhiều sinh trắc học được dùng	'01'
Đặc điểm khuôn mặt	'02'
Âm lượng	'04'
Dấu vân tay	'08'
Võng mạc	'10'
Mống mắt	'20'
Hình học tay	'40'
Động lực chữ ký	'80'
Động lực gõ phím	'0100'
Chuyển động môi	'0200'
Hình ảnh mặt nhiệt	'0400'
Hình ảnh tay nhiệt	'0800'
Dáng đi	'1000'
Mùi cơ thể	'2000'
DNA	'4000'
Hình dáng tai	'8000'
Hình học ngón tay	'010000'
Dấu cánh tay	'020000'
Mẫu mạch máu	'040000'
Dấu chân	'080000'
Các giá trị RFU khác	

CHÚ THÍCH Một số loại sinh trắc học có thể không thích hợp cho các ứng dụng bằng cách sử dụng thẻ.

Bảng C.3 - Loại phụ sinh trắc học được quy định trong ISO/IEC 19785

b8	b7	b6	b5	b4	b3	b2	b1	Loại phụ sinh trắc học
0	0	0	0	0	0	0	0	Không có thông tin được đưa ra
						0	1	Bên phải
						1	0	Bên trái
			0	0	0			Không có ý nghĩa
			0	0	1			Ngón cái
			0	1	0			Ngón trỏ
			0	1	1			Ngón giữa
			1	0	0			Ngón tay đeo nhẫn
			1	0	1			Ngón út
								Các giá trị RFU khác

C.2.2 Sử dụng các định dạng dữ liệu sinh trắc học chuẩn hóa và độc quyền

Trong trường hợp dữ liệu xác minh sinh trắc học bao gồm dữ liệu xác minh sinh trắc học với cấu trúc chuẩn theo sau dữ liệu xác minh sinh trắc học với một cấu trúc cụ thể của bên sản xuất, một cấu trúc lồng nhau BHT nên được áp dụng như trong Bảng C.4.

Bảng C.4 - BIT với các BHT lồng ghép đối với dữ liệu sinh trắc học của định dạng chuẩn và độc quyền (ví dụ)

Thẻ	Độ dài	Giá trị						
'7F60'	Thay đổi	BIT						
		Thẻ	**Độ dài**	**Giá trị**				
		'80'	1	Tham chiếu thuật toán				
		'83'	1	Bộ định tính dữ liệu tham chiếu				
		'06'	Thay đổi	OID của bộ tiêu chuẩn CBEFF, xem CHÚ THÍCH 6 trong Bảng C.1				
		'A1'	Thay đổi	BHT (mức 1)				
				Thẻ	**Độ dài**	**Giá trị**		
				...		Các DO phổ biến, xem Bảng C.1		
				'A1'	Thay đổi	BHT (mức 2)		
						Thẻ	**Độ dài**	**Giá trị**
						'87'	2	Chỉ định dạng của dữ liệu xác minh sinh trắc học, ví dụ: mã định danh chỉ định dạng của cơ quan có thẩm quyền
						'88'	2	Loại định dạng của dữ liệu xác minh sinh trắc học, được quy định bởi chỉ định dạng
				'A2'	Thay đổi	BHT (mức 2)		
						Thẻ	**Độ dài**	**Giá trị**
						'87'	2	Chỉ định dạng của dữ liệu xác minh sinh trắc học, ví dụ: bên sản xuất thẻ
						'88'	2	Loại định dạng của dữ liệu xác minh sinh trắc học, được quy định bởi chỉ định dạng

C.2.3 Sử dụng nhiều loại hay loại phụ sinh trắc học

Nếu trong cùng một ứng dụng một số loại sinh trắc học hoặc phân nhóm sinh trắc học được sử dụng độc lập và tham chiếu bởi bộ định tính dữ liệu tham chiếu khác nhau (tương tự như một mật khẩu cho chữ ký và mật khẩu riêng biệt để xác thực), sau đó là một cấu trúc nhóm BIT với các BIT lồng nhau được áp dụng, xem Bảng C.5.

Bảng C.5 - Khuôn mẫu nhóm BIT với các BIT lồng nhau đối với ứng dụng có nhiều dữ liệu tham chiếu với các bộ định tính dữ liệu tham chiếu (ví dụ)

Thẻ	Độ dài	Giá trị						
'7F61'	Thay đổi	Mẫu nhóm thông tin sinh trắc học						
		Thẻ	Độ dài	Giá trị				
		'02'	1	'02' = Số các BIT				
		'7F60'	Thay đổi	BIT 1				
				Thẻ	Độ dài	Giá trị		
				'80'	1	Tham chiếu thuật toán		
				'83'	1	Bộ định tính dữ liệu tham chiếu		
				'06'	Thay đổi	OID của bộ tiêu chuẩn CBEFF, xem CHÚ THÍCH 6 của Bảng C.1		
				'A1'	Thay đổi	BHT		
						Thẻ	Độ dài	Giá trị
						...		
						'81'	1-3	Loại sinh trắc học, ví dụ: vân tay
						'82'	1	Loại phụ sinh trắc học, ví dụ: dấu tay nón trỏ phải
						'87'	2	Chỉ định dạng của dữ liệu xác minh sinh trắc học
						'88'	2	Loại định dạng của dữ liệu xác minh sinh trắc học, được quy định bởi chỉ định dạng
		'7F60'	Thay đổi	BIT 2				
				Thẻ	Độ dài	Giá trị		
				'80'	1	Tham chiếu thuật toán		
				'83'	1	Bộ định tính dữ liệu tham chiếu		

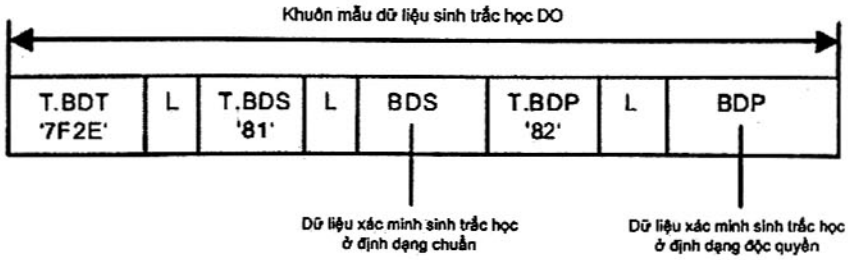
Thẻ	Độ dài	Giá trị						
				'06'	Thay đổi	OID của bộ tiêu chuẩn CBEFF, xem CHÚ THÍCH 6 của Bảng C.1		
				'A1'	Thay đổi	BHT		
						Thẻ	**Độ dài**	**Giá trị**
						...		
						'81'	1-3	Loại sinh trắc học, ví dụ: vân tay
						'82'	1	Loại phụ sinh trắc học, ví dụ: dấu tay ngón trỏ phải
						'87'	2	Chỉ định dạng của dữ liệu xác minh sinh trắc học
						'88'	2	Loại định dạng của dữ liệu xác minh sinh trắc học, được quy định bởi chỉ định dạng

C.2.4 Sử dụng sinh trắc học đa hình

Trong trường hợp một số tính năng sinh trắc học (theo nghĩa của sinh trắc học đa phương thức hoặc kết hợp) phải được xác nhận qua ví dụ để có được quyền truy cập vào dữ liệu nhất định hoặc một phím cụ thể, các nhóm BIT với BIT lồng nhau được áp dụng và thực hiện việc xác minh bằng cách gửi nhiều lệnh VERIFY. Các điều kiện truy cập thuộc các định nghĩa đối tượng được bảo vệ có liên quan, trong đó kết hợp các tính năng sinh trắc học phải được xác minh thành công.

C.2.5 Trình bày dữ liệu xác minh sinh trắc học

Việc mã hóa và định dạng các lệnh để xác minh sinh trắc học có thể mang dữ liệu xác minh sinh trắc học vào thẻ, được nêu trong TCVN 11167-4 (ISO/IEC 7816-4). Các khả năng mã hóa cho các trường dữ liệu lệnh được nêu tại Điều 6.2 của TCVN 11167-11 (ISO/IEC 7816-11). Hình C.1 thể hiện ví dụ của trường dữ liệu lệnh liên quan đến các ví dụ được đưa ra trong Bảng C.4.



Hình C.1 - Khuôn mẫu dữ liệu sinh trắc học trong trường lệnh (ví dụ)

C.3 Đối tượng dữ liệu thông tin sinh trắc học sử dụng trong trường hợp đối chiếu ngoài thẻ

C.3.1 Xây dựng và sử dụng chung

Đối tượng dữ liệu cho đối chiếu ngoài thẻ được trình bày như BIT, trong đó bao gồm:

- Khuôn mẫu tiêu đề sinh trắc học BHT,
- Khối dữ liệu sinh trắc học BDB gồm dữ liệu tham chiếu sinh trắc học có thể theo sau bởi một dữ liệu và
- Các DO tùy chọn liên quan đến an ninh, xem Điều C.3.4.

Việc sử dụng các cấu trúc dữ liệu được trình bày trong các mục tiếp theo không bị giới hạn thẻ IC, tức là cấu trúc dữ liệu cũng có thể được sử dụng trong các loại thẻ, ví dụ: thẻ dải từ, thẻ nhớ quang học hoặc thẻ có mã vạch 2 chiều.

C.3.2 Sử dụng một loại hay loại phụ sinh trắc học

Trong bảng C.7, các DO có liên quan cho đối chiếu ngoài thẻ được quy định, nếu một loại sinh trắc học duy nhất hoặc kiểu phụ được sử dụng.

Bảng C.7 - Đối tượng dữ liệu thông tin sinh trắc học sử dụng trong trường hợp đối chiếu ngoài thẻ

Thẻ	Độ dài	Giá trị					Ưu tiên
'7F60'	Thay đổi	Khuôn mẫu thông tin sinh trắc học (BIT)					
		Thẻ	**Độ dài**	**Giá trị**			
		'06'	Thay đổi	OID của bộ tiêu chuẩn CBEFF, xem CHÚ THÍCH 6 của Bảng C.1			Bắt buộc nếu không mặc định sử dụng
		'A1'	Thay đổi	Khuôn mẫu tiêu đề sinh trắc học (BHT) phù hợp với CBEFF			Bắt buộc
				Thẻ	**Độ dài**	**Giá trị**	
				'80'	2	Số phiên bản tiêu đề bảo trợ (mặc định '0101')	Bắt buộc nếu không mặc định sử dụng
				'90'	Thay đổi	Chỉ mục, mã định danh đơn nhất sử dụng đối với việc tham chiếu tập dữ liệu sinh trắc học này trong một ngữ cảnh ứng dụng bên ngài thẻ	Tùy chọn
				'81'	1-3	Loại sinh trắc học, xem Bảng C.2	Tùy chọn

Thẻ	Độ dài	Giá trị					Ưu tiên
				'82'	1	Loại phụ sinh trắc học, xem Bảng C.3	Tùy chọn, sử dụng chỉ với loại sinh trắc học
				'83'	7	Ngày tạo và thời gian của dữ liệu sinh trắc học (CCYYMMDDhhmmss)	Tùy chọn
				'84'	Thay đổi	Người tạo	Tùy chọn
				'85'	8	Thời gian hiệu lực (từ CCYYMMDD tới CCYYMMDD)	Tùy chọn
				'86'	2	Mã định danh sản phẩm (PID) tạo ra dữ liệu tham chiếu sinh trắc học, các giá trị được gán bởi IBIA, xem: www.ibia.org	Tùy chọn
				'87'	2	Chủ định dạng của dữ liệu xác minh sinh trắc học, các giá trị được gán bởi IBIA, xem: www.ibia.org	Bắt buộc
				'88'	2	Loại định dạng của dữ liệu xác minh sinh trắc học, được quy định bởi chủ định dạng	Bắt buộc
		'5F2E'/'7F2E'	Thay đổi	Dữ liệu tham chiếu sinh trắc học (nguyên thủy/nhân tạo), xem Bảng C.8)			Bắt buộc
		'53'/'73'	Thay đổi	Dữ liệu tùy ý đối với dữ liệu (nguyên thủy/nhân tạo), xem CHÚ THÍCH 2 và 3			Tùy chọn

CHÚ THÍCH 1 Chỉ có các đối tượng dữ liệu từ CBEFF được trình bày, có liên quan tới đối chiếu ngoài thẻ.

CHÚ THÍCH 2 Đối tượng dữ liệu bổ sung không được trình bày trong cấu trúc CBEFF chính.

CHÚ THÍCH 3 Dữ liệu là sẵn có với thế giới bên ngoài khi xác minh thành công (nếu có) (xem đặc tả BioAPI).

Sự khác biệt chính với Bảng C.1 là các DO với tham chiếu thuật toán và bộ định tính dữ liệu tham chiếu (tham chiếu khóa được sử dụng bởi thẻ) không được trình bày và thay vào đó khối dữ liệu sinh trắc học (BDB), bao gồm dữ liệu tham chiếu sinh trắc học và có thể là một dữ liệu kèm theo mẫu tiêu đề sinh trắc học (BHT). Một khối chữ ký (SB) cũng có thể được trình bày, nhưng được mã hóa trong một tiêu chuẩn TCVN ISO/IEC 7816 theo sự phù hợp, xem Điều C.3.4.

Bảng C.8 - Khuôn mẫu dữ liệu sinh trắc học

Thẻ	Độ dài	Giá trị		
'7FCE'	Thay đổi	Khuôn mẫu dữ liệu sinh trắc học		
		Các DO có thể được nhúng vào khuôn mẫu dữ liệu sinh trắc học		
		Thẻ	Độ dài	Giá trị
		'80'/'A0'	Thay đổi	Thách thức đối với việc nhắc báo người dùng (nguyên thủy/nhân tạo), xem Bảng C.9 DO này chỉ liên quan đối với các loại sinh trắc học động.
		'81'/'A1'	Thay đổi	Dữ liệu sinh trắc học với cấu trúc chuẩn hóa (nguyên thủy/nhân tạo)
		'82'/'A2'	Thay đổi	Dữ liệu sinh trắc học với cấu trúc độc quyền (nguyên thủy/nhân tạo)

Bảng C.9 – Khuôn mẫu thừa nhận

Thẻ	Độ dài	Giá trị		
'A0'	Thay đổi	Khuôn mẫu thừa nhận		
		Các DO có thể được nhúng vào mẫu thử thách		
		Thẻ	Độ dài	Giá trị
		'90'	Thay đổi	Bộ định tính thừa nhận '00' = Không thông tin nào được đưa ra (không quy định) '01' = Mã hóa UTF8 (mặc định) Các giá trị RFU khác
		'80'	Thay đổi	Thừa nhận

C.3.3 Sử dụng cấu trúc lồng nhau

Trong Bảng C.10, một ví dụ về việc sử dụng cấu trúc lồng nhau được chỉ ra. Sự khác biệt chính với Bảng C.5 là con trỏ đến dữ liệu tham chiếu sinh trắc học (tức là bộ định tính dữ liệu tham chiếu) được thay thế bằng chính dữ liệu tham chiếu dữ liệu sinh trắc học của nó.

Bảng C.10 - Mẫu nhóm BIT có BIT lồng nhau đối với ứng dụng với dữ liệu tham chiếu sinh trắc học của nhiều loại sinh trắc học (ví dụ)

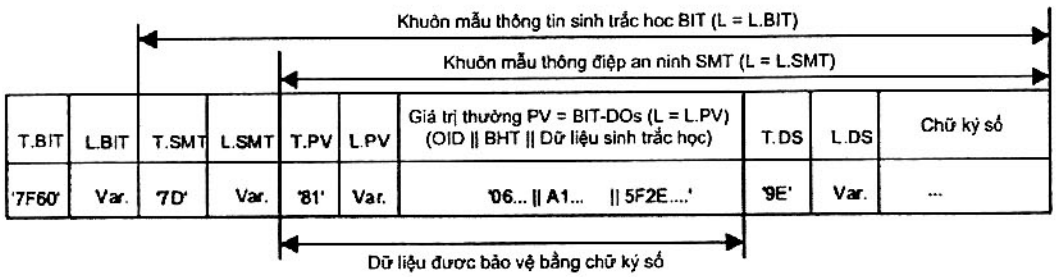
Thẻ	Độ dài	Giá trị						
'7F61'	Thay đổi	Khuôn mẫu nhóm thông tin sinh trắc học						
		Thẻ	Độ dài	Giá trị				
		'02'	1	Số các BIT trong mẫu nhóm				
		'7F60'	Thay đổi	BIT 1				
				Thẻ	Độ dài	Giá trị		
				'06'	Thay đổi	OID của bộ tiêu chuẩn CBEFF, xem CHÚ THÍCH 6 của Bảng C.1		
				'A1'	Thay đổi	BHT		
						Thẻ	Độ dài	Giá trị
						'81'	1-3	Loại sinh trắc học, ví dụ: đặc trưng khuôn mặt
						'87'	2	Chỉ định dạng của dữ liệu tham chiếu sinh trắc học
						'88'	2	Loại định dạng của dữ liệu tham chiếu sinh trắc học, quy định bởi chỉ định dạng
				'5F2E'	Thay đổi	Dữ liệu tham chiếu sinh trắc học		
		'7F60'	Thay đổi	BIT 2				
				Thẻ	Độ dài	Giá trị		
				'06'	Thay đổi	OID của bộ tiêu chuẩn CBEFF, xem CHÚ THÍCH 6 của Bảng C.1		
				'A1'	Thay đổi	BHT		
						Thẻ	Độ dài	Giá trị
						'81'	1-3	Loại sinh trắc học, ví dụ: vân tay
						'82'	1	Loại phụ sinh trắc học, ví dụ: ngón tay trỏ trái
						'87'	2	Chỉ định dạng của dữ liệu tham chiếu sinh trắc học
						'88'	2	Loại định dangk của dữ liệu tham chiếu sinh trắc học, quy định bởi chỉ định dạng
				'5F2E'	Thay đổi	Dữ liệu tham chiếu sinh trắc học		

C.3.4 Vấn đề an ninh

Một số khả năng, làm thế nào để bảo đảm BIT hoặc làm thế nào để cấp quyền truy cập cho các BIT và để truyền tải nó một cách an toàn được nêu trong Phụ lục B và Phụ lục D. Các tính năng bảo mật được mô tả trong ISO/IEC 19785 đối với:

- chỉ báo các tùy chọn tính bảo mật
- chỉ báo các tùy chọn tính toàn vẹn
- cung cấp một trường cho một chữ ký hoặc MAC

được hỗ trợ hoàn toàn bằng cách sử dụng khuôn mẫu thông điệp an ninh (SMT) và các DO liên quan (xem Phụ lục D). Việc chỉ báo các tùy chọn tính bảo mật và tính toàn vẹn trong 2 trường đặc biệt trong BHT là không cần thiết bởi vì sự ưu tiên của một lược đồ mã hóa, một chữ ký số hoặc một MAC được chỉ định bởi các thẻ tương ứng. Một ví dụ đơn giản của việc sử dụng SMT được trình bày trong Hình C.2. Hơn nữa, ví dụ phức tạp hơn được đưa ra trong Phụ lục D.



Hình C.2 - Khuôn mẫu thông tin sinh trắc học an toàn (ví dụ)

C.4 Thông tin đăng ký IBIA

Việc tuân thủ CBEFF yêu cầu chủ định dạng đăng ký với IBIA với một mã định danh duy nhất được giao cho chủ định dạng. Loại định dạng được gán bởi chủ định dạng và thể hiện định dạng dữ liệu sinh trắc học cụ thể theo quy định của chủ định dạng. Đó là khuyến nghị rằng chủ định dạng đăng ký loại định dạng được sử dụng với các IBIA cho các mục đích lưu trữ và xuất bản. IBIA cũng sẽ đăng ký các giá trị ID sản phẩm (xem Bảng C.1 và C.7). Số lượng được đảm bảo là duy nhất.

IBIA sẽ không gán giá trị giữa 'FFF0' - 'FFFE' cho chủ định dạng và các ID sản phẩm. Các giá trị này là sẵn có để thử nghiệm.

Đối với thông tin đăng ký, xem www.ibia.org.

Phụ lục D

(tham khảo)

Sử dụng khuôn mẫu thông điệp an ninh

D.1 Thuật ngữ viết tắt

Thuật ngữ	Tiếng Anh	Tiếng Việt
BD	Biometric Data	Dữ liệu sinh trắc học
BER	Basic Encoding Rules	Quy tắc mã hóa cơ bản
BHT	Biometric Header Template	Khuôn mẫu tiêu đề sinh trắc học
BIT	Biometric Information Template	Khuôn mẫu thông tin sinh trắc học
CC	Cryptographic Checksum	Bộ kiểm tra mã hóa
CCT	Cryptographic Checksum Template	Khuôn mẫu bộ kiểm tra mã hóa
CT	Confidentiality Template	Khuôn mẫu bảo mật
CG	Cryptogram	Lược đồ mã hóa
DE	Data Element	Phần tử dữ liệu
DO	Data Object	Đối tượng dữ liệu
DS	Digital Signature	Chữ ký số
DST	Digital Signature Template	Khuôn mẫu chữ ký số
KR	Key Reference	Tham chiếu khóa
L	Length	Độ dài
MAC	Message Authentication Code	Mã chứng thực thông điệp
PD	Personal Data	Dữ liệu cá nhân
PDT	Personal Data Template	Khuôn mẫu dữ liệu cá nhân
PV	Plain Value	Giá trị thường
SM	Secure Messaging	Thông điệp an ninh
SMT	Secure Messaging Template	Khuôn mẫu thông điệp an ninh
T	Tag	Thẻ
TLV	Tag-Length-Value	Giá trị-độ dài-thẻ
||	Concatenation	Kết hợp

D.2 Thông điệp an ninh liên quan tới đối tượng dữ liệu và việc sử dụng chúng

Có thể có một nhu cầu để bảo vệ khuôn mẫu thông tin sinh trắc học BIT trong trường hợp đó thẻ được sử dụng như thành phần của BIT (xem thêm NISTIR 6529 và ANSI X9.84):

- BIT có tính riêng tư (mã hóa)
- BIT có tính toàn vẹn (đã ấn định hoặc đánh địa chỉ MAC)
- BIT có tính riêng tư và toàn vẹn.

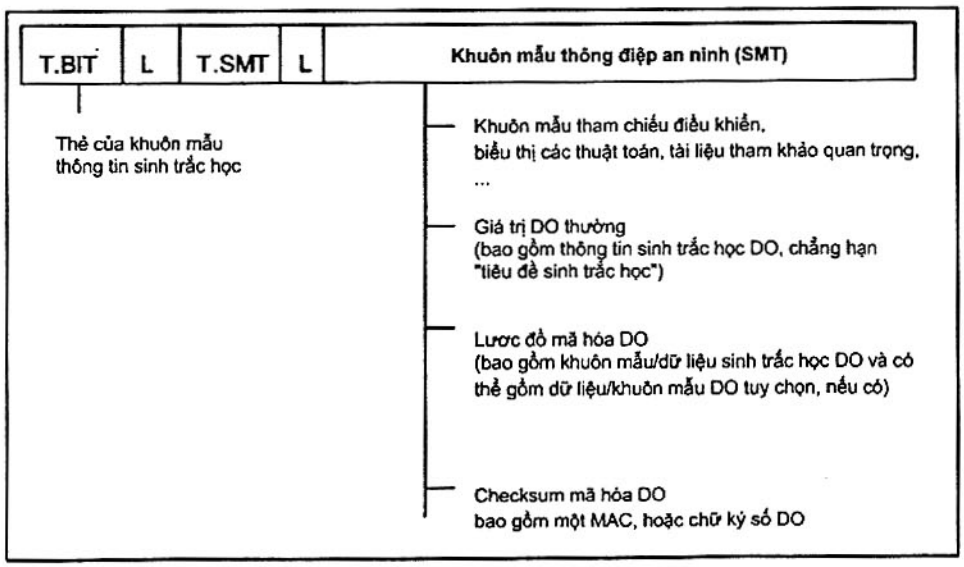
Các cách thức cho tính riêng tư và toàn vẹn theo ngữ cảnh thẻ được đề cập với thông điệp an ninh (SM) được quy định trong TCVN 11167-4 (ISO/IEC 7816-4). Có 2 phương pháp:

1) Trước khi đọc các BIT, các khóa SM nhằm đạt được tính riêng tư và toàn vẹn là tự động thiết lập với việc truyền tải khóa hoặc các cơ chế thỏa thuận khóa.
2) Các BIT được bảo đảm chính nó theo một cách tĩnh, tức là bằng cách áp dụng kỹ thuật mẫu SM như mô tả dưới đây.

Nếu trường giá trị của BIT phải được bảo đảm theo một cách tĩnh, thì trường giá trị được nhúng vào trong một mẫu SM, trong đó:

- Tất cả các đối tượng dữ liệu còn lại là văn bản thuần được đưa vào một mẫu giá trị thuần,
- Tất cả các đối tượng dữ liệu được mã hóa được đặt trong một lược đồ mã hóa

và nếu tính toàn vẹn là cần thiết, một hàm checksum DO mã hóa hoặc chữ ký số DO được thể hiện. Nếu các đối tượng dữ liệu giống như tham chiếu thuật toán và tham chiếu khóa cho phép hệ thống dịch vụ nhằm xác minh tính toàn vẹn và khôi phục giá trị thuần của dữ liệu mã hóa là cần thiết thì chúng được trình bày theo khuôn mẫu tham chiếu kiểm soát (xem Hình D.1).



Hình D.1 - Khuôn mẫu thông tin sinh trắc học kết hợp với SMT

Việc mã hóa các DO có liên quan cho một khuôn mẫu thông điệp an ninh SMT được trình bày trong Bảng D.1.

Bảng D.1 - Đối tượng dữ liệu SMT (tập con)

Thẻ	Độ dài	Giá trị		
'7D'	Thay đổi	Khuôn mẫu thông điệp an ninh SMT		
		Thẻ	**Độ dài**	**Giá trị**
		'xx'	Thay đổi	Khuôn mẫu tham chiếu kiểm soát, xem thẻ D.2 (thẩm quyền được bảo vệ)
		'81'	Thay đổi	Giá trị thường (PV), bao gồm một chuỗi các DE hay DO mã hóa BER-TLV, nhưng không có các DO liên quan tới SM, xem CHÚ THÍCH (thẩm quyền được bảo vệ)
		'85'	Thay đổi	Lược đồ mã hóa (CG), giá trị thường bao gồm các DO mã hóa BER-TLV, nhưng không có các DO liên quan tới SM (thẩm quyền được bảo vệ)
		'8E'	Thay đổi	Bộ kiểm tra mã hóa (CC), ví dụ: một mã chứng nhận thông điệp (MAC)
		'9E'	Thay đổi	Chữ ký số (DS)

CHÚ THÍCH Theo quan điểm của SM, giá trị thường luôn là nguyên thủy.

Khuôn mẫu thông điệp an ninh có thể chứa các khuôn mẫu tham chiếu kiểm soát:

- Khuôn mẫu checksum mã hóa (CCT)
- Khuôn mẫu chữ ký số (DST)
- Khuôn mẫu bảo mật (CT).

Những khuôn mẫu tham chiếu kiểm soát này gồm nhiều đối tượng dữ liệu hơn để quy định thuật toán và một tham chiếu khóa (xem Bảng D.2).

Bảng D.2 – Khuôn mẫu tham chiếu kiểm soát và các DO liên quan (tập con)

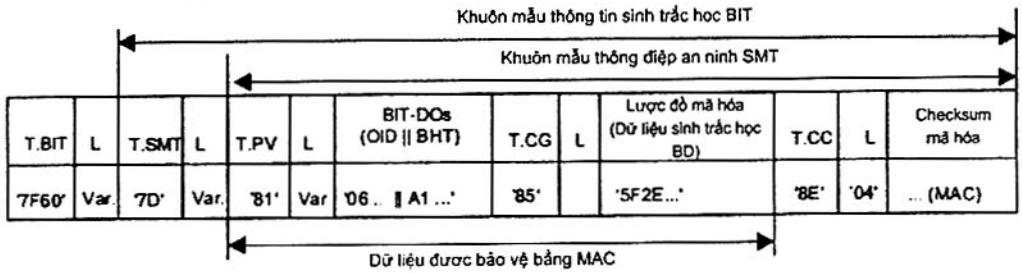
Thẻ	Độ dài	Giá trị		
'B5'	Thay đổi	Khuôn mẫu kiểm tra mã hóa (CCT)		
'B7'	Thay đổi	Khuôn mẫu chữ ký số (DST)		
'B9'	Thay đổi	Khuôn mẫu bảo mật (CT)		
		Các DO liên quan đối với CCT, DST và CT		
		Thẻ	**Độ dài**	**Giá trị**
		'80	Thay đổi	Tham chiếu thuật toán
		'83'	Thay đổi	- Tham chiếu với một khóa bí mật đối với việc sử dụng trực tiếp (liên quan tới thuật toán đối xứng) - Tham chiếu của một khóa phổ biến (liên quan tới thuật toán bất đối xứng)
		'84'	Thay đổi	- Tham chiếu với một khóa bí mật đối với biến đổi khóa (liên quan tới thuật toán đối xứng) - Tham chiếu của một khóa cá nhân (liên quan tới thuật toán bất đối xứng)

CHÚ THÍCH Bổ sung đối tượng dữ liệu được quy định trong TCVN 11167-4 (ISO/IEC 7816-4).

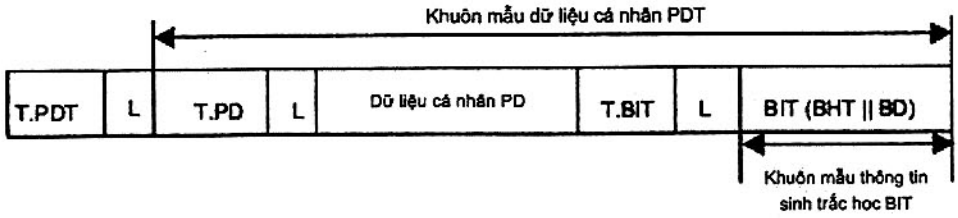
D.3 Ví dụ mã hóa

Các ví dụ mã hóa thể hiện:

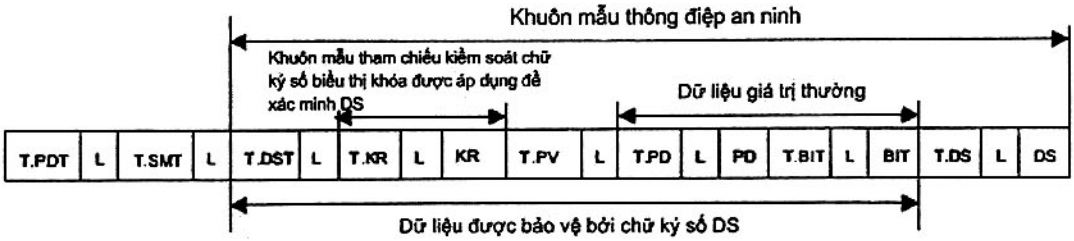
- Một khuôn mẫu thông tin sinh trắc học, nơi các đối tượng dữ liệu thông tin sinh trắc học (tiêu đề sinh trắc học) được theo sau bởi một lược đồ mã hóa gồm dữ liệu sinh trắc học và được cả bảo vệ bởi một MAC (xem Hình D.2) và
- Một số loại dữ liệu ứng dụng (ví dụ: dữ liệu cá nhân để định danh) được kết hợp với một Khuôn mẫu thông tin sinh trắc học và được đảm bảo theo nhiều cách khác nhau (xem Hình D.3 – D.5).



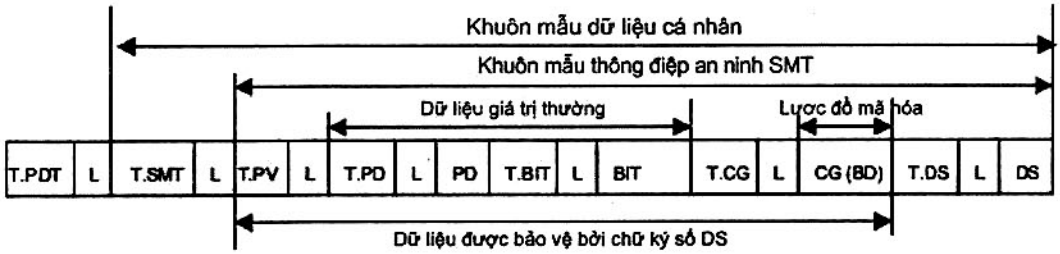
Hình D.2 - Khuôn mẫu BIT với SMT nhúng (ví dụ)



Hình D.3 - Khuôn mẫu dữ liệu cá nhân với BIT (ví dụ)



Hình D.4 - Khuôn mẫu dữ liệu cá nhân với BIT được bảo vệ bởi một chữ ký số (ví dụ)



Hình D.5 - Khuôn mẫu dữ liệu cá nhân được bảo vệ bởi một chữ ký số và bao gồm bên cạnh các DO khác một lược đồ mã hóa đối với dữ liệu sinh trắc học (ví dụ)

Thư mục tài liệu tham khảo

[1] TCVN 11167 (ISO/IEC 7816) Thẻ định danh - Thẻ mạch tích hợp (tất cả các phần).

[2] ISO/IEC 19784 BioAPI Specification.

[3] ANSI X9.84-2001 Biometric Information Management and Security.

[4] NISTIR 6529-A Common Biometric Exchange Format Framework.