TCVN **TIÊU CHUẨN QUỐC GIA**

TCVN 12042:2017
ISO 24761:2009/ COR 1:2013

Xuất bản lần 1

CÔNG NGHỆ THÔNG TIN - CÁC KỸ THUẬT AN TOÀN - NGỮ CẢNH XÁC THỰC CHO SINH TRẮC HỌC

Information technology - Security techniques - Authentication context for biometrics

HÀ NỘI - 2017

Mục lục

Lời nói đầu

TCVN 12042:2017 hoàn toàn tương đương ISO/IEC 24761:2009/Cor 1:2013

TCVN 12042:2017 do Học viện Công nghệ Bưu chính Viễn thông phối hợp với Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam biên soạn, Bộ Thông tin và Truyền thông đề nghị, Tổng cục Tiêu chuẩn Đo lường Chất lượng thẩm định, Bộ Khoa học và Công nghệ công bố.

Công nghệ thông tin - Các kỹ thuật an toàn - Ngữ cảnh xác thực cho sinh trắc học

Information technology - Security techniques - Authentication context for biometics

1 Phạm vi áp dụng

Tiêu chuẩn này quy định cấu trúc và các phần tử dữ liệu của Ngữ cảnh xác thực cho sinh trắc học (ACBio), được sử dụng để kiểm tra tính hợp lệ của kết quả một quá trình xác minh sinh trắc học được thực thi tại một địa điểm từ xa. Tiêu chuẩn này cho phép bất kỳ Báo cáo thể hiện ACBio đi kèm bất kỳ mục dữ liệu nào tham gia vào bất kỳ quá trình sinh trắc học có liên quan đến việc xác minh và thu nạp. Đặc tả của ACBio có thể được áp dụng không chỉ để xác minh sinh trắc học theo phương thức đơn lẻ mà còn để kết hợp đa phương thức.

Tiêu chuẩn này đặc tả cú pháp mã hóa của một Báo cáo thể hiện ACBio. Cú pháp mã hóa của một Báo cáo thể hiện ACBio dựa trên một giản đồ Cú pháp thông điệp mật mã (CMS) trừu tượng với giá trị cụ thể có thể được biểu diễn bằng cách sử dụng một mã hóa nhị phân ngắn gọn hoặc mã hóa XML mà con người có thể đọc được.

Tiêu chuẩn này không quy định các giao thức được sử dụng giữa các thực thể như các Đơn vị xử lý sinh trắc học (BPU), đối tượng yêu cầu, và bộ xác nhận. Tiêu chuẩn này quy định về nội dung và mã hóa của các Báo cáo thể hiện ACBio cho các hoạt động xử lý khác nhau.

2 Tài liệu viện dẫn

Các tài liệu viện dẫn sau rất cần thiết cho việc áp dụng tiêu chuẩn này. Đối với tài liệu viện dẫn ghi năm công bố thì áp dụng phiên bản được nêu. Đối với 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).

ISO/IEC 8824 (all parts) | ITU-T Recommendations X.680-683, Information technology - Abstract Syntax Notation One (ASN.1) *(Công nghệ thông tin - Chú giải cú pháp trừu tượng (ASN.1))*

ISO/IEC 8825-4 | ITU-T Recommendation X.693, Information technology - ASN.1 encoding rules: XML Encoding Rules (XER) *(Công nghệ thông tin - ASN.1 quy tắc mã hóa: Nguyên tắc mã hóa XML (XER))*

ISO/IEC 9594-2 | ITU-T Recommendation X.501, Information technology - Open Systems Interconnection - The Directory: Models *(Công nghệ thông tin - Liên kết các hệ thống mở - Thư mục: Các mô hình)*

ISO/IEC 9594-8 | ITU-T Recommendation X.509, Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks *(Công nghệ thông tin - Liên kết các hệ thống mở - Thư mục: Các khung chứng nhận thuộc tính và khóa công khai)*

ISO/IEC 19785-1, Information technology - Common Biometric Exchange Formats Framework - Part 1: Data element specification *(Công nghệ thông tin - Khung định dạng trao đổi sinh trắc học phổ biến - Phần 1: Mô tả chi tiết thành phần dữ liệu)*

ISO/IEC 19785-3, Information technology - Common Biometric Exchange Formats Framework - Part 3: Patron format specifications *(Công nghệ thông tin - Khung định dạng trao đổi sinh trắc học phổ biến - Phần 3: Các đặc điểm kỹ thuật định dạng bảo trợ)*

RFC 3852, Cryptographic Message Syntax (CMS), July 2004 *(Cú pháp thông điệp mật mã (CMS))*

RFC 5911, New ASN.1 Modules for Cryptographic Message Syntax (CMS) and S/MIME, June 2010 (Các Mô đun đối với *Cú pháp thông điệp mật mã (CMS))*

3 Thuật ngữ và định nghĩa

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

3.1

Báo cáo thể hiện ACBio (ACBio instance)

Báo cáo được tạo ra bởi một Đơn vị xử lý sinh trắc học (BPU) tuân thủ theo tiêu chuẩn này để thể hiện tính hợp lệ của kết quả của một hoặc nhiều quá trình con được thực thi trong BPU

3.2

Ngữ cảnh xác thực cho sinh trắc học (authentication context for biometrics)

ACBio

Tiêu chuẩn đặc tả hình thức và dạng mã của các Báo cáo thể hiện ACBio

3.3

(Thuộc) Sinh trắc học (biometric)

Gắn liền với các lĩnh vực sinh trắc học

3.4

Đơn vị xử lý sinh trắc học (biometric processing unit)

BPU

Thực thể thực thi một hoặc nhiều quá trình con nhằm thực hiện một xác minh sinh trắc học theo mức an toàn đồng nhất

CHÚ THÍCH: Bộ cảm biến, thẻ thông minh và thiết bị so sánh là các ví dụ về BPU.

3.5

Chứng nhận Đơn vị xử lý sinh trắc học (biometric processing unit certificate)

Chứng nhận BPU (BPU certificate)

Chứng nhận X.509 cấp cho BPU bởi một tổ chức chứng nhận dùng để cho phép bộ xác nhận xác định tính tin cậy của BPU

3.6

Tổ chức chứng nhận Đơn vị xử lý sinh trắc học (biometric processing unit certification organization)

Tổ chức chứng nhận BPU (BPU certification organization)

Tổ chức phát hành chứng nhận BPU

3.7

Báo cáo chức năng Đơn vị xử lý sinh trắc học (biometric processing unit function report)

Báo cáo chức năng BPU (BPU function report)

Báo cáo về các chức năng của BPU, bao gồm các kết quả đánh giá cho mỗi chức năng trong BPU

3.8

Chỉ số IO Đơn vị xử lý sinh trắc học (biometric processing unit IO Index)

Chỉ số IO BPU (BPU IO Index)

Số nguyên được gán cho mỗi luồng dữ liệu sinh trắc học giữa các BPU bởi đối tượng, chẳng hạn như phần mềm, trong đó sử dụng các chức năng của BPU để bộ xác nhận có thể tái tạo lại lưu lượng dữ liệu giữa các BPU

3.9

Báo cáo Đơn vị xử lý sinh trắc học (biometric processing unit report)

Báo cáo BPU (BPU report)

Báo cáo về một BPU, chứa một báo cáo chức năng BPU và một báo cáo an toàn BPU

3.10

Báo cáo an toàn Đơn vị xử lý sinh trắc học (biometric processing unit security report)

Báo cáo an toàn BPU (BPU security report)

Báo cáo về mức độ an toàn của một BPU, bao gồm kết quả đánh giá mức độ an toàn của BPU

3.11

Mẫu sinh trắc học (biometric sample)

Thông tin thu được từ bộ cảm biến sinh trắc học, hoặc trực tiếp hoặc sau khi xử lý

CHÚ THÍCH: xem **mẫu sinh trắc học thô** (3.33), **mẫu sinh trắc học trung gian** (3.26) và **mẫu sinh trắc học đã qua xử lý** (3.31)

3.12

Khuôn mẫu tham chiếu sinh trắc học (biometric reference template)

Mẫu sinh trắc học hoặc tổ hợp các mẫu sinh trắc học đã được lưu trữ như một tham chiếu để so sánh trong tương lai

CHÚ THÍCH: xem **khuôn mẫu tham chiếu sinh trắc học thô** (3.34), **khuôn mẫu tham chiếu sinh trắc học trung gian** (3.27) và **khuôn mẫu tham chiếu sinh trắc học đã qua xử lý** (3.32)

3.13

Chứng nhận khuôn mẫu tham chiếu sinh trắc học (biometric reference template certificate)

Chứng nhận BRT (BRT certificate)

Chứng nhận cấp cho một khuôn mẫu tham chiếu sinh trắc học bởi tổ chức chứng nhận BRT cho phép bộ xác nhận xác định tính xác thực của khuôn mẫu tham chiếu sinh trắc học

3.14

Tổ chức chứng nhận khuôn mẫu tham chiếu sinh trắc học (biometric reference template certification organization)

Tổ chức chứng nhận BRT (BRT certification organization)

Tổ chức phát hành chứng nhận BRT

3.15

Xác minh sinh trắc học (biometric verification)

Ứng dụng trả về kết quả đúng hoặc sai cho một yêu cầu về sự tương đồng giữa một hoặc nhiều khuôn mẫu tham chiếu sinh trắc học và một hoặc nhiều mẫu sinh trắc học nhận dạng bằng cách thực hiện một hoặc nhiều so sánh

3.16

Sinh trắc học (biometrics)

Nhận dạng tự động cá thể dựa vào đặc trưng sinh học và hành vi của cá thể đó

3.17

Đối tượng yêu cầu (claimant)

Cá thể <xác minh sinh trắc học> đang tìm kiếm, và là đối tượng của, xác minh sinh trắc học

3.18

So sánh (comparison)

Ước lượng, tính toán và đo lường sự tương đồng hoặc không tương đồng giữa một hoặc nhiều mẫu sinh trắc học nhận dạng và một hoặc nhiều khuôn mẫu tham chiếu sinh trắc học

3.19

Quyết định so sánh (comparison decision)

Sự xác định xem liệu mẫu sinh trắc học nhận dạng và khuôn mẫu tham chiếu sinh trắc học có cùng nguồn gốc sinh trắc học, dựa trên điểm số so sánh, chính sách quyết định (bao gồm các giá trị ngưỡng) và các đầu vào có thể khác để quyết định so sánh

3.20

Điểm số so sánh (comparison score)

Giá trị số học (hoặc tập hợp các giá trị), là kết quả của so sánh

3.21

Giá trị kiểm soát (control value)

Số ngẫu nhiên được cung cấp bởi một bộ xác nhận, là phương tiện mà bộ xác nhận có thể kiểm tra xem liệu Báo cáo thể hiện ACBio có được tạo ra theo yêu cầu của bộ xác nhận hay không

3.22

Thu nạp (enrol)

Thu thập một hoặc nhiều mẫu sinh trắc học từ một cá thể và tiếp theo xây dựng một hoặc nhiều khuôn mẫu tham chiếu sinh trắc học mà sau đó có thể được sử dụng để xác minh hoặc xác định danh tính của cá thể

3.23

Sự thu nạp (enrolment)

Quá trình thu thập một hoặc nhiều mẫu sinh trắc học từ một cá thể và tiếp theo xây dựng một khuôn mẫu tham chiếu sinh trắc học mà sau đó có thể được sử dụng để xác minh hoặc xác định danh tính của cá thể

3.24

Tổ chức thu nạp (enrolment organization)

Tổ chức xử lý việc thu nạp, tạo ra và lưu trữ khuôn mẫu tham chiếu sinh trắc học

3.25

Tổ chức đánh giá (evaluation organization)

Tổ chức đánh giá chức năng hoặc an toàn Đơn vị xử lý sinh trắc học

3.26

Mẫu sinh trắc học trung gian (intermediate biometric sample)

Mẫu sinh trắc học thu được bằng cách xử lý một mẫu sinh trắc học thô, dùng để tiếp tục xử lý

3.27

Khuôn mẫu tham chiếu sinh trắc học trung gian (intermediate biometric reference template)

Mẫu sinh trắc học trung gian hoặc tổ hợp các mẫu sinh trắc học trung gian được sử dụng như một khuôn mẫu tham chiếu sinh trắc học

3.28

Phù hợp (match)

Quyết định (các) mẫu sinh trắc học nhận dạng và khuôn mẫu tham chiếu sinh trắc học là từ cùng một cá thể

3.29

Không phù hợp (non-match)

Quyết định (các) mẫu sinh trắc học nhận dạng và khuôn mẫu tham chiếu sinh trắc học không từ cùng một cá thể

3.30

Phù hợp trên thẻ (on-card matching)

Thực hiện so sánh và đưa ra quyết định dựa trên một thẻ tích hợp vi mạch nơi mà các khuôn mẫu tham chiếu sinh trắc học được duy trì trên thẻ nhằm tăng cường tính an toàn và tính riêng tư

CHÚ THÍCH: Thuật ngữ "phù hợp" không được chấp nhận và được thay thế bằng thuật ngữ "so sánh" trong ISO/IEC JTC 1/SC 37. Tuy nhiên, thuật ngữ "phù hợp trên thẻ" là một thuật ngữ được sử dụng nhiều trong ISO/IEC JTC 1/SC 17. Vì vậy, thuật ngữ này được sử dụng trong tiêu chuẩn này.

3.31

Mẫu sinh trắc học đã qua xử lý (processed biometric sample)

Mẫu sinh trắc học thích hợp để so sánh

3.32

Khuôn mẫu tham chiếu sinh trắc học đã qua xử lý (processed biometric reference template)

Mẫu sinh trắc học đã qua xử lý hoặc tổ hợp các mẫu sinh trắc học đã qua xử lý được sử dụng như khuôn mẫu tham chiếu sinh trắc học

3.33

Mẫu sinh trắc học thô (raw biometric sample)

Mẫu sinh trắc học được thu thập trực tiếp từ bộ cảm biến sinh trắc học

3.34

Khuôn mẫu tham chiếu sinh trắc học thô (raw biometric reference template)

Mẫu sinh trắc học thô hoặc tổ hợp các mẫu sinh trắc học thô được sử dụng như một khuôn mẫu tham chiếu sinh trắc học

3.35

Quá trình con (subprocess)

Một phần của quá trình xác minh sinh trắc học hoặc thu nạp thường thực hiện thu thập dữ liệu, xử lý tín hiệu trung gian, xử lý tín hiệu cuối cùng, lưu trữ, so sánh, hoặc quyết định

3.36

Chỉ số quá trình con (subprocess index)

Số nguyên duy nhất được gán cho mỗi quá trình con trong một Đơn vị xử lý sinh trắc học (BPU) bởi tổ chức cung cấp BPU

3.37

Chỉ số IO quá trình con (subprocess IO index)

Số nguyên duy nhất được gán cho mỗi luồng dữ liệu giữa các quá trình con trong một Đơn vị xử lý sinh trắc học (BPU) để bộ xác nhận có thể tái tạo lại lưu lượng dữ liệu giữa các quá trình con trong BPU

3.38

Bộ xác nhận (validator)

Thực thể <xác minh sinh trắc học> tạo ra một quyết định chấp nhận hay không chấp nhận kết quả của quá trình xác minh sinh trắc học, dựa trên các chính sách của ứng dụng tương ứng, sử dụng một hoặc nhiều quyết định so sánh và thông tin có thể khác, được hỗ trợ bởi các Báo cáo thể hiện ACBio

4 Thuật ngữ viết tắt

ACBio	Authentication Context for Biometrics	Ngữ cảnh xác thực cho sinh trắc học
ASN.1	Abstract Syntax Notation One as defined in ISO/IEC 8824	Chú giải cú pháp trừu tượng như được định nghĩa trong ISO/IEC 8824
BER	Basic Encoding Rules (of ASN.1)	Nguyên tắc mã hóa cơ bản (của ASN.1)
BIR	Biometric Information Record	Bản ghi thông tin sinh trắc học
BPU	Biometric Processing Unit	Đơn vị xử lý sinh trắc học
BRT certificate	Biometric Reference Template	Chứng nhận khuôn mẫu tham chiếu sinh trắc

	certificate	học
CBEFF	Common Biometric Exchange Formats Framework as defined in ISO/IEC 19785-1	Khung định dạng giao dịch sinh trắc học phổ biến như được định nghĩa trong ISO/IEC 19785-1
CMS	Cryptographic Message Syntax as defined in RFC 3852	Cú pháp thông điệp mật mã như được định nghĩa trong RFC 3852
IO	Input/Output	Đầu vào/Đầu ra
OCM	On-Card Matching	Phù hợp trên thẻ
STOC	Store On Card	Lưu trữ trên thẻ
URI	Universal Resource Identifier	Định danh tài nguyên toàn cầu
XML	eXtensible Markup Language	Ngôn ngữ đánh dấu mở rộng

5 Mô hình và khung ACBio

5.1 Mô hình quá trình thu nạp, xác minh sinh trắc học và Đơn vị xử lý sinh trắc học (BPU)

Thiết kế ACBio dựa vào các quá trình con xác minh sinh trắc học sau đây:

a) Thu thập dữ liệu

Quá trình con này thu thập thông tin sinh trắc học từ đối tượng yêu cầu và chuyển đổi thành mẫu sinh trắc học thô. Các mẫu sinh trắc học thô được chuyển đến quá trình con xử lý tín hiệu trung gian để tiếp tục xử lý.

b) Xử lý tín hiệu trung gian

Quá trình con này tiếp nhận mẫu sinh trắc học thô và chuyển mẫu đó thành mẫu sinh trắc học trung gian. Các mẫu sinh trắc học trung gian được chuyển đến một quá trình con xử lý tín hiệu trung gian khác hoặc các quá trình con xử lý tín hiệu cuối cùng để tiếp tục xử lý.

c) Xử lý tín hiệu cuối cùng

Quá trình con này tiếp nhận mẫu sinh trắc học trung gian và chuyển mẫu đó thành mẫu sinh trắc học đã qua xử lý. Các mẫu sinh trắc học đã qua xử lý được chuyển hoặc đến quá trình con so sánh (xác minh) hoặc đến quá trình con lưu trữ (thu nạp).

d) Lưu trữ

Quá trình con này lưu trữ một trong ba kiểu khuôn mẫu tham chiếu sinh trắc học; khuôn mẫu tham chiếu sinh trắc học thô ((1) trong Hình 1 và Hình 2), khuôn mẫu tham chiếu sinh trắc học trung gian ((2) trong Hình 1 và Hình 2), hoặc khuôn mẫu tham chiếu sinh trắc học đã qua xử lý ((3) trong Hình 1 và Hình 2). Một trong ba kiểu khuôn mẫu tham chiếu sinh trắc học sẽ được so sánh với mẫu sinh trắc học để xác minh.

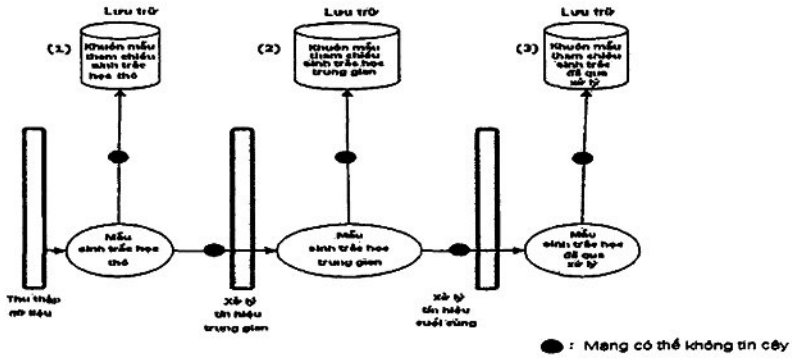
e) So sánh

Quá trình con này tiếp nhận mẫu sinh trắc học là mẫu có được ban đầu từ đối tượng yêu cầu mà có thể có hoặc không được tiếp tục xử lý và một khuôn mẫu tham chiếu sinh trắc học. Quá trình con này so sánh mẫu sinh trắc học và khuôn mẫu tham chiếu sinh trắc học đã qua xử lý và tính toán nét tương đồng, kết quả tính toán được gọi là điểm số so sánh. Điểm số so sánh được chuyển đến các quá trình con quyết định.

f) Quyết định

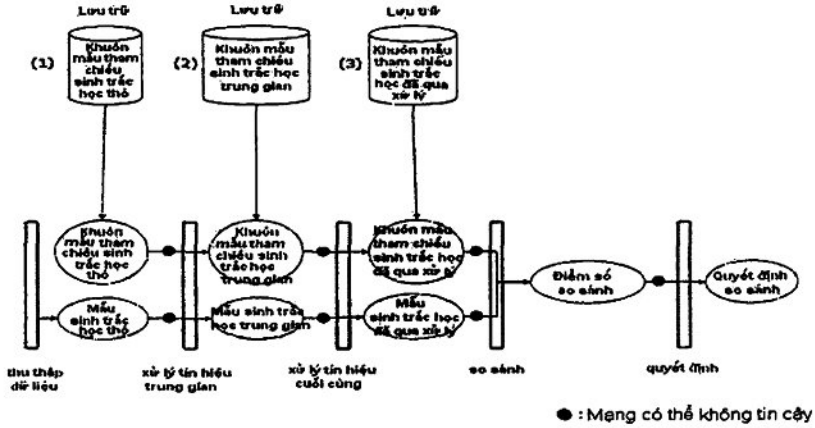
Quá trình con này tiếp nhận điểm số so sánh từ quá trình con so sánh, đánh giá điểm số theo nguyên tắc đã được xác định trước trong chính sách an toàn được sử dụng, quyết định tính hợp lệ về danh tính của đối tượng yêu cầu và cho ra quyết định so sánh, phù hợp hoặc không phù hợp, được gửi đến bộ xác nhận.

Hình 1 dưới đây cho thấy ba mô hình quá trình thu nạp sinh trắc học, nơi mà quá trình con lưu trữ lưu trữ mẫu sinh trắc học thô, mẫu sinh trắc học trung gian và mẫu sinh trắc học đã qua xử lý.



Hình 1- Mô hình quá trình thu nạp sinh trắc học

Hình 2 dưới đây cho thấy ba mô hình quá trình xác minh sinh trắc học, nơi mà quá trình con lưu trữ lưu trữ khuôn mẫu tham chiếu sinh trắc học thô, khuôn mẫu tham chiếu sinh trắc học trung gian và khuôn mẫu tham chiếu sinh trắc học đã qua xử lý.



Hình 2 – Mô hình quá trình xác minh sinh trắc học

5.2 Khung cho sử dụng ACBio

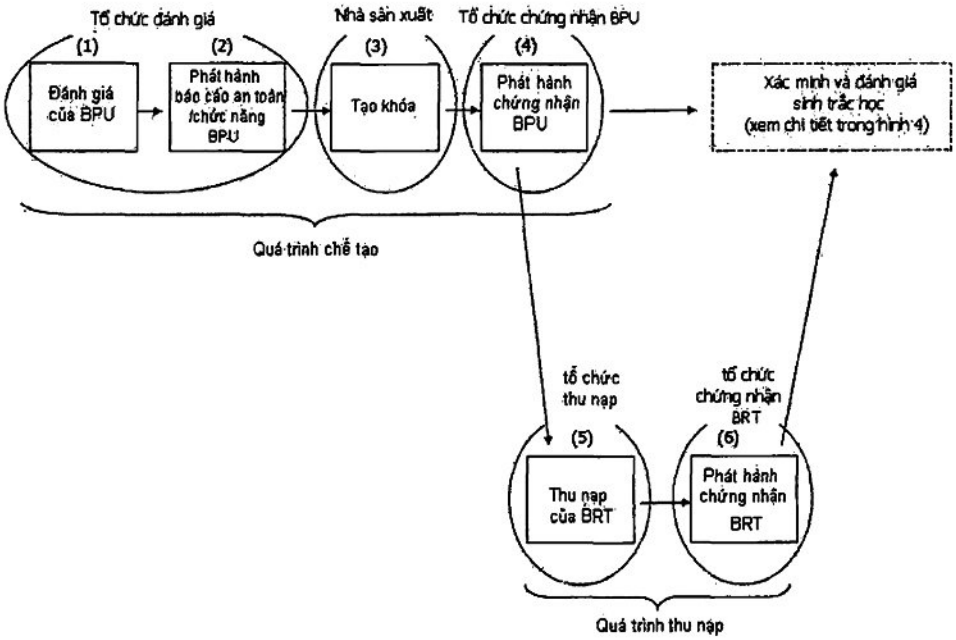
ACBio cung cấp thông tin cho bộ xác nhận của quá trình xác minh sinh trắc học về mức độ tin cậy của quá trình xác minh sinh trắc học.

Điều 5.2.1 đến 5.2.3 mô tả các chuẩn bị trong quá trình chế tạo của BPU mà kết quả là quá trình so sánh và thu nạp của BPU tạo ra khuôn mẫu tham chiếu sinh trắc học, cách mà Báo cáo thể hiện ACBio được tạo ra trong quá trình này và làm thế nào mà xác minh sinh trắc học là hợp lệ.

5.2.1 Chuẩn bị cho việc sử dụng ACBio

Để xác nhận tính hợp lệ quá trình xác minh sinh trắc học với ACBio, việc chuẩn bị là cần thiết ngoài việc thu thập và lưu trữ (thu nạp) các khuôn mẫu tham chiếu sinh trắc học của đối tượng yêu cầu.

Chuỗi các bước chuẩn bị cho việc sử dụng các ACBio được thể hiện trong Hình 3, tách biệt nhau trong quá trình chế tạo, quá trình thu nạp và quá trình xác minh tiếp theo.



Hình 3 – Chuẩn bị cho việc sử dụng ACBio và sự thực hiện xác minh sinh trắc học

5.2.1.1 *Chuẩn bị trong quá trình chế tạo*

Mức độ an toàn và mức độ hiệu suất chức năng (chất lượng) của từng chức năng trong mỗi BPU được đánh giá bởi một hoặc nhiều tổ chức đánh giá có thể bao gồm các nhà sản xuất của sản phẩm (phần mềm hoặc phần cứng tạo thành BPU ((1) trong Hình 3).

Sau khi đánh giá, báo cáo chức năng BPU (Xem 7.2.1) và báo cáo an toàn BPU (Xem 7.2.2) được đưa ra bởi tổ chức đánh giá ((2) trong Hình 2), tổ chức đã tạo ra báo cáo BPU.

Các nhà sản xuất các sản phẩm tạo thành BPU sẽ tạo ra một khóa cho hệ thống mã hoá đối xứng hoặc một cặp của hệ thống mã hóa khóa bất đối xứng tùy thuộc vào BPU, cho mỗi BPU ((3) trong Hình 3).

Khóa phải được xác nhận và có chứng nhận BPU (Xem 7.1) được phát hành bởi tổ chức chứng nhận BPU mà có thể là nhà sản xuất các sản phẩm của BPU ((4) trong Hình 3).

Báo cáo BPU hoặc tham chiếu tới báo cáo này, chứng nhận BPU hoặc tham chiếu tới chứng nhận này, và khóa được lưu trữ trong mỗi BPU trước khi chuyển giao sản phẩm của BPU. Mỗi BPU phải có phương tiện để tạo ra chữ ký số hoặc một mã xác thực thông điệp để bộ xác nhận có thể xác nhận tính toàn vẹn của Báo cáo thể hiện ACBio.

5.2.1.2 Chuẩn bị trong quá trình thu nạp

Đối với xác minh sinh trắc học, một khuôn mẫu tham chiếu sinh trắc học sẽ được tạo ra và thu nạp trước với tổ chức thu nạp ((5) trong Hình 3).

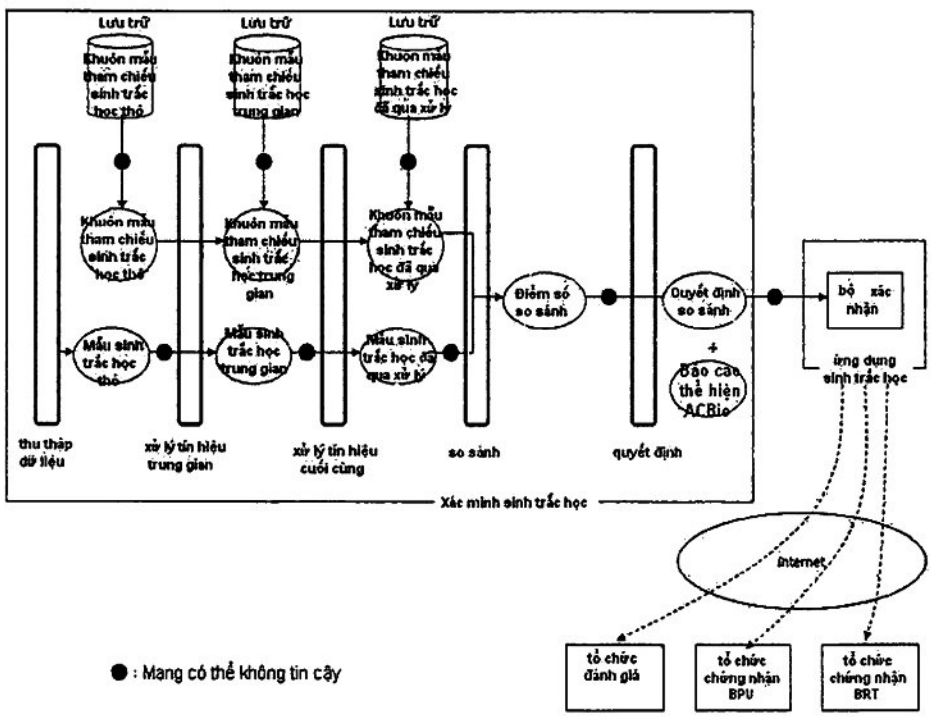
Sử dụng ACBio cho việc xác nhận một quá trình xác minh sinh trắc học, một chứng nhận khuôn mẫu tham chiếu sinh trắc học được gọi là chứng nhận BRT (xem điều 8) sẽ được phát hành bởi một tổ chức chứng nhận BRT ((6) trong Hình 3).

Chứng nhận BRT hoặc tham chiếu tới chứng nhận sẽ được lưu trữ trong BPU nơi khuôn mẫu tham chiếu sinh trắc học đã được chứng nhận đang lưu trữ.

Trong quá trình thu nạp, các Báo cáo thể hiện ACBio nên được tạo ra để xác nhận độ tin cậy của quá trình thu nạp. Việc xác nhận với những Báo cáo thể hiện ACBio này có thể được thực hiện bởi quá trình con lưu trữ cũng như bộ xác nhận của quá trình xác minh sinh trắc học.

5.2.2 Xác minh sinh trắc học và ACBio

Hình 4 cho thấy các chi tiết của quá trình xác minh sinh trắc học và quá trình xác nhận chúng.



Hình 4 – Quá trình xác minh sinh trắc học và xác nhận

Trong quá trình xác minh sinh trắc học, mỗi BPU sẽ tự đóng gói Báo cáo thể hiện ACBio của nó có chứa thông tin chứng nhận BPU (bản thân chứng nhận BPU hoặc tham chiếu tới chứng nhận), thông tin báo cáo BPU (bản thân báo cáo BPU hoặc cham chiếu tới báo cáo) và thông tin chứng nhận BRT (bản thân chứng nhận BPU hoặc tham chiếu tới chứng nhận) nếu BPU bao gồm các quá trình con lưu trữ vào các dữ liệu kiểu **ACBioContentInformation** (Xem 6). Các dữ liệu kiểu **ACBioContentInformation** phải chứa một giá trị từ bộ xác nhận, gọi là giá trị kiểm soát và các giá trị hàm băm của đầu vào/đầu ra dữ liệu sinh trắc học đến/từ BPU, cho phép bộ xác nhận để xác nhận sự nhất quán của việc truyền tải dữ liệu sinh trắc học giữa các BPU.

Bằng cách chèn thêm chữ ký số hoặc mã xác thực thông điệp vào dữ liệu kiểu **ACBioContentInformation** với khóa của BPU, Báo cáo thể hiện ACBio được tạo ra.

5.2.3 Xác nhận quá trình xác minh sinh trắc học sử dụng ACBio

Trong khung ACBio này, bộ xác nhận không chỉ tiếp nhận các quyết định so sánh, kết quả xác minh sinh trắc học, mà còn (những) Báo cáo thể hiện ACBio để bộ xác nhận có thể xác nhận kết quả xác minh sinh trắc học đã thực thi.

Bộ xác nhận có thể xác nhận tính xác thực và tính toàn vẹn của một Báo cáo thể hiện ACBio bằng cách xác minh chữ ký số hoặc mã xác thực thông điệp với chứng nhận BPU. Bộ xác nhận có thể có mức độ an toàn và mức độ hiệu suất chức năng của BPU bằng cách tham chiếu tới báo cáo BPU và tính xác thực của khuôn mẫu tham chiếu sinh trắc học được sử dụng trong quá trình xác minh sinh trắc học bằng cách tham chiếu tới chứng nhận BRT. Bộ xác nhận cũng có thể xác nhận tính nhất quán của thông tin liên lạc giữa các BPU và giữa bộ xác nhận và quá trình xác minh sinh trắc học bằng cách kiểm tra khối quá trình sinh trắc học và giá trị kiểm soát trong (những) Báo cáo thể hiện ACBio tương ứng. Với tất cả những điều này, bộ xác nhận có thể quyết định mức độ tin cậy cho kết quả xác minh sinh trắc học.

Nếu cần thiết, bộ xác nhận có thể kết nối với các tổ chức có liên quan như tổ chức chứng nhận BPU, tổ chức đánh giá và tổ chức chứng nhận BRT, như thể hiện trong Hình 4.

6 Báo cáo thể hiện ACBio

Một Báo cáo thể hiện ACBio là dữ liệu kiểu **ACBioInstance** của ASN.1 được quy định trong ký pháp ASN.1 như sau:

```
ACBioInstance ::= SEQUENCE {
        contentType CONTENT-TYPE.&id({ContentTypeACBio}),
        content [0] EXPLICIT CONTENT-TYPE.&Type
                ({ContentTypeACBio}{@contentType})}
```

Kiểu **ACBioInstance** tương ứng với kiểu **ContentInfo** của CMS. Kiểu này sau đó bị ràng buộc bởi tập hợp đối tượng mở rộng trong khi trước đây bị ràng buộc bởi tập hợp đối tượng chỉ chứa hai đối tượng **signedDataACBio** và **authenticatedDataACBio**. Hai đối tượng thuộc lớp **CONTENT-TYPE** này được định nghĩa như sau:

```
ContentTypeACBio CONTENT-TYPE ::= {signedDataACBio | authenticatedDataACBio}
signedDataACBio CONTENT-TYPE ::= {
        SignedDataACBio
        IDENTIFIED BY id-signedDataACBio }
id-signedDataACBio OBJECT IDENTIFIER ::=
        {iso(1) standard(0) acbio(24761) contentType(2) signedDataACBio(1)}
authenticatedDataACBio CONTENT-TYPE ::= {
        AuthenticatedDataACBio
        IDENTIFIED BY id-authenticatedDataACBio }
id-authenticatedDataACBio OBJECT IDENTIFIER ::=
        {iso(1) standard(0) acbio(24761) contentType(2) authenticatedDataACBio(2)}
```

SignedDataACBio và **AuthenticatedDataACBio** được quy định như sau:

```
SignedDataACBio ::= SIGNEDDATA { EncapsulatedContentInfoACBio }
AuthenticatedDataACBio ::= AUTHENTICATEDDATA { EncapsulatedContentInfoACBio }
```

Kiểu **SignedDataACBio** và **AuthenticatedDataACBio** đã được quy định bên trên thay thế cho CMS kiểu **SignedData** và **AuthenticatedData** cùng với các định nghĩa sau:

```
SIGNEDDATA { EncapsulatedContentInfo } ::= SEQUENCE {
        version CMSVersion,
        digestAlgorithms SET OF DigestAlgorithmIdentifier,
        encapContentInfo EncapsulatedContentInfo,
        certificates [0] IMPLICIT CertificateSet OPTIONAL,
        crls [1] IMPLICIT RevocationInfoChoices OPTIONAL,
        signerInfos SignerInfos}

AUTHENTICATEDDATA { EncapsulatedContentInfo } ::= SEQUENCE {
        version CMSVersion,
        originatorInfo [0] IMPLICIT OriginatorInfo OPTIONAL,
        recipientInfos RecipientInfos,
        macAlgorithm MessageAuthenticationCodeAlgorithm,
        digestAlgorithm [1] DigestAlgorithmIdentifier OPTIONAL,
        encapContentInfo EncapsulatedContentInfo,
        authAttrs [2] IMPLICIT AuthAttributes OPTIONAL,
        mac MessageAuthenticationCode,
        unauthAttrs [3] IMPLICIT UnauthAttributes OPTIONAL}
```

Các kiểu sau đây xuất hiện trong các đặc điểm kỹ thuật của hai kiểu trên, **SIGNEDDATA** và **AUTHENTICATEDDATA**, được đưa vào từ RFC 3852: **CMSVersion, DigestAlgorithmIdentifier, SignerInfos, OriginatorInfo, RecipientInfos, MessageAuthenticationCodeAlgorithm, AuthAttributes, MessageAuthenticationCode, UnauthAttributes**.

Do các kiểu **CertificateSet** và **RevocationInfoChoices** trong RFC 3852 không tuân thủ với phiên bản hiện thời của ASN.1 đã được tiêu chuẩn hóa năm 2002 trong Bộ ISO/IEC 8824, chúng không thể được đưa vào và được định nghĩa lại như sau:

CertificateSet, RevocationInfoChoices được định nghĩa như sau:

```
CertificateSet ::= SET OF CertificateChoices

CertificateChoices ::= CHOICE {
        certificate Certificate,
        v2AttrCert [2] IMPLICIT AttributeCertificateV2,
        other [3] IMPLICIT OtherCertificateFormat}

AttributeCertificateV2 ::= AttributeCertificate

OtherCertificateFormat ::= SEQUENCE {
        otherFormat OTHERCERTIFICATE.&id({OtherCertificate}),
        otherCert OTHERCERTIFICATE.&Type({OtherCertificate}{@otherFormat})}

OTHERCERTIFICATE ::= TYPE-IDENTIFIER

OtherCertificate OTHERCERTIFICATE ::= {...}

RevocationInfoChoices ::= SET OF RevocationInfoChoice

RevocationInfoChoice ::= CHOICE {
        crl CertificateList,
        other [1] IMPLICIT OtherRevocationInfoFormat }

OtherRevocationInfoFormat ::= SEQUENCE {
        otherRevInfoFormat OTHERREVOCATION.&id({OtherRevocation}),
        otherRevInfo OTHERREVOCATION.&Type({OtherRevocation}{@otherRevInfoFormat}) }

OTHERREVOCATION ::= TYPE-IDENTIFIER

OtherRevocation OTHERREVOCATION ::= {...}
```

Kiểu **EncapsulatedContentInfo** là một tham số trong định nghĩa trên và không được đưa vào từ CMS. Trong định nghĩa kiểu **SignedDataACBio** và **AuthenticatedDataACBio**, kiểu dưới đây thay thế **EncapsulatedContentInfo**.

```
EncapsulatedContentInfoACBio ::= SEQUENCE {
        eContentType CONTENT-TYPE.&id({ContentTypeACBioContentInfo}),
        eContent [0] EXPLICIT OCTET STRING
        (CONTAINING CONTENT-TYPE.&Type
                ({ContentTypeACBioContentInfo}{@eContentType}))}

ContentTypeACBioContentInfo CONTENT-TYPE ::= {acbioContentInformation}
```

Như trong định nghĩa trên, **kiểu EncapsulatedContentInfoACBio** bị ràng buộc bởi một tập hợp đối tượng có chứa đối tượng đơn lẻ **acbioContentInformation** của lớp **CONTENT-TYPE**. Đối tượng này được định nghĩa như sau:

```
acbioContentInformation CONTENT-TYPE ::= {
        ACBioContentInformation ::= SEQUENCE {
                version Version DEFAULT v1,
                bpuInformation BPUInformation,
                controlValue OCTET STRING (SIZE(16)),
                biometricProcess BiometricProcess,
                brtCertificateInformation BRTCertificateInformation OPTIONAL}
        Version ::= INTEGER { v1(1) } ( v1, ... ) }
```

id-acbioContentInformation OBJECT IDENTIFIER ::=
{iso(1) standard(0) acbio(24761) contentType(2) acbioContent(3)}

Do đó một Báo cáo thể hiện ACBio là một dữ liệu kiểu **ACBioInstance**, về cơ bản giống như kiểu CMS **ContentInfo**, với nội dung của kiểu **SignedDataACBio** hoặc **AuthenticatedDataACBio** về nội dung của kiểu **ACBioContentInformation**.

Bảng 1 cho thấy cấu trúc của kiểu **ACBioContentInformation**. Kiểu **ACBioContentInformation** bao gồm năm trường, phiên bản, khối thông tin BPU, giá trị kiểm soát, khối quá trình sinh trắc học và thông tin chứng nhận BRT. Bốn trường đầu tiên là bắt buộc. Một Báo cáo thể hiện ACBio có trường cuối cùng khi và chỉ khi các BPU có chứa quá trình con lưu trữ. Chữ ký của **SignedDataACBio** hoặc mã xác thực thông điệp của **AuthenticatedDataACBio** được tạo ra với khóa (riêng) của BPU.

Phiên bản là phiên bản của định dạng **ACBioContentInformation**.

Bảng 1 – Thông tin nội dung ACBio

ACBioContentInformation	
	Phiên bản
	Khối thông tin BPU
	Thông tin tham chiếu chứng nhận BPU
	Thông tin báo cáo BPU
	Giá trị kiểm soát
	Khối quá trình sinh trắc học
	SubprocessIndex[1]
	.
	.
	SubprocessIndex[L]
	BPUIOExecutionInformation[1] (cho đầu vào)
	.
	.
	BPUIOExecutionInformation[M] (cho đầu vào)
	BPUIOExecutionInformation[1] (cho đầu ra)
	.
	.
	BPUIOExecutionInformation[N] (cho đầu ra)
	Thông tin chứng nhận BRT

Trong ký pháp ASN.1, kiểu **ACBioContentInformation** được quy định như sau:

```
ACBioContentInformation ::= [14] IMPLICIT SEQUENCE {
        version Version DEFAULT v0,
        bpuInformation BPUInformation,
        controlValue OCTET STRING (SIZE(16)),
        biometricProcess BiometricProcess,
        brtCertificateInformation BRTCertificateInformation OPTIONAL}

Version ::= INTEGER { v0(0) } ( v0, ... )
```

Thẻ **ACBioContentInformation** được lựa chọn để chữ ký số hoặc mã xác thực thông điệp có thể được tính cho dữ liệu kiểu này trên một thẻ IC sử dụng câu lệnh được quy định tại tiêu chuẩn ISO/IEC 7816-4.

Kiểu **BPUInformation** được định nghĩa trong 6.1. Chi tiết của từng kiểu trong **BPUInformation** được định nghĩa tại điều 7.

Giá trị kiểm soát là một chuỗi 8 bit của 16 byte chiều dài mà bộ xác nhận có thể kiểm tra được yêu cầu của bộ xác nhận đối với Báo cáo thể hiện ACBio được tạo ra. Giá trị này được thiết lập cho trường **controlValue** để tránh lặp lại một quá trình xác minh sinh trắc học.

Kiểu **BiometricProcess** được định nghĩa trong 6.2. Kiểu **BRTCertificateInformation** được định nghĩa trong 6.3. Chi tiết của kiểu **BRTCertificate**, được sử dụng trong **BRTCertificateInformation**, được định nghĩa tại điều 8.

6.1 Khối thông tin BPU

Khối thông tin BPU mang thông tin tĩnh của BPU, thông tin mà không phụ thuộc vào từng sự thực hiện. Khối này là bắt buộc và bao gồm hai thành phần, thông tin tham chiếu chứng nhận BPU và thông tin báo cáo BPU. ASN.1 kiểu **BPUInformation** được định nghĩa cho khối thông tin này:

BPUInformation ::= SEQUENCE {
bpuCertificateReferrerInformation BPUCertificateReferrerInformation OPTIONAL,
bpuReportInformation BPUReportInformation}

Thông tin tham chiếu chứng nhận BPU của kiểu **BPUCertificateReferrerInformation** được định nghĩa như sau là thông tin tham chiếu tới chứng nhận X.509 cho khóa (công khai) của BPU. Nếu Báo cáo thể hiện ACBio có chứng nhận BPU trong trường **certificates** trong trường hợp **SignedDataACBio** được sử dụng hoặc trong trường **certs** trong **originatorInfo** của trường hợp **AuthenticatedDataACBio** được sử dụng, thông tin tham chiếu chứng nhận BPU có thể bị bỏ qua. Chứng nhận BPU được quy định trong 7.1.

BPUCertificateReferrerInformation ::= SEQUENCE {
bpuCertificateReferrer URI,
crlsReferrer URI OPTIONAL}

URI ::= VisibleString (SIZE(1..MAX))

Thông tin báo cáo BPU của kiểu **BPUReportInformation** là bản thân báo cáo BPU hoặc tham chiếu tới báo cáo. Báo cáo BPU chứa thông tin về chức năng được thực hiện trong BPU và thông tin về mức độ an toàn của BPU. Báo cáo BPU được định nghĩa trong 7.2.

BPUReportInformation ::= CHOICE {
bpuReport [0] EXPLICIT BPUReport,
bpuReportReferrer URI}

6.2 Khối quá trình sinh trắc học

Khối quá trình sinh trắc học mang thông tin thời gian thực hiện của BPU, thông tin này phụ thuộc vào từng sự thực hiện. Khối này bao gồm ba thành phần, **subprocessIndexList** là danh sách các chỉ số của các quá trình con được thực thi trong BPU, **bpuInputExecutionInformationList** chứa các thông tin về dữ liệu đầu vào cho BPU và **bpuOuputExecutionInformationList** chứa các thông tin về dữ liệu đầu ra từ BPU. Nếu BPU gửi/nhận dữ liệu đến/từ các BPU khác, thì các thành phần tương ứng trong khối này là bắt buộc.

ASN.1 kiểu **BiometricProcess** được định nghĩa như dưới đây:

BiometricProcess ::= SEQUENCE {
subprocessIndexList SubprocessIndexList,
bpuInputExecutionInformationList BPUIOExecutionInformationList OPTIONAL,
bpuOuputExecutionInformationList BPUIOExecutionInformationList }

SubprocessIndexList ::= SEQUENCE SIZE (1..MAX) OF SubprocessIndex
BPUIOExecutionInformationList ::= SEQUENCE OF BPUIOExecutionInformation

subprocessIndexList là danh sách các dữ liệu của kiểu **SubprocessIndex**. Kiểu này cũng được sử dụng cho **subprocessIndex** trong kiểu **FunctionDefinition** (xem 7.2.1.1.1) trong đó mô tả các chức năng của một quá trình con trong BPU. Một Báo cáo thể hiện ACBio chứa nhiều dữ liệu của kiểu

FunctionDefinition như số lượng các quá trình con trong BPU. Các **subprocessIndex** trong kiểu **FunctionDefinition** tương ứng với quá trình con được thực thi phải được thiết lập cho **subprocessIndexList** nêu trên.

bpuInputExecutionInformationList bao gồm các phần tử của kiểu **BPUIOExecutionInformation** như nhiều các dữ liệu đầu vào cho BPU.

bpuOuputExecutionInformationList bao gồm các phần tử của kiểu **BPUIOExecutionInformation** như nhiều các dữ liệu đầu ra từ BPU.

Ví dụ, trong trường hợp một BPU chỉ chứa quá trình con lưu trữ như thẻ STOC, không có **bpuInputExecutionInformationList** nhưng **bpuOuputExecutionInformationList** với một phần tử tương ứng với đầu ra của khuôn mẫu tham chiếu sinh trắc học từ quá trình con lưu trữ.

Định nghĩa cho kiểu **BPUIOExecutionInformation** được đưa ra như sau:

```
BPUIOExecutionInformation ::= SEQUENCE {
        dataType DataType,
        bpuIOIndex IOIndex,
        subprocessIOIndex IOIndex,
        hash Hash}
Hash ::= SEQUENCE {
        algorithmIdentifier AlgorithmIdentifier,
        hashValue OCTET STRING}
```

BPUIOInformation bao gồm bốn thành phần, **datatype, bpuIOIndex, subprocessIOIndex** và **hash**.

datatype cho thấy kiểu dữ liệu đầu vào/đầu ra đến/từ BPU. Kiểu **DataType** được định nghĩa trong 7.2.1.2.

Trong quá trình thực thi, các chương trình ứng dụng, trong đó sử dụng các chức năng của BPU, sẽ gán duy nhất một số nguyên cho mỗi luồng dữ liệu sinh trắc học từ/đến các BPU. Số nguyên này được đưa ra bởi các chương trình ứng dụng sẽ được thiết lập cho **bpuIOIndex**. Nếu một BPU khác tạo ra một Báo cáo thể hiện ACBio với cùng một số nguyên trong **bpuIOIndex** trong khối quá trình sinh trắc học, thì có nghĩa là đã có một giao tiếp giữa hai BPU này. Bằng cách này, bộ xác nhận có thể tái tạo lại lưu lượng dữ liệu giữa các BPU.

Các **subprocessIOIndex** của phần tử tương ứng với **bpuInputStaticInformationList/bpuOutputStaticInformationList** trong khối thông tin BPU sẽ được thiết lập cho **subprocessIOIndex** của **BPUIOExecutionInformation**. Sự kết hợp của **bpuIOIndex** và **subprocessIOIndex** tạo ra sự kết nối giữa các lưu lượng dữ liệu bên trong BPU và lưu lượng dữ liệu trong toàn bộ quá trình xác minh sinh trắc học.

hash chứa giá trị hàm băm của dữ liệu đầu vào/đầu ra đến/từ BPU và định danh của thuật toán băm. Kiểu **AlgorithmIdentifier** được đưa vào từ ISO/IEC 9594-2 | ITU-T Khuyến nghị X.501.

6.3 Thông tin chứng nhận BRT

BRTcertificateInformation chứa một danh sách các chứng nhận BRT hoặc danh sách tham chiếu tới mỗi chứng nhận BRT, như các ký pháp ASN.1 sau đây. Chứng nhận BRT bao gồm các thông tin về khuôn mẫu tham chiếu sinh trắc học được lưu trữ trong BPU. Một Báo cáo thể hiện ACBio phải có các thông tin chứng nhận BRT khi và chỉ khi các BPU chứa quá trình con lưu trữ. Danh sách của nhiều hơn một phần tử được sử dụng nếu xác minh kết hợp đa phương thức sinh trắc học được sử dụng. Chứng nhận BRT được quy định tại điều 8.

```
BRTCertificateInformation ::= CHOICE {
        brtCertificateList BRTCertificateList,
        brtCertificateReferrerList BRTCertificateReferrerList}
BRTCertificateList ::= SEQUENCE SIZE (1..MAX) OF BRTCertificate
BRTCertificateReferrerList ::= SEQUENCE SIZE (1..MAX) OF URI
```

7 Định nghĩa các thành phần trong BPUInformationBlock

7.1 Chứng nhận BPU

Chứng nhận BPU là chứng nhận X.509 cho khóa (công khai) của BPU. Cấu trúc của chứng nhận BPU được mô tả trong Bảng 2.

Bảng 2 – Chứng nhận BPU

trường		nội dung
tbsCertificate	version	như thông thường
	serialNumber	như thông thường
	signature	như thông thường
	validity	như thông thường
	issuer	bên thứ ba tin cậy hoặc tổ chức chứng thực công cộng trong các nhà cung cấp mà sản xuất/bán các sản phẩm của BPU
	subject	định danh của chủ thể bao gồm các thông tin như số serial của sản phẩm, tên các sản phẩm của BPU, và tên của các nhà cung cấp sản phẩm
	subjectPublicKeyInfo	như thông thường
	issuerUniqueIdentifier	như thông thường
	subjectUniqueIdentifier	như thông thường
	extensions	
signatureAlgorithm		như thông thường
signatureValue		như thông thường

Các phần cơ bản của chứng nhận BPU bao gồm 9 trường; **version, serialNumber, signature, validity, issuer, subject, subjectPublicKeyInfo, issuerUniqueIdentifier** và **subjectUniqueIdentifier**, tất cả đều là trường con của trường **tbsCertificate** thuộc kiểu **Certificate** đối với chứng nhận X.509 được định nghĩa trong ISO/IEC 9594-8. Ở đây, trường **issuer** là một tổ chức thứ ba đáng tin cậy hoặc một tổ chức chứng thực công cộng trong các nhà cung cấp mà sản xuất/bán các sản phẩm của BPU. Trường **subject** là định danh mà sự mô tả là đối tượng của ISO/IEC 9594-2 và sẽ bao gồm số sê ri của sản phẩm, tên sản phẩm, phiên bản của BPU, tên của các nhà cung cấp sản phẩm. Số sê ri của sản phẩm trong trường đối tượng sẽ là mục phân cấp của định danh. Tên sản phẩm và phiên bản sẽ là mục tiếp theo mục phân cấp. Bảy đặc tính khác trong trường cơ bản được sử dụng như bình thường.

Chứng nhận BPU sẽ được lưu trữ trong trường **certificates** của trường kiểu **SignedDataACBio** hoặc **AuthenticatedDataACBio** trong Báo cáo thể hiện ACBio, hoặc tham chiếu đến chứng nhận BPU sẽ được lưu trữ trong **bpuCertificateReferrerInformation** (xem 6.1).

7.2 BPUReportInformation

Thông tin báo cáo BPU chứa thông tin về các chức năng được thực hiện trong BPU và thông tin về mức độ an toàn của BPU. Hoặc là chính báo cáo BPU hoặc thông tin tham chiếu với báo cáo sẽ được thiết lập trong **BPUReportInformation**. Trong ký pháp ASN.1, **BPUReportInformation** được mô tả như sau:

```
BPUReportInformation ::= CHOICE {
        bpuReport [0] EXPLICIT BPUReport,
        bpuReportReferrer URI}
```

BPUReport được định nghĩa một cách tương tự như **ACBioInstance**. Một báo cáo BPU bao gồm hai trường; trường đầu tiên của giá trị cố định của **id-contnetBPUReport** và trường thứ hai của kiểu **ContentBPUReport**, là một dữ liệu **SIGNEDDATA** biểu hiện bằng tham số với nội dung đã được đóng gói của kiểu **BPUReportContentInformation**, trong đó bao gồm hai thành phần, **bpuFunctionReport** và **bpuSecurityReport**. Chữ ký sẽ được tạo ra bằng cách sử dụng khóa riêng của các nhà cung cấp sản phẩm của BPU.

CHÚ THÍCH: Các chức năng và luồng dữ liệu trong một BPU trong sự thu nạp có thể khác trong việc xác minh sinh trắc học. Trong trường hợp đó, hai BPUReports có thể được chuẩn bị, một cho sự thu nạp, một để xác minh sinh trắc học. Nếu không, một BPUReport có thể được chuẩn bị cho cả việc thu nạp và xác minh sinh trắc học. Trường hợp thứ hai được ghi trong 7.2.1.

Trong ký pháp ASN.1, BPUReport được mô tả như sau:

```
BPUReport ::= SEQUENCE {
        contentType CONTENT-TYPE.&id({ContentTypeBPUReport}),
        content [0] EXPLICIT CONTENT-TYPE.&Type
                ({ContentTypeBPUReport}{@contentType})}

ContentTypeBPUReport CONTENT-TYPE ::= {contentBPUReport }

ContentBPUReport CONTENT-TYPE ::= {
        ContentBPUReport
        IDENTIFIED BY id-contentBPUReport }

EncapsulatedContentInfoBPUReport ::= SEQUENCE {
        eContentType CONTENT-TYPE.&id({ContentTypeBPUReportContentInfo}),
        eContent [0] EXPLICIT OCTET STRING
                        ( CONTAINING CONTENT-TYPE.&Type
                ({ContentTypeBPUReportContentInfo}{@eContentType}))}

ContentTypeBPUReportContentInfo CONTENT-TYPE ::= { bpuReportContentInformation }

BPUReportContentInformation ::= SEQUENCE {
        bpuFunctionReport BPUFunctionReport,
        bpuSecurityReport BPUSecurityReport}
```

BPUFunctionReport và **BPUSecurityReport** được định nghĩa trong 7.2.1 và 7.2.2.

Các kiểu **BPUReport** và **BPUReportContentInformation** bị ràng buộc với tập hợp đối tượng có chứa một đối tượng duy nhất của lớp **CONTENT-TYPE**. Những đối tượng được định nghĩa như sau:

```
bpuReport CONTENT-TYPE ::= {
        BPUReport
        IDENTIFIED BY id-bpuReport }
bpuReportContentInformation CONTENT-TYPE ::= {
        BPUReportContentInformation
        IDENTIFIED BY id-bpuReportContentInformation }
```

7.2.1 BPUFunctionReport

Báo cáo chức năng BPU chứa thông tin về các chức năng được thực hiện trong BPU và dữ liệu đầu vào/đầu ra đến/từ BPU. Các thông tin về chức năng bao gồm các định nghĩa và mức độ hiệu suất hoạt động (chất lượng) của chức năng. Trong ký pháp ASN.1, **BPUFunctionReport** được mô tả như sau:

```
BPUFunctionReport ::= SEQUENCE {
        bpuSubprocessInformationList BPUSubprocessInformationList,
        bpuInputStaticInformationList BPUIOStaticInformationList OPTIONAL,
        bpuOutputStaticInformationList BPUIOStaticInformationList

BPUSubprocessInformationList ::= SEQUENCE SIZE(1..MAX) OF BPUSubprocessInformation

BPUIOStaticInformationList ::= SEQUENCE SIZE(1..MAX) OF BPUIOStaticInformation
```

bpuSubprocessInformationList là danh sách các phần tử kiểu **BPUSubprocessInformation** có số lượng bằng số lượng các quá trình con được thực hiện trong BPU. Kiểu **BPUSubprocessInformation** được xác định trong 7.2.1.1.

bpuInputStaticInformationList là một danh sách các phần tử kiểu **BPUIOStaticInformation** có số lượng bằng số lượng dữ liệu đầu vào cho các BPU. **bpuOutputStaticInformationList** là danh sách các phần tử kiểu **BPUIOStaticInformation** có số lượng bằng số lượng dữ liệu đầu ra từ BPU. Kiểu **BPUIOStaticInformation** được định nghĩa trong 7.2.1.2.

Trong sự thu nạp, quá trình con lưu trữ sẽ đưa ra giá trị băm của mẫu sinh trắc học đầu vào được lưu trữ dưới dạng khuôn mẫu tham chiếu sinh trắc học, và giá trị băm sẽ được đặt trong chứng nhận BRT. Vì vậy, **bpuOutputStaticInformationList** sẽ như một thành viên nếu nó là một biểu thức cho một BPU với quy trình con lưu trữ trong sự thu nạp.

CHÚ THÍCH: Khi chức năng và luồng dữ liệu trong sự thu nạp của BPU khác với trong xác minh sinh trắc học, số lượng các phần tử trong bpuSubprocessInformationList có thể không bằng số lượng các quá trình con trong BPU. Đây có thể là tổng số lượng các quá trình con trong sự thu nạp và trong xác minh sinh trắc học. Trong trường hợp này, bpuSubprocessInformationList được chia thành hai nhóm, một dành cho sự thu nạp và một để xác minh sinh trắc học.

subprocessName của functionDefinition trong một thành viên của nhóm bpuSubprocessInformationList có thể có cùng giá trị với giá trị của subprocessName của functionDefinition trong một thành viên của nhóm còn lại nhưng giá trị của trường subprocessIndex sẽ khác với các thành viên tương ứng trong danh sách. Nếu bpuSubprocessInformaitonList được biểu hiện như trên, thì bpuInputStaticInformationList và bpuOutputStaticInformationList cũng được biểu diễn bằng cách tương tự: có thể có hai thành viên trong danh sách mà giá trị của subprocessIOIndex của một thành viên khác với thành viên còn lại trong khi giá trị dataType là giống nhau.

7.2.1.1 BPUSubprocessInformation

BPUSubprocessInformation chứa thông tin về các chức năng và kết quả đánh giá của quá trình con, của kiểu **FunctionDefinition** và **QualityEvaluation** định nghĩa tương ứng tại 7.2.1.1.1 và 7.2.1.1.2.

```
BPUSubprocessInformation ::= SEQUENCE {
        functionDefinition FunctionDefinition,
        qualityEvaluation QualityEvaluation OPTIONAL}
```

7.2.1.1.1 FunctionDefinition

FunctionDefinition bao gồm sáu thành phần; **subprocessName**, **subprocessIndex**, **inputIndex1**, **inputIndex2**, **outputIndex** và **functionDescription**.

subprocessName là kiểu **SubprocessName** và có một giá trị đại diện cho tên của quá trình con.

Cho mỗi quá trình con trong BPU, các nhà cung cấp sản phẩm của BPU sẽ gán giá trị nguyên duy nhất. **subprocessIndex** là một chỉ số như vậy cho các quá trình con.

Một cặp thành phần biometricType và biometricSubtype cho biết phương thức của dữ liệu sinh trắc được xử lý trong quá trình con. Các kiểu BiometricType và BiometricSubType được định nghĩa trong ISO/IEC 19785-3. biometricType là bắt buộc nếu subprocessName không lấy giá trị so sánh hoặc quyết định.

Để mỗi luồng dữ liệu đi vào hoặc đi từ bất kỳ quá trình con nào trong BPU, nhà cung cấp sản phẩm của BPU sẽ gán giá trị nguyên. Các số nguyên này được gán duy nhất trong BPU. Nếu một đầu vào/đầu ra đến/từ một quá trình con được đưa ra, thì nó sẽ ở trong một trong những luồng và đưa ra số nguyên để được gán cho các luồng dữ liệu một cách tự nhiên. **inputIndex1**, **inputIndex2** và **outputIndex** được đưa ra theo cách này. Bất kỳ quá trình con nào ngoại trừ thu thập dữ liệu sẽ có inputIndex1. Quá trình con so sánh sẽ có cả hai inputIndex1 và inputIndex2.

descriptionFunction là để mô tả bổ sung các chức năng của quá trình con.

Ký pháp ASN.1 cho kiểu **FunctionDefinition** được đưa ra như sau:

```
FunctionDefinition ::= SEQUENCE {
        subprocessName SubprocessName,
        subprocessIndex SubprocessIndex,
        biometricType BiometricType OPTIONAL,
        biometricSubtype BiometricSubtype OPTIONAL,
        inputIndex1 IOIndex OPTIONAL,
        inputIndex2 IOIndex OPTIONAL,
        outputIndex IOIndex,
        functionDescription OCTET STRING (SIZE(1..MAX)) OPTIONAL}
SubprocessName ::= ENUMERATED {
        data-capture(1),
        intermediate-signal-processing(2),
        final-signal-processing(3),
        storage(4),
        comparison(5),
        decision(6),
```

```
        sample-fusion(7),
        feature-fusion(8),
        score-fusion(9),
        decision-fusion(10),
        ...}
SubprocessIndex ::= INTEGER (0..65535)
IOIndex ::= INTEGER (0..65535)
```

7.2.1.1.2 QualityEvaluation

QualityEvaluation bao gồm **biometricProcessQualityInformation** và **qualityEvaluationExtensionInformation**. **biometricProcessQualityInformation** hoặc chứa những báo cáo đánh giá về kiểm thử hiệu suất sinh trắc học của quá trình con hoặc tham chiếu tới báo cáo. **qualityEvaluationExtensionInformation** là trường để mở rộng trong tương lai. Trường này bao gồm một báo cáo hay tham chiếu tới báo cáo. Trong ký pháp ASN.1, **QualityEvaluation** được mô tả như sau:

```
QualityEvaluation ::= SEQUENCE {
        biometricProcessQualityInformation BiometricProcessQualityInformation OPTIONAL,
        qualityEvaluationExtensionInformation QualityEvaluationExtensionInformation
        OPTIONAL}
BiometricProcessQualityInformation ::= CHOICE {
        biometricProcessQuality BiometricProcessQuality,
        biometricProcessQualityReferrer URI}
QualityEvaluationExtensionInformation ::= CHOICE {
        qualityEvaluationExtension QualityEvaluationExtension,
        qualityEvaluationExtensionReferrer URI}
BiometricProcessQuality ::= OCTET STRING (SIZE(1..MAX))
QualityEvaluationExtension ::= OCTET STRING (SIZE(1..MAX)) -- For extension
```

CHÚ THÍCH: **BiometricProcessQuality** và **QualityEvaluationExtension** không được quy định trong tiêu chuẩn này. Trong SC 37/WG 5, một số phần của tiêu chuẩn ISO/IEC 19795 về kiểm thử hiệu suất và báo cáo sinh trắc học đã được chuẩn hóa và một số khác đang được chuẩn hóa ở thời điểm hiện tại. Và định dạng có thể đọc được bằng máy của kiểm thử và báo cáo hiệu suất sinh trắc học đã bắt đầu được tiêu chuẩn hoá như ISO/IEC 29120 trong SC 37/WG 5. Khi đã được chuẩn hóa, khuyến khích sử dụng định dạng máy có thể đọc được quy định trong tiêu chuẩn ISO/IEC 29120 như **BiometricProcessQuality**. Trước khi tiêu chuẩn hóa, các trường này được sử dụng với đặc điểm kỹ thuật theo định nghĩa của nhà cung cấp, người sử dụng hoặc hiệp hội của họ.

7.2.1.2 BPUIOStaticInformation

BPUIOStaticInformation là một kiểu dữ liệu cho thông tin về đầu vào/đầu ra đến/từ BPU và bao gồm bốn thành phần; **dataType** và **subprocessIOIndex**.

```
BPUIOStaticInformation ::= SEQUENCE {
        dataType DataType,
        subprocessIOIndex IOIndex}
```

dataType thuộc kiểu **DataType** bao gồm hai thành phần, **processedLevel** và **purpose**. Trước đây lấy một giá trị tương ứng với một trong những dữ liệu thô, dữ liệu trung gian, dữ liệu đã qua xử lý, điểm số

so sánh, hoặc quyết định so sánh. Sau đó lấy một giá trị tương ứng với khuôn mẫu tham chiếu sinh trắc học hoặc mẫu sinh trắc học.

Sẽ có thành phần **purpose** nếu thành phần đầu tiên **processedLevel** lấy giá trị từ **raw-data** cho **processed-data**. Sẽ không có thành phần **purpose** nếu **processedLevel** lấy giá trị **comparison-score comparison-decision hoặc hashed-data**.

Một đầu vào/đầu ra đến/từ một BPU là một trong những đầu vào/đầu ra đến/từ một quá trình con trong BPU. **subprocessIOIndex** là giá trị tương ứng của **inputIndex1/inputIndex2/outputIndex** của một dữ liệu nhất định kiểu **FunctionDefinition** trong thông tin quá trình con BPU.

```
DataType ::= SEQUENCE {
        processedLevel ProcessedLevel,
        purpose Purpose OPTIONAL}
ProcessedLevel ::= ENUMERATED {
        raw-data(1),
        intermediate-data(2),
        processed-data(3),
        comparison-score(4),
        comparison-result(5),
        hashed-data(6),
        ...}
Purpose ::= ENUMERATED {
        reference(1),
        sample(2)}
```

7.2.2 BPUSecurityReport

BPUSecurityReport bao gồm ba thành phần, **CryptoModuleSecurityInformation**, **BiometricProcessSecurityInformation** và **SecurityEvaluationExtensionInformation**. Mỗi kiểu có chứa hoặc báo cáo đánh giá hoặc tham chiếu tới báo cáo. Trong ký pháp ASN.1, **BPUSecurityReport** được mô tả như sau:

```
BPUSecurityReport ::= SEQUENCE {
   cryptoModuleSecurityInformation CryptoModuleSecurityInformation                OPTIONAL,
   biometricProcessSecurityInformation BiometricProcessSecurityInformation        OPTIONAL,
   securityEvaluationExtensionInformation SecurityEvaluationExtensionInformation OPTIONAL}
CryptoModuleSecurityInformation ::= CHOICE {
   cryptoModuleSecurity CryptoModuleSecurity,
   cryptoModuleSecurityReferrer URI}
BiometricProcessSecurityInformation ::= CHOICE {
   biometricProcessSecurity BiometricProcessSecurity,
   biometricProcessSecurityReferrer URI}
```

CHÚ THÍCH: **CryptoModuleSecurity** và **BiometricProcessSecurity** được sử dụng để chỉ ra mức độ an toàn của các mô-đun/quá trình bằng cách tham chiếu đến một chỉ số thích hợp. Tham chiếu này có thể là mức độ an toàn được tiêu chuẩn hóa hoặc giữ độc quyền.

```
SecurityEvaluationExtensionInformation ::= CHOICE {
        securityEvaluationExtension SecurityEvaluationExtension,
```

securityEvaluationExtensionReferrer URI}

CryptoModuleSecurity ::= OCTET STRING (SIZE(1..MAX))

BiometricProcessSecurity ::= OCTET STRING (SIZE(1..MAX))

SecurityEvaluationExtension ::= OCTET STRING (SIZE(1..MAX)) -- For extension

8 Chứng nhận BRT

Chứng nhận BRT là một chứng nhận cho khuôn mẫu tham chiếu sinh trắc học được ban hành bởi tổ chức chứng nhận BRT nhất định. Chứng nhận chứa thông tin về khuôn mẫu tham chiếu sinh trắc học được lưu trữ trong BPU, chẳng hạn như tổ chức phát hành và thời gian hiệu lực...

Kiểu **BRTCertificate** được định nghĩa tương tự như **BPUReport**. Chứng nhận BRT bao gồm hai trường; trường đầu tiên là giá trị cố định của **id-contentBRTCertificate** và trường thứ hai của kiểu **ContentBRTCertificate**, dữ liệu **SIGNEDDATA** được tham số hóa với nội dung được đóng gói của kiểu **BRTCContentInformation**. Chữ ký sẽ được tạo ra bằng cách sử dụng khóa riêng tư của tổ chức chứng nhận BRT.

Trong ký pháp ASN.1, **BRTCertificate** được mô tả như sau:

```
BRTCertificate ::= SEQUENCE {
        contentType CONTENT-TYPE.&id({ContentTypeBRTCertificate}),
        content [0] EXPLICIT
            CONTENT-TYPE.&Type({ContentTypeBRTCertificate}{@contentType})}
ContentTypeBRTCertificate CONTENT-TYPE ::= { contentBRTCertificate }

ContentBRTCertificate ::= SIGNEDDATA { EncapsulatedContentInfoBRTCertificate }

EncapsulatedContentInfoBRTCertificate ::= SEQUENCE {
        eContentType CONTENT-TYPE.&id({ContentTypeBRTCertificateContentInfo}), eContent
        [0] EXPLICIT OCTET STRING
         ( CONTAINING CONTENT-TYPE.&Type
            ({ContentTypeBRTCertificateContentInfo}{@eContentType})}
ContentTypeBRTCertificateContentInfo CONTENT-TYPE ::= { brtcContentInformation }
```

Các thuộc tính sau liên kết kiểu **ContentBRTCertificate** với **id-contentBRTCertificate** và kiểu **BRTCContentInformation** với **id-brtcContentInformation**.

Kiểu **BRTCertificate** và **EncapsulatedContentInfoBRTCertificate** bị ràng buộc với tập hợp đối tượng có chứa một đối tượng đơn lẻ của lớp **CONTENT-TYPE** được định nghĩa như sau:

```
contentBRTCertificate CONTENT-TYPE ::= {
        ContentBRTCertificate
        IDENTIFIED BY id-contentBRTCertificate }
id-contentBRTCertificate    OBJECT IDENTIFIER ::=
        {iso(1) standard(0) acbio(24761) contentType(2) brtCertificate(6)}
brtcContentInformation CONTENT-TYPE ::= {
        BRTCContentInformation
        IDENTIFIED BY id-brtcContentInformation  }
```

```
id-brtcContentInformation OBJECT IDENTIFIER ::=
        {iso(1) standard(0) acbio(24761) contentType(2) brtcContent(7)}
```

8.1 BRTCContentInformation

BRTCContentInformation được biểu thị với CBEFF BIR (Hồ sơ thông tin sinh trắc học) được quy định trong tiêu chuẩn ISO/IEC 19785-1. **BRTCContentInformation** bao gồm hai phần, **sbhForBRTC** và **bdbForBRTC**. Biểu thị trước đây, SBH (Tiêu đề sinh trắc học tiêu chuẩn) của CBEFF được áp dụng. Sau đó sử dụng định nghĩa mới là định dạng BDB (Khối dữ liệu sinh trắc học) cho chứng nhận BRT.

Kiểu **BRTCContentInformation** được mô tả như sau:

```
BRTCContentInformation ::= SEQUENCE {
        sbhForBRTC SBHForBRTC,
        bdbForBRTC BDBForBRTC}
```

sbhForBRTC thuộc kiểu **SBHForBRTC** và có bảy phần tử; **version**, **brtcIndex**, **brtcValidityPeriod**, **brtQuality**, **bdbEncryptionOptions**, **bdbIntegrityOptions** và **bdbFormatForBRC**. Kiểu của mỗi phần tử được quy định trong tiêu chuẩn ISO/IEC 19785-3.

version được sử dụng để xác định các phiên bản của định dạng **SHBForBRTC**.

brtcIndex chỉ ra chỉ số của chứng nhận BRT.

brtcValidityPeriod chứa thời hạn hiệu lực của chứng nhận BRT. **biometricType** cùng với **biometricSubtype** hiển thị phương thức của tham chiếu sinh trắc học.

brtQuality chứa chất lượng của khuôn mẫu tham chiếu sinh trắc học.

optionBDBEncryption và **optionBIRIntegrity** là tùy chọn mã hóa và tùy chọn toàn vẹn và được thiết lập giá trị **FALSE**.

bdbFormatForBRTC chỉ ra kiểu định dạng sở hữu và kiểu định dạng của **BDBForBRTC**.

Trong ký pháp ASN.1, **sbhForBRTC** được mô tả như sau:

```
SBHForBRTC ::= SEQUENCE {
        version CBEFFVersion,
        brtcIndex BIRIndex,
        brtcValidityPeriod BDBValidityPeriod,
        biometricType BiometricType,
        biometricSubtype BiometricSubtype OPTIONAL,
        brtQuality Quality,
        bdbEncryptionOptions EncryptionOptions(FALSE), bdbIntegrityOptions
        IntegrityOptions(FALSE), bdbFormatForBRTC BDBFormat}
```

bdbForBRTC thuộc kiểu **BDBForBRTC** và có tám phần tử; **version**, **originalBDBHashList**, **originalBIRReferrer**, **originalBIRpatronFormat**, **originalBDBPosition**, **userInformation**, **pkiCertificateInformation** và **enrolmentACBioInstances**.

version là phiên bản của định dạng **BDBForBRTC**. Trường tùy chọn **issuerAndSerialNumberBRTC** của kiểu **IssuerAndSerialNumberBRTC** được lấy từ RFC 3852 là một cặp thông tin, nhà phát hành chứng nhận BRT và số sê ri duy nhất được phát hành bởi nhà phát hành. OCSP có thể được áp dụng để kiểm tra tính hợp lệ của chứng nhận BRT.

originalBDBHashList là một danh sách của **Hash**. **Hash** có hai trường, giá trị hàm băm và nhận dạng thuật toán của thuật toán băm. Đầu tiên là giá trị hàm băm của khuôn mẫu tham chiếu sinh trắc học. Nếu **originalBDBHashList** có chứa nhiều hơn một phần tử, chúng thuộc một khuôn mẫu tham chiếu sinh trắc học đơn lẻ và các thuật toán băm khác nhau.

originalBIRReferrer là tham chiếu đến BIR ban đầu.

originalBDBPosition chỉ ra vị trí của khuôn mẫu tham chiếu sinh trắc học tương ứng với chứng nhận BRT này trong BDB ban đầu.

userInformation là một trường tùy chọn của kiểu **UserInformation**, trong đó có định danh, tên và định danh duy nhất của người có khuôn mẫu tham chiếu sinh trắc học là đối tượng của chứng nhận BRT.

pkiCertificateInformation là trường tùy chọn và chứa thông tin về chứng nhận khóa công khai X.509 của người sử dụng, số sê-ri của chứng nhận, tên của tổ chức phát hành và định danh duy nhất của chứng nhận. Trường này liên kết chứng nhận BRT với chứng nhận X.509.

enrolmentACBioInstances là một danh sách tùy chọn các Báo cáo thể hiện ACBio được tạo ra khi thu nạp khuôn mẫu tham chiếu sinh trắc học.

Trong ký pháp ASN.1, **BDBForBRTC** được mô tả như sau:

```
BDBForBRTC ::= SEQUENCE {
        version Version DEFAULT v0,
        issuerAndSerialNumberBRTC IssuerAndSerialNumber OPTIONAL, originalBDBHashList
        HashList, originalBIRReferrer URI OPTIONAL,
        originalBIRPatronFormat PatronFormat,
        originalBDBPosition INTEGER,
        userInformation UserInformation OPTIONAL,
        pkiCertificateInformation PKICertificateInformation OPTIONAL,
        enrolmentACBioInstances SequenceOfACBioInstances OPTIONAL}

HashList ::= SEQUENCE SIZE(1..MAX) OF Hash

UserInformation ::= SEQUENCE {
        userIdentifier OCTET STRING,
        userName Name OPTIONAL,
        userUniqueIdentifier UniqueIdentifier OPTIONAL}

PKICertificateInformation ::= SEQUENCE {
        pkiCertificateSerialNumber CertificateSerialNumber, pkiCertificateIssuerName Name
        OPTIONAL, pkiCertificateIssuerUniqueIdentifier UniqueIdentifier OPTIONAL}

SequenceOfACBioInstances ::= SEQUENCE SIZE(1..MAX) OF ACBioInstance
```

8.2 Các giá trị Sở hữu định dạng và Kiểu định dạng

Định dạng sở hữu cho **BDBForBRTC** sẽ sử dụng giá trị 0102 hex (258 chữ số thập phân), được đăng ký nhận dạng định dạng bảo trợ ISO/IEC JTC1 SC27. Kiểu định dạng cho BRC sẽ sử dụng giá trị 0001 hex (1 chữ số thập phân), đã được đăng ký bởi SC27 làm giá trị cho các **BDBForBRTC**.

Kết quả giá trị định danh đối tượng ASN.1 cho **BDBForBRTC** là:

{iso registration-authority cbeff(19785) organization(0) iso-iec-jtc1-SC27 (258)
bdbs(0) biometric-reference-template-certificate (1)}

Phụ lục A

(Quy định)

Mô-đun ASN.1 cho ACBio

```
AuthenticationContextForBiometrics {iso(1) standard(0) acbio(24761) module(1) acbio(2)
version1(1)}

DEFINITIONS AUTOMATIC TAGS ::= BEGIN

IMPORTS

-- ASN.1 Module AlgorithmInformation in RFC 5912
        AlgorithmIdentifier
        FROM AlgorithmInformation-2009 {iso(1) identified-organization(3) dod(6)

internet(1) security(5)

            mechanisms(5) pkix(7) id-mod(0) id-mod-algorithmInformation-02(58)} --

RFC 5280 revised as RFC 5912

        Certificate, CertificateList, CertificateSerialNumber, Name, UniqueIdentifier
        FROM PKIX1Explicit-2009 { iso(1) identified-organization(3) dod(6) internet(1)
        security(5) mechanisms(5) pkix(7) id-mod(0) id-mod-pkix1-explicit-02(51) }


-- RFC 5755  revised as RFC 5912
        AttributeCertificate
        FROM PKIXAttributeCertificate-2009 { iso(1) identified-organization(3) dod(6)
internet(1)
                security(5) mechanisms(5) pkix(7) id-mod(0) id-mod-attribute-cert-02(47) }


-- ISO/IEC 19785 Common Biometric Exchange Formats Framework
        BiometricType, BiometricSubtype, CBEFFVersion, BIRIndex,
        BDBValidityPeriod,Quality,EncryptionOptions, IntegrityOptions,
        BDBFormat, PatronFormat
        FROM CBEFF-DATA-ELEMENTS {iso standard 19785 modules(0)
        types-for-cbeff-data-elements(1) }
-- RFC 3852 Cryptographic Message Syntax revised as RFC 5911
        CMSVersion, DigestAlgorithmIdentifier,
        SignerInfos, OriginatorInfo, RecipientInfos,
        MessageAuthenticationCodeAlgorithm, IssuerAndSerialNumber,
        AuthAttributes, MessageAuthenticationCode, UnauthAttributes,

        CONTENT-TYPE
        FROM CryptographicMessageSyntax2009{
                iso(1) member-body(2) us(840) rsadsi(113549)
                pkcs(1) pkcs-9(9) smime(16) modules(0) cms-2004-02(41) };

ACBioInstance ::= SEQUENCE {

        contentType CONTENT-TYPE.&id({ContentTypeACBio}),
        content [0] EXPLICIT CONTENT-TYPE.&Type
                ({ContentTypeACBio}{@contentType})}

ContentTypeACBio  CONTENT-TYPE  ::=  {signedDataACBio  |
                        authenticatedDataACBio}

SignedDataACBio ::= SIGNEDDATA { EncapsulatedContentInfoACBio }
```

```
AuthenticatedDataACBio ::= AUTHENTICATEDDATA { EncapsulatedContentInfoACBio }

EncapsulatedContentInfoACBio ::= SEQUENCE {
        eContentType CONTENT-TYPE.&id({ContentTypeACBioContentInfo}),
        eContent [0] EXPLICIT OCTET STRING
           ( CONTAINING CONTENT-TYPE.&Type
                ({ContentTypeACBioContentInfo}{@eContentType}))}

ContentTypeACBioContentInfo CONTENT-TYPE ::= {acbioContentInformation}

ACBioContentInformation ::= SEQUENCE {
        version Version DEFAULT v1,
        bpuInformation BPUInformation,
        controlValue OCTET STRING (SIZE(16)),
        biometricProcess BiometricProcess,
        brtCertificateInformation BRTCertificateInformation OPTIONAL}

Version ::= INTEGER { v1(1) } ( v1, ... )

BPUInformation ::= SEQUENCE {
        bpuCertificateReferrerInformation BPUCertificateReferrerInformation
                OPTIONAL,
        bpuReportInformation BPUReportInformation}

BPUCertificateReferrerInformation ::= SEQUENCE {
        bpuCertificateReferrer URI,
        crlsReferrer URI OPTIONAL}

URI ::= VisibleString (SIZE(1..MAX))

BPUReportInformation ::= CHOICE {
        bpuReport [0] EXPLICIT BPUReport,
        bpuReportReferrer URI}

BPUReport ::= SEQUENCE {
        contentType CONTENT-TYPE.&id({ContentTypeBPUReport}),
        content [0] EXPLICIT CONTENT-TYPE.&Type
                ({ContentTypeBPUReport}{@contentType})}

ContentTypeBPUReport CONTENT-TYPE ::= {contentBPUReport }

ContentBPUReport ::= SIGNEDDATA { EncapsulatedContentInfoBPUReport }

EncapsulatedContentInfoBPUReport ::= SEQUENCE {
        eContentType CONTENT-TYPE.&id({ContentTypeBPUReportContentInfo}),
        eContent [0] EXPLICIT OCTET STRING
                ( CONTAINING CONTENT-TYPE.&Type
           ({ContentTypeBPUReportContentInfo}{@eContentType}))}

ContentTypeBPUReportContentInfo CONTENT-TYPE ::= { bpuReportContentInformation }

BPUReportContentInformation ::= SEQUENCE {
        bpuFunctionReport BPUFunctionReport,
        bpuSecurityReport BPUSecurityReport}

BPUFunctionReport ::= SEQUENCE {
        bpuSubprocessInformationList BPUSubprocessInformationList,
        bpuInputStaticInformationList BPUIOStaticInformationList OPTIONAL,
        bpuOutputStaticInformationList BPUIOStaticInformationList }

BPUSubprocessInformationList ::= SEQUENCE SIZE(1..MAX) OF BPUSubprocessInformation

BPUSubprocessInformation ::= SEQUENCE { functionDefinition
```

```
        FunctionDefinition, qualityEvaluation
        QualityEvaluation OPTIONAL}

FunctionDefinition ::= SEQUENCE {
        subprocessName SubprocessName,
        subprocessIndex SubprocessIndex,
        biometricType BiometricType OPTIONAL,
        biometricSubtype BiometricSubtype OPTIONAL,
        inputIndex1 IOIndex OPTIONAL,
        inputIndex2 IOIndex OPTIONAL,
        outputIndex IOIndex,
        functionDescription OCTET STRING (SIZE(1..MAX)) OPTIONAL}

SubprocessName ::= ENUMERATED {

        data-capture(1),
        intermediate-signal-processing(2),
        final-signal-processing(3),
        storage(4),
        comparison(5),
        decision(6),
        sample-fusion(7),
        feature-fusion(8),
        score-fusion(9),
        decision-fusion(10),
        ...}

SubprocessIndex ::= INTEGER (0..65535)

IOIndex ::= INTEGER (0..65535)

QualityEvaluation ::= SEQUENCE {
        biometricProcessQualityInformation  BiometricProcessQualityInformation  OPTIONAL,
        qualityEvaluationExtensionInformation QualityEvaluationExtensionInformation
OPTIONAL}

BiometricProcessQualityInformation ::= CHOICE {
        biometricProcessQuality BiometricProcessQuality,
        biometricProcessQualityReferrer URI}

QualityEvaluationExtensionInformation ::= CHOICE {

qualityEvaluationExtension QualityEvaluationExtension,
        qualityEvaluationExtensionReferrer URI}

BiometricProcessQuality ::= OCTET STRING (SIZE(1..MAX))

QualityEvaluationExtension ::= OCTET STRING (SIZE(1..MAX)) -- For extension

BPUIOStaticInformationList ::= SEQUENCE SIZE(1..MAX) OF BPUIOStaticInformation

BPUIOStaticInformation ::= SEQUENCE {
        dataType DataType,
        subprocessIOIndex IOIndex}

DataType ::= SEQUENCE {
        processedLevel ProcessedLevel,
        purpose Purpose OPTIONAL}

ProcessedLevel ::= ENUMERATED {
        raw-data(1),
        intermediate-data(2),
        processed-data(3),
```

```
        comparison-score(4),
        comparison-result(5),
        hashed-data(6),
        ...}

Purpose ::= ENUMERATED {
        reference(1),
        sample(2)}

BPUSecurityReport ::= SEQUENCE {
        cryptoModuleSecurityInformation CryptoModuleSecurityInformation
                OPTIONAL,
        biometricProcessSecurityInformation BiometricProcessSecurityInformation
                OPTIONAL,
        securityEvaluationExtensionInformation
                SecurityEvaluationExtensionInformation OPTIONAL}

CryptoModuleSecurityInformation ::= CHOICE {
        cryptoModuleSecurity CryptoModuleSecurity,
        cryptoModuleSecurityReferrer URI}

BiometricProcessSecurityInformation ::= CHOICE {
        biometricProcessSecurity BiometricProcessSecurity,
        biometricProcessSecurityReferrer URI}

SecurityEvaluationExtensionInformation ::= CHOICE {
        securityEvaluationExtension SecurityEvaluationExtension,
        securityEvaluationExtensionReferrer URI}

CryptoModuleSecurity ::= OCTET STRING (SIZE(1..MAX))

BiometricProcessSecurity ::= OCTET STRING (SIZE(1..MAX))

SecurityEvaluationExtension ::= OCTET STRING (SIZE(1..MAX)) -- For extension

BiometricProcess ::= SEQUENCE {
        subprocessIndexList SubprocessIndexList,
        bpuInputExecutionInformationList BPUIOExecutionInformationList OPTIONAL,
        bpuOuputExecutionInformationList BPUIOExecutionInformationList }

SubprocessIndexList ::= SEQUENCE SIZE(1..MAX) OF SubprocessIndex

BPUIOExecutionInformationList ::= SEQUENCE SIZE(1..MAX) OF BPUIOExecutionInformation

BPUIOExecutionInformation ::= SEQUENCE {
        dataType DataType,
        bpuIOIndex IOIndex,
        subprocessIOIndex IOIndex,
        hash Hash}

Hash ::= SEQUENCE {
        algorithmIdentifier AlgorithmIdentifier,
        hashValue OCTET STRING}

BRTCertificateInformation ::= CHOICE {
        brtCertificateList BRTCertificateList,
        brtCertificateReferrerList BRTCertificateReferrerList}

BRTCertificateList ::= SEQUENCE SIZE(1..MAX) OF BRTCertificate

BRTCertificateReferrerList ::= SEQUENCE SIZE(1..MAX) OF URI

BRTCertificate ::= SEQUENCE {
```

```
        contentType CONTENT-TYPE.&id({ContentTypeBRTCertificate}),
        content [0] EXPLICIT
            CONTENT-TYPE.&Type({ContentTypeBRTCertificate}{@contentType})}

ContentTypeBRTCertificate CONTENT-TYPE ::= { contentBRTCertificate }

ContentBRTCertificate ::= SIGNEDDATA { EncapsulatedContentInfoBRTCertificate }

EncapsulatedContentInfoBRTCertificate ::= SEQUENCE {
        eContentType CONTENT-TYPE.&id({ContentTypeBRTCertificateContentInfo}),
        eContent [0] EXPLICIT OCTET STRING
            ( CONTAINING CONTENT-TYPE.&Type
                ({ContentTypeBRTCertificateContentInfo}{@eContentType})}

ContentTypeBRTCertificateContentInfo CONTENT-TYPE ::= { brtcContentInformation }

BRTCContentInformation ::= SEQUENCE {
        sbhForBRTC SBHForBRTC,
        bdbForBRTC BDBForBRTC}

SBHForBRTC ::= SEQUENCE {
        version CBEFFVersion,
        brtcIndex BIRIndex,
        brtcValidityPeriod BDBValidityPeriod,
        biometricType BiometricType,
        biometricSubtype BiometricSubtype OPTIONAL,
        brtQuality Quality,
        bdbEncryptionOptions EncryptionOptions(FALSE),
        bdbIntegrityOptions IntegrityOptions(FALSE),
        bdbFormatForBRTC BDBFormat}

BDBForBRTC ::= SEQUENCE {
        version Version DEFAULT v1,
        issuerAndSerialNumberBRTC IssuerAndSerialNumber OPTIONAL,
        originalBDBHashList HashList,
        originalBIRReferrer URI OPTIONAL,
        originalBIRPatronFormat PatronFormat,
        originalBDBPosition INTEGER,
        userInformation UserInformation OPTIONAL,
        pkiCertificateInformation PKICertificateInformation OPTIONAL,
        enrolmentACBioInstances SequenceOfACBioInstances OPTIONAL}

HashList ::= SEQUENCE SIZE(1..MAX) OF Hash

UserInformation ::= SEQUENCE {
        userIdentifier OCTET STRING,
        userName Name OPTIONAL,
        userUniqueIdentifier UniqueIdentifier OPTIONAL}

PKICertificateInformation ::= SEQUENCE {
        pkiCertificateSerialNumber CertificateSerialNumber,
        pkiCertificateIssuerName Name OPTIONAL,
        pkiCertificateIssuerUniqueIdentifier UniqueIdentifier OPTIONAL}

SequenceOfACBioInstances ::= SEQUENCE SIZE(1..MAX) OF ACBioInstance

-- Useful Definitions

SIGNEDDATA { EncapsulatedContentInfo } ::= SEQUENCE { version
        CMSVersion,
        digestAlgorithms SET OF DigestAlgorithmIdentifier,
        encapContentInfo EncapsulatedContentInfo,
```

```
        certificates [0] IMPLICIT CertificateSet OPTIONAL,
        crls [1] IMPLICIT RevocationInfoChoices OPTIONAL,
        signerInfos SignerInfos}

AUTHENTICATEDDATA { EncapsulatedContentInfo } ::= SEQUENCE {
        version CMSVersion,
        originatorInfo [0] IMPLICIT OriginatorInfo OPTIONAL,
        recipientInfos RecipientInfos,
        macAlgorithm MessageAuthenticationCodeAlgorithm,
        digestAlgorithm [1] DigestAlgorithmIdentifier OPTIONAL,
        encapContentInfo EncapsulatedContentInfo,
        authAttrs [2] IMPLICIT AuthAttributes OPTIONAL,
        mac MessageAuthenticationCode,
        unauthAttrs [3] IMPLICIT UnauthAttributes OPTIONAL}

CertificateSet ::= SET OF CertificateChoices

CertificateChoices ::= CHOICE {
        certificate Certificate,
        v2AttrCert [2] IMPLICIT AttributeCertificateV2,
        other [3] IMPLICIT OtherCertificateFormat}

AttributeCertificateV2 ::= AttributeCertificate

OtherCertificateFormat ::= SEQUENCE {
        otherFormat OTHERCERTIFICATE.&id({OtherCertificate}),
        otherCert OTHERCERTIFICATE.&Type({OtherCertificate}{@otherFormat})}

OTHERCERTIFICATE ::= TYPE-IDENTIFIER

OtherCertificate OTHERCERTIFICATE ::= {...}

RevocationInfoChoices ::= SET OF RevocationInfoChoice

RevocationInfoChoice ::= CHOICE {
        crl CertificateList,
        other [1] IMPLICIT OtherRevocationInfoFormat }

OtherRevocationInfoFormat ::= SEQUENCE {

otherRevInfoFormat OTHERREVOCATION.&id({OtherRevocation}),

otherRevInfo OTHERREVOCATION.&Type({OtherRevocation}{@otherRevInfoFormat}) }

OTHERREVOCATION ::= TYPE-IDENTIFIER

OtherRevocation OTHERREVOCATION ::= {...}

-- contentType object identifiers

id-signedDataACBio OBJECT IDENTIFIER ::=
        {iso(1) standard(0) acbio(24761) contentType(2) signedDataACBio(1)}

id-authenticatedDataACBio OBJECT IDENTIFIER ::=
        {iso(1) standard(0) acbio(24761) contentType(2) authenticatedDataACBio(2)}

id-acbioContentInformation OBJECT IDENTIFIER ::=
        {iso(1) standard(0) acbio(24761) contentType(2) acbioContent(3)}

id-contnetBPUReport OBJECT IDENTIFIER ::=
        {iso(1) standard(0) acbio(24761) contentType(2) bpuReport(4)}

id-bpuReportContentInformation OBJECT IDENTIFIER ::=
        {iso(1) standard(0) acbio(24761) contentType(2) bpuReportContent(5)}

id-contentBRTCertificate    OBJECT IDENTIFIER ::=
```

```
        {iso(1) standard(0) acbio(24761) contentType(2) brtCertificate(6)}

id-brtcContentInformation OBJECT IDENTIFIER ::=
        {iso(1) standard(0) acbio(24761) contentType(2) brtcContent(7)}

-- ContentType objects

signedDataACBio CONTENT-TYPE ::= {
        SignedDataACBio
        IDENTIFIED BY id-signedDataACBio }

authenticatedDataACBio CONTENT-TYPE ::= {
        AuthenticatedDataACBio
        IDENTIFIED BY id-authenticatedDataACBio }

acbioContentInformation CONTENT-TYPE ::= {
        ACBioContentInformation
        IDENTIFIED BY id-acbioContentInformation }

contentBPUReport CONTENT-TYPE ::= {
        ContentBPUReport
        IDENTIFIED BY id-contnetBPUReport }

bpuReportContentInformation CONTENT-TYPE ::= {
        BPUReportContentInformation
        IDENTIFIED BY id-bpuReportContentInformation }

contentBRTCertificate CONTENT-TYPE ::= {
        ContentBRTCertificate
        IDENTIFIED BY id-contentBRTCertificate }

brtcContentInformation CONTENT-TYPE ::= {
        BRTCContentInformation
        IDENTIFIED BY id-brtcContentInformation }

END – AuthenticationContextForBiometrics
```

Phụ lục B

(Tham khảo)

Ví dụ về sự thực hiện

B.1 Ví dụ về sự thực hiện đối với ACBio

Trong tiêu chuẩn này, các giao thức cho ACBio không được xác định. Trong Phụ lục này, hai ví dụ về sự thực hiện ACBio được đưa ra bao gồm các giao thức; một cho trường hợp mô hình STOC (Lưu trữ trên thẻ), trường hợp còn lại là mô hình OCM (Phù hợp trên thẻ).

B.1.1 Ví dụ về sự thực hiện đối với mô hình STOC

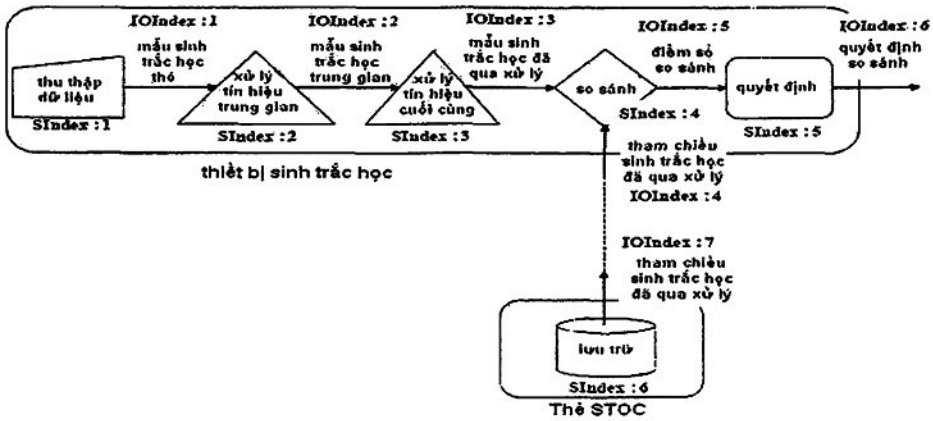
Trong ví dụ này, chúng ta giả định rằng mô hình STOC này của một quá trình xác minh sinh trắc học bao gồm hai BPU, một là thiết bị sinh trắc học mà có chức năng thu thập dữ liệu, xử lý tín hiệu trung gian, xử lý tín hiệu cuối cùng, so sánh và quyết định và BPU còn lại là một thẻ STOC lưu trữ khuôn mẫu tham chiếu sinh trắc học đã qua xử lý. Ví dụ này chủ yếu tập trung vào thẻ STOC.

B.1.1.1 Quá trình đánh giá

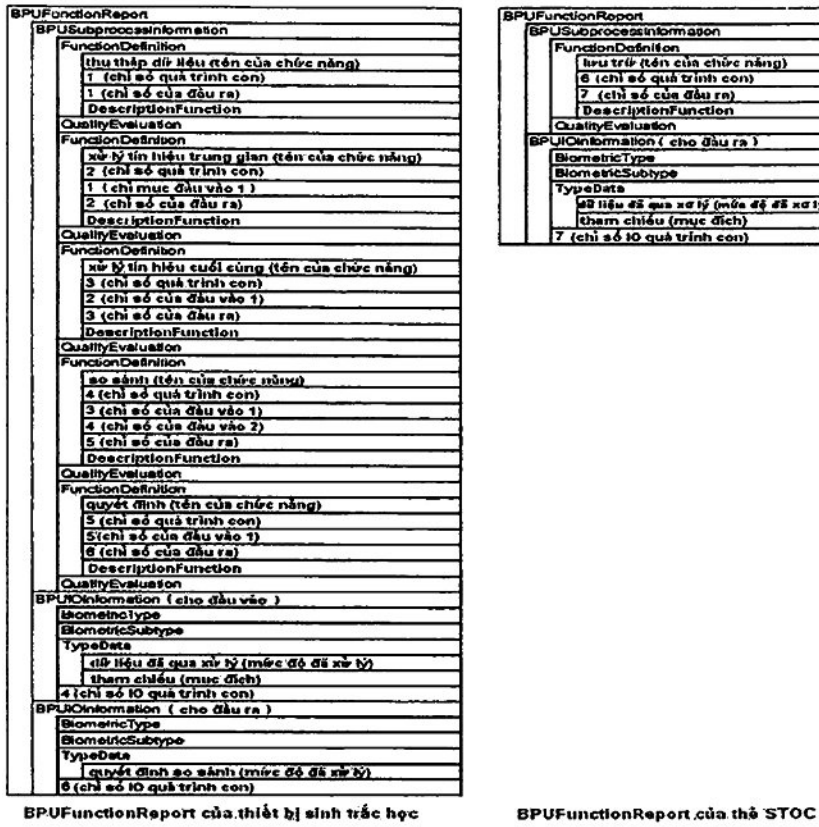
Sản phẩm của các BPU, tức là thẻ STOC và các thiết bị sinh trắc học được sử dụng trong quá trình xác minh sinh trắc học, nên được đánh giá tại một tổ chức đánh giá nhất định và ban hành báo cáo BPU của tổ chức đó.

B.1.1.2 Quá trình chế tạo

Các nhà cung cấp BPU nên đánh chỉ số mỗi quá trình con và luồng dựa theo nguyên tắc trong 7.2.1. Nếu các quá trình con và luồng trong thiết bị sinh trắc học và trong thẻ STOC đã được lập chỉ số như Hình B.1, thì BPUFunctionReport của thiết bị sinh trắc học và của thẻ STOC sẽ được thể hiện trong Hình B.2. Trong Hình B.1, Sindex nghĩa là chỉ số quá trình con và IOIndex nghĩa là chỉ số IO quá trình con.

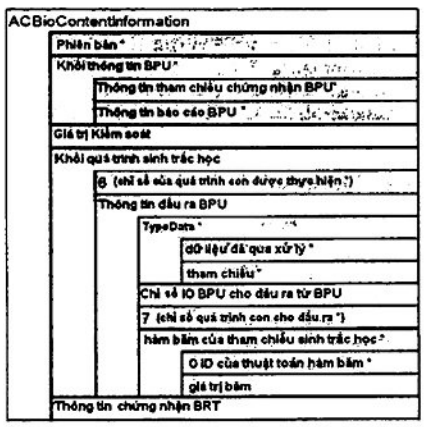


Hình B.1 – Quá trình xác minh sinh trắc học của thẻ STOC và ví dụ về chỉ số



Hình B.2 – Ví dụ về các BPUFunctionReport cho mô hình STOC

Trong trường hợp này, một khối dữ liệu của các loại **ACBioContentInformation** nên được lưu trữ trong một thẻ STOC trước như trong Hình B.3. Trong Hình B.3, các phần tử dữ liệu được đánh dấu * (nền đậm) là dữ liệu cố định và các thiết lập trong lĩnh vực thẻ STOC trước trong khi không được đánh dấu * (không nền) đều được để trống để thực hiện trong quá trình thu nạp và thực hiện sau đó.



Hình B.3 – Khối dữ liệu được lưu trữ trên thẻ STOC trong quá trình chế tạo

Trong Hình B.3, các trường không được đánh dấu * (không nền), ngoại trừ thông tin chứng nhận BRT có độ dài cố định của riêng trường đó. Độ dài của trường Thông tin chứng nhận BRT không được xác định trong quá trình chế tạo nhưng được xác định trong quá trình thu nạp. Cần lưu ý rằng khu vực cho **ACBioContentInformation** nên có các vùng liên tiếp đủ cho thông tin chứng nhận BRT.

Bảng dưới đây là định dạng BER-TLV của **ACBioContentInformation** cho thẻ STOC, tương đương với cấu trúc dữ liệu của Hình B.3.

Bảng B.1 – Định dạng BER-TLV của ACBioContentInformation cho thẻ STOC

Tag	L	Giá trị								
'AE'	Var.	ACBioContentInformation								
		Tag	L	Giá trị						
		'02'	1	Phiên bản						
		'A0'	Var.	Khối thông tin BPU						
				Tag	L	Giá trị				
				'A0'	Var.	Thông tin tham chiếu chứng nhận BPU				
				'A1'	Var.	Thông tin báo cáo BPU				
		'04'	16	Giá trị kiểm soát						
		'A2'	Var.	Khối quá trình sinh trắc học						
				Tag	L	Giá trị				
				'02'	1	chỉ số của quá trình con 1 được thực hiện				
				'A1'	Var.	Thông tin đầu ra				
						Tag	L	Giá trị		
						'A0'	6	Kiểu Dữ liệu		
								Tag	L	Giá trị
								'0A'	1	dữ liệu đã qua xử lý
								'0A'	1	tham chiếu
						'02'	1	chỉ số IO BPU cho đầu ra từ BPU		
						'02'	1	chỉ số quá trình con cho đầu ra		
						'A1'	Var.	thông tin hàm băm của đầu ra		
								'06'	Var.	ID OID của thuật toán hàm băm
								'04'	Var.	Giá trị băm của đầu ra
		'A3'	Var.	Thông tin chứng nhận BRT						

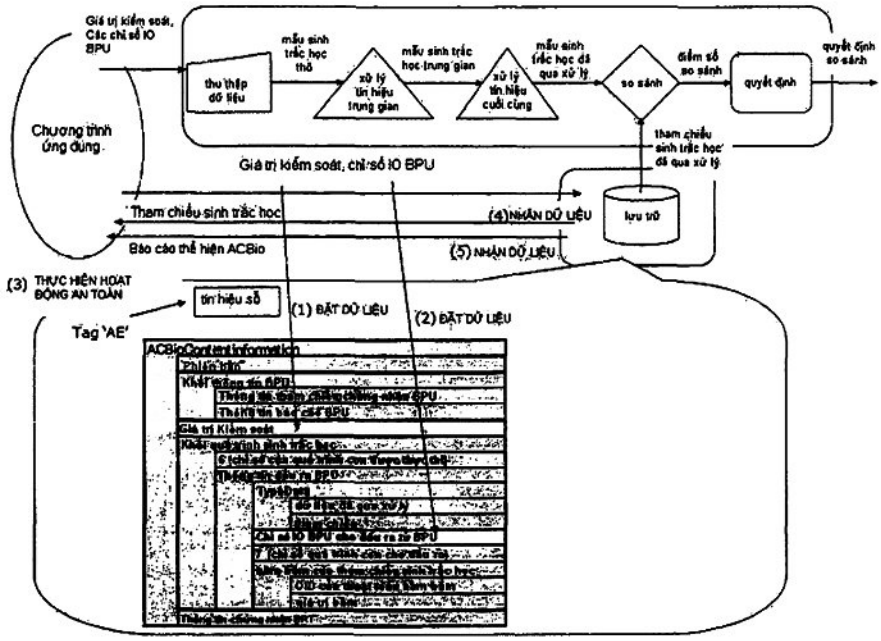
B.1.1.3 Quá trình thu nạp

Khuôn mẫu tham chiếu sinh trắc học được lưu trữ vào thẻ STOC trong quá trình này. Chứng nhận BRT được cấp cho khuôn mẫu tham chiếu sinh trắc học và chứng nhận BRT hoặc tham chiếu đến chứng nhận được lưu trữ trong **brtCertificateInformation** của **ACBioContentInformation**. Độ dài của trường kiểu **ACBioContentInformation** phải được điều chỉnh bằng cách tăng thêm độ dài của Thông tin chứng nhận BRT cộng với độ dài của trường Tag và trường L.

B.1.1.4 Quá trình thực thi

Trong một thực thi của xác minh sinh trắc học, hai đầu vào được cung cấp cho một thẻ STOC; đầu tiên là giá trị kiểm soát từ bộ xác nhận, thứ hai là chỉ số IO BPU với đầu ra từ thẻ STOC. Thẻ STOC nên thiết lập "Giá trị Kiểm soát" đầu tiên ((1) ĐẶT DỮ LIỆU trong Hình B.4), thứ hai đến "chỉ số IO BPU cho đầu ra từ BPU" ((2) ĐẶT DỮ LIỆU trong Hình B 4), tương ứng.

Tiếp theo thẻ STOC ký số toàn bộ trường của kiểu **ACBioContentInformation** ((3) THỰC HIỆN HOẠT ĐỘNG AN TOÀN trong Hình B.4) để có được Báo cáo thể hiện ACBio và gửi nó như đầu ra ((5) NHẬN DỮ LIỆU trong Hình B.4)) cùng với các sinh trắc học xử lý mẫu tham khảo ((4) NHẬN DỮ LIỆU trong Hình B.4)).



Hình B.4 – Sự tạo thành Báo cáo thể hiện ACBio trên thẻ STOC dựa vào sự thực hiện một xác minh sinh trắc học

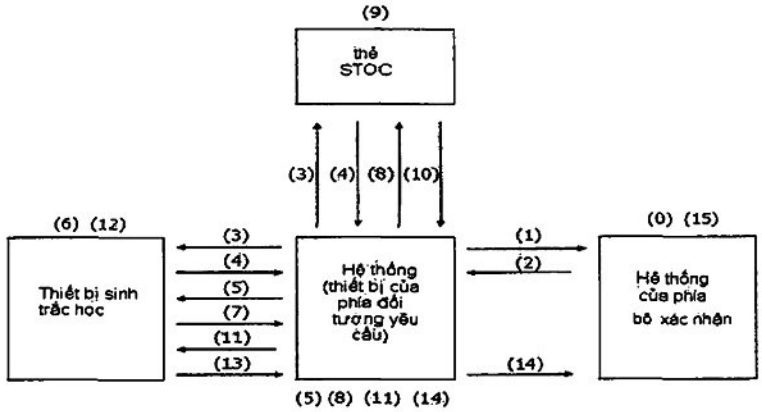
Hình B.5 mô tả một dãy lệnh nhằm sinh ra Báo cáo thể hiện ACBio trên thẻ STOC với BIT là từ viết tắt cho Khuôn mẫu thông tin sinh trắc học, một thuật ngữ được sử dụng trong chuỗi tiêu chuẩn ISO/IEC 7816.

Câu lệnh/phản ứng	Ý nghĩa
PUT DATA <Control Value> OK	Đặt giá trị kiểm soát như tham số đầu vào
PUT DATA <BPU IO Index Output> OK	Đặt chỉ số IO BPU cho đầu ra như tham số đầu vào
PERFORM SECURITY OPERATION <'AE', 'BC'> OK	Tính toán chữ ký số cho ACBioContentInformation và đặt nó vào trường chữ ký số của cấu trúc SignedData trong Báo cáo thể hiện ACBio
GET DATA BIT	Nhận tham chiếu sinh trắc học đã qua xử lý như đầu ra
GET DATA BIT	Nhận Báo cáo thể hiện ACBio như đầu ra

Hình B.5 – Chuỗi lệnh cho sự tạo thành Báo cáo thể hiện ACBio trên thẻ STOC

B.1.1.5 Ví dụ về giao thức

Chúng ta giả định sự tồn tại của hệ thống về phía bộ xác nhận và một hệ thống (thiết bị) của phía đối tượng yêu cầu mà chỉ có chức năng để truyền/nhận thông điệp tới/từ bên thứ ba khác, như thể hiện trong Hình B.6.



Hình B.6 – Ví dụ về giao thức cho mô hình STOC

Ví dụ về giao thức cho mô hình STOC này như sau:

(0) Trước đó, bộ xác nhận thiết lập các chính sách xác minh ACBio cho mỗi phần tử dữ liệu của các Báo cáo thể hiện ACBio dựa trên các chính sách của các ứng dụng tương ứng (xem B.3 cho một ví dụ về chính sách xác minh ACBio).

(1) Đối tượng yêu cầu gửi yêu cầu xác minh sinh trắc học tới bộ xác nhận, thông qua hệ thống (thiết bị) của phía đối tượng yêu cầu.

(2) Hệ thống của phía bộ xác nhận gửi giá trị kiểm soát và danh sách ứng viên của thuật toán băm và thuật toán chữ ký số theo chính sách xác minh ACBio và yêu cầu thực thi xác minh sinh trắc học bao gồm sự tạo thành Báo cáo thể hiện ACBio vào hệ thống (thiết bị) của phía đối tượng yêu cầu.

(3) Hệ thống (thiết bị) của đối tượng yêu cầu đòi hỏi các thuật toán có sẵn cho các thiết bị sinh trắc học và thẻ STOC.

(4) Thiết bị sinh trắc học và thẻ STOC trả về các thuật toán có sẵn cho hệ thống (thiết bị) của phía đối tượng yêu cầu.

(5) Hệ thống (thiết bị) của phía đối tượng yêu cầu quyết định các thuật toán hàm băm và thuật toán chữ ký và gửi giá trị kiểm soát của bộ xác nhận, các thuật toán hàm băm và thuật toán chữ ký cho thiết bị sinh trắc học và yêu cầu thực thi việc thu thập dữ liệu, xử lý tín hiệu trung gian và xử lý tín hiệu cuối cùng cho thiết bị sinh trắc học.

(6) Thiết bị sinh trắc học thu thập thông tin sinh trắc học từ đối tượng yêu cầu và tạo ra mẫu sinh trắc học đã qua xử lý thông qua quá trình con thu thập dữ liệu, xử lý tín hiệu trung gian xử lý tín hiệu cuối cùng.

(7) Thiết bị sinh trắc học sẽ gửi thông báo chấm dứt xử lý tín hiệu cuối cùng cho hệ thống (thiết bị) của phía đối tượng yêu cầu.

(8) Hệ thống (thiết bị) của phía đối tượng yêu cầu gửi các giá trị kiểm soát của bộ xác nhận, các thuật toán hàm băm và thuật toán chữ ký đã chọn ở bước (5) và Chỉ số IO BPU cho dữ liệu đầu ra (khuôn mẫu tham chiếu sinh trắc học đã qua xử lý) của thẻ STOC, vào thẻ STOC. Và hệ thống (thiết bị) của phía đối tượng yêu cầu cũng có thể yêu cầu sự tạo thành của một Báo cáo thể hiện ACBio và truyền tải khuôn mẫu tham chiếu sinh trắc học đã qua xử lý và các Báo cáo thể hiện ACBio, tới thẻ STOC.

(9) Thẻ STOC tạo ra một Báo cáo thể hiện ACBio. Xem B.1.1.4 để biết chi tiết.

(10) Thẻ STOC gửi khuôn mẫu tham chiếu sinh trắc học đã qua xử lý và Báo cáo thể hiện ACBio cho hệ thống (thiết bị) của phía đối tượng yêu cầu.

(11) Hệ thống (thiết bị) của phía đối tượng yêu cầu gửi khuôn mẫu tham chiếu sinh trắc học đã qua xử lý nhận được từ thẻ STOC, chỉ số IO BPU được gán cho khuôn mẫu tham chiếu sinh trắc học đã qua xử lý và chỉ số IO BPU được gán cho quyết định so sánh của thiết bị sinh trắc học, cho thiết bị sinh trắc học. Và hệ thống (thiết bị) của phía đối tượng yêu cầu cũng yêu cầu thực thi các quá trình con so sánh và quyết định cho thiết bị sinh trắc học.

(12) Thiết bị sinh trắc học tiếp nhận khuôn mẫu tham chiếu sinh trắc học đã qua xử lý và thực thi các quá trình con so sánh và quyết định. Thiết bị sinh trắc học cũng tạo ra một Báo cáo thể hiện ACBio bởi các thủ tục tiếp theo;

a) Khôi phục lại khối thông tin BPU và đặt nó vào **bpuInformation** của **ACBioContentInformation**.

b) Thiết lập giá trị kiểm soát của bộ xác nhận cho **controlValue** của **ACBioContentInformation**.

c) Tạo khối quá trình sinh trắc học như sau:

c-1) Thiết lập các chỉ số quá trình con cho **subprocessIndexList**. Các chỉ số quá trình con được chỉ định bởi các nhà cung cấp sản phẩm của thiết bị sinh trắc học cho mỗi quá trình con tương ứng với chức năng thu thập dữ liệu, xử lý tín hiệu trung gian, xử lý tín hiệu cuối cùng, so sánh và quyết định.

c-2) Để tạo trường **bpuInputExecutionInformationList**, nên thực hiện những việc sau đây. Đặt giá trị **processed-data** và giá trị **reference** tương ứng với **processedLevel** và **purpose** của **datatype**. Thiết lập chỉ số IO BPU, gán cho đầu vào của thiết bị sinh trắc học, cho **bpuIOIndex**. Thiết lập chỉ số IO quá trình con của các dữ liệu đầu vào (khuôn mẫu tham chiếu sinh trắc học đã qua xử lý) cho quá trình con so sánh, được chỉ định bởi nhà cung cấp sản phẩm của thiết bị sinh trắc học, cho **subprocessIOIndex**. Thiết lập cặp giá trị hàm băm của khuôn mẫu tham chiếu sinh trắc học đã qua xử lý nhận được và các thuật toán hàm băm cho **hash**.

c-3) Để tạo trường **bpuOutputExecutionInformationList**, nên thực hiện việc sau đây. Thiết lập giá trị **comparison-decision** cho **processedLevel** của **dataType**. Thiết lập các chỉ số IO BPU, gán cho dữ liệu đầu ra của thiết bị sinh trắc học, cho **bpuIOIndex**. Thiết lập chỉ số IO quá trình con của dữ liệu đầu ra (quyết định so sánh) của quá trình con ra quyết định, được chỉ định bởi nhà cung cấp sản phẩm của thiết bị sinh trắc học, cho **subprocessIOIndex**. Thiết lập cặp giá trị hàm băm của quyết định so sánh và các thuật toán hàm băm cho **hash**.

d) Tạo **SignedDataACBio** của dữ liệu trong đó bao gồm các dữ liệu được tạo ra bởi a), b) và c), bằng cách sử dụng thuật toán chữ ký số được chọn trong (5). Nếu chứng nhận BPU được đặt trong **certificates** của **SignedDataACBio**, thông tin tham chiếu chứng nhận BPU trong khối thông tin BPU có thể bị bỏ qua.

(13) Thiết bị sinh trắc học sẽ gửi dữ liệu đầu ra của quá trình con ra quyết định và Báo cáo thể hiện ACBio cho hệ thống (thiết bị) của phía đối tượng yêu cầu.

(14) Hệ thống (thiết bị) của phía đối tượng yêu cầu gửi quyết định so sánh (dữ liệu đầu ra của quá trình con ra quyết định) và hai Báo cáo thể hiện ACBio cho hệ thống của phía bộ xác nhận.

(15) Hệ thống của phía bộ xác nhận tiếp nhận quyết định so sánh và hai Báo cáo thể hiện ACBio. Bộ xác nhận xác nhận các kết quả với các thủ tục tiếp theo;

a) Xác minh tính toàn vẹn của mỗi Báo cáo thể hiện ACBio bằng việc xác minh chữ ký.

b) Xác minh sự tương ứng của giá trị kiểm soát ban đầu được đưa ra bởi bộ xác nhận và giá trị kiểm soát của mỗi Báo cáo thể hiện ACBio.

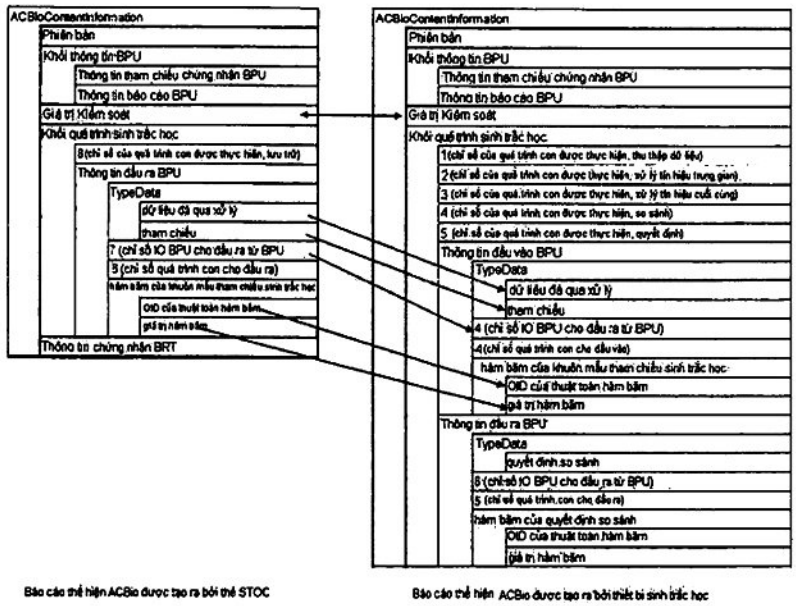
c) Xác minh rằng các mức độ an toàn của hai BPU và mức độ hiệu suất chức năng của mỗi quá trình con được thực thi trong hai BPU đáp ứng được các chính sách xác minh ACBio của bộ xác nhận (xem B.3 cho ví dụ về chính sách xác minh ACBio). Các thông tin về mức độ an toàn của hai BPU và mức độ hiệu suất chức năng của mỗi quá trình con được thực hiện trong hai BPU là nằm trong báo cáo BPU được lưu trữ trong hoặc tham chiếu từ khối thông tin BPU của mỗi Báo cáo thể hiện ACBio.

d) Xác minh tính hợp lệ của khuôn mẫu tham chiếu sinh trắc học được sử dụng. Các thông tin về khuôn mẫu tham chiếu sinh trắc học, chẳng hạn như tổ chức phát hành, thời hạn hiệu lực..., là nằm trong chứng nhận BRT, được lưu trữ trong hoặc tham chiếu từ thông tin chứng nhận BRT của Báo cáo thể hiện ACBio được tạo ra bởi thẻ STOC.

e) Xác minh rằng toàn bộ quá trình xác minh sinh trắc học được thực thi ở phía đối tượng yêu cầu bằng cách kiểm tra các quá trình con được thực thi. Chỉ số quá trình con tương ứng với các quá trình con thực thi được được lưu trữ trong **subprocessIndexList** của khối quá trình sinh trắc học của hai Báo cáo thể hiện ACBio và thực thi các chức năng tương ứng với các chỉ số quá trình con có thể được xác định từ **subprocessName** của **functionDefinition** của hai báo cáo BPU.

f) Xác minh sự phù hợp của các dữ liệu đầu vào và dữ liệu đầu ra truyền tải giữa các BPU bằng cách so sánh nội dung của **dataType**, **bpuIOIndex** và **hashValue** của **bpuOutputExecutionInformationList** trong khối quá trình sinh trắc học của Báo cáo thể hiện ACBio được tạo ra bởi thẻ STOC và nội dung của **bpuIOIndex**, **dataType** và **hashValue** của **bpuInputExecutionInformationList** trong khối quá trình sinh trắc học của Báo cáo thể hiện ACBio được tạo ra bởi thiết bị sinh trắc học.

Hình B.7 minh họa quá trình xác minh trên của quá trình xác minh sinh trắc học sử dụng Báo cáo thể hiện ACBio. Trong Hình B.7, các chỉ số được đưa ra là trong Hình B.1.



Hình B.7 – Sự xác nhận của xác minh sinh trắc học sử dụng ACBio

B.1.2 Ví dụ về sự thực hiện cho mô hình OCM

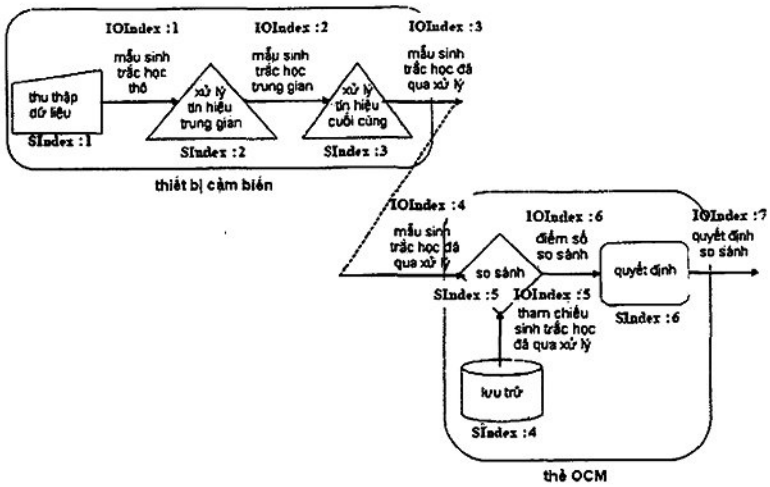
Trong ví dụ này, chúng ta giả định rằng mô hình OCM này của quá trình xác minh sinh trắc học bao gồm hai BPU, một là thiết bị cảm biến có chức năng thu thập dữ liệu, xử lý tín hiệu trung gian và xử lý tín hiệu cuối cùng và BPU còn lại là thẻ OCM có các chức năng lưu trữ, so sánh và quyết định. Ví dụ này chủ yếu tập trung vào thẻ OCM.

B.1.2.1 Quá trình đánh giá

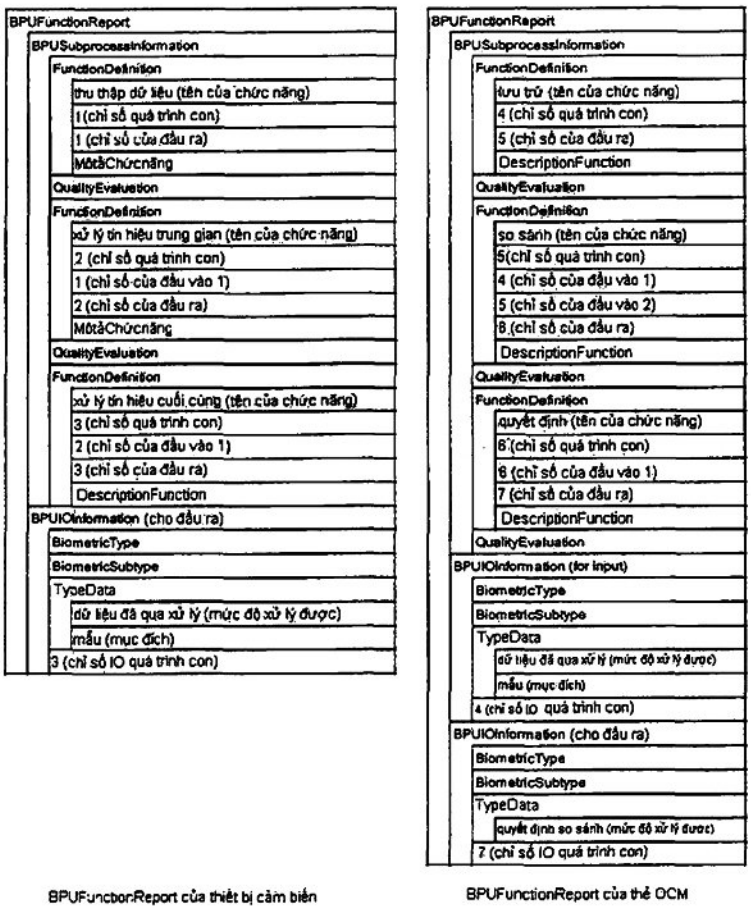
Sản phẩm của BPU, tức là thẻ OCM và các thiết bị cảm biến được sử dụng trong quá trình xác minh sinh trắc học, nên được đánh giá tại một tổ chức đánh giá nhất định và ban hành báo cáo BPU của chúng.

B.1.2.2 Quá trình chế tạo

Các nhà cung cấp BPU nên chỉ số mỗi quá trình con và luồng phù hợp với các quy định trong 7.2.1. Nếu quá trình con và luồng trong thiết bị cảm biến và trong thẻ OCM được lập chỉ số như trong Hình B.8, thì các BPUFunctionReport của thiết bị sinh trắc học và của thẻ OCM được thể hiện trong Hình B.9. Trong Hình B.8, SIndex có nghĩa là chỉ số quá trình con và IOIndex có nghĩa là chỉ số IO quá trình con.

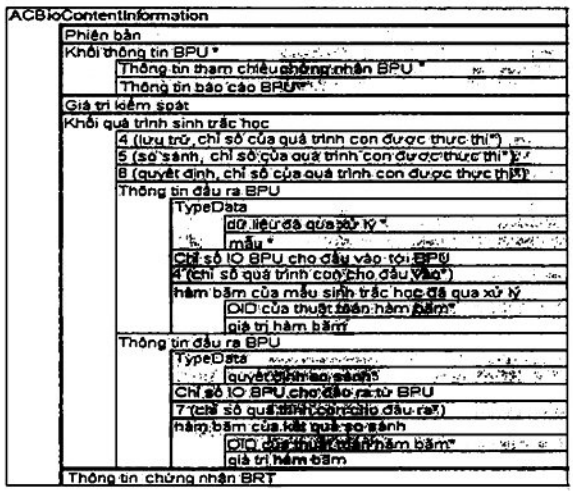


Hình B.8 – Quá trình xác minh sinh trắc học của mô hình OCM và ví dụ về chỉ số



Hình B.9 – Các ví dụ về BPUFunctionReport cho mô hình OCM

Trong trường hợp này, khối dữ liệu kiểu **ACBioContentInformation** nên được lưu trữ trong thẻ OCM trước như trong Hình B.10. Trong Hình B.10, các phần tử dữ liệu được đánh dấu * (nền đậm) là dữ liệu cố định và các thiết lập trong khu vực của thẻ OCM trước không được đánh dấu * (không có nền) đều được để trống để được thực hiện trong quá trình thu nạp và thực hiện sau này.



Hình B.10 – Khối dữ liệu được lưu trữ trong thẻ OCM trên quá trình chế tạo

Trong Hình B.10, các trường không được đánh dấu * (không có nền), ngoại trừ thông tin chứng nhận BRT đã cố định độ dài của riêng trường. Độ dài của trường Thông tin chứng nhận BRT không được xác định vào quá trình chế tạo nhưng được xác định trong quá trình thu nạp. Cần lưu ý rằng khu vực **ACBioContentInformation** nên có khu vực liên tiếp đầy đủ cho thông tin chứng nhận BRT.

Bảng dưới đây là định dạng BER-TLV của **ACBioContentInformation** cho thẻ OCM, tương đương với cấu trúc dữ liệu của Hình B.10.

Bảng B.2 – Định dạng BER-TLV của ACBioContentInformation cho thẻ OCM

Tag	L	Giá trị								
'AE'	Var.	ACBioContentInformation								
		Tag	L	Giá trị						
		'02'	1	Phiên bản						
		'A0'	Var.	Khối thông tin BPU						
				Tag	L	Giá trị				
				'A0'	Var.	Thông tin tham chiếu chứng nhận BPU				
				'A1'	Var.	Thông tin báo cáo BPU				
		'04'	16	Giá trị Kiểm soát						
		'A2'	Var.	Khối quá trình sinh trắc học						
				Tag	L	Giá trị				
				'02'	1	chỉ số của quá trình con 1 được thực thi				
				'02'	1	chỉ số của quá trình con 2 được thực thi				
				'02'	1	chỉ số của quá trình con 3 được thực thi				
				'A0'	Var.	Thông tin đầu vào				
						Tag	L	Giá trị		
						'A0'	6	Kiểu Dữ liệu		
								Tag	L	Giá trị
								'0A'	1	dữ liệu đã qua xử lý
								'0A'	1	mẫu
						'02'	1	Chỉ số IO BPU cho đầu vào tới BPU		
						'02'	1	IO quá trình con		
						'A1'	Var.	Thông tin hàm băm của đầu vào		
								'06'	Var.	OID của thuật toán hàm băm
								'04'	Var.	Giá trị hàm băm của đầu vào
				'A1'	Var.	Thông tin đầu ra				
						Tag	L	Giá trị		
						'A0'	6	Kiểu Dữ liệu		
								Tag	L	Giá trị
								'0A'	1	quyết định so sánh
						'02'	1	chỉ số IO BPU cho đầu ra từ BPU		
						'02'	1	chỉ số quá trình con cho đầu ra		
						'A1'	Var.	Thông tin hàm băm của đầu ra		
								'06'	Var.	OID của thuật toán hàm băm
								'04'	Var.	Giá trị hàm băm của đầu ra
		'A3'	Var.	Thông tin chứng nhận BRT						

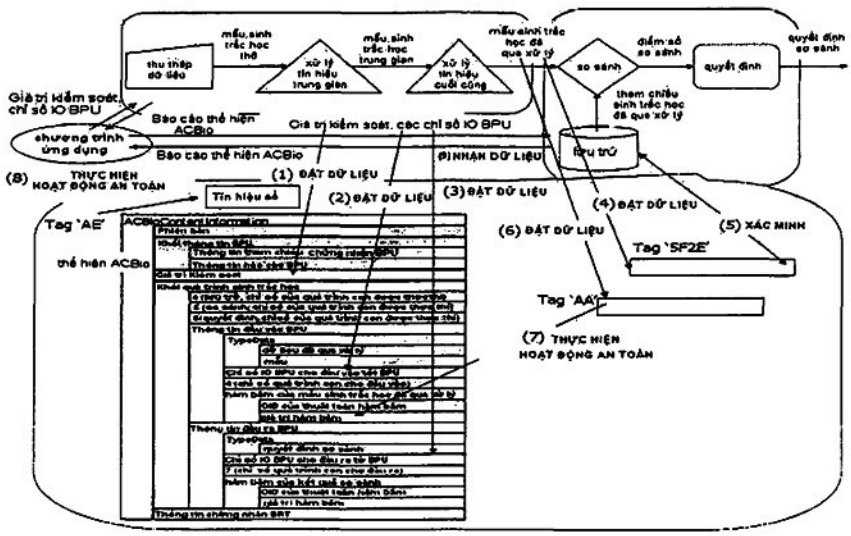
B.1.2.3 Quá trình thu nạp

Khuôn mẫu tham chiếu sinh trắc học được lưu trữ vào thẻ OCM trong quá trình này. Một chứng nhận BRT được cấp cho khuôn mẫu tham chiếu sinh trắc học và chứng nhận BRT hoặc tham chiếu tới chứng nhận được lưu trữ trong **brtCertificateInformation** của **ACBioContentInformation**. Độ dài của trường kiểu **ACBioContentInformation** phải được điều chỉnh bằng cách tăng thêm độ dài của thông tin chứng nhận BRT cộng với độ dài của trường Tag và trường Length.

B.1.2.4 Quá trình thực thi

Dựa vào sự thực hiện của xác minh sinh trắc học, ba yếu tố đầu vào được cung cấp cho thẻ OCM ngoài các mẫu sinh trắc học đã qua xử lý; đầu tiên là giá trị kiểm soát từ bộ xác nhận, thứ hai là chỉ số IO BPU đến đầu vào của mẫu sinh trắc học đã qua xử lý từ thiết bị cảm biến, thứ ba là các chỉ số IO BPU cho đầu ra từ thẻ OCM. Thẻ OCM nên thiết lập "Giá trị Kiểm soát" đầu tiên ((1) ĐẶT DỮ LIỆU trong Hình B.11), thứ hai đến "chỉ số IO BPU cho đầu vào từ BPU" ((2) ĐẶT DỮ LIỆU trong Hình B.11) và thứ ba với "chỉ số IO BPU cho đầu ra từ BPU" ((3) ĐẶT DỮ LIỆU trong Hình B.11), tương ứng.

Sau đó thẻ OCM có được mẫu sinh trắc học đã qua xử lý như đầu vào, lưu trữ mẫu trong khu vực trên thẻ OCM ((4) ĐẶT DỮ LIỆU trong Hình B.11), so sánh mẫu với khuôn mẫu tham chiếu sinh trắc học đã qua xử lý được lưu trữ và đưa ra quyết định so sánh ((5) XÁC MINH trong Hình B.11). Giá trị hàm băm của lưu trữ mẫu sinh trắc học đã qua xử lý được tính toán và sẽ được thiết lập trong "hàm băm của mẫu sinh trắc học đã qua xử lý" ((7) THỰC HIỆN HOẠT ĐỘNG AN TOÀN trong Hình B.11). Việc so sánh cũng được tính toán giá trị hàm băm của nó mà thiết lập "hàm băm của quyết định so sánh". Thẻ OCM ký số toàn bộ trường kiểu **ACBioContentInformation** ((8) THỰC HIỆN HOẠT ĐỘNG AN TOÀN trong Hình B.11) để có được Báo cáo thể hiện ACBio và gửi nó như đầu ra.



Hình B.11 – Sự tạo thành Báo cáo thể hiện ACBio trên thẻ OCM dựa vào sự thực hiện xác minh sinh trắc học

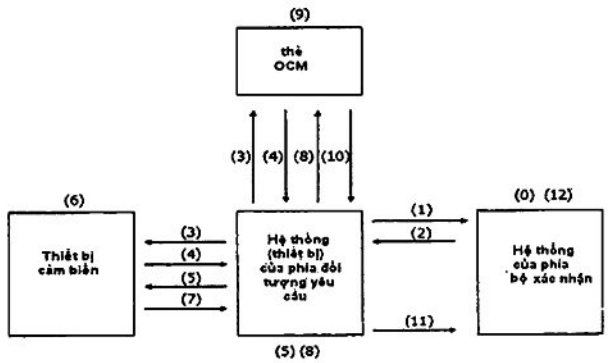
Hình B.12 mô tả một chuỗi lệnh cho sự tạo thành Báo cáo thể hiện ACBio trên thẻ OCM. Như trong Hình B.12, cần thiết để đưa các mẫu sinh trắc học đã qua xử lý hai lần (lệnh thứ tư và lệnh thứ sáu) vào thẻ OCM nếu chỉ lệnh phù hợp tiêu chuẩn ISO/IEC 7816-4 được thực hiện trên thẻ. Sẽ tốt hơn khi thiết lập mẫu một lần nhằm xác nhận và tính giá trị hàm băm của nó. Trong Hình B.12, BIT là từ viết tắt cho Khuôn mẫu thông tin sinh trắc học, một thuật ngữ được sử dụng trong chuỗi tiêu chuẩn ISO/IEC 7816.

Câu lệnh/Phản ứng	Ý nghĩa
PUT DATA <Control Value> OK	Đặt giá trị kiểm soát như tham số đầu vào
PUT DATA <Global Index Input> OK	Đặt chỉ số toàn cầu cho đầu vào và đầu ra của thẻ OCM như các tham số đầu vào
PUT DATA <Global Index Output> OK	Đặt chỉ số toàn cầu cho đầu vào và đầu ra của thẻ OCM như các tham số đầu vào
PUT DATA <Processed Biometric Sample> OK	Đặt mẫu sinh trắc học đã qua xử lý như tham số đầu vào
VERIFY OK	Xác minh sinh trắc học so sánh mẫu sinh trắc học đã qua xử lý và tham chiếu sinh trắc học đã qua xử lý được lưu trữ, cả hai dữ liệu nội bộ (Xem 7816-4)
PUT DATA <Processed Biometric Sample> OK	Đặt mẫu sinh trắc học đã qua xử lý như tham số đầu vào
PERFORM SECURITY OPERATION <'90', 'A0'> OK	Tính giá trị hàm băm của mẫu sinh trắc học đã qua xử lý
PERFORM SECURITY OPERATION <'AE', 'BC'> OK	Tính chữ ký số cho ACBioContentInformation và đưa nó vào trường chữ ký số của SignedData
GET DATA BIT	Nhận Báo cáo thể hiện ACBio như đầu ra

Hình B.12 – Chuỗi câu lệnh cho sự tạo thành Báo cáo thể hiện ACBio trên thẻ OCM

B.1.2.5 Ví dụ về giao thức

Chúng ta giả định sự tồn tại hệ thống của phía bộ xác nhận và một hệ thống (thiết bị) của phía đối tượng yêu cầu mà chỉ có chức năng truyền/nhận thông điệp đi/đến ba đối tượng kia, như Hình B.13.



Hình B.13 – Ví dụ về giao thức cho mô hình OCM

Ví dụ về giao thức cho mô hình OCM này như sau:

Với thiết bị cảm biến ở vị trí của các thiết bị sinh trắc học và thẻ OCM thay cho thẻ STOC, thực hiện bước (0) đến (4) với cùng một cách như trong giao thức được mô tả trong B.1.1.5.

(5) Hệ thống (thiết bị) của phía đối tượng yêu cầu quyết định các thuật toán hàm băm và thuật toán chữ ký và gửi các giá trị kiểm soát của bộ xác nhận, các thuật toán hàm băm, thuật toán chữ ký và chỉ số IO BPU cho dữ liệu đầu ra (mẫu được xử lý sinh trắc học) của thiết bị cảm biến, cho thiết bị cảm biến. Và hệ thống (thiết bị) của phía đối tượng yêu cầu cũng yêu cầu sự thực hiện thu thập dữ liệu, xử lý tín hiệu trung gian và xử lý tín hiệu cuối cùng và tạo thành một Báo cáo thể hiện ACBio cho các thiết bị cảm biến.

(6) Các thiết bị cảm biến sẽ thu thập thông tin sinh trắc học từ đối tượng yêu cầu và tạo ra mẫu sinh trắc học đã qua xử lý thông qua quá trình con thu thập dữ liệu, xử lý tín hiệu trung gian và xử lý tín hiệu cuối cùng. Các thiết bị cảm biến tạo ra một Báo cáo thể hiện ACBio bằng các thủ tục tiếp theo;

a) Khôi phục lại khối thông tin BPU và thiết lập nó cho **bpuInformation** của **ACBioContentInformation**.

b) Thiết lập giá trị kiểm soát của bộ xác nhận cho **controlValue** của **ACBioContentInformation**.

c) Tạo khối quá trình sinh trắc học như sau:

c-1) Thiết lập các chỉ số quá trình con cho **subprocessIndexList**. Các chỉ số quá trình con được chỉ định bởi các nhà cung cấp sản phẩm của thiết bị sinh trắc học cho mỗi quá trình con tương ứng với chức năng thu thập dữ liệu, xử lý tín hiệu trung gian, xử lý tín hiệu cuối cùng.

c-2) Để tạo ra trường **bpuOutputExecutionInformationList**, nên thực hiện như sau. Thiết lập giá trị ***processed-data*** *và giá trị* ***sample*** *tương ứng với* ***processedLevel*** *và* ***purpose*** *của* **dataType**. Thiết lập các chỉ số IO BPU, gán cho dữ liệu đầu ra của thiết bị cảm biến, cho **bpuIOIndex**. Thiết lập chỉ số IO quá trình con của các dữ liệu đầu ra từ quá trình con xử lý tín hiệu cuối cùng, được chỉ định bởi nhà cung cấp thiết bị cảm biến, cho **subprocessIOIndex**. Thiết lập các cặp giá trị hàm băm của mẫu sinh trắc học đã qua xử lý được tạo ra trong các thiết bị cảm biến và thuật toán hàm băm cho **hash**.

d) Tạo **SignedDataACBio** của dữ liệu trong đó bao gồm các dữ liệu được tạo ra bởi a), b) và c), bằng cách sử dụng thuật toán chữ ký số được chọn trong (5). Nếu chứng nhận BPU được thiết lập trong **certificates** của **SignedDataACBio**, thông tin tham chiếu chứng nhận BPU trong khối thông tin BPU có thể được bỏ qua.

(7) Các thiết bị cảm biến sẽ gửi mẫu sinh trắc học đã qua xử lý và Báo cáo thể hiện ACBio cho hệ thống (thiết bị) của phía đối tượng yêu cầu.

(8) Hệ thống (thiết bị) của phía đối tượng yêu cầu gửi mẫu sinh trắc học đã qua xử lý nhận được từ các thiết bị cảm biến, giá trị kiểm soát của bộ xác nhận, các thuật toán hàm băm và thuật toán chữ ký được chọn trong (5), chỉ số IO BPU gán cho các mẫu sinh trắc học đã qua xử lý và chỉ số IO BPU được gán

cho quyết định so sánh của thẻ OCM, cho thẻ OCM. Và, hệ thống (thiết bị) của phía đối tượng yêu cầu cũng yêu cầu việc thực hiện quá trình con lưu trữ, so sánh và quyết định cho thẻ OCM.

(9) Thẻ OCM tiếp nhận mẫu sinh trắc học đã qua xử lý và thực hiện quá trình con lưu trữ, so sánh và quyết định. Thẻ OCM cũng tạo ra các Báo cáo thể hiện ACBio. Xem B.1.2.4 cho các chi tiết.

(10) Thẻ OCM sẽ gửi dữ liệu đầu ra của quá trình con quyết định và Báo cáo thể hiện ACBio cho hệ thống (thiết bị) của phía đối tượng yêu cầu.

(11) Hệ thống (thiết bị) của phía đối tượng yêu cầu gửi quyết định so sánh (dữ liệu đầu ra của quá trình con quyết định) và hai Báo cáo thể hiện ACBio cho hệ thống của phía bộ xác nhận.

(12) Hệ thống của phía bộ xác nhận tiếp nhận quyết định so sánh và hai Báo cáo thể hiện ACBio. Bộ xác nhận xác nhận các kết quả bằng các thủ tục tiếp theo;

a) Xác nhận tính toàn vẹn của mỗi Báo cáo thể hiện ACBio bằng việc xác minh chữ ký.

b) Xác nhận sự tương ứng giá trị kiểm soát ban đầu được đưa ra bởi bộ xác nhận và giá trị kiểm soát của mỗi Báo cáo thể hiện ACBio.

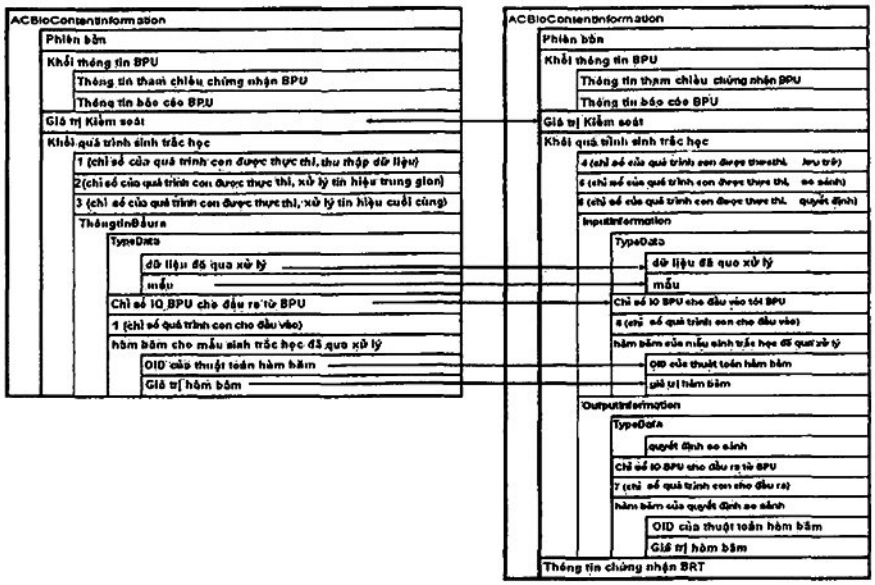
c) Xác nhận mức độ an toàn của hai BPU và mức độ hiệu suất chức năng của mỗi quá trình con thực hiện trong hai BPUs đáp ứng các chính sách xác minh ACBio của bộ xác nhận (xem B.3 cho ví dụ về chính sách xác minh ACBio). Các thông tin về mức độ an toàn của hai BPU và mức độ hiệu suất chức năng của mỗi quá trình con thực hiện trong hai BPU là nằm trong báo cáo BPU được lưu trữ trong hoặc được tham chiếu từ khối thông tin BPU của mỗi Báo cáo thể hiện ACBio.

d) Xác nhận tính hợp lệ của khuôn mẫu tham chiếu sinh trắc học được sử dụng. Các thông tin về khuôn mẫu tham chiếu sinh trắc học, chẳng hạn như tổ chức phát hành, thời hạn hiệu lực..., là nằm trong chứng nhận BRT, được lưu trữ trong hoặc được tham chiếu từ thông tin chứng nhận BRT của Báo cáo thể hiện ACBio được tạo ra bởi các thẻ OCM.

e) Xác nhận toàn bộ quá trình xác minh sinh trắc học thực hiện ở phía đối tượng yêu cầu bằng cách kiểm tra các quá trình con được thực hiện. Chỉ số quá trình con tương ứng với quá trình con được thực hiện được lưu trữ trong **subprocessIndexList** trong khối quá trình sinh trắc học của hai Báo cáo thể hiện ACBio và các chức năng được thực hiện tương ứng với các chỉ số quá trình con có thể được xác định từ **subprocessName** của **functionDefinition** của hai báo cáo BPU.

f) Xác nhận sự phù hợp của dữ liệu đầu vào và dữ liệu đầu ra được truyền tải giữa các BPU bằng cách so sánh nội dung của **dataType**, **bpuIOIndex** và **hashValue** của **bpuOutputExecutionInformationList** trong khối quá trình sinh trắc học của Báo cáo thể hiện ACBio được tạo ra bởi các thiết bị cảm biến và các nội dung của **bpuIOIndex**, **dataType** và **hashValue** của **bpuInputExecutionInformationList** trong khối quá trình sinh trắc học của Báo cáo thể hiện ACBio được tạo ra bởi thẻ OCM.

Hình B.14 minh họa quá trình xác nhận trên của quá trình xác minh sinh trắc học sử dụng Báo cáo thể hiện ACBio. Trong Hình B.14, các chỉ số được đưa ra như trong Hình B.8.

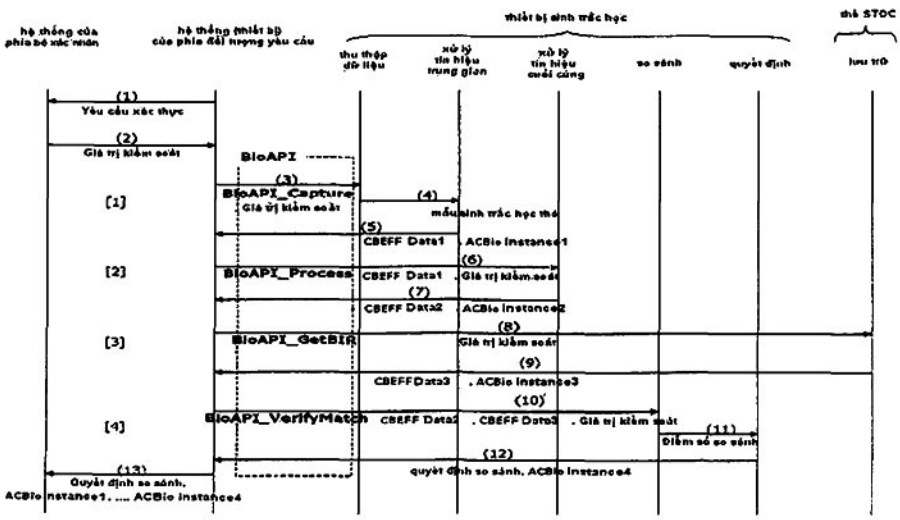


Hình B.14 – Xác nhận của xác minh sinh trắc học sử dụng ACBio

B.2 Mối quan hệ giữa BioAPI, CBEFF và ACBio

Trong Phụ lục này, mối quan hệ giữa các CBEFF, BioAPI và ACBio được hiển thị bằng cách sử dụng một ví dụ về một mô hình STOC, mặc dù việc sử dụng các CBEFF và BioAPI không phải là bắt buộc đối với tiêu chuẩn này.

Chúng ta giả định rằng đây là mô hình STOC như mô tả trong B.1.1. Hình B.15 minh họa mối quan hệ giữa BioAPI, CBEFF và ACBio. Trong hình này, các API như BioAPI_Init, BioAPI_BSPLoad, BioAPI_BSPAttach... được bỏ qua.



Hình B.15 - Mối quan hệ giữa BioAPI, CBEFF và ACBio

Mô hình này là thành phần tương tự với mô hình được định nghĩa tại B.1.1. Nhưng giao thức hơi khác do việc sử dụng các chức năng BioAPI, hiện đang được mở rộng để áp dụng cho ACBio.

[1] Để có được mẫu sinh trắc học trung gian của đối tượng yêu cầu, chương trình ứng dụng gọi BioAPI_Capture và được CBEFF Data1 của mẫu sinh trắc học trung gian từ quá trình con xử lý trung gian cùng với ACBio instance1 như kết quả trả lại.

[2] Tiếp theo chương trình ứng dụng gọi BioAPI_Process với đầu vào của CBEFF Data1 và được CBEFF Data2 của mẫu sinh trắc học trung gian từ quá trình con xử lý tín hiệu với ACBio instance2 như kết quả trả lại.

[3] BioAPI_GetBIR được gọi để có được khuôn mẫu tham chiếu sinh trắc học đã qua xử lý từ quá trình con lưu trữ. CBEFF Data3 của khuôn mẫu tham chiếu sinh trắc học đã qua xử lý được trả về với ACBio instance3.

[4] Các chương trình ứng dụng gọi BioAPI_VerifyMatch với CBEFF Data2 và CBEFF Data3 như đầu vào và được quyết định so sánh là sự trả về với ACBio instance4.

B.3 Chính sách xác minh ACBio

Nhìn chung, chính sách xác minh ACBio phụ thuộc vào chính sách ứng dụng mà sử dụng kết quả xác minh sinh trắc học.

Các mục sau đây là ví dụ về các yếu tố chính sách xác minh ACBio:

- các thuật toán hàm băm có thể chấp nhận của các BPU
- các thuật toán chữ ký số có thể chấp nhận của các BPU
- mức độ an toàn có thể chấp nhận của các BPU
- mức độ hiệu suất chức năng (chất lượng) có thể chấp nhận của mỗi chức năng được thực hiện trong các BPU
    - chất lượng thu thập dữ liệu (chất lượng của các mẫu sinh trắc học thô có được)
    - chất lượng so sánh (độ chính xác;...)
- khuôn mẫu tham chiếu sinh trắc học có thể chấp nhận
    - tính hiệu lực của chứng nhận BRT
    - chất lượng của khuôn mẫu tham chiếu sinh trắc học
- kết quả quá trình xác minh sinh trắc học có thể chấp nhận
    - điểm số so sánh có thể được chấp nhận

B.4 Mức độ an toàn và mức độ hiệu suất chức năng của BPU

Trong khung ACBio, bộ xác nhận kiểm tra rằng liệu kết quả của quá trình xác minh sinh trắc học có đáng tin cậy hay không dựa vào mức độ an toàn của các BPU được sử dụng và mức độ hiệu suất chức năng của các chức năng được thực hiện trong các BPU.

Báo cáo thể hiện ACBio được tạo ra bởi các BPU được thực hiện bao gồm các thông tin về báo cáo BPU tương ứng trong đó bao gồm các báo cáo chức năng BPU và báo cáo an toàn BPU. **qualityEvaluation** của báo cáo chức năng BPU chứa mức độ hiệu suất chức năng của các chức năng được thực hiện trong BPU. Và **cryptoModuleSecurity**, **biometricProcessSecurity** và **securityEvaluationExtension** của báo cáo an toàn BPU bao gồm các mức độ an toàn của BPU.

Dựa vào cả hai mức độ hiệu suất chức năng và mức độ an toàn, một trong hai cơ chế đánh giá hoặc định dạng tiêu chuẩn của bộ máy có thể đọc được báo cáo đánh giá không được định nghĩa lúc này. Vì vậy chỉ có các trường cho kết quả đánh giá được chuẩn bị trong tiêu chuẩn này.

Về đánh giá mức độ hiệu suất chức năng, các tiêu chuẩn sau đây là các hoạt động có liên quan trong ISO/IEC JTC 1/SC 37:

ISO/IEC 19795, Information technology - Biometric performance testing and reporting *(Công nghệ thông tin – Kiểm thử hiệu suất và báo cáo sinh trắc học)*

Về đánh giá mức độ an toàn, các tiêu chuẩn sau đây là các hoạt động có liên quan trong ISO/IEC JTC 1/SC 27:

ISO/IEC 19790, Information technology - Security techniques - Security requirements for cryptographic modules *(Công nghệ thông tin - Các kỹ thuật an toàn - Yêu cầu an toàn cho mô-đun mật mã)*

TCVN 11385:2016, Information technology - Security techniques - Security evaluation of biometrics *(Công nghệ thông tin - Các kỹ thuật an toàn - Đánh giá an toàn sinh trắc học)*

ISO/IEC 15408 (all parts), Information technology - Security techniques - Evaluation criteria for IT security *(Công nghệ thông tin - Các kỹ thuật an toàn - Tiêu chí đánh giá cho an toàn công nghệ thông tin)*

Thư mục tài liệu tham khảo

[1] ISO/IEC 7816-4:2005, Identification cards - Integrated circuit cards - Part 4: Organization, security and commands for interchange *(Thẻ nhận dạng - Thẻ tích hợp vi mạch - Phần 4: Tổ chức, an toàn và câu lệnh để trao đổi)*

[2] ISO/IEC 7816-8:2004, Identification cards - Integrated circuit cards - Part 8: Commands for security operations *(Thẻ nhận dạng - Thẻ tích hợp vi mạch - Phần 8: Câu lệnh để vận hành an toàn)*

[3] ISO/IEC 7816-11:2004, Identification cards - Integrated circuit cards - Part 11: Personal verification through biometric methods *(Thẻ nhận dạng - Thẻ tích hợp vi mạch - Phần 11: Xác minh cá nhân thông qua phương pháp sinh trắc học)*

[4] ISO/IEC 9834-8 | ITU-T Rec. X.667, Information technology - Open Systems Interconnection - Procedures for the operation of OSI Registration Authorities: Generation and registration of Universally Unique Identifiers (UUIDs) and their use as ASN.1 Object Identifier components *(Công nghệ thông tin - Kết nối các hệ thống mở - Thủ tục hoạt động của các cơ quan đăng ký OSI: Sự hình thành và đăng ký danh tính duy nhất phổ biến (các UUID) và sử dụng chúng như các thành phần nhận dạng đối tượng ASN.1)*

[5] ISO 19092, Financial Services - Biometrics - Security framework *(Dịch vụ tài chính - Sinh trắc học - Khung an toàn)*

[6] ISO/IEC 19784-1:2006, Information technology - Biometric application programming interface - Part 1: BioAPI specification *(Công nghệ thông tin - Giao diện chương trình ứng dụng sinh trắc học - Phần 1: Đặc điểm kỹ thuật BioAPI)*

[7] ISO/IEC 19790:2006, Information technology - Security techniques - Security requirements for cryptographic modules *(Công nghệ thông tin - Các kỹ thuật an toàn - Yêu cầu an toàn cho mô-đun mã hóa)*

[8] TCVN 11385:2016, Information technology - Security techniques - Security evaluation of biometrics *(Công nghệ thông tin - Các kỹ thuật an toàn - Đánh giá an toàn sinh trắc học)*

[9] ISO/IEC 19795-1, Information technology - Biometric performance testing and reporting - Part 1: Principles and framework *(Công nghệ thông tin - Kiểm thử hiệu suất chức năng và báo cáo - Phần 1: Nguyên tắc và khung)*

[10] ISO/IEC JTC1/SC 37 Standing Document 2 - Harmonized Biometric Vocabulary *(Từ vựng sinh trắc học hài hòa)*