Poszczególne kroki wymagane przez normę ISO 7816-11 celem weryfikacji tożsamości użytkownika

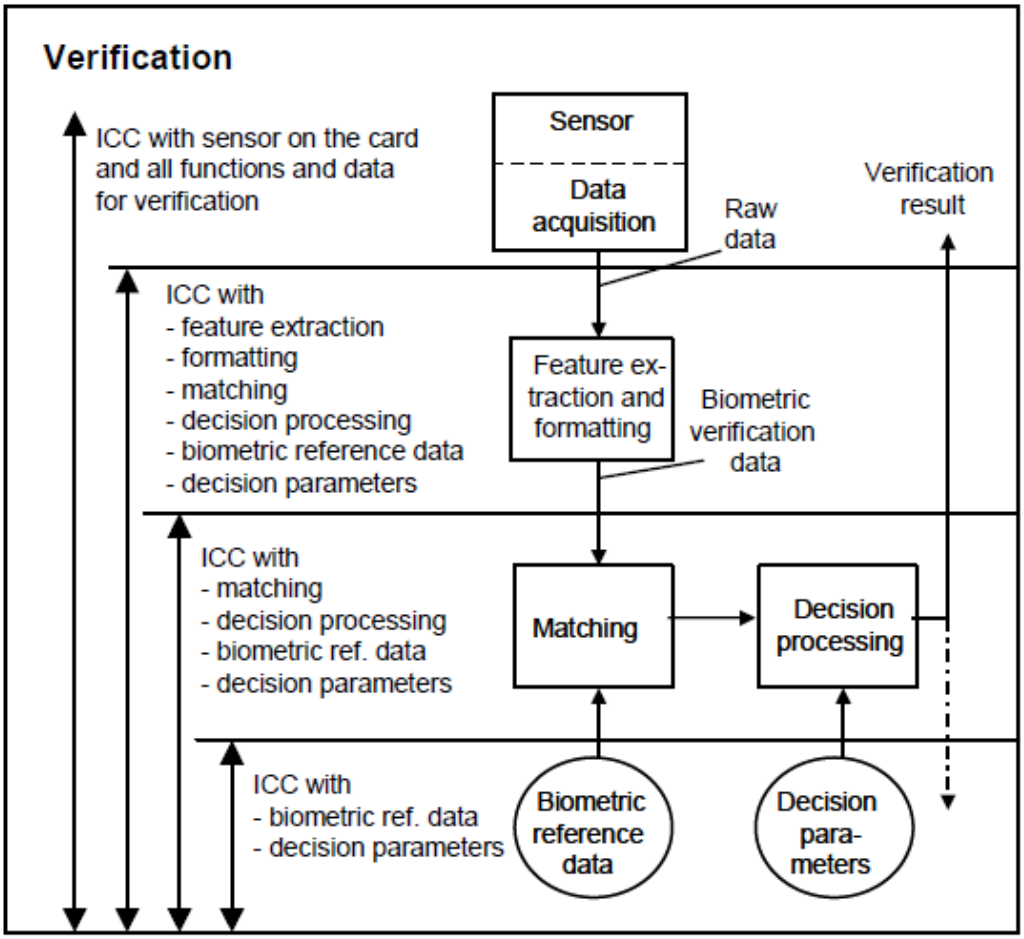
Klasyfikacja metod weryfikacji biometrycznej:

1. Statyczna: wymaga prezentacji cech fizjologicznych osoby autoryzowanej np.:
    a. Kształt ucha
    b. Cechy twarzy
    c. Geometria palca
    d. Odcisk palca
    e. Soczewka
    f. Itp.
2. Dynamiczna: wymaga wykonania pewnej akcji przez osobę autoryzowaną np.:
    a. Ruch ust
    b. Schemat głosowy
    c. Podpis
    d. itp.

Skróty:

- ICC Integrated Circuit(s) Card – układ scalony karty
- IFD Interface Device - Interfejs urządzenia (skanera)

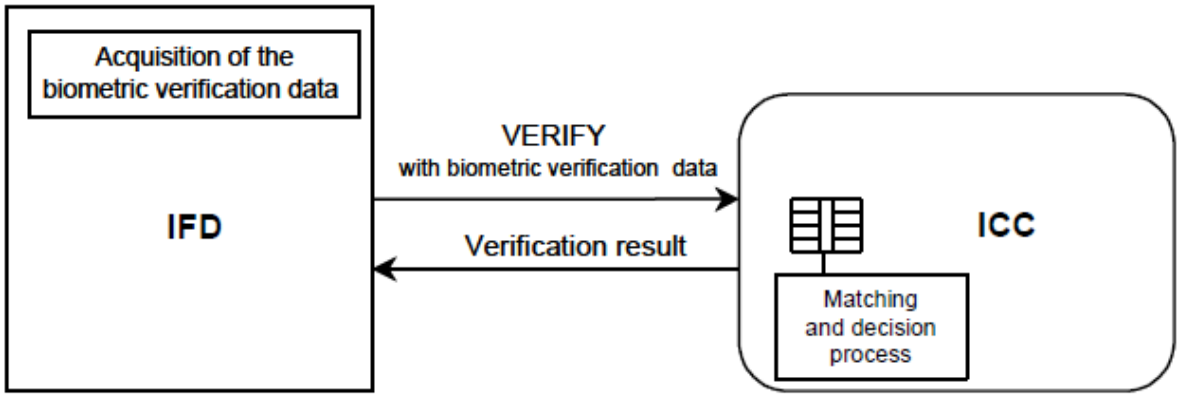
Ogólny proces weryfikacji



Rysunek 1Ogólny schemat procesu weryfikacji

Osoba przykłada kartę do czytnika. Oraz przystępuje do weryfikacji cech biometrycznych. Urządzenie skanujące (*sensor*) wraz z urządzeniem do akwizycji danych[1] (data acquisition) pobiera dane biometryczne od osoby uwierzytelnianej i przekazuje w przetworzonej formie do dalszego etapu weryfikacji. Dane (raw data) są zwykle przetwarzane poza kartą ze względu na znaczną wielkość surowych danych. Podczas tego procesu wyszczególniane i formatowane są cechy biometryczne osoby autoryzowanej do dalszego przetwarzania (porównywania).

[1] pierwszy etap przetwarzania danych polegający na ich przygotowaniu do dalszej obróbki czy interpretacji



Rysunek 2 Schemat komunikacji w statycznej weryfikacji

Kiedy dane biometryczne pobrane od osoby uwierzytelnianej są już gotowe oraz dane z karty zostały załadowane, następuje proces porównania (matching) i zwracany jest wynik. Czasem zdarza się, że karta odnotowuje informacje o (nie)powodzeniu procesu weryfikacji. Porównywanie (matching) odbywa się na karcie z której, odczytywane są wcześniej zapisane (np. w procesie personalizacji karty) dane biometryczne (biometric reference data) oraz parametry decyzyjne (decision parameteres).

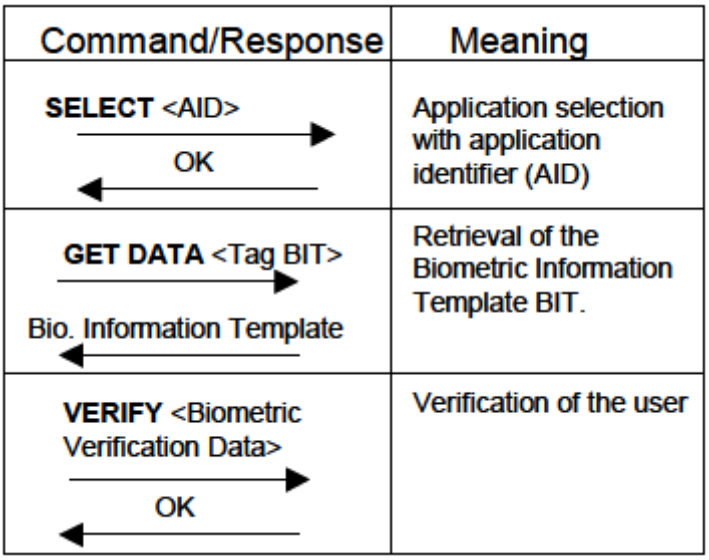
Wyszukiwanie informacji istotnych dla procesu weryfikacji biometrycznej

IFD może wymagać informacji dotyczących procesu weryfikacji. Poniższa lista zawiera elementy informacji, które mogą być wymagane przez IFD:

- Typ cech biometrycznych (np. odcisk palca, kształt dłoni)
- Podtyp cech biometrycznych (np. lewy palec wskazujący)
- Format danych
- Referencja algorytmu (id), jeśli użyty np. w komendzie MANAGE SECURITY ENVIRONMENT
- Identyfikator referencyjnych danych biometrycznych (biometric reference data identifier)
- dodatkowe dane uwierzytelniające, jeśli występują

Proces weryfikacji biometrycznej metodą statyczną:

Proces weryfikacji rozpoczyna się od pobierania szablonu danych biometrycznych (Biometric Information Template), np. przez zastosowanie polecenia GET DATA. Jeśli IFD obsługuje wymagany format wskazany w BIT, a użytkownik przedstawił dane biometryczne do weryfikacji, dane są przetwarzane i dostarczone do karty za pomocą polecenia VERIFY (patrz Rysunek 3).



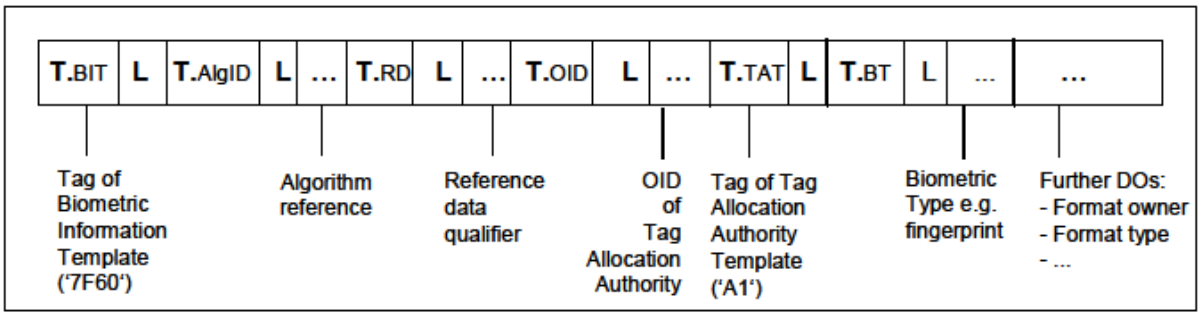
Rysunek 3 Przykład komunikacji bez dodatkowych zabezbieczeń (without secure messaging)

Jeśli BIT nie występuje, oznacza to, że osoba nie używa danych biometrycznych. Jeśli cechy biometryczne używane do weryfikacji są „publiczne" np. twarz, odcisk palca), należy stosować dodatkowe zabezpieczenia komunikacji (secure messaging) (patrz Rysunek 4).

W tym przykładzie, proces weryfikacji rozpoczyna się od uzyskania szablonu wymaganych informacji do weryfikacji (Verification Requirement Information Template - VIT) i odpowiadający im szablon informacji biometrycznych (BIT), który może być przechowywany np. pliku FCI (File Control Information); ID pliku jest niejawnie znane. VIT zawiera informacje, czy weryfikacja biometryczna i / lub weryfikacja hasłem hasło jest dostępna i włączona, czy wyłączona oraz które kwalifikatory danych referencyjnych (KeyRef) muszą być wykorzystane dla danego interfejsu karty. W tym przykładzie BIT zawiera informacje o algorytmie (AlgID), kwalifikatorze danych referencyjnych (KeyRef) oraz dodatkowe informacje, takie jak np. rodzaj i typ danych biometrycznych. (patrz Rysunek 5).

Command/Response	Meaning
SELECT <AID> → OK ←	Selection of the application with Application Identier (AID)
GET DATA <Tag BIT> → Bio. Information Template ←	Retrieval of the Biometric Information Template (BIT).
MANAGE SE <DO Key Ref> → OK ←	Setting the CRT DST with the public key for certificate verification
VERIFY CERTIFICATE <certificate> → OK ←	Verification of the certificate belonging to the biometric unit
GET CHALLENGE → Random Number ←	Requesting a challenge to be used for secure messaging
EXTERNAL AUTHENTICATE <authentication related data> → authentication related data ←	External authentication with establishing of SM keys
VERIFY <Biom. Verification Data, SM protected> → OK ←	User verification with SM protected verification data; response can also be SM protected

Rysunek 4 Przykład komunikacji wraz z dodatkowymi zabezpieczeniami (with secure messaging)



Rysunek 5 Przykład BIT

Jeśli metoda wymaga jakichś informacji z karty przed procesem weryfikacji, dane te mogą być dostarczone w BIT. Dokładny opis BIT znajduje się w dodatku C normy ISO 7816-11:2004

Komenda używana przy statycznej metodzie weryfikacji – VERIFY – opisana jest w normie ISO/IEC 7816-4. Informacje jakie mogą być podane to:

- identyfikator danych biometrycznych (biometric reference data identifier i.e. the qualifier of the reference data)
- dane biometryczne (biometric verification data)

Dane biometryczne (biometric verification data) mogą być zakodowane jako obiekt w formacie BER-TLV (patrz ISO/IEC 7816-4:2013-04 6.2), co jest oznaczone przez bit CLA (patrz ISO/IEC 7816-4). Dla złożonych schematów biometrycznych możliwe jest użycie łańcuchów komend opisanych w normie ISO/IEC 7816-8.

Komendy opisane są przez następujące normy:

- SELECT FILE - ISO 7816-4 6.11
- GET DATA - ISO 7816-4 6.9
- MANAGE SECURITY ENVIRONMENT - ISO 7816-4:2013 11.5.11
- VERIFY - ISO 7816-4 6.12
- GET CHALLENGE - ISO 7816-4 6.15
- EXTERNAL AUTHENTICATE- ISO 7816-4 6.14

Bibliografia

1. ISO/IEC 7816-11:2004(E)
2. ISO/IEC 7816-4:2013
3. http://www.cardwerk.com/smartcards/smartcard_standard_ISO7816.aspx