

**Documenti
elettronici di
identità**

**Guida tecnica per garantire la
qualità e interoperabilità dei
dati Biometrici**



**AGENZIA PER
L'ITALIA DIGITALE**

giugno 2013

**Guida tecnica per garantire la qualità e interoperabilità degli elementi biometrici
nei documenti elettronici di identità**

Versione 1.0

Giugno 2013

INDICE

ACRONIMI

1	Premessa	4
2	Elementi biometrici contenuti nei documenti elettronici di identità.....	5
2.1	Elementi biometrici primari: immagine del volto	5
2.2	Elementi biometrici secondari: impronte digitali	5
3	Le procedure di acquisizione e registrazione degli elementi biometrici per l'emissione del documento	6
3.1	Processo di acquisizione e registrazione della immagine del volto.....	6
3.1.1	Acquisizione della foto	7
3.1.2	Verifica della qualità.....	8
3.1.3	Compressione	8
3.1.4	Codifica	8
3.2	Processo di acquisizione e registrazione delle impronte digitali	9
3.2.1	Acquisizione impronte	10
3.2.2	Verifica qualità	12
3.2.3	Compressione	13
3.2.4	Codifica	13
4	Statistiche sulla qualità	13
5	Componenti HW e SW per la acquisizione degli elementi biometrici.....	14
5.1	Requisiti hw e sw per la acquisizione della immagine del volto.....	14
5.1.1	Dispositivo di acquisizione foto	14
5.1.2	Software verifica conformità e modifica della foto	15
5.1.3	Software compressione immagine volto	17
5.1.4	Software codifica immagine volto e metadati in formato interoperabile.....	17
5.2	Requisiti hw e sw per acquisizione impronte	17
5.2.1	Dispositivo di acquisizione impronte digitali (single finger).....	17
5.2.2	Software per la misura della qualità delle impronte	20
5.2.3	Software per la scelta del miglior campione di impronta	20
5.2.4	Software compressione immagine impronte	20
5.2.5	Software codifica immagine impronte e metadati in formato interoperabile.....	21
6	APPENDICE - Caratteristiche e requisiti della foto	22
6.1	Aspetti generali	22
6.2	Inquadratura e posa.....	22
6.3	Messa a fuoco, colori, luminosità e contrasto	24
6.4	Ornamenti, occhiali e coperture.....	26
7	Riferimenti	28

ACRONIMI

ACRONIMO	DESCRIZIONE
BAC	Basic Access Control
BMP	Image format Windows Bitmap v3
CBEFF	Common Biometric Exchange Formats Framework
CA	Chip Authentication
CTF	Contrast Transfer Function
DG2	Data Group 2 del microprocessore RF del documento (dati codificati del volto)
DG3	Data Group 3 del microprocessore RF del documento (dati codificati delle impronte)
DPI	Dots per Inch
FAR	False Accept Rate
FRR	False Reject Rate
IAFIS	Integrated Automated Fingerprint Identification System
ICAO	International Civil Aviation Organisation
IEC	International Electrotechnical Commission
IQS	Image Quality Specifications
IS	Inspection System (Sistemi di controllo)
ISO	International Organisation for Standardisation
JPEG	Joint Photographic Experts Group
LDS	Logical Data Structure
MIN	Ministero dell'Interno
MRTD	Machine Readable Travel Document
MTF	Modulation Transfer Function
NFIQ	Nist Fingerprint Image Quality
NIST	National Institute of Standards and Technology
PIV	Personal Identity Verification
QA	Quality assurance
RF	Radio Frequency
SDK	Software Development Kit
WSQ	Wavelet Scalar Quantization
XML	Extensible Markup Language

1 Premessa

Gli elementi biometrici registrati nei documenti di identità elettronici sono utilizzati solo al fine di verificare l'identità del titolare attraverso elementi comparativi direttamente disponibili nel documento, escludendo confronti in modalità "uno a molti" a fini di identificazione.

Nella fase di emissione dei documenti vengono acquisiti i dati biometrici del richiedente e registrati nel microprocessore RF del documento.

Nella fase di controllo gli organi preposti possono verificare l'identità del titolare acquisendone gli elementi biometrici per compararli, in modalità 1:1, con i corrispondenti elementi registrati nel documento, mediante un software di riconoscimento biometrico (eventualmente uno per il volto e uno per le impronte) presente nei sistemi di controllo.

Si pongono pertanto due esigenze principali da soddisfare ai fini del corretto riconoscimento biometrico del titolare del documento:

- interoperabilità: i dati biometrici acquisiti con i sistemi di emissione e registrati nei documenti devono essere comparati con quelli i dati biometrici acquisiti al momento della verifica dai sistemi di controllo ed è pertanto necessaria compatibilità di formati;
- qualità: la qualità dei dati biometrici registrati deve essere buona per consentire la verifica dai sistemi di controllo con un elevato livello di accuratezza, ovvero con bassi tassi di false accettazioni (FAR) e di falsi rigetti (FRR).

La interoperabilità richiede che i dati biometrici registrati nei documenti siano conformi agli standard fissati dalla norme tecniche internazionali ICAO [3] e ISO/IEC [4],[5],[7] [8].

Si richiama a questo proposito la Proposta di Risoluzione approvata dal Consiglio della UE il 4.12.2006 [1] in materia di standard minimi comuni di sicurezza per i documenti di identità degli Stati Membri che prevede, con riferimento agli elementi biometrici:

Se le carte d'identità utilizzate per scopi di viaggio contengono identificatori biometrici, questi dati devono essere conservati ed essere leggibili in conformità alle specifiche ICAO sulla biometria (documento 9303, parte 3, Volume 2) e i regolamenti dell'Unione europea e le specifiche tecniche sulla biometria nei passaporti, stabiliti nel regolamento (CE) 2252/2004 [2]. Altri elementi biometrici opzionali possono essere aggiunti per uso nazionale.

La qualità dei dati biometrici acquisiti dipende da numerosi fattori:

- caratteristiche dei dispositivi di acquisizione quali ad esempio risoluzione o distorsione geometrica, dipendenti dalla qualità del dispositivo,
- procedure di acquisizione e software a supporto (ad es. software di controllo qualità),
- qualità intrinseca dei campioni da acquisire,
- competenza dell'operatore e esperienza del soggetto nell'acquisizione,
- ambiente di acquisizione.

L'accuratezza del riconoscimento biometrico in fase di controllo richiede adeguata qualità del software di riconoscimento e dei dati biometrici utilizzati (sia quelli registrati nel documento in fase di emissione che quelli acquisiti in fase di verifica).

Devono essere inoltre garantiti il rispetto della sicurezza e della privacy, sia in fase di emissione che di verifica.

La presente guida tecnica costituisce un documento d'uso per le amministrazioni coinvolte nella emissione dei documenti elettronici di identità, contenente:

- la indicazione circa gli elementi biometrici registrati (cap.2),
- la descrizione delle procedure di acquisizione degli elementi biometrici (cap.3),
- la descrizione dell'archivio statistico per il monitoraggio della qualità delle impronte acquisite (cap. 4),
- le caratteristiche tecniche delle soluzioni hardware e software necessarie a garantire le esigenze di interoperabilità e qualità dei dati biometrici registrati in fase di emissione dei documenti (cap.5),
- le caratteristiche e i requisiti delle foto (cap. 6 - Appendice A),
- i riferimenti tecnici e normativi (cap.7).

2 Elementi biometrici contenuti nei documenti elettronici di identità

2.1 Elementi biometrici primari: immagine del volto

In conformità a quanto previsto dalle norme ICAO, l'immagine del volto del titolare del documento, memorizzata all'interno del microprocessore RF e stampata sul fronte del documento, costituisce l'elemento biometrico primario. Le principali caratteristiche dell'immagine e del relativo processo di acquisizione in formato digitale sono definite dalle norme tecniche ICAO [3] e ISO/IEC [4].

Ai fini del rilascio dei documenti elettronici di identità, gli Enti preposti eseguono una procedura di acquisizione e digitalizzazione dell'immagine del volto del cittadino, ottenuta a partire da una foto cartacea o da una immagine digitale, eventualmente anche acquisita sul posto. L'immagine del volto digitale ottenuta viene successivamente elaborata per consentirne la stampa sul fronte del documento e la memorizzazione all'interno del microprocessore RF in esso contenuto.

L'immagine del volto del cittadino memorizzata nel microprocessore RF deve essere conforme ai requisiti di codifica e formato **FRONTAL** specificati nella norma tecnica ISO/IEC 19794-5 [4].

Al fine di minimizzare lo spazio occupato nel microprocessore RF, tale immagine è compressa in formato JPEG2000 [8].

2.2 Elementi biometrici secondari: impronte digitali

Le impronte digitali del titolare del documento che vengono memorizzate all'interno del microprocessore RF costituiscono gli elementi biometrici secondari. Le principali caratteristiche delle impronte digitali e del relativo processo di acquisizione in formato digitale sono definite dalle norme tecniche ICAO [3], ISO/IEC [5] e ANSI/NIST [6].

Ai fini del rilascio del documento, gli Enti preposti eseguono una procedura di acquisizione a mezzo scansione elettronica di due impronte digitali del cittadino. Le impronte vengono successivamente elaborate per consentirne la memorizzazione all'interno del microprocessore RF in esso contenuto.

Le sopracitate raccomandazioni e norme tecniche definiscono una serie di caratteristiche e requisiti che le impronte acquisite devono possedere, per garantire la interoperabilità e rendere più efficaci le operazioni di riconoscimento.

Le impronte digitali primarie da incorporare nel documento sono le impronte semplici (piane) dell'indice destro e dell'indice sinistro.

In caso di qualità insoddisfacente delle impronte digitali e/o di configurazione alterata degli indici della mano a causa di lesioni, si deve procedere all'acquisizione delle impronte, di qualità soddisfacente, di medi, anulari o pollici¹.

Le impronte digitali vengono memorizzate come immagini all'interno del microprocessore RF in esso contenuto, conformemente alla norma ISO/IEC 19794-4:2005 [5].

La qualità delle immagini delle impronte digitali deve essere conforme alle norme ISO/IEC 19794-4:2005 [5] e ANSI/NIST 1-2007 [6].

Al fine di minimizzare lo spazio occupato nel microprocessore RF si deve ricorrere alla compressione delle immagini attraverso l'algoritmo WSQ, conformemente alle norme tecniche FBI [7].

3 Le procedure di acquisizione e registrazione degli elementi biometrici per l'emissione del documento

Le procedure descritte in questo capitolo sono state definite al fine di assicurare la qualità degli elementi biometrici acquisiti e registrati nel documento e la conformità alle norme ICAO e ISO sopracitate.

3.1 Processo di acquisizione e registrazione della immagine del volto

La acquisizione della immagine del volto in formato digitale può avvenire con due diverse modalità:

1. Acquisizione *'live'*: consente di acquisire foto *ICAO-compliant* (ovvero conformi a ISO/IEC 19794-5) sin dall'inizio del processo di emissione e senza il possibile degrado dovuto alla scansione elettronica della foto cartacea; l'acquisizione *live* è anche vantaggiosa in termini di tempo medio di avanzamento della pratica (si evita che il cittadino debba presentare più volte la foto in caso di non conformità) sia in termini di sicurezza (si evita lo scambio e l'alterazione di fotografie). E' una soluzione che richiede l'allestimento di appositi spazi (è necessario uno sfondo neutro, l'illuminazione deve essere uniforme e ben direzionata), l'utilizzo di fotocamere digitali e software dedicato nonché un'adeguata formazione del personale preposto alla acquisizione.
2. scansione della foto cartacea: oltre al degrado dovuto alla scansione elettronica e alla possibilità di modifiche o scambio della fotografia, se la foto non risulta conforme occorre chiedere al cittadino di ripresentarsi con un'altra foto con il conseguente allungamento dei tempi di rilascio; il vantaggio è quello di non dover attrezzare una postazione di acquisizione presso le questure e i commissariati.

La scelta della soluzione deve essere effettuata considerando non solo aspetti puramente tecnici ma anche economici e organizzativi.

Nel seguito del documento si farà riferimento alla seconda modalità.

La procedura di rilascio o rinnovo del documento prevede, al momento, che il cittadino alleggi alla domanda n. 2 foto identiche frontali, a volto scoperto e a colori conformi alle norme ICAO [3] da una delle quali viene ricavata l'immagine digitale che, successivamente elaborata, viene stampata sul fronte

¹ Il formato di memorizzazione (CBEFF – Common Biometric Exchange File Format) previsto da ISO/IEC 19794-4:2005 [5] classificherà il dito impiegato (indice sinistro, medio destro, ecc.) onde garantire, in fase di verifica, il controllo del dito conforme.

del documento e memorizzata all'interno del microprocessore RF in esso contenuto. Nella Appendice A vengono riportate caratteristiche e requisiti, indicati nella norma ISO 19794-5 [4], che le foto devono possedere al fine di favorire e rendere più efficaci le operazioni di riconoscimento biometrico.

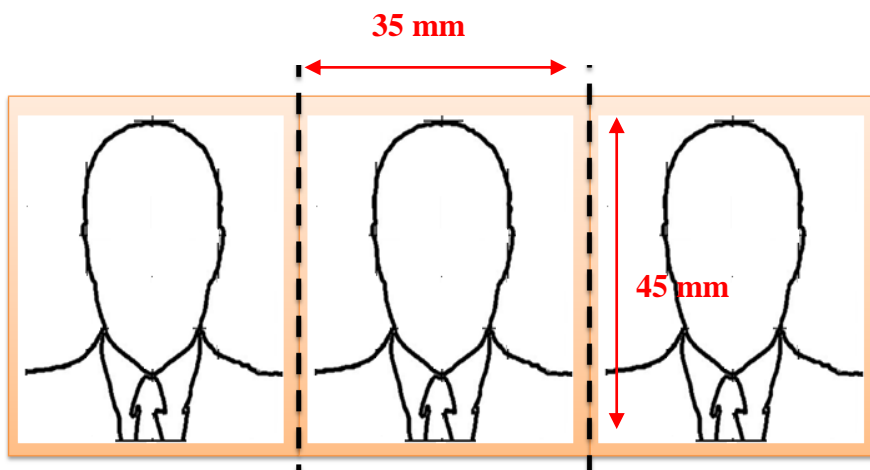
3.1.1 Acquisizione della foto

La procedura di digitalizzazione della foto è eseguita mediante un apposito dispositivo di acquisizione disponibile presso gli Enti deputati alla raccolta dei dati. Le caratteristiche tecniche del dispositivo, riportate al paragrafo 7.1.1, sono state definite con la finalità principale di acquisire la foto cartacea senza introdurre un degrado percettibile della stessa.

Per il corretto svolgimento della procedura di acquisizione, occorre ritagliare, se necessario, la foto in modo che le dimensioni risultino pari a:

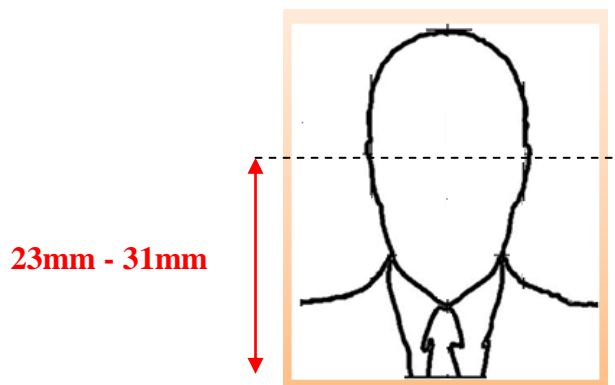
- Larghezza: 35mm
- Altezza: 45mm.

L'eventuale ritaglio della foto deve essere eseguito in modo da assicurare un'acquisizione dell'immagine che ritragga per intero il volto non ruotato del soggetto. Se le copie della foto vengono presentate unite, occorre ritagliarle rispettando le sopracitate dimensioni.



In ogni caso, le foto non devono essere ritagliate per escludere lo sfondo o per raddrizzare la testa, né devono risultare ritoccate, colorate o manomesse in alcun modo.

L'altezza della foto deve essere tale da assicurare che il volto sia contenuto interamente nell'immagine e centrato rispetto al riquadro dell'immagine in modo che l'altezza degli occhi, rispetto la base del riquadro stesso, sia compresa fra un valore massimo di 31 mm e un valore minimo di 23 mm.



Le norme tecniche contenute in [4], riportate al capitolo 8 . Appendice A, definiscono una serie di caratteristiche e requisiti che le foto devono possedere, al fine di favorire e rendere più efficace le operazioni di riconoscimento.

3.1.2 Verifica della qualità

La verifica della qualità della foto e della conformità alle norme richiamate, è effettuata dall'operatore che esegue le operazioni di acquisizione, coadiuvato da un apposito software disponibile all'interno della procedura automatica di acquisizione della foto.

Tale software fornisce una serie di indicazioni circa eventuali difformità della foto in esame rispetto ai parametri standard fissati per ottenere immagini che consentano un efficiente riconoscimento da parte di sistemi automatici, e costituisce esclusivamente un supporto decisionale, lasciando in ogni caso la scelta di accettare o meno la foto presentata all'operatore che esegue l'operazione.

Il software oltre che verificare la conformità della foto alle norme può anche effettuare modifiche alla foto per riportarla al formato full frontal (ritaglio, rotazione, *scaling*).

Le caratteristiche tecniche di tale software e le modalità di valutazione sono riportate al paragrafo 7.1.2.

3.1.3 Compressione

L'immagine digitale della foto acquisita con lo scanner e ritagliata dal software ha una dimensione di circa 700 KB e pertanto deve essere compressa per la registrazione nel microprocessore RF.

Si raccomanda la compressione Jpeg 2000 Part-1 Code Stream Format [8] in quanto consente, a parità di qualità della immagini compressa, una dimensione inferiore rispetto a quella della stessa immagine compressa con Jpeg.

Le dimensioni della foto compressa sono di circa 10 Kb per immagini con compressione JPEG 2000.

Le caratteristiche del software da utilizzare per la compressione JPEG2000 sono riportate al paragrafo 6.1.3.

3.1.4 Codifica

Prima della memorizzazione nel chip RF del documento l'immagine compressa del volto e le informazioni associate devono essere correttamente codificate nel formato descritto dalla LDS (Logical Data Structure), DG2, delle specifiche tecniche ICAO [3], basate sullo standard ISO/IEC 19794-5 [4] e CBEFF (Common Biometric Exchange File Format) [11].

3.2 Processo di acquisizione e registrazione delle impronte digitali

Le impronte digitali devono essere acquisite a partire dal dito indice della mano destra e a seguire dal dito indice della mano sinistra.

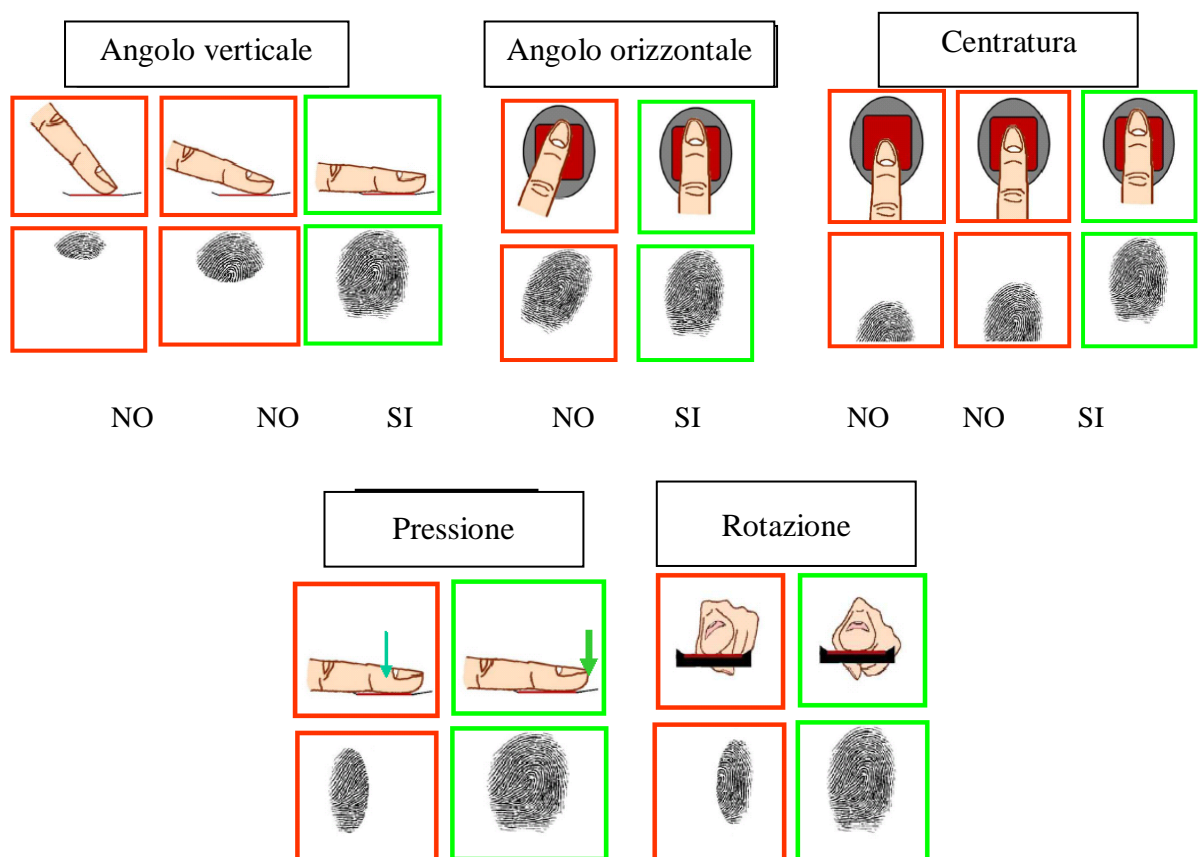
Se non è possibile acquisire l'impronta del dito indice, si può procedere all'acquisizione dell'impronta seguendo l'ordine: dito medio, dito anulare e dito pollice per ciascuna mano.

Al fine di ottenere un'impronta di qualità sufficiente ai fini delle verifiche effettuate mediante i sistemi di controllo, vanno effettuati almeno 3 (tre) tentativi di acquisizione facendo sempre alzare il dito dal sensore tra un tentativo e l'altro. Questa procedura deve essere seguita per ogni dito acquisito.

La gestione della qualità dell'impronta rilevata è effettuata, in automatico, mediante apposito software (Vedi paragrafo 7.2.2)

Al fine di garantire un corretto risultato l'operatore che esegue la procedura di acquisizione deve assicurarsi che:

- il dito poggiato sul sensore sia effettivamente quello richiesto dall'operatore;
- le dita non siano ricoperte da patine o pellicole che possano mascherare la vera impronta sostituendola con una falsa;
- il dito sia posizionato correttamente sulla superficie del dispositivo di acquisizione come indicato nelle figure sottostanti che evidenziano le posizioni corrette (SI) e le posizioni non corrette (NO); in particolare la posizione corretta prevede che il dito sia poggiato di piatto con la giusta pressione del polpastrello, senza inclinazione verticale o orizzontale e senza rotazione laterale.



NO SI NO SI

Figura 1 - Esempi di posizionamento corretto (SI) e non corretto (NO)

In fase di rilevazione delle impronte occorre accertare che non ci siano impedimenti di nessun genere.

Nel caso in cui si riscontrino impedimenti temporanei (ad esempio: ferite, medicazioni, ecc.), non bisogna effettuare la procedura di rilevamento e si procede a rinviare ad altra data la procedura di acquisizione delle immagini delle impronte digitali.

In via generale, si procede acquisendo l'impronta di un dito della mano destra e poi l'impronta di un dito della mano sinistra secondo la procedura descritta nel seguito.

In via generale, in caso di parziali impedimenti sono acquisite le impronte delle dita disponibili ad eccezione del dito mignolo.

Nel caso di totale impossibilità ad acquisire le impronte, si rilascia il documento senza la memorizzazione degli elementi biometrici secondari nel microprocessore RF.

Si prevede, di regola, che le dita delle due mani siano acquisite in sequenza (vedi diagramma semplificato riportato di seguito).

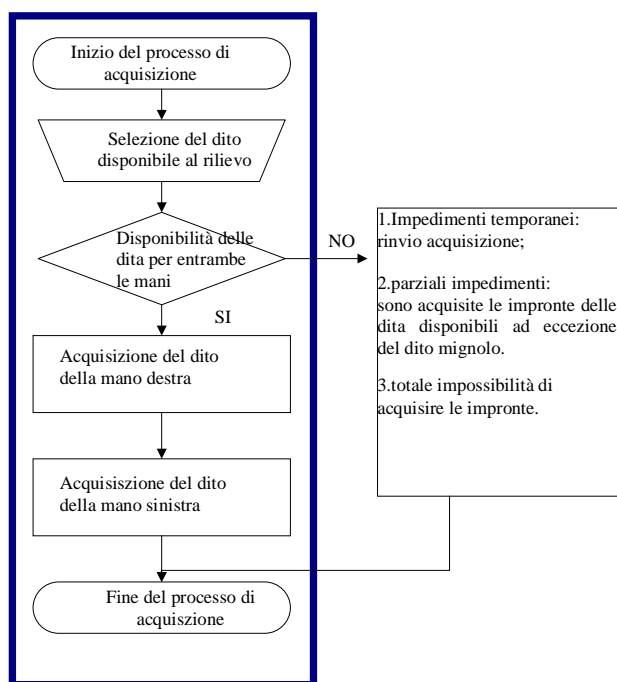


Figura 1 – Diagramma semplificato di acquisizione delle impronte digitali

3.2.1 Acquisizione impronte

La procedura utilizza alcuni moduli software messi a disposizione dal National Institute of Standards and Technology (NIST) per il controllo della qualità e la scelta del miglior campione acquisito [9].

La procedura è già utilizzata per l'acquisizione dell'impronte da inserire nel microprocessore RF del passaporto elettronico ed è descritta nel Draft dello Standard in fase di sviluppo ISO/IEC 29196 "Guidance for biometric enrolment". I risultati forniti in termini di qualità delle impronte acquisite e dei tempi di acquisizione confermano la validità della procedura.

Di seguito viene descritto il processo di acquisizione delle impronte digitali di una mano.

1. L'operatore chiede al cittadino di porre il dito selezionato, secondo l'ordine precedentemente specificato, sulla finestra di scansione del dispositivo di acquisizione.
2. Il soggetto pone il dito richiesto dall'operatore sul dispositivo di acquisizione e ripete questa operazione per 3 (tre) volte, avendo cura di sollevare il dito dal dispositivo ogni volta, al fine di acquisire tre differenti immagini della impronta del dito tra le quali scegliere in automatico la migliore, con le modalità descritte al punto successivo.
3. Il software di acquisizione, in automatico, effettua le seguenti misure:
 - a. Se tutte e tre le immagini acquisite della impronta del dito hanno un buon livello di qualità (NFIQ minore o uguale a 3), viene scelta quella che risulta maggiormente "confrontabile" con le altre due (ovvero quella caratterizzata da un punteggio medio più elevato, fornito dall'algoritmo di confronto Bozorth3, vedi paragrafo 7.2.3);
 - b. Se almeno un'immagine acquisita ha uno scarso livello di qualità (NFIQ maggiore di 3), viene scelta, tra le restanti, quella che risulta maggiormente "confrontabile" con le altre due (ovvero quella caratterizzata da un punteggio medio più elevato, fornito dall'algoritmo di confronto Bozorth3);
 - c. Se tutte le immagini acquisite hanno uno scarso livello di qualità (NFIQ maggiore di 3), si procede con il dito successivo;
 - d. Nel caso in cui per nessun dito di una delle mani si raggiunga un livello di qualità delle impronte acquisite adeguato (NFIQ maggiore di 3) la scelta del dito avviene nel modo seguente a seconda dei casi:
 - 1 - se per un solo dito il livello di qualità di una o più delle impronte acquisite è pari a 4 viene scelta la migliore impronta di questo dito con la procedura descritta in precedenza (punti a e b);
 - 2 - se esiste più di un dito con livello di qualità delle impronte acquisite pari a 4 si procede alla scelta del dito sulla base dell'ordine di acquisizione previsto (indice, medio, anulare e pollice);
 - 3 - se tutte le impronte acquisite hanno un livello di qualità pari a 5 si sceglie la migliore impronta dell'indice con la procedura descritta in precedenza (punto a) .
4. Se l'operatore si accorge che l'acquisizione è caratterizzata da un'insufficiente indice di qualità a causa di una errata esecuzione della procedura (ad esempio dito non posizionato correttamente sul dispositivo), occorre ripetere l'acquisizione indipendentemente dai risultati indicati dal software;
5. Una volta completate le operazioni per la prima mano (destra), si procede con la ripetizione della procedura dal passo 1 al passo 4 per la seconda mano (sinistra).

Di seguito viene riportato lo schema di flusso delle operazioni di acquisizione

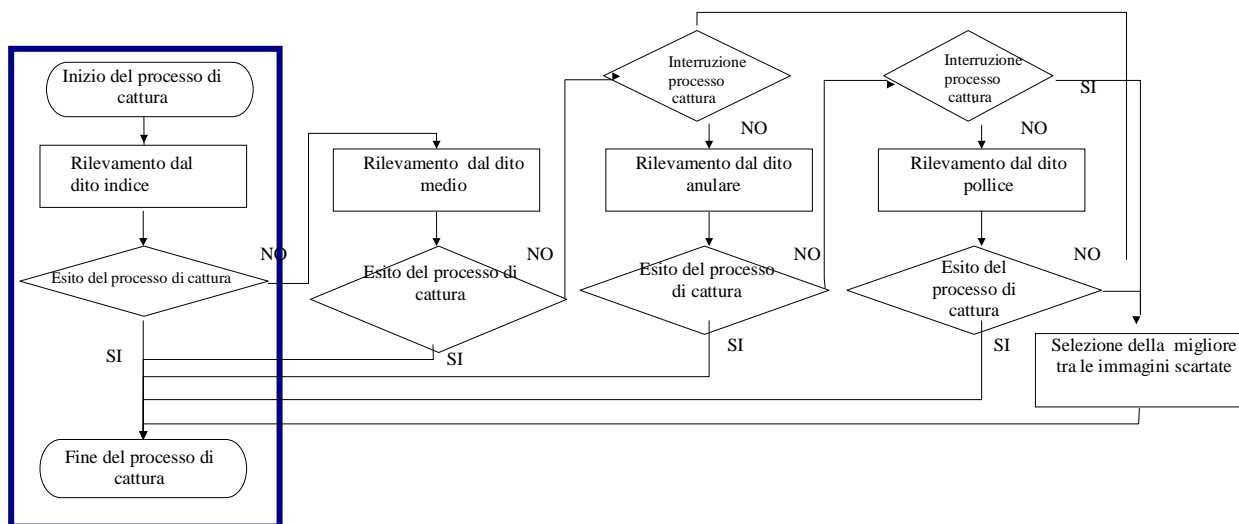


Figura 1 - Diagramma di flusso della procedura operativa di acquisizione delle impronte digitali di una mano

3.2.2 Verifica qualità

La possibilità di verifiche di identità affidabili basate sulle tecnologie delle impronte digitali richiede la registrazione nei documenti di identità elettronici di immagini digitali delle impronte di alta qualità. La verifica della qualità dell'immagine dell'impronta digitale acquisita, viene effettuata con il software NIST Fingerprint Image Quality (NFIQ), che fornisce un indice intero compreso tra 1 (qualità massima) e 5 (qualità minima).

Questo software è utilizzato sia per scegliere le dita di cui acquisire le impronte, sia per misurare il livello di qualità delle impronte registrate nel documento, da memorizzare nel microprocessore RF insieme alle immagini delle impronte stesse.

Tali livelli di qualità devono fare riferimento alla normativa ISO [5] che prevede valori compresi tra 0 (qualità minima) e 100 (qualità massima). Nel seguito sono riportati i valori ISO corrispondenti ai valori NFIQ misurati, da utilizzare in fase di registrazione nel DG3, insieme alle immagini comprese delle impronte:

- 100 (NFIQ = 1);
- 75 (NFIQ = 2);
- 50 (NFIQ = 3);
- 25 (NFIQ = 4);
- 0 (NFIQ = 5).

Viene fissato come valore minimo, per un'impronta di qualità soddisfacente ai fini del riconoscimento automatico, un indice NFIQ pari a 3, per cui si determina che immagini con valori di qualità:

- NFIQ 4 (quattro) e 5 (cinque) devono essere, come prima istanza, scartate.
- NFIQ 1 (uno), 2 (due) e 3 (tre) devono essere accettate.

Qualora nessuna delle impronte acquisite abbia un livello di qualità compreso tra 1 e 3, viene registrata la impronta con la qualità migliore, scelta secondo la procedura descritta al punto d) del paragrafo precedente.

L'applicativo di acquisizione delle impronte deve integrare in una sola procedura sia la funzionalità di acquisizione dell'impronta dal sensore ottico che quella di verifica della qualità effettuata con il software di controllo qualità NFIQ.

La valutazione della qualità dell'immagine dell'impronta deve essere effettuata sui dati dell'immagine non compressa.

3.2.3 Compressione

L'immagine digitale delle impronte acquisite con una risoluzione di 500 ppi (pixel per inch) e un'area di acquisizione di un pollice quadrato, profondità 8 bit, ha una dimensione di 250 KB e pertanto deve essere compressa per la registrazione nel microprocessore RF riportandola a una dimensione compatibile con la capacità del chip e con una riduzione di qualità che non comprometta la accuratezza del riconoscimento biometrico in fase di verifica.

Si raccomanda il ricorso alla compressione delle immagini attraverso l'algoritmo WSQ, conformemente alla norma [6] e [7] per ridurre le dimensioni del file.

La stessa Decisione indica in circa 12 – 15 Kbyte per dito il volume di memorizzazione necessario per le immagini compresse delle impronte digitali.

Il fattore di compressione da utilizzare non deve essere superiore a 15:1, come prescritto dalla norma ISO 19794-4 [5].

Non devono essere effettuate compressioni multiple che degraderebbero significativamente l'immagine.

3.2.4 Codifica

Prima della memorizzazione nel DG3 del microprocessore RF le immagini compresse delle impronte e le informazioni associate, relative alla qualità delle immagini delle impronte e alla indicazione delle dita alle quali sono riferite, devono essere codificate nel formato descritto dalla LDS (Logical Data Structure), DG3, delle specifiche tecniche ICAO [3], basate sullo standard ISO/IEC 19794-4 [5] e CBEFF (Common Biometric Exchange File Format) [11].

4 Statistiche sulla qualità

Si propone di istituire un archivio statistico informatizzato nel quale registrare, in forma anonima (cioè non riconducibile al titolare) le seguenti informazioni raccolte nelle fasi di acquisizione e verifica delle impronte:

- il valore dell'indice di qualità della impronta memorizzata,
- il punteggio fornito dall'algoritmo di confronto (Bozorth3) per la scelta del miglior campione di impronta,
- identificativo del dito scelto per la registrazione della impronta,
- il tempo di acquisizione delle impronte

Lo scopo dell'archivio statistico è quello di raccogliere i dati necessari per il monitoraggio costante della qualità delle impronte acquisite al fine di individuare eventuali degradi del sistema di acquisizione (es. deviazione dai livelli ottimali di taratura degli scanner).

Questi dati potranno servire anche alla creazione di un sistema di valutazione di impatto di eventuali modifiche (cambio degli standard degli emendamenti, modifiche del software).

Le informazioni che si prevede possano essere estratte dall'archivio statistico, in relazione ad un determinato periodo, sono:

- la ripartizione percentuale nei cinque livelli di qualità delle impronte digitali registrate nei permessi di soggiorno;
- il numero di immagini (di impronte digitali), registrate nei documenti di identità, al di sotto della soglia di qualità minima;
- per ciascuna mano, la ripartizione percentuale delle dita scelte in fase di acquisizione delle impronte;
- i tempi medi di acquisizione delle impronte.

Si ritiene che alcuni valori target di qualità raggiungibili siano i seguenti:

- percentuale di immagini al di sotto della soglia minima di qualità, livello NFIQ 4 o 5 (livello ISO 0, 25): < 5%
- percentuale di immagini con livelli di qualità elevata, livello NFIQ 1 o 2 (livello ISO 100 o 75): > 90%

I dati raccolti verranno registrati in modo anonimo e in nessun caso sarà possibile risalire alla impronta o alla persona ad essa correlata.

5 Componenti HW e SW per la acquisizione degli elementi biometrici

La acquisizione e la registrazione degli elementi biometrici del titolare del documento richiedono l'utilizzo di componenti hardware e software di seguito elencate le cui caratteristiche tecniche verranno riportate in dettaglio nei successivi paragrafi:

- volto (paragrafo 5.1)

- Dispositivo di acquisizione foto e relativo software
- Software di verifica qualità (conformità ICAO) e modifica della immagine
- Software di compressione (Jpeg 2000)
- Software di codifica

- impronte (paragrafo 5.2)

- Dispositivo di acquisizione impronte e relativo software
- Software di verifica qualità (NFIQ)
- Software per la scelta del miglior campione da memorizzare
- Software di compressione (WSQ)
- Software di codifica.

5.1 Requisiti hw e sw per la acquisizione della immagine del volto

La postazione di acquisizione, i cui requisiti tecnici non sono oggetto del presente documento, deve essere connessa al dispositivo di acquisizione della foto e dovrà ospitare una applicazione in grado di gestire lo scanner e supportare il processo di acquisizione integrando il software di controllo qualità, il software di compressione e quello di codifica.

5.1.1 Dispositivo di acquisizione foto

Le impronte digitali devono essere memorizzate come immagini, conformemente alla norma ISO [4].

Per acquisire fotografie che rispondano ai requisiti di qualità definiti dalla norma ISO [4] il dispositivo di acquisizione, scanner piano, deve:

- avere una risoluzione di almeno 300 dpi;

- produrre un'immagine senza alcuna compressione in formato Windows Bitmap versione 3 con un rapporto di aspetto dei pixel (pixel aspect ratio) 1:1, ovvero il numero dei ppi (pixels per inch) misurato lungo la direzione verticale deve essere pari a quello misurato lungo la direzione orizzontale;
- garantire un range dinamico pari ad almeno 128 livelli di tono nella regione facciale dell'immagine, definita come la sezione dell'immagine che va dalla fronte al mento e dall'orecchio sinistro a quello destro del soggetto;
- rappresentare l'immagine acquisita in uno spazio di colori a 24-bit RGB, in modo che per ciascun pixel siano utilizzati 8 bit per la codifica delle tre componenti di colore;
- garantire un'illuminazione distribuita in maniera omogenea sull'intera area di acquisizione, mediante l'utilizzo di fonti di luce diffusa e non focalizzata, in modo da assicurare un livello di luminosità uniforme ed una resa dei colori fedele sull'intera immagine acquisita;
- operare un corretto bilanciamento del bianco in modo da evitare la presenza di dominanti cromatiche anomale e più in generale di fenomeni di alterazione dei colori naturali del soggetto e della scena dell'immagine acquisita;

e non deve

- fare utilizzo di tecnologie di scansione che ricostruiscono l'immagine mediante frames video interlacciati;
- introdurre evidenti fenomeni di sovraesposizione o sottoesposizione;
- introdurre evidenti effetti di sfocatura;
- introdurre evidenti alterazioni nel contrasto;
- introdurre evidente distorsione geometrica dell'immagine².

5.1.2 Software verifica conformità e modifica della foto

A differenza della qualità delle impronte per la qualità della immagine del volto non esistono indici sintetici che misurino il livello di qualità complessiva dell'immagine.

Il modulo di verifica della qualità della foto è utilizzato per il controllo della conformità della foto alle norme specificate in [4] dopo la digitalizzazione. Vengono verificate le proprietà geometriche delle immagini e altri parametri tra quelli riportati nella norma tecnica [4] che descrive i requisiti per le immagini del volto.

Il software di verifica può anche effettuare alcune modifiche alla immagine acquisita con lo scanner per renderla conforme alle norme specificate in [4] prima della compressione e codifica.

Tali modifiche sono le seguenti:

- rotazione
- spostamenti verticali e orizzontali
- ridimensionamento
- ritaglio

I test di alcuni software di controllo conformità ICAO delle foto, effettuati da Agid in collaborazione con il BioLab della Università di Bologna su una base dati di immagini in parte conformi ICAO e in parte non conformi, hanno evidenziato che nessuno dei software testati gestisce tutti i requisiti ICAO e nella verifica dei requisiti gestiti vengono commessi errori di valutazione che arrivano, in alcuni casi, fino al 50% [12] [18]. Tali errori rendono inutilizzabile un uso automatico e vincolante per l'operatore del software di verifica della conformità.

² Da verificare mediante l'acquisizione di target geometrici.

Nel seguito vengono riportati i requisiti obbligatori e opzionali del software per la verifica della qualità della fotografia acquisita e della conformità ICAO.

Requisiti obbligatori

- Calcolare la posizione del rettangolo del volto (e restituire coordinate della finestra). Rif. punto 1 tabella.
- Calcolare la posizione del centro degli occhi (e restituire coordinate dei centri). Rif. punto 2 tabella.
- Consentire la centratura e ritaglio della foto secondo i formati *full frontal* e *token* di ISO 19794-5 [4], verificando la rispondenza ai criteri geometrici 3, 4, 5, 6 e 7 in tabella (e gli analoghi criteri per il formato *token*).
- Evidenziare graficamente sulla foto il rettangolo di ritaglio facendo chiaramente capire all'operatore eventuali problematiche che rendono impossibile il ritaglio nel formato richiesto
- Verificare la conformità ai seguenti criteri non-geometrici ICAO (comunicando chiaramente all'operatore le ragioni di eventuali non conformità; non è sufficiente un generico messaggio di foto non conforme):
 - o Foto sfuocata (8 in tabella)
 - o Colore innaturale della pelle (11 in tabella)
 - o Foto troppo chiara / troppo scura (12 in tabella)
 - o Contrasto non sufficiente (13 in tabella)

Requisiti opzionali

- Calcolare la posizione di altre caratteristiche ad esempio bocca e naso (e restituire coordinate)
- Calcolare la conformità rispetto ad altri (non necessariamente tutti) criteri non-geometrici ICAO (criteri da 8 a 30 esclusi quelli obbligatori di cui sopra).
- Fornire soluzione dotata di interfaccia grafica semplificata per l'operatore, con messaggistica avanzata (in italiano) che consenta di comprendere esattamente le eventuali cause di non conformità di una foto.
- Effettuare modifiche di tipo geometrico alla immagine, quali rotazioni, ritaglio, ridimensionamento, ecc. per rimuovere cause di non conformità.

Nella tabella seguente sono riportati i parametri oggetto di valutazione di conformità della foto. L'ultima colonna riporta il riferimento presente nella norma tecnica [4].

N°	Description of the test	Section
Feature extraction accuracy tests		
1	Eye Location Accuracy	
2	Face Location Accuracy (other points)	
Geometric tests (Full Frontal Image Format)		
3	Eye Distance (min 90 pixels)	8.4.1
4	Relative Vertical Position ($0.5B \leq BB \leq 0.7B$)	8.3.3
5	Relative Horizontal Position (no tolerances)	8.3.2
6	Head Image Width Ratio ($0.5A \leq CC \leq 0.71A$)	8.3.4
7	Head Image Height Ratio ($0.7B \leq DD \leq 0.8B$)	8.3.5
Photographic and pose-specific tests		
8	Blurring	7.3.3
9	Looking Away	7.2.3
10	Ink Marked/Creased	A3.2.3
11	Unnatural Skin Tone	7.3.4
12	Too Dark/Light	7.3.2
13	Washed Out	7.4.2.1
14	Pixelation	A3.2.3
15	Hair Across Eyes	A3.2.3
16	Eyes Closed	7.2.3
17	Varied Background	A2.4
18	Roll/Pitch/Yaw Greater 5	7.2.2
19	Flash Reflection on Skin	7.2.10
20	Red Eyes	7.3.4
21	Shadows Behind Head	A3.2.3
22	Shadows Across Face	7.2.7
23	Dark Tinted Lenses	7.2.11
24	Flash Reflection on Lenses	7.2.11
25	Frames too Heavy	A4.3
26	Frame Covering Eyes	7.2.3
27	Hat/Cap	A3.2.3
28	Veil over Face	A3.2.3
29	Mouth Open	7.2.3
30	Presence of Other Faces or Toys too Close to Face	A3.2.3

Il test dei prodotti software per la verifica della conformità ICAO richiede un *data set* di immagini di volti conformi e non conformi ICAO e può essere eseguito secondo le modalità indicate in [12][18].

5.1.3 Software compressione immagine volto

Il software di compressione JPEG2000 utilizzato deve essere conforme alle specifiche definite dalla norma ISO/IEC 15444-1.

Il produttore del software deve dimostrare di aver eseguito il test di conformità per le funzioni di codifica e decodifica JPEG 2000 Part 1 descritto nella raccomandazione Rec. ITU-T T.803 : JPEG 2000 image coding system : conformance testing.

I file per il test sono scaricabili dal sito all'indirizzo :

<http://www.itu.int/net/itu-t/sigdb/speimage/ImageForm-s.aspx?val=10100803>

Non sono ammesse compressioni multiple dell'immagine.

5.1.4 Software codifica immagine volto e metadati in formato interoperabile

Il software di codifica deve generare un record interoperabile contenente l'immagine compressa del volto e le informazioni associate, codificate nel formato descritto dalla LDS (Logical Data Structure), DG2, delle specifiche tecniche ICAO [3], basate sullo standard ISO/IEC 19794-5 [4] e CBEFF (Common Biometric Exchange File Format) [11].

5.2 Requisiti hw e sw per acquisizione impronte

Nella postazione di acquisizione connessa al dispositivo di acquisizione delle impronte dovrà essere installata una applicazione in grado di gestire lo scanner e supportare il processo di acquisizione secondo la procedura descritta nel paragrafo 3.2, integrando il software di controllo qualità, il software di scelta del miglior campione, il software di compressione e quello di codifica.

5.2.1 Dispositivo di acquisizione impronte digitali (single finger)

La norma ISO [5] non fornisce indicazioni puntuali sui requisiti minimi delle immagini da acquisire e quindi dei dispositivi di acquisizione. La norma ISO stabilisce sette livelli con qualità crescente dei dispositivi in funzione delle specifiche applicazioni ed esigenze, riportati nella tabella seguente. Per usi di law enforcement analoghi a quello in esame, la norma ISO suggerisce l'impiego di dispositivi di livello 30 o 31.

Setting level	Scan resolution pixels/centimeter (ppcm)	Scan resolution pixels/inch (ppi)	Pixel depth (bits)	Dynamic range (gray levels)	Certification
10	49	125	1	2	None
20	98	250	3	5	None
30	197	500	8	80	None
35	295	750	8	100	None
31	197	500	8	200	EFTS/F
40	394	1000	8	120	None
41	394	1000	8	200	EFTS/F

Per definire le specifiche dei dispositivi di acquisizione delle impronte AGID ha effettuato uno studio in collaborazione con il Laboratorio di biometria dell'Università di Bologna (BioLab) i cui risultati sono documentati in [13].

Lo studio ha dimostrato che le caratteristiche più importanti di un dispositivo di acquisizione di impronte al fine di massimizzare le prestazioni di riconoscimento automatico da parte di algoritmi sono:

- area di acquisizione,
- accuratezza della risoluzione
- distorsione geometrica;

Per questi parametri è opportuno fare riferimento alle specifiche di maggiore livello qualitativo "IAFIS IQS", o EFTS/F, definite dall'FBI nel documento [14].

Le altre caratteristiche dello scanner: risposta alle frequenze spaziali, rapporto segnale rumore e range dinamico sono importanti ma hanno un impatto minore rispetto alle precedenti sulla accuratezza del riconoscimento biometrico.

Per queste caratteristiche è sufficiente fare riferimento a specifiche di qualità di livello leggermente inferiore quali le specifiche "PIV IQS" definite dall'FBI nel documento [16].

La scelta di apparati di tipo ottico con le caratteristiche di qualità sotto indicate garantisce il raggiungimento di un elevato livello di qualità delle immagini acquisite necessario per ottenere una adeguata accuratezza di riconoscimento da parte di algoritmi automatici.

Area (w×h): $w \geq 25.4\text{mm (1")}$, $h \geq 25.4\text{mm (1")}$

Risoluzione: $500\text{dpi} \pm 1\%$ (IAFIS IQS*)

Distorsione geometrica: requisito IAFIS IQS* così come descritto nel seguito:

Accuratezza geometrica tra le barre

Quando si acquisisce un target a barre multiple parallele da 1.0 cy/mm, con orientamento sia verticale che orizzontale delle barre, il valore assoluto della differenza (D) tra la distanza reale tra le barre parallele del target (X) e la corrispondente distanza misurata nell'immagine (Y) non deve superare i seguenti valori, per almeno il 99% dei casi testati in ciascuna area e in ciascuna delle due direzioni ortogonali:

$D \leq 0.0007$, per $0.00 < X \leq 0.07$ e $D \leq 0.01X$, per $0.07 \leq X \leq 1.50$

Il requisito corrisponde ad una accuratezza posizionale di $\pm 1,0\%$ per le distanze comprese tra 0,07 e 1,5 pollici, e una precisione costante di $\pm 0,0007$ pollici per distanze inferiori o pari a 0,07 pollici.

Dove $D = |Y-X|$, X = distanza reale del target, Y = distanza misurata della immagine (i valori di D, X, Y sono espressi in pollici)

Accuratezza geometrica lungo le barre

Quando si acquisisce un target a barre multiple parallele da 1.0 cy/mm, con orientamento sia verticale che orizzontale delle barre, la differenza massima in direzione, rispettivamente, orizzontale e verticale tra la posizione di due punti qualsiasi posti lungo la immagine di una barra, fino a una distanza massima di 1,5", deve essere inferiore a 0.016" nel 99% dei casi testati, in ciascuna delle due direzioni ortogonali.

Risposta alle frequenze spaziali: requisito PIV IQS** così come descritto nel seguito:

La risposta alle frequenze spaziali può essere misurata utilizzando la funzione di trasferimento del contrasto (CTF) o la funzione di trasferimento della modulazione (MTF).

I valori di CTF o MTF devono superare i valori minimi riportati nella tabella seguente nelle due direzioni orizzontale e verticale e per ogni zona della area di acquisizione, nel range di frequenza da 1.0 a 10.0 cy/mm.

Nessun valore di CTF o MTF deve essere superiore a 1.12.

Frequency (f) in cy/mm at object plane ⁵	Minimum CTF Modulation when using Bar Target	Minimum MTF Modulation when using Sine Wave or Edge Target
1.0	0.920	0.871
2.0	0.822	0.734
3.0	0.720	0.614
4.0	0.620	0.510
5.0	0.526	0.421
6.0	0.440	0.345
7.0	0.362	0.280
8.0	0.293	0.225
9.0	0.232	0.177
10.0	0.174	0.135

Rapporto segnale rumore: Deviazione Standard dei Livelli di Grigio $\sigma \leq 3,5$ in ogni finestra di 0.25×0.25 situata nell'area di acquisizione, acquisendo un target grigio scuro uniforme e un target grigio chiaro uniforme (**PIV IQS ****)

Livelli di grigio: 256

Range Dinamico (DR): per almeno l'80% delle immagini acquisite $DR \geq 150$ (**PIV IQS****)

* **IAFIS IQS:** indica che questo requisito è conforme alle specifiche EBTS/F del'FBI [14]. Le procedure per la verifica di compatibilità sono descritte in [15].

** **PIV IQS:** indica che questo requisito è conforme alle specifiche PIV del'FBI [16]. Le procedure per la verifica di compatibilità sono descritte in [17].

I requisiti tecnici minimi per il Dispositivo di acquisizione impronte digitali (single finger) sono indicati nella tabella seguente:

Caratteristiche	Valore minimo richiesto
Tecnologia sensore	Ottica
Area di Acquisizione minima ³	1"x1" (25,4x25,4 mm)
Area di Acquisizione massima	1,5 x 1,6 " (38,1x40,04 mm)
Risoluzione di output	500 dpi \pm 1% (IAFIS IQS*)
Livelli di Grigio	256
Distorsione Geometrica	requisito (IAFIS IQS*)
Range Dinamico minimo	Almeno l'80% delle immagini acquisite devono avere un range dinamico pari a 150 (PIV IQS**)
Risposta alle Frequenze Spaziali	requisito (PIV IQS**)
Rapporto Segnale Rumore	Deviazione Standard dei Livelli di Grigio $\sigma \leq 3,5$ in ogni finestra di 0.25×0.25 situata nell'area di acquisizione, acquisendo un target grigio scuro uniforme e un target grigio chiaro uniforme (PIV IQS**)

Il fornitore del Dispositivo di acquisizione delle impronte digitali deve poter dimostrare la conformità ai requisiti indicati in tabella, mediante il possesso di un certificato di conformità rilasciato da un laboratorio di prova o attraverso la presentazione di documentazione comprovante l'esito positivo delle

³ l'area effettivamente acquisibile dallo scanner e visibile nell'immagine, e non la dimensione fisica della finestra di acquisizione

prove di laboratorio, da ripetere eventualmente in presenza della Stazione Appaltante, eseguite secondo le procedure indicate in [15] e [17].

I dispositivi di acquisizione delle impronte digitali dovranno essere forniti di appositi kit di pulizia per le lenti e/o per le eventuali parti del dispositivo che, se non perfettamente pulite inficino la qualità dell'immagine acquisita.

I dispositivi di acquisizione delle impronte digitali dovranno essere forniti di SDK da utilizzare a supporto dello sviluppo di funzioni di controllo dell'acquisizione e dell'integrazione all'interno di moduli applicativi.

SDK

Caratteristiche dello SDK:

- funzioni richieste: eliminazione delle impronte latenti e dell'effetto alone ("halo effect")
- funzioni opzionali: indicazioni di possibili cause di cattiva qualità della impronta (es. pressione insufficiente, pressione esagerata, posizione sbagliata dovuta a mancata centratura, scorrimento, ecc.).

La qualità dello SDK può essere valutata attraverso l'ampiezza delle funzioni a disposizione e la facilità di integrazione.

5.2.2 Software per la misura della qualità delle impronte

La verifica della qualità delle immagini delle impronte acquisite deve essere effettuata con il software NIST Fingerprint Image Quality (NFIQ) sviluppato e distribuito dal NIST. La descrizione dell'algoritmo è contenuta in [9].

Per essere certi della corretta implementazione del programma è possibile verificare la conformità della specifica installazione del software NIST confrontando i risultati ottenuti con quelli generati dal software originale testato e pubblicato dal NIST nel 2004. E' sufficiente eseguire il programma "NFIQ compliance test" [10].

5.2.3 Software per la scelta del miglior campione di impronta

La scelta della migliore immagine delle impronte digitali da registrare tra quelle acquisite relative a uno stesso dito viene effettuata utilizzando il software di comparazione Bozorth3 del NIST combinato al software MINDTCT. Il modulo MINDICT estrae le minuzie dalle immagini dalle impronte fornite in input e le sottopone per la comparazione al software Bozorth3 che fornisce in output uno *score* che viene utilizzato per la scelta del miglior campione di impronta secondo la procedura descritta al paragrafo 3.2.1.

5.2.4 Software compressione immagine impronte

Il software utilizzato per la compressione WSQ deve essere conforme alle specifiche WSQ Specification, Part I: Requirements and Guidelines [7].

E' opportuno utilizzare software WSQ certificato FBI, con indicazione del numero di riferimento assegnato dalla FBI.

In alternativa il fornitore del software deve dimostrare di avere eseguito positivamente la procedura di conformità consistente nel confronto tra l'output del software offerto con l'output di una implementazione di riferimento sviluppata presso il NIST.

I criteri di confronto e i requisiti di precisione sono contenuti in WSQ Specification, Annex AA: Procedures for Determining Compliance [7]. I riferimenti sono disponibili nel sito del NIST alla pagina http://www.nist.gov/itl/iad/ig/wsq_compliant.cfm.

5.2.5 Software codifica immagine impronte e metadati in formato interoperabile

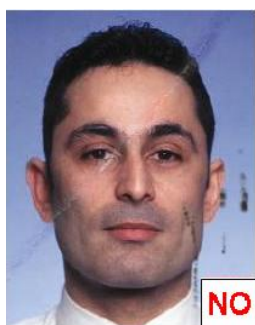
Il software di codifica deve generare un record interoperabile contenente le immagini compresse delle impronte e le informazioni associate, codificate nel formato descritto dalla LDS (Logical Data Structure), DG3, delle specifiche tecniche ICAO [3], basate sullo standard ISO/IEC 19794-5 [4] e CBEFF (Common Biometric Exchange File Format) [11].

6 APPENDICE - Caratteristiche e requisiti della foto

Le norme tecniche contenute in [4] definiscono una serie di caratteristiche e requisiti che le foto devono possedere, al fine di favorire e rendere più efficace le operazioni di riconoscimento.

6.1 Aspetti generali

- Le dimensioni della foto devono essere:
 - Larghezza: 35 mm
 - Altezza: 45 mm.
- L'altezza della foto deve essere tale da assicurare che il volto sia contenuto interamente nell'immagine e centrato rispetto al riquadro dell'immagine.
- La foto deve essere recente, non deve cioè essere stata scattata più di sei mesi prima.
- La foto non deve essere piegata, spillata, presentare scritte o, in generale, essere manomessa o danneggiata.



Danneggiata/macchiata



- La foto deve essere stampata su carta di alta qualità, in modo da ottenere immagini digitalizzate di adeguate qualità e risoluzione.



Scolorita



Punteggiata



6.2 Inquadratura e posa

- Lo sfondo deve essere uniforme di preferenza celeste, beige, marrone chiaro, grigio chiaro oppure bianco, in modo da aumentare il contrasto tra lo sfondo e il volto.

- La foto deve mostrare interamente la testa e la sommità delle spalle, in modo che l'altezza del volto occupi tra il 70% e l'80% dell'altezza della foto.



Troppo vicina



Troppo lontana



- La foto deve riportare solo il soggetto. Non sono ammessi altri oggetti e altri soggetti



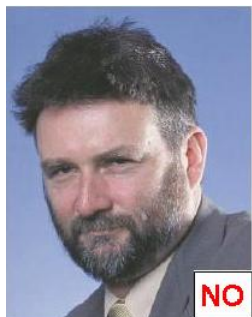
Altro soggetto



Oggetto in evidenza



- Il viso non deve essere inclinato né lateralmente né verticalmente e non sono ammesse posizioni artistiche (cioè, viso girato, spalle alzate, etc..). Inoltre il viso deve essere ripreso frontalmente e lo sguardo deve essere rivolto verso l'obiettivo.



Posizione artistica



Sguardo girato



- La testa deve essere centrata verticalmente.



Testa non centrata



- L'espressione deve essere neutra ed il soggetto deve avere la bocca chiusa e gli occhi ben visibili ed aperti.



Occhi chiusi



6.3 Messa a fuoco, colori, luminosità e contrasto

- Non ci devono essere ombre sul viso o sullo sfondo.



Ombra sulla sfondo



Ombra sul viso



- La foto deve essere a fuoco e il volto chiaramente distinguibile.



Sfocata



- Non devono essere presenti effetti di sovraesposizione/o sottoesposizione.



Troppo scura



Troppo chiara



- La profondità di campo deve essere tale da mostrare chiaramente sia la parte frontale del viso (dalla fronte al mento) sia entrambi i lati del volto (da orecchio ad orecchio).
- Non sono ammesse foto che presentino riflessi ed effetti dovuti a flash o ad altre fonti di illuminazione.



Occhi rossi



Riflesso del flash



- La foto deve avere un contrasto e una luminosità appropriate in modo che siano ben definite le caratteristiche del viso e che si abbia una risoluzione ottimale dei lineamenti e delle parti del viso utilizzati come riferimento in fase di riconoscimento.

- La foto deve essere a colori, e questi devono essere naturali. Non sono ammesse foto con colorazioni diverse da quelle reali.



Colore innaturale



- Lo sfondo deve essere uniformemente illuminato.

6.4 Ornamenti, occhiali e coperture

- Gli occhi non devono essere coperti da capelli.



Occhi coperti da capelli



- Non sono ammessi copricapo a meno di motivi religiosi, culturali o medici. In ogni caso il volto deve essere mostrato chiaramente.



Indossa il cappello



Indossa il berretto



Faccia coperta



Parte del viso coperta



- Non sono ammessi occhiali con lenti colorate. Le lenti devono essere trasparenti in modo che gli occhi siano ben visibili.



Lenti scure



Riflesso sulle lenti



- La montatura degli occhiali non deve coprire gli occhi.



Montatura pesante



Montatura copre occhi



7 Riferimenti

- [1] Draft Resolution of the Representatives of the Governments of the Member States on common minimum security standards for Member States' national identity cards, 15356/06 JAI 598, approvata dal Consiglio UE in data 4.12.2006
- [2] “Regolamento (CE) n. 2252/2004 del Consiglio relativo alle norme sulle caratteristiche di sicurezza e sugli e-lementi biometrici dei passaporti e dei documenti di viaggio rilasciati dagli Stati membri”
- [3] International Civil Aviation Organization (ICAO), Machine Readable Travel Documents, Doc 9303, Part 3: Official Travel Documents (Cards), Third Edition, 2008
- [4] ISO/IEC 19794-5:2005, Biometric Data Interchange Formats – Part 5: Face Image Data
- [5] ISO/IEC19794-4:2005, Biometric Data Interchange Formats – Part 4: Finger Image Data
- [6] ANSI/NIST-ITL 1-2000 Standard "Data Format for the Interchange of Fingerprint, Facial, Scarmark & Tattoo (SMT) Information" FBI: Wavelet Scalar Quantization (WSQ) – www.itl.nist.gov/iad
- [7] IAFIS-IC-0110 (V3) WSQ Gray-scale Fingerprint Image Compression Specification, dicembre 1997, FBI
- [8] ISO/IEC 15444-1:2004, Information technology -- JPEG 2000 image coding system: Core coding system
- [9] NISTIR 7151, E. Tabassi, C.L. Wilson, C.I. Watson, “Fingerprint Image Quality”, Agosto 2004, NIST
- [10] NISTIR 7300, E. Tabassi “Nist Fingerprint Image Quality (NFIQ) Compliance Test, febbraio 2005, NIST
- [11] NISTIR 6529, Common Biometric Exchange File Format (CBEFF), gennaio 2001, NIST
- [12] A. Alessandroni, M. Ferrara, A. Franco, D. Maio, D. Maltoni e L. Palumbo, "Test compliance ICAO su foto del volto in formato Tokenizzabile", Technical Report, DEIS - University of Bologna, March 2008

- [13] A. Alessandrini, R. Cappelli, M. Ferrara and D. Maltoni, "Definition of Fingerprint Scanner Image Quality Specifications by Operational Quality", in proceedings European Workshop on Biometrics and Identity Management (BIOID 2008), Roskilde, Denmark, pp.29-35, May 2008
- [14] Department of Justice, F.B.I., "Electronic Biometric Transmission Specification", IAFIS-DOC-01078-8.1, November 2008
- [15] Nill N.B., Lepley, M.A. "Test Procedures for Verifying IAFIS Image Quality Requirements for Fingerprint Scanners and Printers, V1.1", MITRE Technical Report MTR 05B0000016R1, September 2008.
- [16] FBI, CJIS Division, "Image Quality Specifications for Single Finger Capture Devices", version 071006, 10 July 2006
Disponibile a: <http://www.fbi.gov/hq/cjisd/iafis/piv/pivspec.pdf>.
- [17] Nill N.B., "Test Procedures for Verifying Image Quality Requirements for Personal Identity Verification (PIV) Single Finger Capture Devices", MITRE Technical Report MTR 060170, Dicembre 2006.
- [18] M. Ferrara, A. Franco, D. Maio and D. Maltoni, "Face Image Conformance to ISO/ICAO standards in Machine Readable Travel Documents", IEEE Transactions on Information Forensics and Security, vol.7, no.4, pp.1204-1213, August 2012.