



**ISO/IEC JTC 1/SC 37 N18**

2002-11-01

**Replaces:**

**ISO/IEC JTC 1/SC 37  
Biometrics**

**Document Type:** National Body Contribution

**Document Title:** DIN Contribution to the Inaugural Meeting of ISO/IEC JTC /SC 37 Plenary

**Document Source:** German National Body

**Project Number:**

**Document Status:** This document is circulated to National Bodies for review and consideration at the SC 37 Plenary meeting on 2002 December 11-13 in Orlando, Florida, USA.

**Action ID:** COM

**Due Date:**

**Distribution:**

**Medium:**

**Disk Serial No:**

**No. of Pages:** 26

### DIN contribution to the inaugural meeting of ISO/IEC JTC 1/SC 37, held in Orlando on 2002-12-11/13

Germany commits to an active participation to the broad field of biometric standardization, of which SC37 will undertake a major and important part.

#### 1. Proposal for Allocation of Domains to JTC 1 SCs

Germany has identified several domains of biometrics related standardization as follows:

- 1 Requirements, Security Services and Guidelines
  - 1.1 Selection of biometric mechanisms and tools
  - 1.2 Requirements for the enrolment and de-enrolment process
  - 1.3 Requirements for the verification process
  - 1.4 Integration of biometric mechanisms and tools into a secure infrastructure
  - 1.5 Requirements for identification
  - 1.6 Guidelines for the use and management of biometric systems
  - 1.7 Application Profiles
  
- 2 Security Techniques and Mechanisms
  - 2.1 Integrity mechanisms for biometric data
  - 2.2 Confidentiality mechanisms for biometric data
  - 2.3 Cryptographic (secured) communications protocols for sensors and verification systems
  - 2.4 Authenticity of biometric data
  
- 3 Security Evaluation Criteria
  - 3.1 Protection profiles for biometric equipment and mechanisms
  - 3.2 Evaluation methods and tools for biometrics
  
- 4 Identification Documents, Cards and Tokens specific Issues
  - 4.1 Exchange protocols for biometrics related personal identification
  - 4.2 Data objects and data elements related to biometrics
  - 4.3 Management and security issues
  - 4.4 Applications based on biometric data conventions and formats
  - 4.5 Logical data structure for Identification Documents and Cards
  - 4.6 Requirements for testing related to identification documents and cards
  
- 5 Generic Biometric Mechanisms
  - 5.1 Standardisation of biometric data formats
  - 5.2 Biometric APIs and its integration into software environments
  - 5.3 Compression methods for biometric data
  - 5.4 Evidence of living entity (together with medical standardisation committee)

For the implementation of Resolution 11 of the 17th JTC 1 Plenary Germany requests to SC 37 to concentrate on the domain as provided by above subclause 5 "Generic Biometric Mechanisms", because the other domains as of subclauses 1 to 4 are interpreted as having been covered by the scopes of SC 17 and SC 27.

## 2. Scope of SC 37

Germany believes that the proposed scope of SC 37, as it reads:

*Scope: Development of generic biometric standards which include common file formats and application program interfaces, as well as related application/implementation profiles, to support interoperability and data interchange between applications and systems.*

almost fits to the above domain as of subclause 5, excepting the words "as well as related application/implementation profiles", which should be removed because they conflict with the scope of SC17.

## 3. Taxonomy

Germany proposes a structure of generic biometrics standards. This structure is based on a presentation of Jim Moore IEC TC 56 originally developed and used the following hierarchical structure which Jim Moore used extensively in his book

Software Engineering Standards: A User's Road Map; ISBN 0-8186-8008-3; IEEE Publications

Also this list of existing and forthcoming standards in biometry can be relatively easily accommodated using the proposed interpretations.

Class	Proposed interpretation for biometrics
Terminology Standard (Definitions and Glossary)	Terminology Standards prescribe the terms, mathematical measures, etc. of biometric methods and their application.
Principle Standards (General Description)	Principle standards provide an overview of biometric systems and technologies defining concepts, dependabilities and rationales.
Element Standards (Definition of Datastructure)	Element standards provide guidelines for the datastructure of biometric systems and systems using biometric methods.
Process Standards (Hard- and Softwareinterfaces)	Process standards consist of management process standards and technical process standards applicable to the development and use of biometric systems and systems using biometric methods. E.g. BioAPI, CBEFF etc.
Methods/Tools Standards (Performance and Security Testing)	Methods and tools consist of the analysis tools and test methods applicable to biometric systems and systems using biometric methods

## 4. Proposal for a new work item

Germany submits the attached draft national standard text "Finger minutiae encoding format and parameters for on-card matching". SC 37 is asked to consider an extract of it for an NP addressing the topic "Biometric data formats and related conventions for feature extraction and matching". That extract consists mainly of the clauses 5 and 6 of the attachment, as they touch generic biometric standardization issues. Card related issues, which are also covered by the attached German standard draft, will not be relevant for the considerations in SC 37 and fall under the development within SC 17.

It is proposed that SC 37 specifies a standard series for the proposed topic "Biometric data formats and related conventions for feature extraction and matching", i.e. beyond the specification of the biometric data structures, conventions for feature extraction and matching should be considered to the extend, they are relevant for achieving interoperability.

Content and structure of biometric data formats should be defined – if appropriate – for different processing levels, i.e.

- raw data formats (image formats)
- feature encoded data.

However, this standardization should be performed in a stepped way, so that the outcoming standards will be usable for different usage environments, e.g. for

- no-card related environments,
- environments with cards used as carrier of biometric data (off-card matching),
- environments with cards supporting match-on-card,

in other words for a spectrum of devices with high processing power and big storage capacity on the one side, and for those with restricted processing and storage capabilities on the other side.

In addition, the impact on and definition of different security levels on the selection and encoding of the biometric data should be considered.

With respect to ranking the biometric types, priority should be given to face, fingerprint and iris. The interchange formats to be specified should be:

- face recognition:
  - image based interchange format
  - feature encoding formats (at a later stage)
- fingerprint:
  - image based interchange format
  - finger pattern interchange format
  - finger minutiae interchange format, taking into account the attached German draft standard beside the relevant American standards
- iris:
  - image based interchange format
  - feature encoding format (at least for on-card matching).

Germany believes that the proposed principle for standardization activities should be pursued by SC37 for all generic biometric standards, so that the standards for any kind of biometric type (recognition of finger, face, iris, behaviour, etc.) will allow their applications to different accompanied technologies, like devices, cards, systems, etc. This kind of standardization would then be helpful to better separate the standardization of the SC 37 standards from those undertaken in other subcommittees like in SC 17 and in SC 27.

**ANNEX: German national draft standard DIN V 66400**



## **DIN V 66400**

### **Finger Minutiae Encoding Format and Parameters for On-Card Matching**

**Chairman: Bruno Struif, FhG-SIT**

**Editor: Dr. Robert Müller, G&D**

**Version 0.8**

**04.09.2002**

# Contents

<b>1</b>	<b>Scope</b> .....	<b>3</b>
<b>2</b>	<b>Normative References</b> .....	<b>3</b>
<b>3</b>	<b>Terms and definitions</b> .....	<b>3</b>
<b>4</b>	<b>Symbols and abbreviated terms</b> .....	<b>5</b>
<b>5</b>	<b>Minutiae description</b> .....	<b>5</b>
5.1	Minutia type .....	5
5.2	Minutia location .....	6
5.2.1	Coordinate System .....	6
5.2.2	Minutia placement on a ridge ending.....	6
5.2.3	Minutia placement on a ridge bifurcation.....	7
5.2.4	Minutia placement on a valley bifurcation.....	7
5.3	Minutia direction .....	7
5.3.1	Angle conventions .....	7
5.3.2	Minutia direction on a ridge ending.....	7
5.3.3	Minutia direction on a ridge bifurcation.....	8
5.3.4	Minutia direction on a valley bifurcation.....	8
5.3.5	Other characteristics .....	9
<b>6</b>	<b>Finger minutiae verification data format</b> .....	<b>9</b>
6.1	Biometric data objects for verification.....	9
6.2	Minutia encoding format.....	10
6.2.1	Normal minutia encoding format.....	10
6.2.2	Compact minutia encoding format.....	10
6.3	Number of minutiae, minutia ordering sequence and truncation .....	11
6.4	Encoding of the VERIFY command data field.....	11
<b>7</b>	<b>Parameters relevant to enrollment, matching, verification decision</b> .....	<b>12</b>
7.1	Enrollment.....	12
7.1.1	Number of minutiae.....	12
7.1.2	Number of required finger presentations .....	12
7.2	Matching.....	12
7.2.1	Matching conditions.....	12
7.2.2	Threshold value.....	13
7.2.3	Retry counter .....	13
<b>8</b>	<b>Biometric Information Template</b> .....	<b>14</b>
8.1	Biometric Type .....	14
8.2	Biometric Type Instance.....	14
8.3	Format Owner .....	14
8.4	Format Type .....	14
8.5	Biometric matching algorithm parameters .....	14
8.5.1	Number of minutiae.....	15
8.5.2	Minutiae order .....	15
<b>9</b>	<b>Security aspects of biometric data presentation to the card</b> .....	<b>17</b>
<b>10</b>	<b>Bibliography</b> .....	<b>17</b>
	<b>Annex A (informative) - Values of parameters</b> .....	<b>18</b>
	<b>Annex B (informative) - Biometric Information Template</b> .....	<b>20</b>
	<b>Annex C (informative) - Example of Command Sequence</b> .....	<b>21</b>
	<b>Annex D (informative) - Usage of biometric verification</b> .....	<b>22</b>

# 1 Scope

This document specifies a format to encode fingerprint features for the purpose of on-card matching. The defined encoding and matching parameters are designed to allow the implementation of applications with high security requirements. The standardized coding allows to implement interoperability between different cards and service systems. The interoperability is based on defining a finger minutiae format which is an appropriate solution for on-card matching. This does not exclude the standardization of fingerprint verification mechanisms based on other encoding strategies. Guidelines and values for matching and decision parameters are also given in this document. Secure messaging functions for the cryptographic protection of the biometric verification data are required but outside the scope of this document.

Only the verification data format is addressed in this specification. Standardized verification data may be accompanied by proprietary data. The specification of the format for the reference data is out of scope of this document.

In addition, aspects of enrollment are addressed. The usage of biometric user verification in relation to knowledge-based user verification is described in Annex C.

## 2 Normative References

The following normative documents contain provisions which, through reference in this text, constitute provisions of this proposal:

- ISO/IEC 7816-4: 1995  
Interindustry commands for interchange  
Revised version: CD ISO/IEC 7816-4: 2002
- ISO/IEC FCD 7816-11: 2002  
Personal verification through biometric methods
- ISO/IEC 15408-1: 1999 Information technology - Security techniques - Evaluation criteria for IT security
- Common Criteria

## 3 Terms and definitions

The following definitions apply in this document for the purpose of format specification and parameter specification for on-card matching.

### **biometric data**

data encoding a feature or features used in biometric verification

### **minutia(e)**

characteristic local point pattern occurring in a fingerprint

*Minutiae resemble points in the ridge pattern, where one or more papillary ridges deviate from an uninterrupted flow. The most common minutiae are ridge endings and ridge bifurcations.*

**friction ridge**

friction ridges - or ridges - present on the skin of the fingers and toes, the palms and soles of the feet, which make contact with an incident surface under normal touch (compare ANSI B10.8)

*On the fingers, the unique patterns formed by the friction ridges make up fingerprints.*

**resolution**

the number of pixels (picture elements) per unit distance in the image of the fingerprint

**ridge bifurcation**

point at which a *friction ridge* splits into two ridges or, alternatively, where two separate *friction ridges* combine into one (ANSI B10.8)

**ridge ending**

point at which a *friction ridge* terminates or, alternatively, begins. A *ridge ending* is surrounded on three sides by valley (ANSI B10.8)

**template**

value field of a constructed data object, defined to give a logical grouping of data objects (definition imported from ISO/IEC 7816-6)

WARNING - The term “template” used in this document should not be confused with a processed biometric data sample.

**valley**

furrow between two friction ridges. It does not make contact with an incident surface under normal touch.

**valley bifurcation**

point at which a *valley* splits into two *valleys* or, alternatively, where two separate *valleys* combine into one

## 4 Symbols and abbreviated terms

The following abbreviations apply for the document:

BER	Basic Encoding Rules
BIT	Biometric Information Template
CC	Cryptographic Checksum
DO	Data Object
FAR	False Acceptance Rate
FRR	False Rejection Rate
ICC	Integrated Circuit Card
IFD	Interface Device
PIN	Personal Identification Number
PV	Plain Value
RFU	Reserved for Future Use
S	Score
SM	Secure Messaging
T	Threshold Value
TLV	Tag-Length-Value

## 5 Minutiae description

The minutiae encoding as a common feature-oriented representation is based on agreement on the fundamental notion for representing a fingerprint. Minutiae are points located at the places in the fingerprint image where friction ridges end or split into two ridges. Describing a fingerprint in terms of the location and direction of these ridge endings and bifurcations provides sufficient information to reliably determine whether the biometric verification data – if authentic presented – stem from the same finger as the biometric reference data.

Besides minutiae matching, there are other methods to compare fingerprint images. The correlation-based approach, pattern-matching, neural networks and pore verification fall into this category. Any other methods beside the minutiae verification, however, are out of scope of this document.

### 5.1 Minutia type

Each minutia point has a *type* associated with it. There are two major types of minutia: *ridge ending* and *ridge bifurcation* (or split point).

There are other types of “points of interest” in the friction ridges that occur much less frequently and are more difficult to define precisely. More complex types of minutiae are usually a combination of the basic types defined above. Some points are neither a ridge ending nor a bifurcation. This standard defines therefore additionally a type named “*other*” (compare ANSI B10.8). Therefore, the following types are distinguished:

- *ridge ending* respective *valley bifurcation*
- *ridge bifurcation*
- *other*.

A ridge ending may – alternatively – be regarded as a *valley bifurcation* depending on the method to determine its position (see below). The format type of the biometric information template (see Annex B) indicates the use of ridge endings or valley bifurcations.

## 5.2 Minutia location

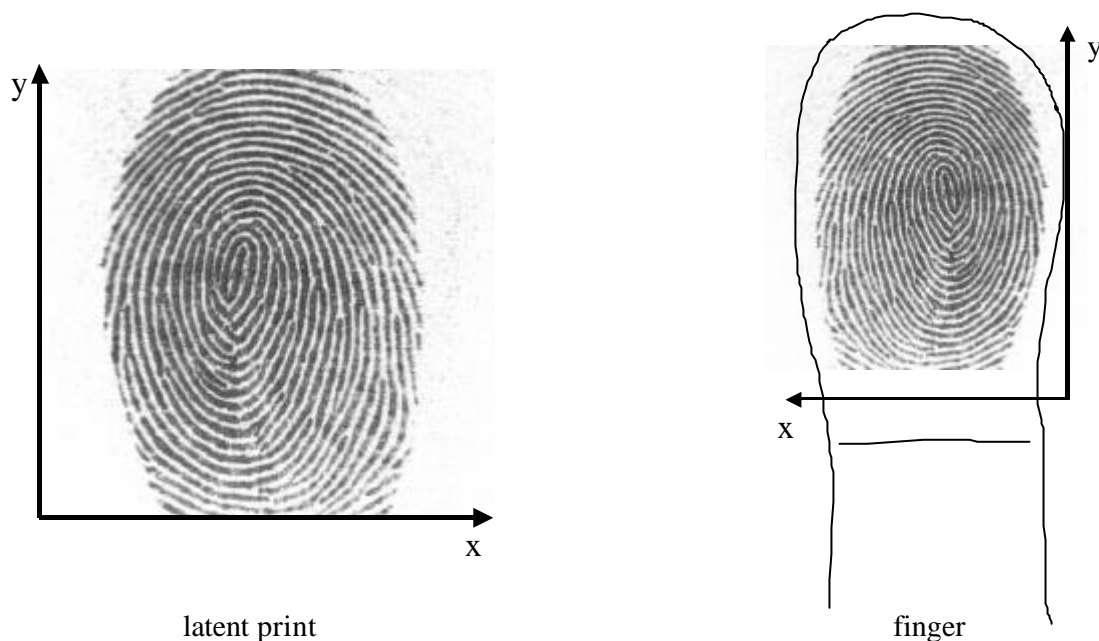
The minutia location is represented by its horizontal and vertical position.

### 5.2.1 Coordinate System

The coordinate system used to express the position of the minutia points of a fingerprint shall be a Cartesian coordinate system. Points shall be represented by their X and Y coordinates, where X is increasing to the right and Y is increasing upward (in the pointing direction of the finger), when viewing on a latent print of the finger (see Figure 1). Note that this is in agreement with typical mathematical graphing practice, but the direction of the Y-axis is the opposite of most imaging and image processing use. When viewing on the finger, X increases from right to left as shown in Figure 1. All X and Y values are non-negative. The X and Y coordinates of the minutia points shall be in metric units. The granularity is one bit per one hundredth of a millimeter in the normal format and one tenth of a millimeter in the compact format:

1 unit =  $10^{-2}$  mm (normal format) or  $10^{-1}$  mm (compact format)

Fingerprint sensors with different spatial resolutions can be used.



**Figure 1 - Coordinate system on a fingerprint**

### 5.2.2 Minutia placement on a ridge ending

The minutia point for a ridge ending shall be defined as the center point of the ending ridge. If the ridges in the digital fingerprint image were thinned down to a single-pixel-wide skeleton, the position of the minutia would be the coordinates of the skeleton point with only one neighbor pixel belonging to the skeleton (see Figure 2).

### 5.2.3 Minutia placement on a ridge bifurcation

The minutia point for a ridge bifurcation shall be defined as the center point of the bifurcating ridge. If the ridges in the digital fingerprint image were thinned down to a single-pixel-wide skeleton, the position of the minutia would be the coordinates of the skeleton point with the following property: Within the eight points that are connected to the minutia point, there have to be six changes from points belonging to the background to points belonging to the skeleton or the other way around (see Figure 3).

### 5.2.4 Minutia placement on a valley bifurcation

The minutia point for a valley bifurcation shall be defined as the center point of the bifurcating valley. If the valleys in the digital fingerprint image were thinned down to a single-pixel-wide skeleton, the position of the minutia would be the coordinates of the skeleton point with the following property: Within the eight points that are connected to the minutia point, there have to be six changes from points belonging to the background to points belonging to the skeleton or the other way around (see Figure 4).

## 5.3 Minutia direction

### 5.3.1 Angle conventions

The angle  $\theta$  of a minutia is scaled to fit to the required granularity (less or equal  $2^8$ ) and to make best use of the coding space of a single byte. The upper bound value 256 is therefore equivalent to the angle  $2\pi$  (or  $360^\circ$ ), that means one bit is equivalent to  $2\pi/256$  (or  $360^\circ/256 = 1,40625^\circ$ ). The angle is measured increasing counterclockwise starting from the horizontal axis to the right.

### 5.3.2 Minutia direction on a ridge ending

The direction of a ridge end is defined as the angle, a tangent to the ending ridge encompasses with the horizontal axis to the right (see Figure 2). Ridge endings are not used in conjunction with valley bifurcations within the same template.

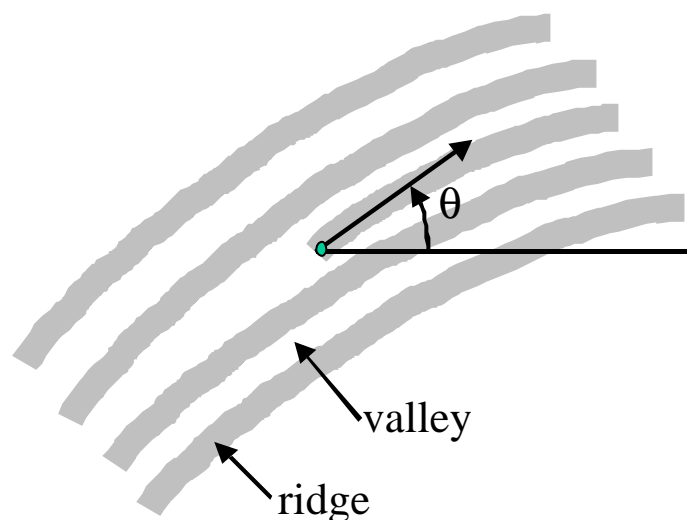


Figure 2 - Location and direction of a ridge end

NOTE - Without loss of generality, gray pixels represent ridges while white pixels represent valleys in the illustration. Whether ridges or valleys correspond to dark or light pixels in a digital fingerprint image depends on the sensor hardware and image processing software.

### 5.3.3 Minutia direction on a ridge bifurcation

A ridge bifurcation has three arms of ridges meeting in one point. Two ridges encompass an acute angle. The tangent to the uppermost ridge lying opposite of the enclosed valley defines the direction of a ridge bifurcation. The direction is again measured as the angle the tangent forms with the horizontal axis to the right (see Figure 3).

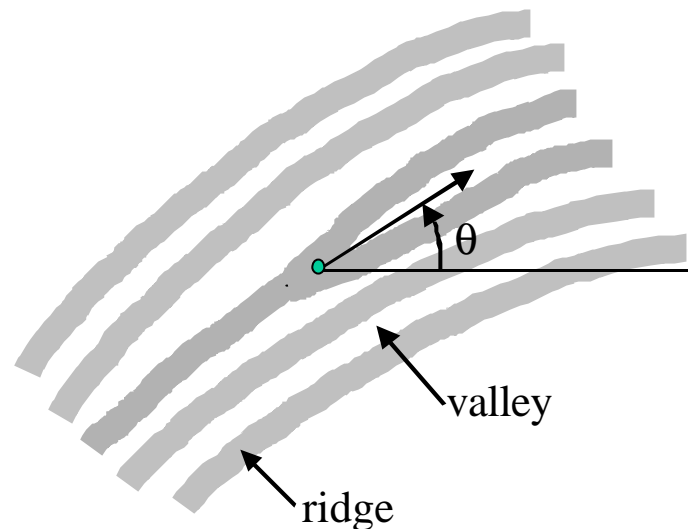


Figure 3 - Location and direction of a ridge bifurcation

### 5.3.4 Minutia direction on a valley bifurcation

A valley bifurcation has three arms of valleys meeting in one point. Two valleys encompass an acute angle. The tangent to the uppermost valley lying opposite of the enclosed ridge defines the direction of a valley bifurcation. The direction is again measured as the angle the tangent forms with the horizontal axis to the right (see Figure 4).

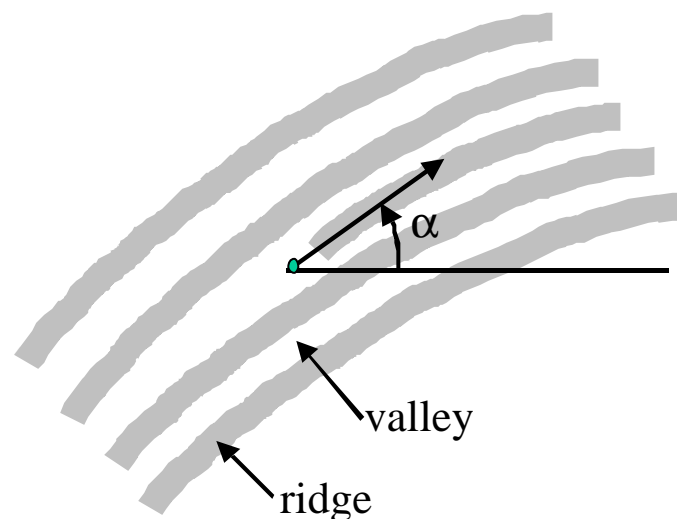


Figure 4 - Location and direction of a valley bifurcation

### 5.3.5 Other characteristics

The encoding of other minutia characteristics, such as minutia quality, is not useful in an interoperable environment.

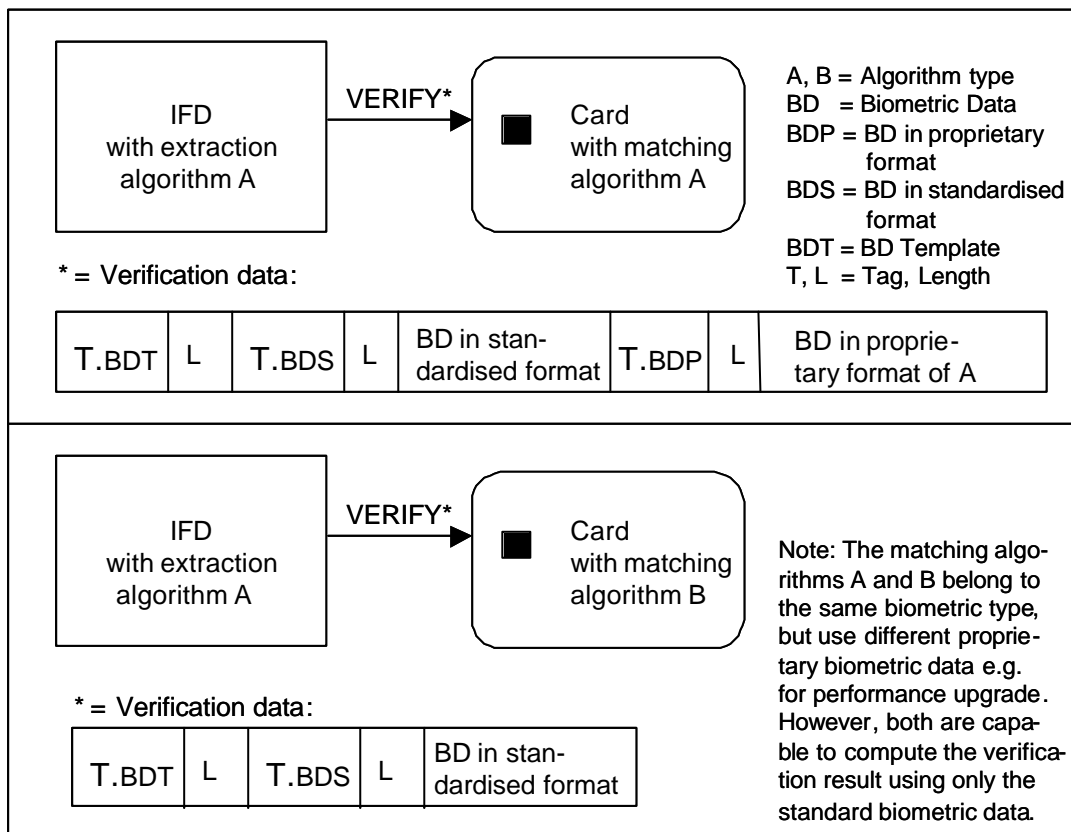
## 6 Finger minutiae verification data format

### 6.1 Biometric data objects for verification

In ISO/IEC 7816-11, the usage of

- standardized biometric data,
- proprietary biometric data and
- standardized biometric data in combination with proprietary biometric data

is outlined. This document specifies the standardized biometric data for fingerprint minutiae encoding, allowing also its use in combination of proprietary data as shown in Figure 5.



**Figure 5 - Usage of standardized and proprietary biometric data (Source: ISO/IEC 7816-11)**

The biometric data objects as described in ISO/IEC 7816-11 are shown in Table 1.

**Table 1 — Biometric data DOs (Source: ISO/IEC 7816-11)**

Tag	L	Value
'5F2E'	x	Biometric data
'7F2E'	x	Biometric data template
		DOs which may be embedded in the biometric data template
		'5F2E' x Biometric data
		'81' / 'A1' x Standard biometric data (primitive / constructed)
		'82' / 'A2' x Proprietary biometric data (primitive / constructed)

In this document the structure of the standard biometric data for fingerprint verification based on minutiae encoding is described.

## 6.2 Minutia encoding format

This document defines two encoding formats for minutiae, the normal encoding format and the compact encoding format.

### 6.2.1 Normal minutia encoding format

With the normal format, a minutia is encoded in 5 bytes (see Table 2):

- minutia type  $t$  (2 bits): 00 = other, 01 = ridge ending respective valley bifurcation, 10 = ridge bifurcation, other values RFU
- coordinate  $x$  (14 bits), unit =  $10^{-2}$  mm
- RFU (2 bits), default value: 00
- coordinate  $y$  (14 bits), unit =  $10^{-2}$  mm
- angle  $\theta$  (8 bits), unit =  $2\pi/256$

**Table 2 — Normal minutia encoding format**

type $t$	x coordinate	RFU	y coordinate	angle $\theta$
	2 bytes		2 bytes	1 byte

### 6.2.2 Compact minutia encoding format

With the compact format, only 3 bytes are used per minutia (see Table 3). This reduction of memory space is only possible at the cost of a reduction in resolution of coordinates and angle.

- coordinate  $x$  (8 bits), unit =  $10^{-1}$  mm
- coordinate  $y$  (8 bits), unit =  $10^{-1}$  mm
- minutia type  $t$  (2 bits): same coding as with the normal format
- angle  $\theta$  (6 bits), unit =  $2\pi/64$

**Table 3 — Compact minutia encoding format**

x coordinate	y coordinate	type t	angle $\theta$
1 byte	1 byte	1 byte	

Note that the maximum value for the x and y coordinate is 25.6mm with the compact format.

### 6.3 Number of minutiae, minutia ordering sequence and truncation

The verification data according to this standard consist of n minutia encoding shown in Table 2 (or alternatively Table 3). The number n depends on

- the minimum number of minutiae required according to the security level (see Annex A)
- the maximum number of minutiae accepted by a specific card e.g. due to buffer restrictions and computing capabilities.

The maximum number of minutiae accepted is therefore an implementation dependent value and shall be indicated in the Biometric Information Template, if the default value is not used (see clause 8 and Annex A).

A card may also require a special ordering of the minutiae presented in the biometric verification data. The ordering scheme shall be indicated in the Biometric Information Template, if the default value is not used (see clause 8).

If the number of minutiae exceeds the maximum number processible by a card, truncation is necessary. The truncation is processed by peeling off minutiae from the convex hull of the minutiae set and before sorting into the order required by the card.

### 6.4 Encoding of the VERIFY command data field

Since minutiae verification data belong to the group of “public verification data” (see clause 9), the verification data shall be protected by secure messaging (SM). The SM-DOs relevant in this case are shown in Table 4 (see also ISO/IEC 7816-4).

**Table 4— SM Data Objects (subset)**

Tag	Meaning
‘81’	Plain Value (PV)
‘8E’	Cryptographic Checksum (CC)
‘99’	Status Bytes

The command data field of the VERIFY command has therefore a general structure as shown in Figure 5.

DO Plain Value			DO Cryptographic Checksum		
T	L	PV	T	L	CC
'81'	variable	Biometric verification data or Biometric verification DOs	'8E'	'04'	Cryptographic Checksum

**Figure 5 - DO sequence in the data field of the VERIFY command**

Whether the PV consists only of the standardised minutia encoding or whether DOs according to table 1 are present shall be indicated with the TLV indication flag of the instruction code (INS byte of the command header, see revised ISO/IEC 7816-4).

If the length of the command data field is greater than 254 byte, command chaining shall be applied.

## **7 Parameters relevant to enrollment, matching, verification decision**

### **7.1 Enrollment**

#### **7.1.1 Number of minutiae**

The number of minutiae is a security sensitive parameter and depending on the security policy of the application. Persons, who do not meet the minimum required number for enrollment, cannot be enrolled. The maximum number of minutiae for the reference data is implementation dependent (see Annex A).

#### **7.1.2 Number of required finger presentations**

The number of required finger presentations during an enrollment process is enrollment system dependent.

### **7.2 Matching**

The verification data is subject to translation (in x- and y-direction), rotation (deviation of the orientation) and distortion. Matching also has to take into account components or factors like FAR/FRR.

#### **7.2.1 Matching conditions**

Result of the matching process is a score, which may denote the number of matching minutiae or any other appropriate value.

In interoperability tests, it may be verified, whether different implementations of the matching algorithm meet a required FAR/FRR e.g. in relation to the strength of function for the respective application.

If minutia types are taken into account in the matching process, then the different types match according to Table 5.

**Table 5 – Minutia type matching**

Type of verification minutia	Match with type of reference minutia
00	00, 01, 02
01	00, 01
02	00, 02
00 = other 01 = ridge ending / valley bifurcation, see note 02 = ridge bifurcation	

NOTE – Whether ridge ending or valley bifurcation is meant, depends on the format type.

### 7.2.2 Threshold value

A verification decision result is positive (i.e. user verification successful), if the score  $S$  as matching result is greater or equal than the required threshold value  $T$ :

$$S \geq T$$

The threshold value depends on several factors or components such as

- Required False Acceptance Rate FAR
- Required False Rejection Rate FRR
- Matching conditions, see 7.2.1
- The amount of minutiae enrolled
- The amount of minutiae presented
- Strength of function.

In Annex A, an example for the computation of  $T$  is given.

### 7.2.3 Retry counter

For On-card matching, a retry counter (which is decremented by subsequent negative verifications and set to its initial value by positive verification) has to be implemented in order to limit the number of trials. The following aspects have impact on the initial value:

- experience of the user
- environmental conditions (e.g. construction of sensor embedding and finger placement)
- quality of verification data
- strength of function

If the retry counter has reached the value 0, then the respective biometric verification method is blocked. Resetting the retry counter to its initial value is possible, if supported, e.g. by using the RESET RETRY COUNTER command (see ISO/IEC 7816-4) with a resetting code (8 digits).

## 8 Biometric Information Template

The Biometric Information Template contains public information about the required biometric verification data and the matching algorithm in the card. A GET DATA command usually precedes the VERIFY command to read the Biometric Information Template. The GET DATA command is optional and the information may also be implicitly known by the interface device or outside world. The Biometric Information Template (coding see Annex B) includes the following items:

- biometric type
- biometric type instance
- format owner
- format type
- biometric matching algorithm parameters as defined in 8.5

### 8.1 Biometric Type

The biometric type indicates the type of biometric technology: fingerprint.

### 8.2 Biometric Type Instance

The biometric type instance, if present, specifies the enrolled finger, e.g. right pointer finger or right thumb.

### 8.3 Format Owner

The format owner of the format specified in this standard is DIN. The value assigned by IBIA (see [www.ibia.org](http://www.ibia.org)) is (to be inserted).

### 8.4 Format Type

The format type denotes one of the fingerprint minutiae formats according to DIN 66400, see Table 6.

**Table 6 — Format types**

<b>Format Type</b>	<b>Meaning</b>
‘0801’	normal format, ridge endings, ridge bifurcations
‘0802’	normal format, valley bifurcations, ridge bifurcations
‘0804’	compact format, ridge endings, ridge bifurcations
‘0808’	compact format, valley bifurcations, ridge bifurcations

NOTE – Format owner and type may change, if the content of this standard is covered by an international standard.

### 8.5 Biometric matching algorithm parameters

Biometric matching algorithm parameters are used to indicate implementation specific values to be observed by the outside world when computing and structuring the biometric verifica-

tion data. They can be encoded as DOs embedded in a biometric matching parameter template (see Annex B).

### 8.5.1 Number of minutiae

For the indication of the minimum and maximum value of minutiae expected by the card the DO Number of minutiae as shown in Table 7 shall be used.

**Table 7 – DO Number of minutiae**

Tag	L	Value
'81'	2	min (1 byte, binary coding)    max (1 byte, binary coding)

If this DO is not present in the BIT, the default values apply (see Annex B).

### 8.5.2 Minutiae order

For the indication of the ordering scheme for minutiae, the DO Minutiae order as shown in Table 8 shall be used.

**Table 8 – DO Minutiae order**

Tag	L	Value
'82'	1	see Table 9

**Table 9 – Values of DO Minutiae order**

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	0	0	0	0	0	no ordering required (default value)
						0	1	ordered ascending
						1	0	ordered descending
			0	0	1			Cartesian x-y, see note 1
			0	1	0			Cartesian y-x
			0	1	1			Angle, see note 2
			1	0	0			Polar, root = center of mass
x	x	x						000, other values are RFU

NOTES –

1. Ordered by ascending/descending x-coordinate, if equal by ascending/descending y-coordinate (first x, then y)
2. The angle represents the orientation of the minutia.

### Detailed description of minutiae ordering

The following description defines the ordering procedure in detail to avoid misunderstandings or misinterpretations.

### **Ordered ascending**

Ordered ascending means, that the ordered sequence begins with the minutia from the original minutiae set, that has the smallest value of the indicated item. The value of this item increases with every successive minutia to the maximum value in the last minutia of the ordered sequence.

### **Ordered descending**

Ordered descending means, that the ordered sequence begins with the minutia from the original minutiae set, that has the largest value of the indicated item. The value of this item decreases with every successive minutia to the minimum value in the last minutia of the ordered sequence.

### **Cartesian x-y**

Cartesian x-y stands for an ordering scheme, where first the x-coordinate is compared and used for ordering. When ordering by ascending cartesian x-y coordinates, the minutia with minimum x-coordinate becomes the first minutia in the ordered sequence. The minutia with the second smallest x-coordinate becomes the second minutia in the ordered sequence. This process continues until the minutia with maximum x-value becomes the last minutia in the ordered sequence. If the x-coordinates in two or more minutiae are equal, the y-coordinate is compared for ordering.

### **Cartesian y-x**

Cartesian y-x stand for an ordering scheme, where first the y-coordinate is compared and used for ordering. If the y-coordinates in two or more minutiae are equal, the x-coordinate is compared for ordering.

### **Angle**

Sorting a minutiae list by angle is done as follows. As defined in a previous section the angle of a minutia begins with value 0 to the right horizontal axis and increases counterclockwise. When ordering by increasing angle, the minutia with the minimum angle value in the ordered sequence becomes the first minutia in the ordered sequence. The minutia with the second smallest angle value becomes the second minutia in the ordered sequence. This process continues until the last minutia in the ordered sequence is defined as the minutia with maximum angle value. No rules for subordering are defined, if the angle values in two or more minutiae are equal. Any possible ordering sequence of the minutiae with the same angle value is legal in this case.

### **Polar**

Polar is an ordering sequence by ascending or descending polar coordinates. First of all, a virtual coordinate root is defined as the center of mass of all minutiae. The polar coordinates of every minutiae are computed as the relative distance and angle to this root coordinate. Without loss of generality, the process of ascending ordering with polar coordinates is described. The minutia with minimum distance to the root becomes the first minutia in the ordered sequence. The minutia with the second smallest distance to the root becomes the second minutia in the ordered sequence. This process continues until the minutia with maximum distance to the root becomes the last minutia in the ordered sequence. If the root-distance of two minutiae or more is equal, the angle of these minutiae is compared. The minutia with the smallest relative angle value becomes the next minutia in the ordered sequence.

#### **NOTE –**

To compute the position of the center of mass of a list of minutiae, the minutiae are considered as objects in a two-dimensional plane acting together as a single entity. The location of the centre of mass can be calculated if

the mass  $m_i$  and location  $(x_i, y_i)$  of each component is known. By definition the centre of mass is located at  $(x_{com}, y_{com})$  where

$$x_{com} = (m_1 x_1 + m_2 x_2 + \dots) / (m_1 + m_2 + \dots)$$
$$y_{com} = (m_1 y_1 + m_2 y_2 + \dots) / (m_1 + m_2 + \dots)$$

In the case of a minutiae list, all minutiae are considered equally weighted, which reduces the computation to (assume  $n$  minutiae).

$$x_{cm} = (x_1 + x_2 + \dots + x_n) / n$$
$$y_{cm} = (y_1 + y_2 + \dots + y_n) / n$$

## 9 Security aspects of biometric data presentation to the card

Fingerprints are left everywhere and therefore this kind of biometric data are considered to be public. An attacker may succeed in getting a good fingerprint of a person, derive from them the biometric verification data and present it to the stolen card of the respective person. To avoid this kind of attack and also replay attacks of data used in a previous verification process, a trusted path between card and service system is required. Such a trusted path is achieved by cryptographic means, e.g. using secure messaging according to ISO/IEC 7816-4/11. The specification of those secure messaging functions is usually application dependent and outside the scope of this document.

## 10 Bibliography

- ANSI B10.8 – Finger Minutiae Extraction and Format Standard for One-to-One Matching, 2001
- ANSI/NIST ITL 1-2000 „Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo (SMT) Information” (NIST Special Publication 500-245)
- NISTIR 6529, “Common Biometric Exchange File Format (CBEFF)”: 2001, 3. January (new version under development)
- German ordinance for electronic signature (Signaturverordnung - SigV)  
Bonn, 16.11.2001, Bundesgesetzblatt Jahrgang 2001 Teil I Nr. 59, 21.11.2001
- A. Jain, S. Pankanti: „Fingerprint Classification and Matching“, Massachusetts State University,
- S. Pankanti, S. Prabhakar, A. Jain: „On the Individuality of Fingerprints“, Massachusetts State University, 2002

## **Annex A (informative) - Values of parameters**

### **A.1 Number of minutiae**

The recommended minimum number of minutiae required for enrollment is 16 and for verification is 12. The strength of function (see note at the end of this clause) may have impact on these values.

The maximum number of minutiae to be sent to a card is implementation dependent and related to

- transmission time
- memory resources
- execution time
- security aspects

The recommended maximum value for enrollment and verification is 60. It is up to the extraction device to limit the number of minutiae sent to the card to 60 or the indicated value (see 8.5.1).

NOTE:

In the Common Criteria, the following definitions are given:

Strength of Function (SOF) – A qualification of a Target of Evaluation (TOE) security function expressing the minimum efforts assumed to defeat its expected security behaviour by directly attacking its underlying security mechanisms

SOF-basic – A level of TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.

SOF-medium - A level of TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.

SOF-high - A level of TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organised breach of TOE security by attackers possessing a high attack potential.

### **A.2 Initial value of the retry counter**

The recommended initial value lies in the range of 5 and 15. The security policy of the application provider and the required strength of function have impact on the possible range and the value applied.

### **A.3 Threshold value**

The treatment of the threshold value is dependent on the implemented matching strategy. In the following an example of the calculation of a threshold value is presented.

The threshold value T considered in this example is a dynamic value to be calculated for each verification process and depends on

- Ar: amount of minutiae in the reference data
- Av: amount of minutiae in the verification data
- Avmin: minimum amount of minutiae required in the verification data
- Avmax: maximum amount of minutiae in the verification data relevant for threshold computation
- Tmin: minimum threshold value, which denotes the minimum amount of minutiae to be matched for positive verification
- Tmax: maximum threshold value, which denotes the maximum required amount of minutiae to be matched for positive verification

T is computed as follows:

$$T = T_{min} + (A_c - A_{vmin}) * (T_{max} - T_{min}) / (A_{vmax} - A_{vmin})$$

with

$$A_c = qA_r + (1 - q)A_v,$$

whereby Ac is the calculated amount of minutiae and the qualifier q the weight for Ar and Av

and

Avmin = min. amount of minutiae to be presented in a verification process

Avmax = max. amount of minutiae considered relevant in a verification process.

The values of Tmax, Tmin, Avmax, Avmin and q chosen for this example are shown in Table A.1.

**Table A.1 – Values for threshold computation (example)**

Qualifier q	Tmin	Tmax	Avmin	Avmax
0.66	6	12	12	60

The values in Table A.1 together with the above formula have the following meaning:

- the amount of the reference minutiae have more significance than the amount of the verification minutiae (2/3 to 1/3)
- a score of 4 matching minutiae is generally rejected and leads to a negative verification result ( $S < T$ , Tmin required = 6)
- a score of 5 matching minutiae leads to positive verification ( $S \geq T$ ), if the respective person has a minimum of verification minutiae (12)
- a score of 12 matching minutiae leads in any case to a positive verification (Tmax required = 12).

NOTE – At court, some countries require 12 matching minutiae. However, the application area, the environment conditions and security requirements are different at court and for oncard-matching.

## Annex B (informative) - Biometric Information Template

Structure and coding of the BIT are in compliance with ISO/IEC FCD 7816-11 and its Annex C, which uses the DOs defined in CBEFF.

**Table B.1 — Biometric information data objects in case of on-card matching (example)**

Tag	L	Value			Meaning; Presence		
'7F60'	'1F'	Biometric Information Template (BIT)					
		Tag	L	Value			
		'83'	'01'	'81'	Reference data qualifier for VERIFY or MANAGE SE command; optional		
		'06'	'06'	...	OID of CBEFF standard body, {2 16 840 1 101 3}		
		'A1'	'14'	Biometric Header Template			
				Tag	L	Value	Meaning; Presence
				'81'	'01'	'08'	Biometric type ('08' = fingerprint, see ISO/IEC 7816-11), optional
				'82'	'01'	'05'	Biometric subtype ('05' = right pointer finger, see ISO/IEC 7816-11); optional, use with biometric type only
				'87'	'02'	'xxxx'	Format owner DIN; mandatory
				'88'	'02'	'0801'	Format type; mandatory ('0801' = normal format, ridge ending, ridge bifurcation, see Tab. 6)
				'B1'	'04'	'81020C28'	Biometric matching algorithm parameters (min = 12, max = 40 minutiae); optional

## Annex C (informative) – Coding example of commands

Coding example of the GET DATA command/response for retrieving the BIT:

Command-APDU:

CLA	INS	P1-P2	Lc
00	CA	7F60	00

Response APDU:

T.BIT	L.BIT	BIT	SW1-SW2
7F60	1F	830181 0606... A114 810108 820105 8702... 88020801 B10481020C28	9000

Coding example of the VERIFY command/response with secure messaging:

Command-APDU:

CLA	INS	P1	P2	Lc	T.PV	LPV	T.BD	L.BD	BD	T.CC	L.CC	CC
08	20	00	81	A2	81	819A	5F2E	8196	30 Minutiae (150 bytes)	8E	04	MAC

Response APDU:

T.SB	L.SB	SB	T.CC	L.CC	CC	SW1-SW2
99	02	9000	8E	04	MAC	9000

## **Annex D (informative) - Usage of biometric verification**

### **D.1 General concept**

On successful matching of the biometric verification data with the biometric reference data stored in the card, the card sets the security status to

- “User verification successful” or - more specific -
- “Biometric user verification successful” or – if several several biometric reference data with different qualifier references are used –
- “Biometric user verification with qualifier reference ‘xx’ successful”.

This security status can be referenced in the security attributes of keys and files, e.g.

- usage of the signature key requires as security condition the successful presentation of a PIN or biometric verification data
- read access to a certain file is free, but write access to the respective file is only possible after successful presentation of a PIN or biometric data.

Reference data have usually an identifier, allowing the coexistence of several reference data, e.g. a signature PIN and an authentication service PIN. Also biometric reference data can have an identifier in order to distinguish them from a PIN or to differentiate the usage, e.g. right thumb for protecting the signature key and right pointer finger for the protection of the authentication key.

### **D.2 Relation to knowledge based user verification**

Biometric user verification is an alternative method to knowledge based user verification and usually – if implemented – used in coexistence with it. The reason for the coexistence is that biometric user verification may fail or is not applicable due to certain circumstances, which would lead to a denial of service. A denial of service, however, is in most cases not acceptable both from the viewpoint of the user and the application provider.