INTERNATIONAL STANDARD

ISO/IEC 19794-11

First edition
2013-02-15

Information technology — Biometric data interchange formats —

Part 11: **Signature/sign processed dynamic data**

Technologies de l'information — Formats d'échange de données biométriques —

Partie 11: Données dynamiques traitées de signature/signe

Reference number
ISO/IEC 19794-11:2013(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 19794-11 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology,* Subcommittee SC 37, *Biometrics*.

ISO/IEC 19794 consists of the following parts, under the general title *Information technology — Biometric data interchange formats*:

- *Part 1: Framework*
- *Part 2: Finger minutiae data*
- *Part 3: Finger pattern spectral data*
- *Part 4: Finger image data*
- *Part 5: Face image data*
- *Part 6: Iris image data*
- *Part 7: Signature/sign time series data*
- *Part 8: Finger pattern skeletal data*
- *Part 9: Vascular image data*
- *Part 10: Hand geometry silhouette data*
- *Part 11: Signature/sign processed dynamic data*
- *Part 13: Voice data*
- *Part 14: DNA data*

Introduction

There are several commercial implementations of signature/sign verification based on the analysis of the dynamic features of signing. This part of ISO/IEC 19794 specifies an interchange format using signature/sign dynamic features that can be used to provide signature/sign verification. This data format enables interoperability without compromising any developers' Intellectual Property Rights.

A group of features are identified that are mandatory across all compliant implementations in order to ensure interoperability but the biometric interchange record format also supports proprietary data. The use of proprietary data is regulated in a similar manner to that used in ISO/IEC 19794-7, ensuring that comparable performance is achieved between the mandatory and proprietary features.

The features recorded represent significant dynamic events during the signing process, and thus represent an intelligent compression of the ISO/IEC 19794-7 format. From these other features can be calculated or estimated. Furthermore, using the significant events 19794-7 format can be extrapolated, and therefore other signature/sign feature data can be calculated or estimated.

The biometric interchange record format is a sequence of signature/sign representations, preceded by a general header that is common to all representations. Each signature/sign representation is recorded as a representation header followed by a sequence of Dynamic-event data for each signature/sign dynamic event.

In addition to the Dynamic-event data recorded for each signature/sign dynamic event, additional data is recorded representing overall features of the signature/sign representation. It should be noted that all recorded data for the signature/sign representation is recorded before any transformations are applied (e.g. rotation or time warping). The data recorded is either raw data or derived from the raw data.

This part of ISO/IEC 19794 does not specify the analysis to be undertaken by any particular comparison algorithms. The signature/sign features recorded in the data format can be used for analysis by many different comparison algorithms.

The format described is based on features (segmentation based on dynamic events) instead of sample points as described in ISO/IEC 19794-7.

The format defined in this part of ISO/IEC 19794 has the version number 1.0.

Annex A is normative and is intended to specify elements of conformance testing methodology, test assertions, and and test procedures ass applicable to this part of ISO/IEC 19794.

Annex B is informative and formally specifies the biometric interchange record format using the ASN.1 (see ISO/IEC 8824) notation and the ASN.1 Packed Encoding Rules (see ISO/IEC 8825-2), enabling the use of ASN.1 tools to assist implementation.

Annex C is informative. It gives guidance on the suitability of signature/sign for secure comparison purposes using the features recorded in the biometric interchange record format defined in this part of ISO/IEC 19794. Annex C identifies three indicators of signature/sign suitability: quantity of data, complexity of signature/sign, and consistency of signature/sign. Annex C suggests measurements that can be made in accessing these indicators, but does not quantify suitable measurements or provide any structure for recording the indicators.

Information technology — Biometric data interchange formats —

Part 11:
Signature/sign processed dynamic data

1 Scope

For the purpose of biometric comparison, this part of ISO/IEC 19794 specifies a data interchange format for processed signature/sign behavioural data extracted from a time series, captured using devices such as digitizing tablets, pen-based computing devices, or advanced pen systems.

The data interchange format is generic, in that it may be applied and used in a wide range of application areas where handwritten signs or signature/signs are involved. No application-specific requirements or features are addressed in this part of ISO/IEC 19794.

This part of ISO/IEC 19794 contains definitions of relevant terms, a description of what data is extracted, and a data format for containing the data, together with advice on whether a set of user's signature/sign is suitable for identification purposes using this part of ISO/IEC 19794.

It is advisable that stored and transmitted biometric data is time-stamped and that cryptographic techniques be used to protect their authenticity, integrity, and confidentiality; however, such provisions are beyond the scope of this part of ISO/IEC 19794.

2 Conformance

A biometric data record conforms to this part of ISO/IEC 19794 if it satisfies all of the normative requirements related to:

A) Its data structure, data values and the relationships between its data elements, as specified in Clause 8 of this part of ISO/IEC 19794.

B) The relationship between its data values and the input biometric data from which the biometric data record was generated, as specified in Clause 8 of this part of ISO/IEC 19794.

A system that produces biometric data records is conformant to this part of ISO/IEC 19794 if all biometric data records that it outputs conform to this part of ISO/IEC 19794 (as defined above). A system does not need to be capable of producing biometric data records that cover all possible aspects of this part of ISO/IEC 19794, but only those that are claimed to be supported by the system.

A system that uses biometric data records is conformant to this part of ISO/IEC 19794 if it can read, and use for the purpose intended by that system, all biometric data records that conform to this part of ISO/IEC 19794 (as defined above). A system does not need to be capable of using biometric data records that cover all possible aspects of this part of ISO/IEC 19794, but only those that are claimed to be supported by the system.

3 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 19785-2, *Information technology — Common Biometric Exchange Formats Framework — Part 2: Procedures for the operation of the Biometric Registration Authority*

ISO/IEC 19794-1, *Information technology — Biometric data interchange formats — Part 1: Framework*

4 Terms and definitions

For the purposes of this document the terms and definitions given in ISO/IEC 19794-1 and the following apply.

4.1
dynamic event
either a **pen-up**, **pen-down**, or **turning point** event

4.2
pen-down
event from which on the pen tip is touching the writing plane

4.3
dynamic-event data
data that records pen position, pressure and time for a given signature/sign **dynamic event**

4.4
pen-up
event from which on the pen tip is not touching the writing plane, after a **pen-down** event

4.5
signature/sign representation
data recorded from a single signature/sign

NOTE A **signature/sign representation** always starts with a **pen-down** event and ends with a **pen-up** event, but there can be more **pen-up** and **pen-down** events within the **signature/sign representation**.

4.6
turning point
event from which the sign of the inclination derived from adjacent samples of either X, Y or F channel changes

5 Conventions

5.1 Coordinate system

The coordinate system used to express the pen position shall be a two-dimensional Cartesian coordinate system. The x-axis shall be the horizontal axis of the writing plane, with the x coordinates increasing to the right starting at 0. The y-axis shall be the vertical axis of the writing plane, with y coordinates increasing upwards starting at 0.

5.2 Byte order

The more significant bytes of any multi-byte quantity are stored at lower addresses in memory than (and are transmitted before) less significant bytes.

Within a byte, the bits are numbered from 8 to 1, where bit 8 is the ‘most significant bit’ (MSB) and bit 1 the ‘least significant bit’ (LSB).

5.3 Registered format type identifier

The data records specified in this part of ISO/IEC 19794 may be embedded in a CBEFF- (ISO/IEC 19785-1) compliant biometric information record (BIR). This clause lists the BDB (biometric data block) format owner identifier and the BDB format type identifier that shall be used if embedded in a CBEFF BIR. This identifier is registered with IBIA, the CBEFF Registration Authority (see ISO/IEC 19785-2).

The format owner of the formats defined in ISO/IEC 19794 is ISO/IEC JTC 1/SC 37. The format owner identifier is 257 (0101Hex). Table 1 lists the format type identifier for the format defined in this part of ISO/IEC 19794.

Table 1 — Format type identifiers

CBEFF BDB format type identifier	Short name	Full object identifier
16 (0010_{Hex})	signature-sign-processed-dynamic	{iso(1) registration-authority(1) cbeff(19785) biometric-organization(0) jtc1-sc37(257) bdbs(0) signature-sign-processed-dynamic(16)}

6 Data format relationships

The processed data format described in this part of ISO/IEC 19794 may not be the final format used by dynamic signature/sign analysis algorithms for signature/sign feature analysis. The format is a segmentation based signature data format with sufficient information to derive signature/sign features for a variety of algorithms. Its use is shown in the flowchart in Figure 1.

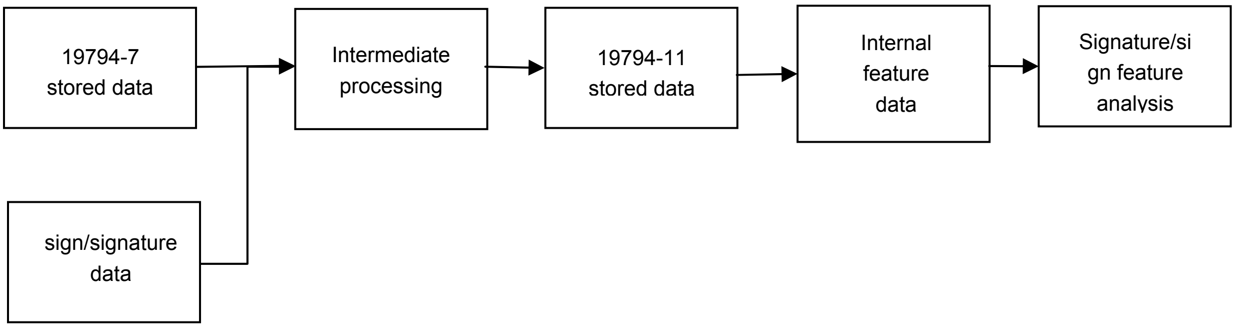

Figure 1 — Data format flowchart

7 Recorded Signature/sign data

7.1 Overview

By recording dynamic-event data at significant signature/sign dynamic events of: Pen-down, Pen-up, and Turning point, these can be combined into larger segments and/or extrapolated into the whole signing sequence for any feature analysis to be applied.

Signature/sign data will be recorded as a sequence of Dynamic-event data for each significant dynamic event, followed by an overall feature data set.

7.2 Dynamic-event data

Whenever a dynamic signature event occurs:

a) Pen-down

b) Pen-up

c) Turning point

The X, Y coordinates, pressure F, time T, and type of event shall be recorded.

7.2.1 Pen-down

Pen-down is an event from which the pen tip is touching on the writing plane. Pen-down is detected when the following change of F channel occurs.

$F_{n-1} = 0$ and $F_n > 0$

7.2.2 Pen-up

Pen-up is an event from which the pen tip is leaving from the writing plane. Pen-up is detected when the following change of F channel occurs.

$F_{n-1} > 0$ and $F_n = 0$

7.2.3 Turning point

A turning point is an event in which the sign of the inclination derived from adjacent samples of either X, Y or F channel changes, where Q denotes either X or Y of F channel. Two types of turning points are defined as follows,

Type-1: Changing from positive to zero or negative, in this type the turning point of Q channel shall satisfy the following conditions,

$$\begin{aligned}&sign(Q_{n-1} - Q_{n-2}) = sign(Q_n - Q_{n-1}) = positive, \quad and\\&sign(Q_{n+2} - Q_{n+1}) = sign(Q_{n+1} - Q_n) = zero \quad or \quad negative\end{aligned}$$

or

$$\begin{aligned}&sign(Q_{n-1} - Q_{n-2}) = sign(Q_n - Q_{n-1}) = zero, \quad and\\&sign(Q_{n+2} - Q_{n+1}) = sign(Q_{n+1} - Q_n) = negative\end{aligned}$$

where Q_n is the turning point of Q channel.

Type-2: Changing from negative to zero or positive, in this type the turning point of Q channel shall satisfy the following conditions,

$$\begin{aligned}&sign(Q_{n-1} - Q_{n-2}) = sign(Q_n - Q_{n-1}) = negative, \quad and\\&sign(Q_{n+2} - Q_{n+1}) = sign(Q_{n+1} - Q_n) = zero \quad or \quad positive\end{aligned}$$

or

$$sign(Q_{n-1} - Q_{n-2}) = sign(Q_n - Q_{n-1}) = zero, \quad and$$
$$sign(Q_{n+2} - Q_{n+1}) = sign(Q_{n+1} - Q_n) = positive$$

where Q_n is the turning point of Q channel.

Before calculating the sign of the inclination derived from adjacent samples, X, Y and F channels should be smoothed using a moving average filter of M points as follows (M shall be an odd number),

$$Q_i = \frac{1}{M} \sum_{m=-\frac{M-1}{2}}^{\frac{M-1}{2}} Q_{i+m}$$

,where Q_i is the i-th sample of Q channel.

The unit of measurement of X and Y is millimetres (mm) and the unit of measurement of F is Newtons (N), and the unit of measurement of T is milliseconds (ms). To restore the actual values, the integer values given in the BDIR body are to be divided by a scaling value given in the Representation Header. By choosing appropriate scaling values, different resolutions can be expressed for several applications.

7.3 Overall features Data

Other parameters that need to be recorded for overall signature/sign dynamic analysis are:

a) Total time

Total time T is defined as the time difference between the first recorded time to the last recorded time of a signature/sign.

The unit of measurement is milliseconds (ms).

To restore the actual value, the integer value given in the Total Time field is to be divided by a T Scaling Value given in the Representation Header.

b) Total number of points aquired TNP (this is a function of time and the sampling time capacities of the digitiser)

The total number of points measured is defined as the total number of coordinates recorded for a signature/sign as an integer.

c) Mean values

X_{mean} – Mean value of X values

Y_{mean} – Mean value of Y values

F_{mean} – Mean value of pressure (F) values

X_{mean}, Y_{mean} and F_{mean} are the arithmetic mean of the X, Y, and F values while the pen is in contact with the digitizer.

The unit of measurement for X_{mean}, and Y_{mean} is millimetres (mm). The unit of measurement of F_{mean} is Newtons (N).

To restore the actual value, the integer value given in the X and Y Mean Values field are to be divided by respectively by X and Y Scaling Value given in the Representation Header.

d) Standard deviation values

S_x – Standard deviation X value

S_y – Standard deviation Y value

S_f – Standard deviation F value

S_x, S_y and S_f are the standard deviation of the X, Y and F values.

Where $S = \sqrt{\dfrac{\sum (v-m)^2}{n}}$

v=values of X , Y, or F

m=arithmetic mean of X, Y or F

n=number of values

The unit of measurement for S_x and S_y is millimetres (mm).

The unit of measurement for S_f is Newtons (N).

To restore the actual value, the integer value given in the X and Y Standard deviation values field are to be divided by respectively by X and Y Scaling Value given in the Representation Header.

e) Correlation coefficient

Rxy – 1000 x (1+correlation coefficient of all (X,Y) data to 3 significant digits). This will always be positive.

Where the correlation coefficient of all XY data $R = \dfrac{n \cdot \sum_i (x_i \cdot y_i) - \sum_i x_i \cdot \sum_i y_i}{\sqrt{\left(n \cdot \sum_i x_i^2 - \left(\sum_i x_i\right)^2\right) \cdot \left(n \cdot \sum_i y_i^2 - \left(\sum_i y_i\right)^2\right)}}$

n = number of values

8 Signature/sign processed dynamic record format

8.1 Overview

This part of ISO/IEC 19794 standard defines the composition of the signature/sign processed dynamic record. Each record shall pertain to a single subject and shall contain a signature/sign processed dynamic record (consisting of one or more representations). The organization of the record format is as follows:

a) A single fixed-length (15-byte) general record header containing information about the overall record; and

b) A representation body containing a single signature/sign processed dynamic record for each signature/sign representation, consisting of:

  i) A variable-length header containing data pertaining to a single signature/sign representation

  ii) Dynamic-event data and overall feature data pertaining to a single signature/sign representation

  iii) Optional extended data (as described in clause 8.7).

8.2 General record header

The structure of the General Record Header shall be defined inTable 2.

Table 2 — Signature/sign processed dynamic data block header

General record header field	Length	Comments
Format Identifier	4 Bytes	The format identifier shall be recorded in four bytes. The format identifier shall consist of three characters "SPD" followed by a zero byte as a NULL string terminator.
Version number	4 Bytes	The number for the version of that part of ISO/IEC 19794 used for constructing the BDIR shall be placed in four bytes. This version number shall consist of three ASCII numerals followed by a zero byte as a NULL string terminator. The first and second character will represent the major version number and the third character will represent the minor revision number. The version number shall be “010” – Version 1 revision 0.
Length of record	4 Bytes	The length (in bytes) of the entire BDIR shall be recorded in four bytes. This count shall be the total length of the BDIR including the general record header and one or more representation records.
Number of representations	2 Bytes	The total number of representation records contained in the BDIR shall be recorded in two bytes. A minimum of one representation is required.
Certification flag	1 byte	The one-byte certification flag shall indicate whether each representation header includes a certification block. Its value shall be 00Hex to indicate that no representation contains a certification block. NOTE The certification flag has been added for upward compatibility with later versions of the format in which representation headers may contain certification blocks.

8.3 Representation header

8.3.1 Overview

The fields of the representation header shall be those defined in Table 3 and Table 6.

Table 3 — Common elements of the representation header

Name	Length	Harmonized text for record format definitions
Representation Length	4 bytes	Denotes the length in bytes of the representation header including the representation header fields.
Capture date and time	9 bytes	The capture date and time field shall indicate when the capture of this representation started in Coordinated Universal Time (UTC). The capture date and time field shall consist of 9 bytes. Its value shall be encoded in the form given in ISO/IEC 19794-1.
Capture device technology identifier	1 byte	The capture device technology ID shall be encoded in one byte. This field shall indicate the class of capture device technology used to acquire the captured biometric sample. A value of 00Hex indicates unknown or unspecified technology. See Table 4 — for the list of possible values.
Capture device vendor identifier	2 bytes	The capture device vendor identifier shall identify the biometric organisation that owns the product that created the BDIR. The capture device algorithm vendor identifier shall be encoded in two bytes carrying a CBEFF biometric organization identifier (registered by IBIA or other approved registration authority). A value of all zeros shall indicate that the capture device vendor is unreported.
Capture device type identifier	2 bytes	The capture device type identifier shall identify the product type that created the BDIR. It shall be assigned by the registered product owner or other approved registration authority. Registered product types shall include all valid combinations of writing tablet and pen as a single product where applicable. A value of all zeros shall indicate that the capture device type is unreported. If the capture device vendor identifier is 0000_{Hex}, then also the capture device type identifier shall be 0000_{Hex}.
Quality record	1 to n bytes	A quality record shall consist of a length field followed by zero or more quality blocks. The length field shall consist of one byte. It shall represent the number of quality blocks as an unsigned integer. Each quality block shall consist of – a quality score, – a quality algorithm vendor identifier, and – a quality algorithm identifier. A quality score should express the predicted comparison performance of a representation. A quality score shall be encoded in one byte as an unsigned integer. Allowed values are – 0 to 100 with higher values indicating better quality, – 255, i.e. ff_{Hex}, for indicating that an attempt to calculate a quality score failed. The quality algorithm vendor identifier shall identify the provider of the quality algorithm. The quality algorithm vendor identifier shall be encoded in two bytes carrying a CBEFF biometric organization identifier (registered by IBIA or other approved registration authority). A value of all zeros shall indicate that the quality algorithm vendor is unreported. The quality algorithm identifier shall identify the vendor's quality algorithm that created the quality score. It shall be assigned by the provider of the quality algorithm or an approved registration authority. The quality algorithm identifier shall be encoded in two bytes. A value of all zeros shall indicate that the quality algorithm is unreported.

8.3.2 Format for capture device technology ID

Table 4 — Capture device technology ID

Name	**Length**	**Class of device technology**
Capture device technology ID	1 byte	Capture device technology ID shall be encoded in 1 byte where: 00_{HEX} is Unknown or unspecified 01_{HEX} is Electromagnetic 02_{HEX} is Semiconductor 04_{HEX} is Special pen with acceleration sensors 08_{HEX} is Special pen with optical sensors All other values are reserved by SC 37 for future use.

8.3.3 Format for quality descriptor

This part of ISO/IEC 19794 shall support a variable number of quality scores per representation, as shown in Figure 2. Each score should be encoded using the 5-byte quality block shown in Table 5 — and the text that follows.

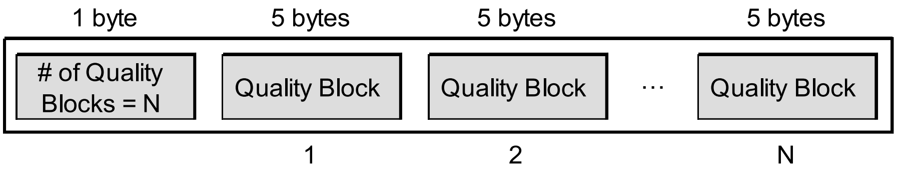

Figure 2 — Support for multiple quality blocks

Table 5 — Structure of quality fields

Description		Length	Valid values	Note
Number of Quality Blocks		1 byte	0 to 255	This field is followed by the number of 5-byte Quality Blocks reflected by its value. A value of zero (0) means that no attempt was made to assign a quality score. In this case, no Quality Blocks are present.
Quality Block	Quality Score	1 byte	0 to 100 255	0: lowest 100: highest 255: failed attempt to assign a quality score
	Quality algorithm vendor ID	2 bytes	0 to FFFF_{Hex}	Quality Algorithm Vendor ID shall be registered with IBIA or other approved registration authority as a CBEFF biometric organization in accordance with CBEFF vendor ID registry procedures in ISO/IEC 19785-2. A value of all zeros shall indicate that the value for this field is unreported.
	Quality algorithm ID	2 bytes	0 to FFFF_{Hex}	Quality Algorithm ID shall be registered with IBIA or other approved registration authority as a CBEFF organization in accordance with CBEFF product registry procedures in ISO/IEC 19785-2. A value of all zeros shall indicate that the value for this field is unreported.

Quality Score – 1 byte – Quality score, as defined in ISO/IEC 29794-1, shall be a quantitative expression of the predicted verification performance of the biometric sample. Valid values for Quality Score are integers between 0 and 100, where higher values indicate better quality. A value of 255 is to handle a special case. An entry of 255 shall indicate a failed attempt to calculate a quality score. This value of Quality Score is harmonized with ISO/IEC 19784-1, where 255 is -1.

NOTE 1 BioAPI, unlike ISO/IEC 19794 uses signed integers.

Quality Algorithm Vendor ID – 2 bytes – To enable the recipient of the quality score to differentiate between quality scores generated by different algorithms, the provider of quality scores shall be uniquely identified by the this two-byte field. This is registered with the IBIA or other approved registration authority.

Quality Algorithm ID – 2 bytes – Specifies an integer product code assigned by the vendor of the quality algorithm. It indicates which of the vendor’s algorithms (and version) was used in the calculation of the quality score and should be within the range 1 to 65535.

NOTE 2 Multiple quality scores calculated by the same algorithm (same vendor ID and algorithm ID) shall not be present in a single representation.

8.3.4 Signature/sign processed dynamic elements of representation header

Table 6 — Signature/sign processed dynamic elements of representation header

Description	Length	Valid values	Notes
X scaling value	2 bytes	Exponent 0x0 to 0x1F Fraction 0x0 to 0x7FF	An X scaling value that shall consist of 2 bytes. The 5 most significant bits of the first byte shall constitute the exponent field *E*, and the remaining 11 bits shall constitute the fraction field *F*. The exponent field *E* contains an unsigned integer representing the base 2 exponent of the scaling value biased by 16. For the exponent, signed integer values in the range from –16 to 15 are allowed. For encoding the exponent value, 16 is to be added in order to get an unsigned value. For decoding the exponent value, 16 is to be subtracted from the contents of *E*. The fraction field *F* contains the bit field that lies, in binary notation, to the right of the binary point of the mantissa of the scaling value. The mantissa shall be scaled to the range 1 ≤ mantissa < 2. The scaling value is calculated by $s=\left(1+\frac{F}{2^{11}}\right).2^{E-16}$ The scaling value has a range from 2^{-16} to $(1+2047/2048)\cdot 2^{15}$, i.e. from 0,0000152587890625 to 65520. Example: s=1 when E=16 and F=0 If unknown the scaling value is set to 00_{HEX}.

Description	Length	Valid values	Notes
Y scaling value	2 bytes	Exponent 0x0 to 0x1F Fraction 0x0 to 0x7FF	A Y scaling value that shall consist of 2 bytes. The 5 most significant bits of the first byte shall constitute the exponent field *E*, and the remaining 11 bits shall constitute the fraction field *F*. The exponent field *E* contains an unsigned integer representing the base 2 exponent of the scaling value biased by 16. For the exponent, signed integer values in the range from –16 to 15 are allowed. For encoding the exponent value, 16 is to be added in order to get an unsigned value. For decoding the exponent value, 16 is to be subtracted from the contents of *E*. The fraction field *F* contains the bit field that lies, in binary notation, to the right of the binary point of the mantissa of the scaling value. The mantissa shall be scaled to the range 1 ≤ mantissa < 2. The scaling value is calculated by $s=\left(1+\frac{F}{2^{11}}\right).2^{E-16}$ The scaling value has a range from 2^{-16} to $(1+2047/2048)\cdot 2^{15}$, i.e. from 0,0000152587890625 to 65520. Example: s=1 when E=16 and F=0 If unknown the scaling value is set to 00_{HEX}.
T scaling value	2 bytes	Exponent 0x0 to 0x1F Fraction 0x0 to 0x7FF	A T scaling value that shall consist of 2 bytes. The 5 most significant bits of the first byte shall constitute the exponent field *E*, and the remaining 11 bits shall constitute the fraction field *F*. The exponent field *E* contains an unsigned integer representing the base 2 exponent of the scaling value biased by 16. For the exponent, signed integer values in the range from –16 to 15 are allowed. For encoding the exponent value, 16 is to be added in order to get an unsigned value. For decoding the exponent value, 16 is to be subtracted from the contents of *E*.

Description	Length	Valid values	Notes
			The fraction field *F* contains the bit field that lies, in binary notation, to the right of the binary point of the mantissa of the scaling value. The mantissa shall be scaled to the range 1 ≤ mantissa < 2. The scaling value is calculated by $s=\left(1+\frac{F}{2^{11}}\right).2^{E-16}$ The scaling value has a range from 2^{-16} to $(1+2047/2048)\cdot 2^{15}$, i.e. from 0,0000152587890625 to 65520. Example: s=1 when E=16 and F=0 If unknown the scaling value is set to 00_{HEX}.
F scaling value	2 bytes	Exponent 0x0 to 0x1F Fraction 0x0 to 0x7FF	An F scaling value that shall consist of 2 bytes. The 5 most significant bits of the first byte shall constitute the exponent field *E*, and the remaining 11 bits shall constitute the fraction field *F*. The exponent field *E* contains an unsigned integer representing the base 2 exponent of the scaling value biased by 16. For the exponent, signed integer values in the range from –16 to 15 are allowed. For encoding the exponent value, 16 is to be added in order to get an unsigned value. For decoding the exponent value, 16 is to be subtracted from the contents of *E*. The fraction field *F* contains the bit field that lies, in binary notation, to the right of the binary point of the mantissa of the scaling value. The mantissa shall be scaled to the range 1 ≤ mantissa < 2. The scaling value is calculated by $s=\left(1+\frac{F}{2^{11}}\right).2^{E-16}$ The scaling value has a range from 2^{-16} to $(1+2047/2048)\cdot 2^{15}$, i.e. from 0,0000152587890625 to 65520. Example: s=1 when E=16 and F=0 If unknown the scaling value is set to 00_{HEX}

Description	Length	Valid values	Notes
Number of Dynamic-event data records	4 bytes	0x1 to 0xFFFFFFFF	Number of Dynamic-event data records shall represent the total number of Dynamic-event data records in the signature/sign representation.
Number of samples for moving average filter	1byte	0x1 to 0xFF	Number of samples for moving average. M shall be an odd number. $Q_i = \frac{1}{M} \sum_{m=-\frac{M-1}{2}}^{\frac{M-1}{2}} Q_{i+m}$

8.4 Representation body

Any dynamic signature/sign event shall result in Dynamic-event data being recorded as described in Table 7. Thus turning points in both X and Y planes are recorded (and if data available, even if the pen is not in contact with the writing plane), pen up and pen down events are recorded, and if pressure is available then turning points in F are optionally recorded.

Table 7 — Dynamic-event data record

Description	Length	Valid values	Notes
X	2 bytes	0x0 to 0xFFFF	X coordinates shall be recorded as 2 bytes. Integer values in the range from -32768 to 32767 are allowed. These values shall be encoded as unsigned integers after adding 32768 to each value. Hence, for non-negative numbers, bit 8 of the most significant byte has the value 1; for negative numbers, bit 8 of the most significant byte has the value 0. For decoding these values, 32768 is to be subtracted from each recorded value.
Y	2 bytes	0x0 to 0xFFFF	Y coordinates shall be recorded as 2 bytes. Integer values in the range from -32768 to 32767 are allowed. These values shall be encoded as unsigned integers after adding 32768 to each value. Hence, for non-negative numbers, bit 8 of the most _significant byte has the value 1; for negative numbers, bit 8 of the most significant byte has the value 0. For decoding these values, 32768 is to be subtracted from each recorded value.
F	2 bytes	0x0 to 0xFFFF	Pressure shall be recoded as 2 bytes. Integer values in the range 0 to 65535 are allowed. These values shall be encoded as unsigned integers.

Description	Length	Valid values	Notes
			If pressure is not measured then the values are set to 0.
T	2 bytes	0x0 to 0xFFFF	Time shall be recorded as 2 bytes. Integer values in the range from 0 to 65535 are allowed. These values shall be encoded as unsigned integers
Type of Event	1 byte	0x0 to 0x1F	Type of Event shall be recorded as 1 byte where: Bit 1 is Pen-up Bit 2 is Pen-down Bit 3 is X turning point Bit 4 is Y turning point Bit 5 is F turning point Bit 6 is Type of X turning point Bit 7 is Type of Y turning point Bit 8 is Type of F turning point When each event happens, it shall be encoded with the value 1. For turning point, types of turning point shall be encoded with the value 0 for type-1 and the value 1 for type-2.

8.5 Overall feature data

Table 8 — Overall feature data

Description	Length	Valid values	Notes
Total time	2 bytes	0x0 to 0xFFFF	Total time shall be recorded as two bytes. Integer values in the range 0 to 65535 are allowed. These values shall be encoded as unsigned integers.
X_{mean}	2 bytes	0x0 to 0xFFFF	Mean X shall be recorded as 2 bytes. Integer values in the range from -32768 to 32767 are allowed. These values shall be encoded as unsigned integers after adding 32768 to each value. Hence, for non-negative numbers, bit 8 of the most significant byte has the value 1; for negative numbers, bit 8 of the most significant byte has the value 0. For decoding these values, 32768 is to be subtracted from each recorded value.

Description	Length	Valid values	Notes
Y_{mean}	2 bytes	0x0 to 0xFFFF	Mean Y shall be recorded as 2 bytes. Integer values in the range from -32768 to 32767 are allowed. These values shall be encoded as unsigned integers after adding 32768 to each value. Hence, for non-negative numbers, bit 8 of the most significant byte has the value 1; for negative numbers, bit 8 of the most significant byte has the value 0. For decoding these values, 32768 is to be subtracted from each recorded value.
F_{mean}	2 bytes	0x0 to 0xFFFF	Mean pressure shall be recorded as 2 bytes. Integer values in the range 0 to 65535 are allowed. These values shall be encoded as unsigned integers
Standard deviation X	2 bytes	0x0 to 0xFFFF	X standard deviation shall be recorded as 2 bytes. Integer values in the range 0 to 65535 are allowed. hese values shall be encoded as unsigned integers.
Standard deviation Y	2 bytes	0x0 to 0xFFFF	Y standard deviation shall be recorded as 2 bytes. Integer values in the range from 0 to 65535 are allowed. These values shall be encoded as unsigned integers
Standard deviation F	2 bytes	0x0 to 0xFFFF	Pressure standard deviation shall be recorded as 2 bytes. Integer values in the range from 0 to 65535 are allowed. These values shall be encoded as unsigned integers
Correlation coefficient	2 bytes	0x1 to 0xFFFF	The correlation coefficient shall be recorded as 2 bytes. Integer values in the range 1 to 65535 are allowed. These values shall be encoded as unsigned integers.

8.6 Extended data

The extended data length field shall indicate the number of contents bytes in the optional extended data field. The length field shall consist of 2 bytes, representing the number of subsequent contents bytes as an unsigned integer. Values in the range 0 to 65535 are allowed.

The optional extended data field allows for inclusion of additional data that may be used by comparison algorithms. The structure of the extended data field is not prescribed by this part of ISO/IEC 19794. If extended data is present and the comparison algorithm does not recognize its format, the algorithm shall ignore it.

NOTE Comparison algorithms claiming to use data blocks conforming to the format defined in this part of ISO/IEC 19794 should be capable of achieving equivalent biometric performance in terms of error rates when processing data blocks without extended data and when processing data blocks with extended data. If extended data is present and the comparison algorithm does not require it, the algorithm shall ignore it.

Annex A
(normative)

Conformance testing methodology

This part of ISO/IEC 19794 specifies a biometric data interchange format for storing, recording, and transmitting one or more signature/sign representations. Each representation is accompanied by modality-specific metadata contained in a header record. This annex establishes tests for checking the correctness of the record.

The objective of this part of ISO/IEC 19794 cannot be completely achieved until biometric products can be tested to determine whether they conform to those specifications. Conforming implementations are a necessary prerequisite for achieving interoperability among implementations; therefore there is a need for a standardised conformance testing methodology, test assertions, and test procedures as applicable to specific modalities addressed by each part of ISO/IEC 19794. The test assertions will cover as much as practical of the ISO/IEC 19794 requirements (covering the most critical features), so that the conformity results produced by the test suites will reflect the real degree of conformity of the implementations to ISO/IEC 19794 data interchange format records. This is the motivation for the development of this conformance testing methodology.

This normative annex is intended to specify elements of conformance testing methodology, test assertions, and test procedures as applicable to this part of ISO/IEC 19794. For this edition of this part of ISO/IEC 19794, the content of this annex will be available as a separate document (Amendment), to supplement this part of ISO/IEC 19794.

Annex B
(informative)

ASN.1 specification of the data format

B.1 Abstract syntax of the signature/sign processed dynamic data encodings

The body of this part of ISO/IEC 19794 specifies the complete bit-level representations of the signature/sign processed dynamic data BDIR format that are suitable for transfer or storage.

It can, however, be useful to define the information content of this format independently of the bit-level representation (its abstract syntax). This enables:

a) different encodings to be used (for example, an XML encoding) where appropriate;

b) different in-core representations to be used, using structures suited for easy processing with the C, C++ or Java programming languages;

c) a wider range of tools to be used in the implementation of these formats;

d) easier in-core representation on machines that do not have a big-endian hardware architecture; and

e) a more easily understood description of the values in the formats.

The abstract syntax is specified in this Annex using ASN.1 (ISO 8824-1 [1]). The signature/sign processed dynamic data standard encodings are obtained by application of the ASN.1 Basic Packed Encoding Rules (BASIC-PER – see ISO 8825-2 [2]), unaligned variant, to the ASN.1 modules given in the clause A.2, including additional PER Encoding Instructions. The resulting encodings are exactly the same as those specified in the body of this part of ISO/IEC 19794.

Using the abstract syntax as the schema, tools can convert between any encoding of the values and in-core representations on any hardware architecture and for any programming language. Tools that convert these specifications to programming language data structures are called ASN.1 compilers, and are supported by run-time routines that will convert between an in-core value and any desired (specified) encoding in the ISO/IEC 8825 multi-part standard (this includes XML encodings). These tools are supported by multiple vendors. In particular, tools that convert between the signature/sign processed dynamic data standard encoding and in-core representations of the values are available for most hardware architectures and most programming languages.

B.2 Signature/sign processed dynamic data format

```
Signature/signSignDynamicFormatModule
      {iso standard 19794 signature/sign-sign-processed-dynamic(11) modules(0)
      version(0)}
      DEFINITIONS
      PER INSTRUCTIONS
      -- This specifies that PER Encoding Instructions are to be applied
      AUTOMATIC TAGS ::=
      BEGIN

Signature/signSignDynamicBlock ::= SEQUENCE {
      header GeneralHeader,
      body   Body  }
```

```
GeneralHeader ::= SEQUENCE {
      formatId               [NULL] IA5String ("SPD"),
      standardVersion              [NULL] IA5String (SIZE (3)),
        -- " 10" (space-one-zero) for this version
      lengthofRecord               [SIZE 32]INTEGER,
      numberofRepresentations      [SIZE 16]INTEGER,
      certificationFlag            [SIZE 8]INTEGER}

Body ::= SEQUENCE {
      representation         RepresentationHeaderValues,
      RepresentationBodyValues}

RepresentationHeaderValues ::= SEQUENCE {
      ReprsentationLength          [SIZE 32] INTEGER (1..MAX)
      captureDateTime              CaptureDateTimeValues,
      captureDeviceTechId          INTEGER (0..255),
      captureDeviceVendId          INTEGER (0..65535),
      captureDeviceTypeId          INTEGER (0..65535),
      qualityRecord                QualityBlockValues,
      certificationRecord          INTEGER (0),
      xchannelScaling              ScalingValue,
      ychannelScaling              ScalingValue,
      tchannelScaling              ScalingValue,
      fchannelScaling              ScalingValue,
      numberofDynamicEvents        [SIZE 32] INTEGER (1..MAX)
      numberofAveragingSamples     INTEGER (1..255)}

CaptureDateTimeValues ::= OCTETSTRING (SIZE (9))

-- The Octet String shall contain the 9 bytes specified in ISO/IEC 19794-1

QualityBlockValues ::= SEQUENCE {
      numberof Qualityblocks [SIZE 8] INTEGER (0..255),
      SEQUENCE OF {
      qualityScore           [SIZE 8] INTEGER (0..100,255),
      qualityalgorithmVendId [SIZE 16] INTEGER (1..65535),
      qualityalgorithmId     [SIZE 16] INTEGER (1..65535)} }

ScalingValue ::= SEQUENCE {
      exponent               INTEGER (-16..15),
      fraction               INTEGER (0..2047)}

RepesentationBodyValues ::= SEQUENCE {
      DynamicEventData,
      FeatureData,
      extendedData [LENGTH 16] OCTET STRING OPTIONAL}

DynamicEventData ::= SEQUENCE {
      xCoordinate            INTEGER (-32768..32767),
      yCoordinate            INTEGER (-32768..32767),
      fValue                 INTEGER (0..65535),
      timeValue              INTEGER (0..65535)
      typeofEvent            [SIZE 8] INTEGER (0..255)}

FeatureData ::=  SEQUENCE {
      totalTime        INTEGER (0..65535),
      meanValues       OverallMeanValues,
      sdValues         StandardDeviation,
      cCoefficient     INTEGER (1  65535) }

OverallMeanValues ::=  SEQUENCE {
      meanX            INTEGER (-32768..32767),
      meanY            INTEGER (-32768..32767),
      meanF            INTEGER (0  65535) }

StandardDeviation ::=  SEQUENCE {
      sdX              INTEGER (0  65535),
      sdY              INTEGER (0  65535),
      sdF              INTEGER (0  65535) }

END
```

Annex C
(informative)

Signature/signs Suitable for use in Authentication

It is the data content of a signature/sign that makes it suitable for authentication. So what are the aspects of a signature/sign that can be measured to ensure suitable data content?

There are three aspects that are known to provide good indicators:

- Quantity of data
- Complexity of signature/sign
- Consistency of signature/sign

C.1 Quantity of Data

Is there sufficient number of digitized coordinates to analyse? This quantity aspect could be related to the resolution of the digitizer but is more importantly related to how quickly the person scribes their signature/sign. If too quick then insufficient coordinates are recorded resulting in insufficient data to analyse. Typically it arises from someone signing with their initials very quickly. Their initials may have sufficient complexity and be very consistent, yet with insufficient numerical data to drive the dynamic signature/sign analysis algorithms. So such signature/signs should be rejected at enrolment. This is a similar restriction to password authentication systems setting a minimum number of digits – say 7 or 8 to attempt to ensure a sufficient level of security.

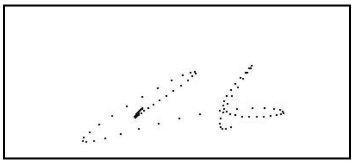

Figure C.1 — Example of a signature/sign that is complex enough but with insufficient quantity of data

Quantity of data as a suitability measurement is easily measured by counting the number of digitized points recorded and ensuring their total is above a minimal acceptable.

C.2 Complexity of Signature/sign

Why are we concerned about the complexity of signature/sign? Although analysing the dynamics of a signature/sign makes forgeries very difficult there is still a need to have sufficient complex data to extend the dynamic possibilities. What does this mean? Complexity of signature/signs can be thought of in a similar way that authentication systems reject users picking simple PINs such as 1234, or 9999 because they are more easily guessed; or passwords having to contain upper and lower case alpha characters and/or the inclusion of numeric and special characters.

So what is complex? Well it is probably easier to describe what is too simple. Everyone would accept that a ‘cross’ is too simple. Even with dynamic analysis such a ‘mark’ or signature/sign is more easily forged and therefore offers little or no security in an authentication system.

What represents complexity in a signature/sign is ‘loops’. It is loops that ensure dynamic diversity. It is loops that create the variability of speed, acceleration, deceleration, vectors and the like. A simple ‘cross’ has none, or only a few pieces of loop data, therefore very little dynamic diversity – insufficient complexity. That is, insufficient complexity to be considered secure in an authentication system. So such signature/signs should be rejected at enrolement.

Again the suitability measurement is easily measured by counting the number of loops recorded and ensuring their total is above a minimal acceptable.

C.3 Consistency of a signature/sign

Why do we want to check for the consistency of a person’s signature/sign? Surely the whole point of any workable signature/sign biometric system is that it copes with a person’s variety of signing. Well yes any workable signature/sign biometric system must cope with the natural variations any person has in signing their signature/sign. However, any biometric signature/sign system should also ensure that the resulting variability analysis does not leave a person’s biometric signature/sign open to exploitation by an impostor. That is, that so much variability lowers the security level to allow a poor forgery to be falsely accepted.

Equally any biometric signature/sign system should also try and enforce enrolment cooperation – or rather reject users that do not cooperate during enrolment. It is clear that someone providing enrolment representations of their signature/sign as ‘fred’, ‘john’, ‘bill’, ‘jack’ should be rejected at the point of enrolment. Such names turned into signature/signs are inconsistent – they have too much variability outside the normal distribution expected in signature/sign variability.

It is ‘normal distribution’ that lies at the heart of establishing the consistency of a signature/sign. Any dynamic feature of a signature/sign follows a normal distribution. Any signature/sign should then have sufficient dynamic features being closely clustered to ensure its uniqueness, providing the opportunity for verification in an authentication system. If too many of the dynamic features being measured and analysed have too much variability, or insufficient clustering, then the signature/sign should be deemed inconsistent or too variable at enrolment. To allow such a signature/sign to go forward to completion of enrolment would open that user up to their signature/sign being exploited by impostors, albeit the biometric system may well cope with the acceptance of their own albeit very variable signature/signs.

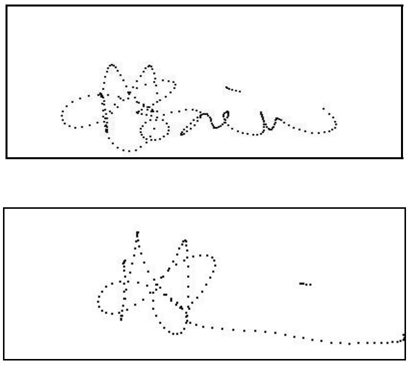

Figure C.2 — Example of the same signature/sign with considerable variability

If there was just one or two considerably variable signature/signs in all the signature/signs offered during enrolment then they could individually be rejected as ‘outliers’. If all or the majority of the representation signature/signs express too much inconsistency then the signature/sign should be rejected as ‘too variable’.

Consistency of signature/sign is the most difficult of quality measurements to determine, because it is all a matter of balance between usability and security. For example, balancing the number of signature/sign representations taken against the time taken to enrol with continuous cooperation from the user. Although a user during enrolment may have the ability to reject a particular representation themselves as being unrepresentative of their ‘norm’, experience in trials shows they rarely do.

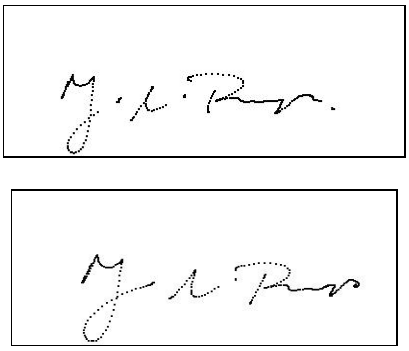

Figure C.3 — Example of Two Quality Signature/signs

Genuine user cooperation is essential to good quality enrolment. Ensuring users understand the need for them to develop a consistent signature/sign with sufficient complexity and data quantity is a significant element of user instruction in any signature/sign biometric system.

Bibliography

[1] ISO/IEC 8824-1, *Information technology — Abstract Syntax Notation One (ASN.1): Specification of basic notation*

[2] ISO/IEC 8825-2, *Information technology — ASN.1 encoding rules: Specification of Packed Encoding Rules (PER)*

[3] ISO/IEC 8825-6, *Information technology — ASN.1 encoding rules: Registration and application of PER encoding instructions*

[4] ISO/IEC 19794-7, *Information technology — Biometric data interchange formats — Part 7: Signature/sign time series data*

ICS 35.040

Price based on 23 pages