Biometric recognition procedures

Requirements and Test Methods

DRAFT

Foreseen as version VdS 3112en : 2010-07 (01)

These guidelines have been agreed upon with the interested public and may be used with immediate effect as base for testing and certification. Up to final publishing of the guidelines changes of these may be anticipated.

Publisher and publishing house: VdS Schadenverhütung GmbH

Amsterdamer Str. 172-174
50735 Köln, Germany
Phone: +49 221 77 66-0, Fax: +49 221 77 66-341

VdS Guidelines for Alarm Systems

Biometric recognition procedures

Requirements and Test Methods

DRAFT

Foreseen as version VdS 3112 : 2010-07 (01)

These guidelines have been agreed upon with the interested public and may be used with immediate effect as base for testing and certification. Up to final publishing of the guidelines changes of these may be anticipated.

Content

1 General

1.1 Scope

These guidelines contain the requirements and test methods for biometric recognition procedures in alarm systems.

These guidelines for security techniques, biometric recognition procedures, requirements and test methods shall be applied for products of intrusion detection techniques, access control and electronic keys which use biometric identification features and contain determinations for the evaluation and testing of biometric features. Further applications are in principle not excluded and are included in these guidelines, if biometric features are applied.

The requirements stipulated in the guidelines for the respective products (e. g. concerning codes that may be distinguished) are transferred by these guidelines and amended by adequate test methods.

These guidelines shall be applied in conjunction with the Guidelines for Intruder Alarm Systems, General Requirements and Test Methods, VdS 2227 and the Guidelines for Alarm Systems, Protection against Environmental Influences, Requirements and Test Methods, VdS 2110. The Guidelines for Fire Prevention and Security Technology, Software, Requirements and Test Methods, VdS 2203, also apply for system components controlled by software.

1.2 Validity

These guidelines for security techniques, biometric recognition procedures, requirements and test methods are valid from 01 July 2009.

2 Normative References

These guidelines contain dated and undated references to other publications. The normative references are cited at the appropriate places in the clauses, the publications listed hereafter. For dated references, subsequent amendments to and revisions of any of these publications apply to these guidelines only when announced by a change of these guidelines. For undated references the latest edition of the publication referred will be applied.

- **VdS 2110** Guidelines for Intruder Alarm Systems, Protection against Environmental Influences, Requirements and Test Methods
- **DIN EN 50130-4** Alarm systems, part 4: Electromagnetic compatibility – product family standard
- **DIN EN 50130-5** Alarm systems, part 5: Environmental test methods
- **EN 60950-1** Information Technology Equipment – Part 1: General Requirements
- **ISO/IEC 19795-1** Information technology – Biometric performance testing and reporting – Part 1: Principles and framework
- **ISO/IEC 19795-2** Information technology – Biometric performance testing and reporting – Part 2: Testing methodologies and for technology and scenario evaluation
- **VdS 2227** Guidelines for Intruder Alarm Systems, General Requirements and Test Methods

- **VdS 2119** Guidelines for intruder alarm systems, ancillary control equipment, requirements
- **VdS 2358** Guidelines for access control systems, requirements
- **VdS 2359** Guidelines for access control systems, test methods
- **VdS 2396** Guidelines for physical security, high security locks for safes and strongrooms, requirements and test methods

3 Terms, definitions and abbreviations

The general terms and definitions are contained in the Guidelines for Intruder Alarm systems, General requirements and test methods, VdS 2227. Additionally the following terms are valid:

Biometric features
The characteristic information that is captured by the biological attributes or properties of a person.

False acceptance rate (FAR)
FAR is the frequency at which a non-authorised person is accepted as authorised. It is calculated as follows:

$$\mathbf{FAR} = \frac{\textbf{Number of successful unauthorised verifications}}{\textbf{Total number of unauthorised verification attempts}}$$

Note: FAR is calculated in proportion 1:1.

False rejection rate (FRR)
FRR is the frequency at which authorised persons are rejected by mistake. It is calculated as follows:

$$\mathbf{FRR} = \frac{\textbf{Number of rejected verification attempts of authorised persons}}{\textbf{Total number of all verification attempts of authorised persons}}$$

Note: FRR is calculated in proportion 1:1

Enrolment (Learning)
Capture of biometric features of a person and following processing and storage of templates as reference sample of this person.

Identification mode
Operation status where a live template is compared with all filed reference templates (1:N – comparison).

Live template
Template which is generated during a recognition procedure.

Reference template
Template which has been generated during the enrolment procedure and which is base for the comparison for the recognition process.

Sample
Information (rough data) of body specific features which is generated by a sensor.

Template
Dataset which is generated of the extracted biometric features of a person via an algorithm. Templates therefore are depending of the generated algorithm.

Verification mode
Operation status at which a live template is compared with a certain reference template (1:1 comparison).

3.1 Abbreviations

The following abbreviations are used in these guidelines:

FAR False acceptance rate

FRR False rejection rate

IFM Identification feature medium

4 Introduction

4.1 General

Characteristic biometric features or properties of a person may be used for the determination of identity. For biometric recognition procedures this is made in an automatic procedure by capturing, processing and evaluation of the captured personal data. This procedure may be divided in different processes.

4.2 Biometric processes

4.2.1 Enrolment

In order to being able to recognise a person on base of its biometric features, these features first have to be captured, processed and stored as reference sample.

The reference template such way formed of the biometric features is stored in a database.

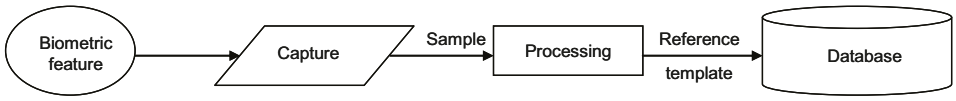

Figure 1: Course of an enrolment

4.2.2 Identification/verification

Same as for the enrolment the biometric features are captured and processed so that a live template may be generated which is compared with a biometric reference template from the enrolment database. As a complete conformity of the live templates with the reference template does not exist, a value of similarity is determined at the comparison of the two templates.

For the verification the live template is compared only with one reference template of the enrolment database which represents the indicated identity. If the value of similarity exceeds the threshold then the verification was successful.

For the identification all reference samples filed in the enrolment database are compared with the live template. That identity is taken for which the comparison has the closest similarity and has exceeded the threshold.

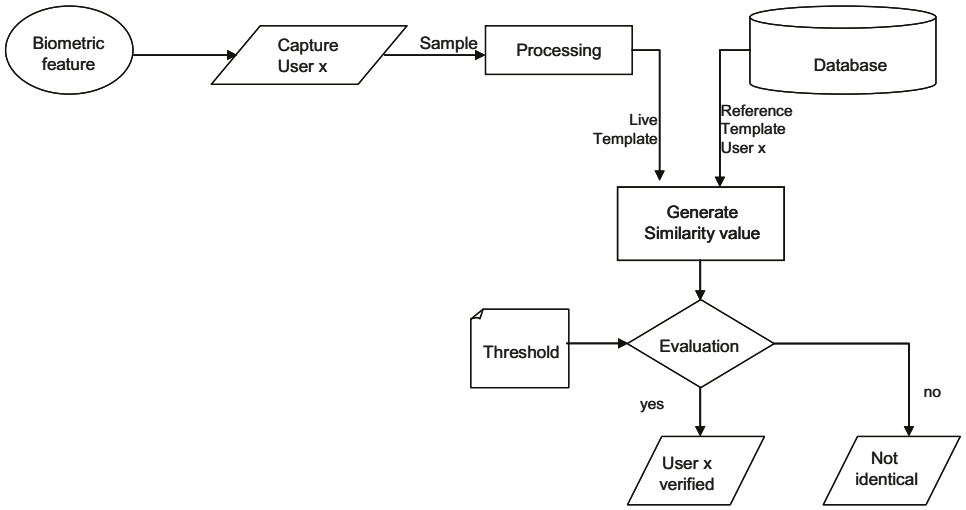

Figure 2: Course of the verification

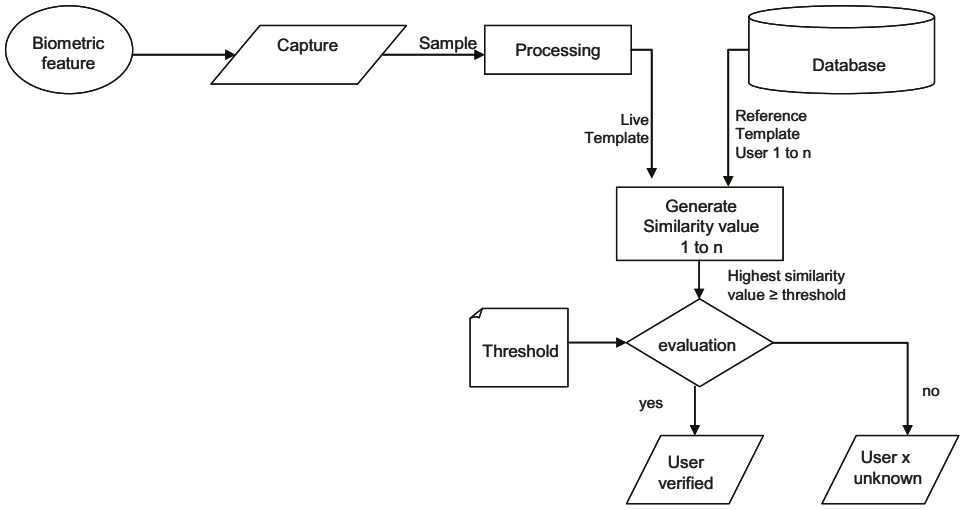

Figure 3: Course of the identification

4.3 Key data

The requirements for biometric identification features are set up in analogy to other identification features.

In order to be able to compare biometric features with other identification features (mental or material), the number of specifiable codes may be consulted.

Note: A change of the working point calibration of an installed system shall not lead to a higher FAR (see chapter operation security).

4.3.1 False acceptance rate

The false acceptance rate with the following definition is available for measurement of biometric appliances:

$$\mathbf{FAR} = \frac{\textbf{Number of successful unauthorised verifications}}{\textbf{Total number of unauthorised verification attempts}}$$

The FAR is calculated that way that the number of attempts refers to 1:1 comparison (verifications). It represents the probability that an unauthorised person has verified against the reference template successfully. This way the reciprocal value of the FAR is the number of specifiable combinations.

Example: An FAR of 10^{-4} would mean 10^{4} specifiable codes.

A comparison 1:n as applied for identification the probability of a false acceptance against an FAR is raising for the verification.

If $\mathbf{FAR_v}$ is the probability of a false acceptance in the verification mode, the probability of a non-occurrence of a false acceptance for a comparison sample is

$$\mathbf{1-FAR_v}.$$

For a comparison with N samples (number of the reference templates filed in the database) the probability of a non-occurrence of a false acceptance is as follows:

$$\mathbf{(1-FAR_v)^N}$$

The probability on the other hand that at least one false acceptance occurs in the identification mode is then

$$\mathbf{FAR_I=1-(1-FAR_v)^N}$$

This leads to the fact that devices with identification mode shall be evaluated according to the resulting $\mathbf{FAR_I}$ which raises following the raising number of stored reference templates.

4.3.2 False rejection rate

The false rejection rate is closely linked to the operationability. It is defined as follows:

$$\mathbf{FRR} = \frac{\textbf{Number of rejected verification attempts of authorised persons}}{\textbf{Total number of all verification attempts of authorised persons}}$$

The FRR is calculated here, such that the number of attempts refers to comparisons (verifications) 1:1.

The false rejection rate sticks together with the false acceptance rate. The lower the FAR the higher is the FRR and vice-verse.

5 Requirements

In the scope of these guidelines biometric recognition procedures are treated as part of products in the field of intrusion detection, access control techniques and electronic locks. The requirements valid and specific for these products therefore are the same relevant for biometric recognition, too. Additional or deviating requirements in connection with the specific characteristics of biometric recognition procedures are described in the following clauses.

5.1 Protection against environmental influences

The requirements which are valid for the respective device and contained in the respective product guidelines are to be applied (e. g. in the guidelines for alarm systems, ancillary control equipment, VdS 2119 for the use in intruder alarm systems).

5.2 Functional reliability

The requirements for functional reliability which are valid for the respective device and contained in the respective product guidelines are to be applied (e. g. in the guidelines for alarm systems, ancillary control equipment, VdS 2119 for the use in intruder alarm systems).

The device shall be operated with a working point calibration (combination FAR/FRR) so that the required minimum number of combinations as described in the product specific guidelines is fulfilled (e. g. according to table “possible combinations of IM in VdS 2119).

Special requirements on the documentation referring to special characteristics of biometric recognition procedures are to be considered.

Example: The documentation shall include information on the working point calibration.

Note: The FAR is calculated according to clause 4.3.1.

5.3 Operational security

For the operational security of the given device the requirements according to the respective product specific guidelines are valid (e. g. in the guidelines VdS 2119 for ancillary control equipment for the use in intruder alarm systems).

Furthermore the following special requirements are valid:

5.3.1 Working point calibration

It is to be ensured by appropriate measures that the working point calibration cannot be changed by unauthorised persons (example: for intruder alarm systems a change of the working point calibration in access level 1 and 2 is not admitted).

5.3.2 Storage of working point calibration

If a working point calibration is possible during operational status of the system, a change of the calibration shall be filed. The following data shal be stored: new calibrated value, date, time, authorised person. The durance of the storage or the number of the changes to be stored depends on the indications in the product specific guidelines.

5.3.3 Automatic working point calibration

An automatic (adaptive) adoption of the working point calibration (e. g. for compensating of bad samples due to a contaminated sensor) is not admitted.

5.3.4 Maximum false rejection rate (FRR)

By the use of biometric recognition procedures the probability raises that the identification of authorised persons does not succeed despite correct application of the recognition procedure. The FRR chosen with the working point calibration shall not exceed the value of 10 %.

5.3.5 Enrolment with granting rights

If the enrolment is connected with the granting of rights the product specific requirements shall be fulfilled (example: enrolment of an ancillary control equipment is connected directly with the control authorisation. This leads to the fact that an enrolment is admitted only for access level 3 and 4).

5.4 Tamper security

5.4.1 Tamper protection

The requirements as defined in the product specific guidelines for the respective device are to be applied (e. g. in the guidelines VdS 2119 for ancillary control equipment for the use in intruder alarm systems).

5.4.2 Compromising of biometric features

5.4.2.1 Copy of biometric features

The successful use of copies of biometric attributes or its characteristic biometric features shall be avoided according to the following table depending of the respective profile:

Profile	Offender profile	Possibility to copy biometric features
Profile 1	Layman	Reactivation of latency images
Profile 2	Semi-profi	Copy with simple means, e. g. use of drawings
Profile 3	Expert	Overcoming with adapted copies

Profile 1: The biometric recognition procedure shall be designed at least such that an overcoming with simple means by persons without expert know-how (layman) is not possible.

Profile 2: The biometric recognition procedure shall be designed at least such that an overcoming with raised effort (expenses and time) by persons with restricted expert know-how (semi-profi) is not possible.

Profile 3: The biometric recognition procedure shall be desgined at least such that an overcoming only with high effort (expenses and time) by persons with expert know-how and system know-how (expert) is possible.

Note: The profile to be applied result of the product specific guidelines, whereas pofile 1 is valid for the lowest class and profile 3 for the highest class.

5.4.3 Storage of templates

Templates shall be stored in a coded manner or shall be readable only by a access key if the memory is accessible (e. g. the memory is outside the security area). Alternatively the memory content shall be deleted in case of unauthorised access.

5.5 Documentation

The requirements concerning the documentation as defined in the product specific guidelines shall be applied (e. g. the guidelines VdS 2119 for ancillary control equipment for use in intruder alarm systems).

6 Test methods

6.1 Protection against environmental influences

The requirements for the protection against environmental influences of the product as defined in the product specific guidelines are tested in the frame of the product tests (e. g. in the guidelines VdS 2119 for ancillary control equipment for the use in intruder alarm systems). The respective test methods are described in the Guidelines for Alarm Systems, Protection against environmental influences, requirements and test methods, VdS 2110.

6.2 Functional reliability

It is checked if the requirements on the functional reliability as stipulated in the respective product specific guidelines (e. g. in the guidelines VdS 2119 for ancillary control equipment for the use in intruder alarm systems) are fulfilled.

With suitable means it is to be proven that the required FAR-values with the indicated working point calibrations are reached. A standardised and reproducible test is to be applied as far as possible.

Furthermore it is checked if the documentation considers in a complete, consistent and reproducible manner the special technical characteristics of biometric recognition procedures. At least a description of the working point calibration (combination FAR/FRR) has to be available for the correct application.

6.3 Operational security

It is checked if the requirements on the operational security as stipulated in the respective product specific guidelines (e. g. in the guidelines VdS 2119 for ancillary control equipment for the use in intruder alarm systems) are fulfilled.

6.3.1 Working point calibration

Furthermore it is checked if the working point calibration is possible for unauthorised persons (e. g. in access level 1 or 2). The test has failed, if this is possible.

6.3.2 Storage of working point calibration

Furthermore it is checked if in case a working point calibration is possible, a storage of each process influencing the working point with at least the following indications is proceeded: newly adjusted value, date, time, authorised person.

The durance of storage or the number of changes to be stored depends on the indications in the product specific guidelines and is also checked on fulfilment of the requirements.

6.3.3 Automatic working point calibration

It is checked if an automatic (adaptive) adaption of the working point calibration (e. g. for compensating of bad samples due to a contaminated sensor) is possible. If this is the case the test has failed.

6.3.4 Maximum false rejection rate (FRR)

For working point calibration as chosen according to these guidelines it is checked on an experiential manner or on base of standardised and reproducible procedures if the value of the FRR does not exceed 10 %.

A false rejection is counted as such, if three attempts with the same biometric feature in series are rejected.

6.3.5 Enrolment with granting of rights

It is checked if the requirements for granting rights as defined in the product specific guidelines in connection with the enrolment are fulfilled (Example: Enrolment in an ancillary control equipment is connected directly with the ACE. This leads to the fact that the enrolment is possible only for access level 3 and 4).

6.4 Tamper security

6.4.1 Tamper protection

It is checked if the requirements on tamper protection as defined in the respective product specific guidelines (e. g. in the guidelines VdS 2119 for ancillary control equipment for the use in intruder alarm systems) are fulfilled.

6.4.2 Compromising of biometric features

It is checked if the device has resistance against attacks of offender profiles 1 to 3 according to clause 5.4.2.1.

6.4.2.1 Storage of templates

It is checked if templates are stored in a coded manner or can be readout only by access keys, it the storage is accessible or if alternatively the storage content is deleted in case of unauthorised access.

6.5 Documentation

It is to be checked if the required documentation as defined in the respective product specific guidelines (e. g. in the guidelines VdS 2119 for ancillary control equipment for the use in intruder alarm systems) is completely, consistently and in a reproducible manner available.