ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation

ITU-T X.1095 (11/2023)

SERIES X: Data networks, open system communications and security

Information and network security – Telebiometrics

Entity authentication service for pet animals using telebiometrics

ITU-T X-SERIES RECOMMENDATIONS

Data networks, open system communications and security

PUBLIC DATA NETWORKS	X.1-X.199
OPEN SYSTEMS INTERCONNECTION	X.200-X.299
INTERWORKING BETWEEN NETWORKS	X.300-X.399
MESSAGE HANDLING SYSTEMS	X.400-X.499
DIRECTORY	X.500-X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600-X.699
OSI MANAGEMENT	X.700-X.799
SECURITY	X.800-X.849
OSI APPLICATIONS	X.850-X.899
OPEN DISTRIBUTED PROCESSING	X.900-X.999
INFORMATION AND NETWORK SECURITY	X.1000-X.1099
General security aspects	X.1000-X.1029
Network security	X.1030-X.1049
Security management	X.1050-X.1069
Telebiometrics	**X.1080-X.1099**
SECURE APPLICATIONS AND SERVICES (1)	X.1100-X.1199
CYBERSPACE SECURITY	X.1200-X.1299
SECURE APPLICATIONS AND SERVICES (2)	X.1300-X.1499
CYBERSECURITY INFORMATION EXCHANGE	X.1500-X.1599
CLOUD COMPUTING SECURITY	X.1600-X.1699
QUANTUM COMMUNICATION	X.1700-X.1729
DATA SECURITY	X.1750-X.1799
IMT-2020 SECURITY	X.1800-X.1819

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1095

Entity authentication service for pet animals using telebiometrics

Summary

Recommendation ITU-T X.1095 defines an entity authentication infrastructure for pet animals using telebiometrics. It specifies multimodal telebiometrics, which uses nose patterns and faces of pet animals. This Recommendation is applicable in various pet animal services such as registration, insurance and e-health care for pet animals. Entity authentication for pet animals is always performed in a non-cooperative environment, therefore it is necessary to define criteria for acquiring suitable multimodal telebiometrics for pet entity authentication. There are also requirements for devices that acquire multimodal telebiometrics, and architecture in the operating platform for stable multimodal telebiometric applications for pet animals.

This Recommendation specifies functional requirements for biometric capture devices and data acquisition of biometrics for pet entity authentication. A platform architecture, performance testing methodology and privacy issues are also defined.

The following topics are addressed in the scope of this Recommendation:

– Pet animals cover dogs and cats;

– Multimodal telebiometrics cover nose patterns and faces;

– Biometric capture devices cover digital cameras, mobile cameras, specific cameras such as infrared cameras, high-speed cameras and optical scanners.

History *

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T X.1095	2023-11-13	17	11.1002/1000/15708

Keywords

Cat, dog, entity authentication, face, multimodal telebiometrics, nose pattern, pet animals, registration.

* To access the Recommendation, type the URL https://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T X.1095

Entity authentication service for pet animals using telebiometrics

1 Scope

This Recommendation specifies functional requirements for biometric capture devices and data acquisition of biometrics for pet entity authentication. A platform architecture, performance testing methodology and privacy issues are also defined.

The following topics are addressed within the scope of this Recommendation:

– Pet animals, referring dogs and cats;

– Multimodal telebiometrics, referring to nose pattern and face;

– Biometric capture devices, referring to digital cameras, mobile cameras, specific cameras such as infrared cameras, high-speed cameras and optical scanners.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 biometric capture device [b-ISO/IEC 2382-37]: Device that collects a signal from a biometric characteristic and converts it to a captured biometric sample.

3.1.2 detection error trade-off (DET) [b-ISO/IEC 19795-1]: Relationship between false-negative and false-positive errors of a binary classification system as the discrimination threshold varies.

3.1.3 digital camera [b-ISO 29301]: Device that detects the image using a chip-arrayed image sensor, such as a charge-coupled device (CCD) or complementary metal-oxide semiconductor (CMOS), that converts a visual image to an electric signal.

3.1.4 equal error rate (EER) [b-ISO/IEC 2382-37]: Value at which the FRR [false reject rate] and FAR [false accept rate] are equal.

3.1.5 false accept rate (FAR) [b-ISO/IEC 2382-37]: Proportion of biometric transactions with false biometric claims erroneously accepted.

3.1.6 false reject rate (FRR) [b-ISO/IEC 2382-37]: Proportion of verification transactions with true biometric claims erroneously rejected.

3.1.7 failure to enrol (FTE) [b-ISO/IEC 2382-37]: Failure to create and store a biometric enrolment data record for an eligible biometric capture subject in accordance with a biometric enrolment policy.

3.1.8 failure to acquire (FTA) [b-ISO/IEC 2382-37]: Failure to accept for subsequent comparison the biometric sample of the biometric characteristic of interest output from the biometric capture process.

3.1.9 false match [b-ISO/IEC 2382-37]: Comparison decision of a match for a biometric probe and a biometric reference that are from different biometric capture subjects.

3.1.10 false non-match [b-ISO/IEC 2382-37]: Comparison decision of a non-match for a biometric probe and a biometric reference that are from the same biometric capture subject and of the same biometric characteristic.

3.1.11 optical image stabilization [b-ISO 20954-1]: Function that compensates for image displacement on the focal plane due to movement of a handheld camera by moving a part or whole of the optical system and/or image sensor, based on a means of camera movement detection.

3.1.12 optical scanner [b-ISO 6196-7]: A scanner that uses light for examining patterns.

3.1.13 scenario evaluation [b-ISO/IEC 2382-37]: Evaluation that measures end-to-end system performance in a prototype or simulated application with a test crew.

3.1.14 technology evaluation [b-ISO/IEC 2382-37]: Offline evaluation of one or more algorithms for the same biometric modality using a pre-existing or especially-collected corpus of samples.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 guardian: Person that takes care of pet animals in their homes or in shelters.

3.2.2 mobile camera: A camera that is integrated into a smartphone or mobile device.

3.2.3 nose pattern: Biometric pattern of wrinkles on the nose of pet animals.

3.2.4 pan: The degree of horizontal movement of a camera head without changing the position of the camera.

3.2.5 specific camera: A camera that is designed for a specific purpose or use, such as an infrared camera or high-speed camera.

3.2.6 tilt: The degree of vertical movement of a camera head without changing the position of the camera.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CCD Charge-Coupled Device

CMOS Complementary Metal-Oxide Semiconductor

DB Database

FAR False Accept Rate

FRR False Error Rate

FTA Failure To Acquire

FTE Failure To Enrol

OIS Optical Image Stabilization

PII Personal Identifiable Information

ROI Region Of Interest

5 Conventions

None.

6 Prerequisites

None.

7 Overview of multimodal telebiometrics for pet entity authentication

7.1 Types of multimodal telebiometrics

7.1.1 Nose pattern

The nose pattern is a biometric marker that is unique in pet animals with wrinkles on the nose. The nose pattern comprises ridges and troughs. The ridges are a flattened area placed relatively high, and the troughs are an elongated and sunken area placed relatively low. The ridges and troughs are mapped as a polygonal pattern, and this complex pattern is a biometric marker that is unique for each pet animal.

7.1.2 Face

The face, with its geometric features between the eyes, nose and muzzle represents a unique biometric marker for the identity of pet animals.

7.2 Characteristics of telebiometrics for pet entity authentication

7.2.1 Nose pattern

Figure 1 shows an example of the characteristics of the nose pattern of two pet animals.

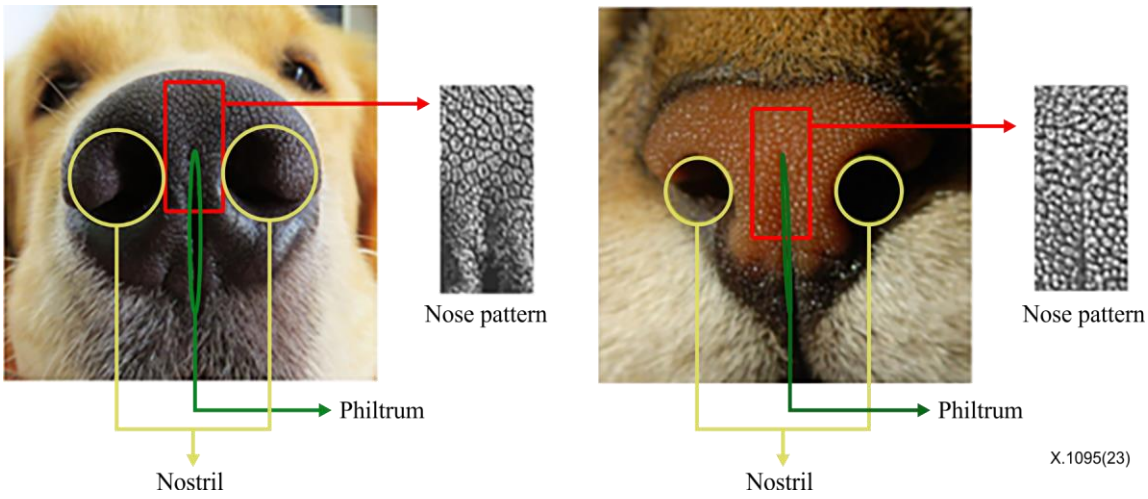

Figure 1 – Characteristics of the nose pattern of pet animals

The nose pattern is mainly found between the nostrils of the pet animals and has a very complex skin folding pattern. The complex pattern represents the unique identity of each pet animal.

7.2.2 Face

Figure 2 shows an example of the characteristics of the face of pet animals.

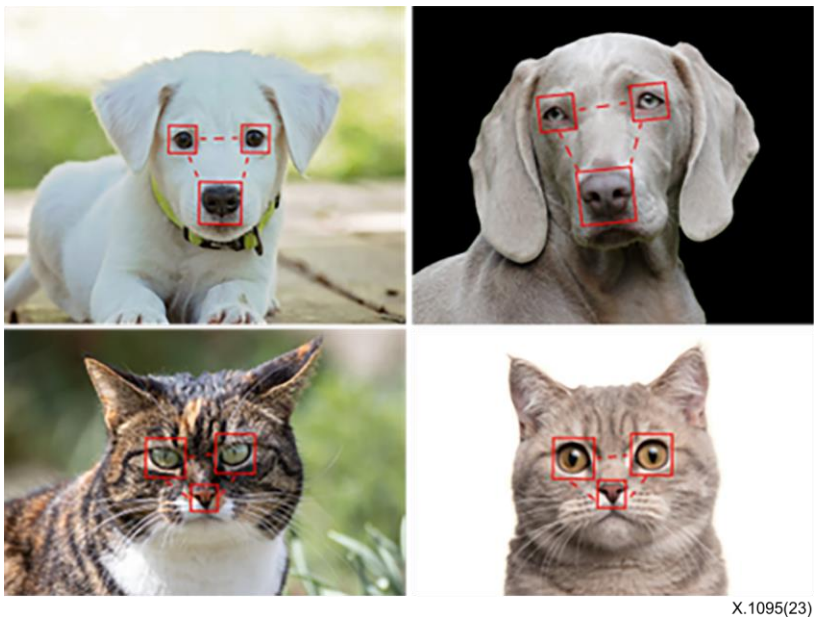

Figure 2 – Characteristics of the face of pet animals

The face has unique geometric features for each pet animal as it does in humans, and it these can be extracted by detecting the eyes, nose and muzzle of the pet animals.

8 Requirements for biometric capture devices for pet entity authentication

8.1 Types of biometric capture devices

In general, sensors for detecting the biometrics of pet animals at a distance can be classified into three types of image recording devices such as mobile cameras, digital cameras and specific cameras. Optical scanners can be a sensor for detecting biometrics through contact.

8.2 Functional requirements for biometric capture devices for pet animals

Biometric capture devices should be able to cope with the unexpected movements of pet animals. Sensors for detecting biometrics at a distance should meet the minimum requirements for image resolution, shutter speed, ISO and aperture. Sensors for detecting biometrics through contact should position the biometrics of the pet animals on a prism area of the optical scanner. The minimum requirements can be determined by the quality of the region of interest (ROI) images containing the biometrics of the pet animals. The ROI images of the nose pattern should contain more than 60% of biometrics and the ratio of the biometrics should be measured by the number of pixels within the images.

Table 1 – Minimum requirements for sensors used at a distance

S No.	Items	Requirements
1	Pixels	5 megapixels (MP)
2	Sensor size	1/3 inch
3	Aperture	f/1.8
4	Resolution	1 080 × 1 080 pixels
5	Shutter speed (indoor)	1/1 000th of a second to 1 second
6	Shutter speed (outdoor)	1/500th of a second to 1 second
7	ISO	200 to 400

Table 2 – Minimum requirements for sensors using in contact

S No.	Items	Requirements
1	Pixels	2 megapixels (MP)
2	Resolution	500 DPI
3	Frames per second (fps)	10 fps
4	Image format	RAW, BMP, WSQ, JPEG 2000

Table 3 – Minimum requirements for ROI for nose pattern

S No.	Items	Requirements
1	Size of ROI	256 × 256 pixels
2	Ratio of biometrics (in ROI)	60%

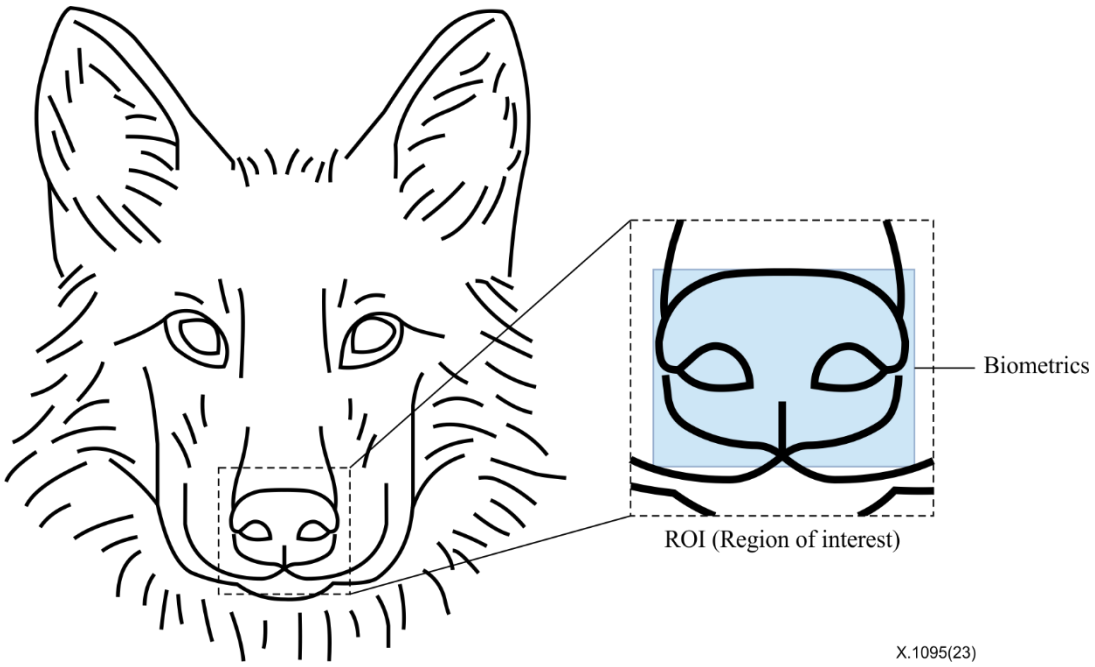

Figure 3 – An example of the ROI image for the nose pattern of pet animals

8.3 Data interchange format for biometric capture devices

For pet entity authentication using biometrics, the procedures shown in Figure 4 must be followed. The procedure has a client-server structure based on the sensors and can be either separable or integral, depending on whether or not there is a communication unit.

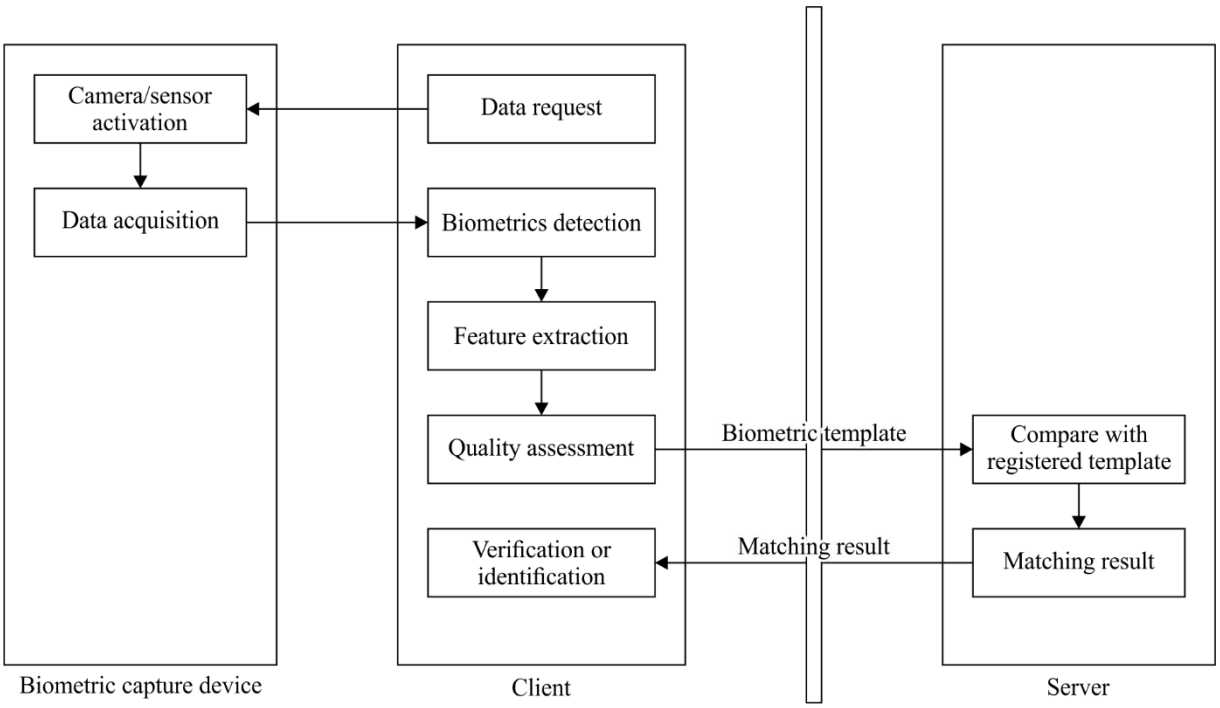

Figure 4 – Biometric data flow for biometric capture devices based on a client-server structure

Figure 5 describes the data interchange format for biometric capture devices. This format consists of a file header representing basic information, biometric raw and feature data. A security block can be configured as necessary.

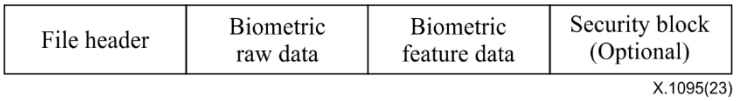

Figure 5 – Data interchange format for biometric capture devices

8.3.1 File header

The file header format consists of basic information that summarizes the characteristics of the biometric raw and feature data, including sensor, time and measurement information.

8.3.2 Biometric raw data

The biometric raw data format consists of a length header indicating the length of the raw data, signal quality and raw data array measured from the biometric capture devices.

8.3.3 Biometric feature data

The biometric feature data format consists of a length header indicating the length of the feature data and binarized data which implements unique features of each pet animal extracted from the biometric raw data.

8.3.4 Security block

The security block is optional and contains additional security parameters. It indicates whether or not all biometric data are signed and whether the raw or feature data are encrypted.

9 Requirements for an architecture of the pet entity authentication platform

9.1 Overview

The pet entity authentication model using telebiometrics comprises data acquisition, data transmission and biometric authentication processes. Figure 6 shows an entity authentication model using a mobile camera. The main application models for the pet entity authentication platform include rescuing abandoned animals, pet insurance, pet health care and pet travelling.

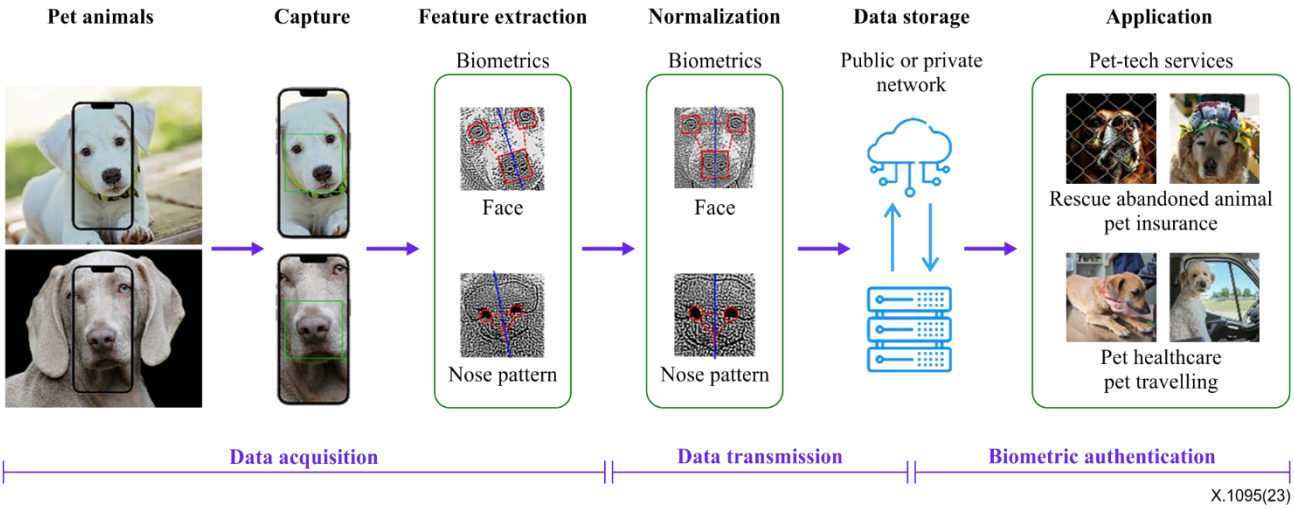

Figure 6 – Telebiometric authentication model for pet entity authentication

9.2 Functional requirements for pet entity authentication mechanism

9.2.1 Data acquisition and pre-processing

The biometrics of pet animals are gathered from the biometric capture devices and are pre-processed for signal optimization before the feature is extracted. Biometric raw data are pre-processed through analogue or digital filters. In the case of using cameras as the biometric capture device, filters should be optimized to reduce noise from unconstrained illumination and motion of the pet animals. In the case of using an optical scanner as the biometric capture device, filters should be optimized to reduce noise from unconstrained motion and moisture on the nose of pet animals. If the quality of the filtered biometric raw data is not enough to perform entity authentication for each pet animal, the gathered data should be discarded and the acquisition process should be repeated.

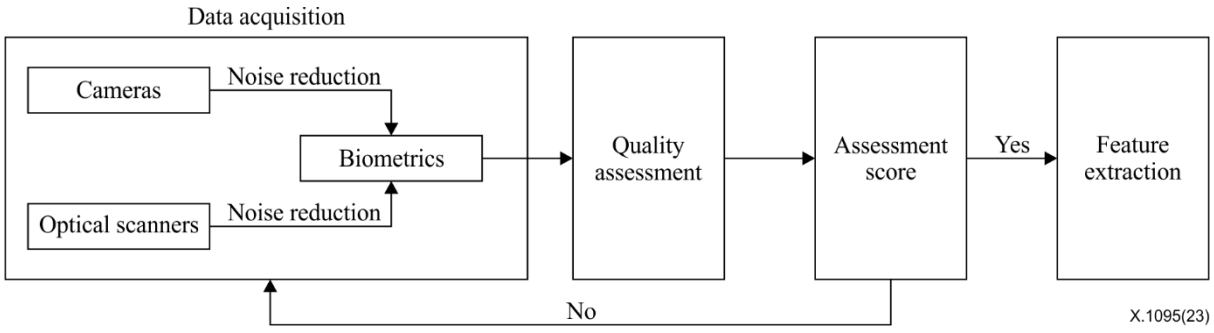

Figure 7 – Data acquisition and pre-processing model for pet entity authentication mechanism

9.2.2 Feature extraction and registration in a biometric database

Individual characteristic feature points are extracted from the biometrics. An algorithm extracts biometric features that minimize intra-individual variability and maximize inter-individual variability for each biometric characteristic. The extracted biometric features are then registered in a database

(DB). If there is an attempt to authenticate the same pet animal later, the biometric feature dataset is loaded onto the DB through the ID, and the pet animal is authenticated through a comparison of the feature points.

9.2.3 Matching algorithm

In 1:1 verification, registered biometric feature data are compared one-to-one with the feature data of the pet animal for which authentication is being attempted. When authentication is attempted, the features extracted from the measured biometrics are compared with the registered features on the DB. The ID of the pet animal is presented and the registered biometric feature data from the DB are loaded as shown in Figure 8. A similarity score between features is calculated and the results are passed if the score exceeds a threshold level. The similarity score should be calculated through objective mathematical calculations, such as the Euclidean distance or the Mahalanobis distance.

In 1:*N* identification, the data of the pet animal to be identified are compared with all the data on the DB. Since the data comparison is performed on all the registered data, the trials of the matching process increase exponentially depending on the number of the registered pet animals. In this analysis process, it is preferable to use a majority of the agreement analysis methods to increase the reliability of the agreement calculation, and a process of comprehensively evaluating the results of the calculation is also required. A pet animal that has the highest degree of agreement is judged to be the same entity as the requester of the identification and the result should be provided.

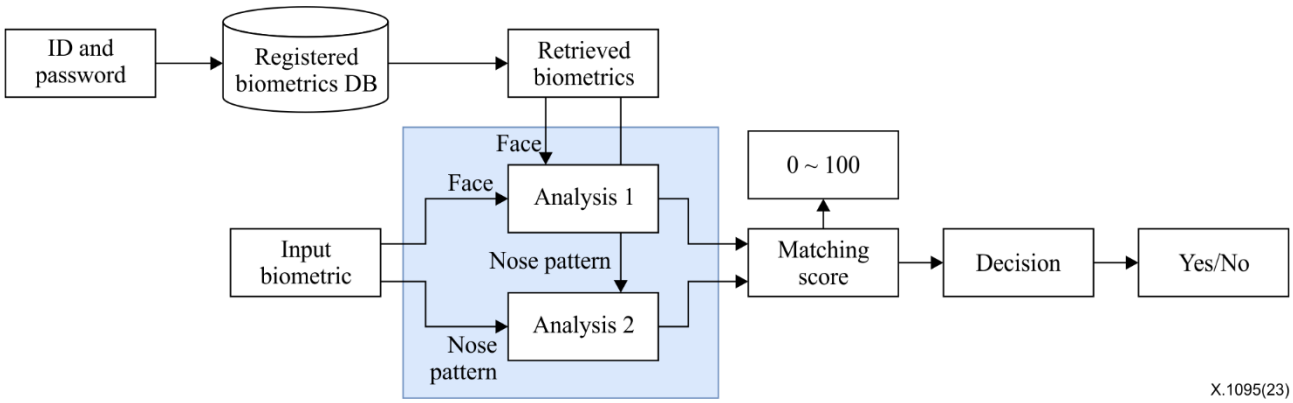

Figure 8 – 1:1 verification process for pet entity authentication

9.3 Functional requirements for telebiometric transmission protocol

This clause defines the functional requirements for a telebiometric transmission protocol. Transferred biometric data must demonstrate a certain measure of compliance, interoperability and security. A telebiometric transmission protocol is an application protocol and is implemented in combination with standards-based communication protocols whether wired or wireless.

9.4 General requirements of testing DB for pet entity authentication

9.4.1 Data acquisition requirement for testing DB

Data acquisition is the most crucial point due to an accuracy issue in entity authentication mechanisms. It is also important to consider the data acquisition environments and uncooperative characteristics of pet animals.

Biometric data of the pet animals can be acquired with bias due to illuminating lights and exposure to biometric capture devices. Therefore, it is needed to acquire biometric data on pet animals in a controlled environment. To manage objective criteria on performance tests, the specification of several conditions for acquisition environments should be followed.

Pet animals present uncooperative biometric capture subjects. To acquire appropriate images for the telebiometrics application of pet animals, a process that cleans parts of target biometrics is needed. To construct testing DB, the acquisition process can be performed multiple times.

9.4.2 Procedure and method for the construction of testing DB

Acquisition of telebiometrics should proceed in a relaxed environment with pet animals to avoid inducing unexpected actions. The environment can be set up with the help of a guardian, vet or an animal trainer. In the case of using cameras, it is recommended to proceed with acquisition in an indoor environment where a specific level of illumination can be maintained.

9.4.3 Metadata features of testing DB

Telebiometrics database for pet entity authentication comprises a common environment, device and characteristic metadata.

Table 4 – Common metadata of testing DB

Class	Features	Meaning
DB_Info	Country	
	City	
	Supplier	
	RegisterDate	
	RevisionDate	
	RevisionHistory	
	Version	

Table 5 – Environment and device metadata of testing DB

Class	Features	Meaning
Environment_Info	ExperimentCondition	Lux
Device_Info	DeviceType	
	MaxResolution	

Table 6 – Characteristic metadata of testing DB

Class	Features	Meaning
File_Info	FileFormat	
	FileName	
	DirectoryPath	
	FileSize	
Biometrics_Info	BiometricType	Nose pattern, face
	RawData	Image or video
	ImageResolution	
Subject_Info	BirthDate	
	Gender	
	Breed	

Table 6 – Characteristic metadata of testing DB

Class	Features	Meaning
Guardian_Info	GuardianID	
Miscellaneous_Info	OrderOfRepeat	
	Comment	

9.4.4 Data interchange formats for testing DB

Telebiometrics of pet animals and related information should be stored in a specific DB through an encryption and compression process on a server. The compressed information is only accessible to designated persons who proceed with related projects.

10 Performance testing methodology for pet entity authentication mechanisms

10.1 General

This clause defines guidelines for performance testing methodology based on technology and scenario evaluations. The main performance evaluation criteria are failure to enrol (FTE), failure to acquire (FTA), false reject rate (FRR), false accept rate (FAR), equal error rate (EER), and decision-error trade-off (DET) plots. The technology evaluation of the telebiometric authentication algorithm is an offline evaluation that repeatedly evaluates the recognition performance of the algorithm together with its processing speed, targeting an evaluation DB composed of biometric sample data collected in advance and a standardized DB. The performance of various algorithms can be compared with this evaluation method.

10.2 Technology evaluation procedures

10.2.1 Construction of the testing DB

In technology evaluation, the testing DB should meet the minimum requirements listed in Table 7. The testing DB should include at least 500 subjects, 2 to 20 biometrics per subject, over two acquisition environments, and a total of 1 000 to 10 000 biometrics to cover a diverse range of breeds and ages of pet animals. Especially, the acquisition environment should consider the presence of the guardian, dog trainer or handler during the acquisition process to prevent accidents such as dog bites. Also, movements of the pet animals, out-of-focus biometric capture devices and moisture on biometrics should be controlled to appropriate levels.

Table 7 – Minimum requirements for testing DB

Class	Requirements
Number of subjects (*N*)	500
Number of breeds	10
Biometrics per subject (*M*)	2 to 20
Number of acquisition environment	2
Resolution	1 080 × 1 080 pixels
Size of ROI	256 × 256 pixels
Ratio of biometrics (in ROI)	60%
Minimum transactions on comparison decisions with the same biometric subjects	500 (= ${}_{M}C_{2}\times N$)

Table 7 – Minimum requirements for testing DB

Class	Requirements
Minimum transactions on comparison decisions with different biometric subjects	499,500 ($= {}_{N}C_{2} \times M^{2}$)

10.2.2 Sample quality test

The testing DB should reflect the variability of the pet animals, and the variability should be constrained within a specific range to analyse the competitiveness of the performance evaluation. To ensure that the testing DB is constructed in a suitable condition to perform evaluation, a sample quality test of the DB should be performed.

10.2.3 Technology test

The process of technology test is composed of two steps: the preparation step and the evaluation step. The preparation step is processed as follows:

1) Contact and provide a brief introduction of the evaluation environment.
2) Prepare documents that describe detailed contracts, outcomes and evaluation processes.
3) Share a sample DB that meets the minimum requirements of a testing DB.
4) Perform testing in advance on a small scale using the sample DB.

The evaluation step is processed as follows:

1) Perform testing with a standardized DB.
2) Analyse the results of the performance test and report the results.

10.2.4 Analysis tests and reporting results

The analysis and reporting procedure should be carried out as follows:

1) Description of the technology used.
2) Introduction of evaluation environments and criteria.
3) Specification of the testing DB used.
4) Evaluation of the quality of the testing DB.
5) Procedure for testing performance evaluation.

10.3 Scenario evaluation procedures

10.3.1 Planning the evaluation

Before conducting the scenario evaluation, the following should be prepared: the testing scenario, evaluation metrics, environments, testing algorithms and participants. The items listed in Table 8 should also be checked in advance.

Table 8 – Scenario test checklist

Items	Description
Scenario features	Definition of application: Objective of the evaluation and scenario Evaluation metrics: FAR, FRR, etc. Environment and platform: Indoor or outdoor
Evaluation policy	Policy related to the whole evaluation process
Level of trials	Maximum and minimum levels of registration and authentication trials

Table 8 – Scenario test checklist

Number of repeats	The number of participants needed to visit the platform
Minimum number of participants	Calculation based on the rule of 3 Estimates with FAR Estimates with FRR
Recording method	Method to record the results of registration and authentication

10.3.2 Scenario test

Participants of the scenario test should register the biometrics for the first time on enrolment. *N* stands for the total visits of the participants. If registration fails for some participants, these participants can only take part in the imposter matching part of the test.

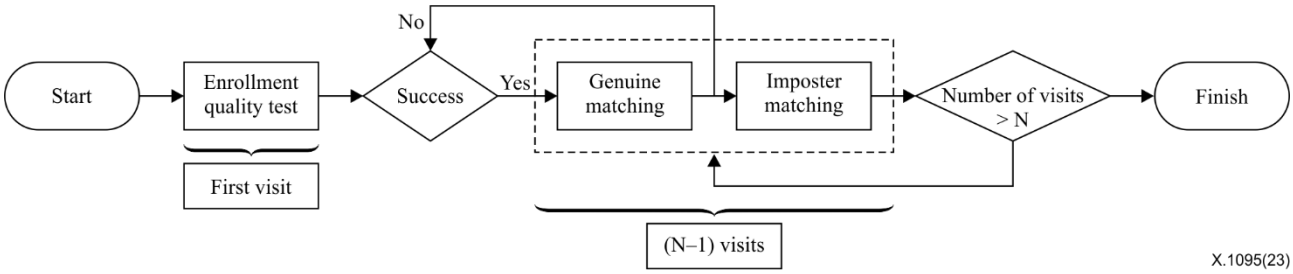

Figure 9 – General protocol of the scenario test

10.3.3 Analysis tests and reporting results

The reporting of scenario evaluation results comprises a summary, planning, procedure, data log, data analysis, data storage and the results of the evaluation.

1) Summary: summary of information about the participants, evaluation results and so on.
2) Scenario: description of the overall settings of the evaluation such as the objectives, metrics and environments.
3) Planning: a detailed explanation of the evaluation plan.
4) Procedure: description of the process of the initial contacts to the end of the evaluation.
5) Data log: list of participants, results of registration and authentication.
6) Data analysis: report of the results of the main-metrics and submetrics.
7) Data storage: explanation of the method of data storage and space.
8) Result of evaluation: table of each metric and conclusion on the testing algorithm.

11 Personally identifiable information (PII) protection of entity authentication service for pet animals and their guardians

11.1 Personally identifiable information (PII) protection policy

A personally identifiable information (PII) protection policy is required when the telebiometric mechanism is applied to the entity authentication platform to minimize the risk of leaking personal information about the guardians of pet animals.

11.1.1 Separation of DB

To protect the personal information of guardians from outside attacks using the pet animal DB, it is required to separate the guardian DB from the pet animal DB. A guardian ID should be separated logically and physically from the biometrics of pet animals. In this case, a common identifier that can

recognize both the guardian and the pet animal is needed. The common identifier should satisfy the security requirements as follows:

1) Extraction of the guardian ID and biometrics of pet animals should be prohibited by only using the common identifier.

2) If a certain DB is being attacked and modified illegally, managers of each DB should be able to notice and report it.

3) If one manager attempts to modify the contents of a DB with a private key, the other manager should be able to notice the change.

11.1.2 Guardian information

Personal information contained in the guardian information should be protected. Examples of the personal information of a guardian are name, phone number, birth date, address, sentence, voice and media. When a manager, who operates the entity authentication services for pet animals using telebiometrics, tries to collect personal information from a guardian, the following policy must be secured.

1) Identifier of the guardian should be properly used and be informed about their usage in advance.

2) Depending on the restriction regulation of data collection, the manager needs to be cautious not to collect data that is not necessary.

3) If the manager has to connect to the personal information of each guardian, each guardian should receive a request for an agreement from the manager on using their information elsewhere.

Appendix I

Use case for database construction scenario for pet entity authentication

(This appendix does not form an integral part of this Recommendation.)

I.1 Requirements for database construction for pet entity authentication

I.1.1 Data acquisition environment

To execute objective performance tests, various types of environmental parameters should be considered. This scenario describes the types of places, illumination and camera angle for the biometric capture devices used in database construction. Only the nose pattern is obtained as biometrics data.

The setting can be indoor or outdoor. Illumination can be set in various directions, and the camera angle can be set in a horizontal and vertical position along the frontal face of the pet animal.

Figure I.1 – Example of positioning illumination lamps in database construction

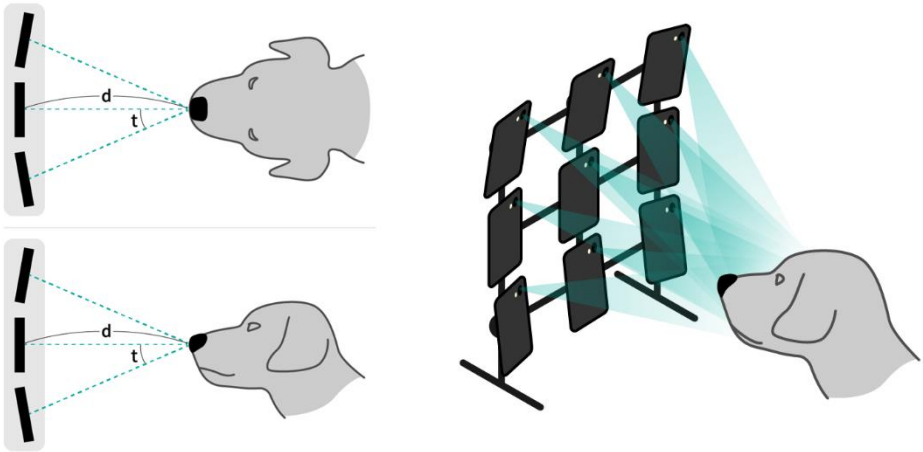

Figure I.2 – Example of positioning biometric capture devices at various angle

I.1.2 Biometric capture devices

To minimize an unexpected bias in image quality that can occur with cameras, it is recommended to use cameras equipped with optical image stabilization (OIS) and USB 3.0 systems. The number of cameras is calculated by the parameters of environmental conditions containing the illumination and camera angles.

Table I.1 – Example of calculating the number of biometric capture devices

Devices	The number of pan parameters (*A*)	The number of tilt parameters (*B*)	The number of devices (*C* = *A***B*)
Mobile camera	3	3	9

I.2 Requirements for the database construction process

I.2.1 Preparation process

Adequate places for database construction are places where pet animals are numerous, such as pet playgrounds, pet parks, animal shelters and rabies vaccination events. It is required to prepare introduction signs and guidelines for participants. To prevent accidents such as dog bites, safety rules should be noticed in advance and animal experts such as animal trainers and vets need to be present.

I.2.2 Main process

I.2.2.1 Input metadata

Pet animals and their guardians who are participating in the database construction need to agree to the privacy policy. After the privacy policy is reviewed, the guardians input the metadata except for the biometrics of pet animals.

I.2.2.2 Prepare biometrics data acquisition

The cameras have to be placed at a distance of about 20 cm to 40 cm from a pet animal. Guardians hold up the face of their pet animals and help them remain calm. A part of the biometrics needs to be cleansed before the acquisition of the biometrics data.

I.2.2.3 Biometrics data acquisition

The biometrics should be acquired when the camera is well-focused on them. If there are many cameras, a capture timing must be aligned to the spot when more than two cameras are well-focused on the biometrics. The number of acquisitions is calculated based on the parameters of the type of place, illumination and camera angles. This process can be repeated until the biometrics have been collected in various conditions.

Table I.2 – Example of calculating the number of acquisition

The number of indoor illumination (*A*)	The number of outdoor illumination (*B*)	The number of pan parameters (*C*)	The number of tilt parameters (*D*)	The number of acquisition (*E* = (*A* + *B*)**C***D*)
3	1	3	3	36

I.3 Metadata features

In this scenario, metadata features follow the features of clause 9.4.3.

Table I.3 – Common metadata of testing DB

Class	Features	Type
DB_Info	Country	
	City	
	Supplier	
	RegisterDate	
	RevisionDate	
	RevisionHistory	
	Version	

Table I.4 – Environment and device metadata of testing DB

Class	Features	Type
Environment_Info	ExperimentCondition	Lux
Device_Info	DeviceType	
	MaxResolution	

Table I.5 – Characteristic metadata of testing DB

Class	Features	Type
File_Info	FileFormat	
	FileName	
	DirectoryPath	
	FileSize	
Biometrics_Info	BiometricType	Nose pattern
	RawData	Image or video
	ImageResolution	
Subject_Info	BirthDate	
	Gender	
	Breed	
Guardian_Info	GuardianID	
Miscellaneous_Info	OrderOfRepeat	
	Comment	

I.4 Rescue service for lost pets based on pet entity authentication using telebiometrics

By executing performance tests, verified telebiometrics using the nose pattern of pet animals can be applied to rescue services for lost pets.

Appendix II

Use case for telebiometric entity authentication model for pet animals

(This appendix does not form an integral part of this Recommendation.)

II.1 Requirements for an architecture of the pet entity authentication platform

II.1.1 Overview

This scenario describes the use case and application of the pet entity authentication platform. This is a service that requires accurate identification of the pet animals, implements telebiometric features in its platform architecture and utilizes the unique ID of the pet animals with the unique ID of their guardians. One example of the pet entity authentication platform architecture is shown in Figure II.1.

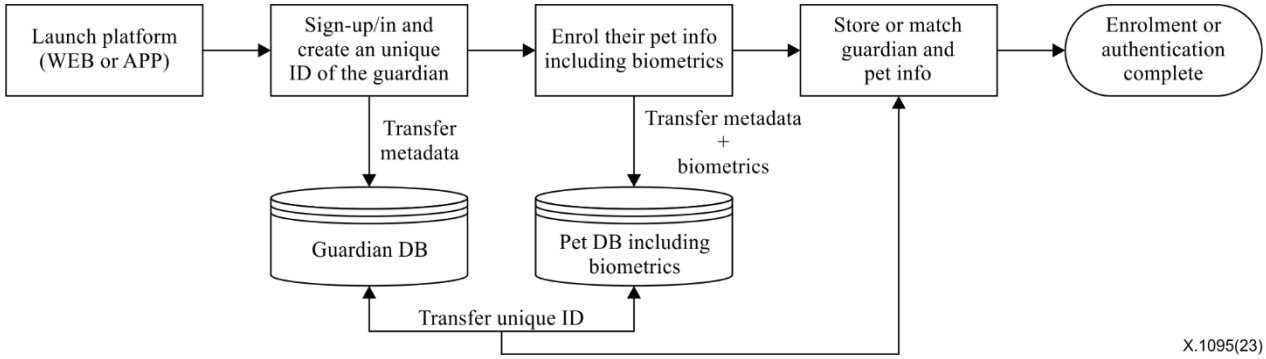

Figure II.1 – The architecture of pet entity authentication platform

II.1.2 Enrolment

To use the specific features of the pet entity authentication platform such as pet adoption services and pet insurance, the guardians have to enrol their personal information and the information of their pet animals including biometrics (see Figure II.2). If there is duplicated information about the pet animal, the enrolment can be blocked to prevent an abusive event.

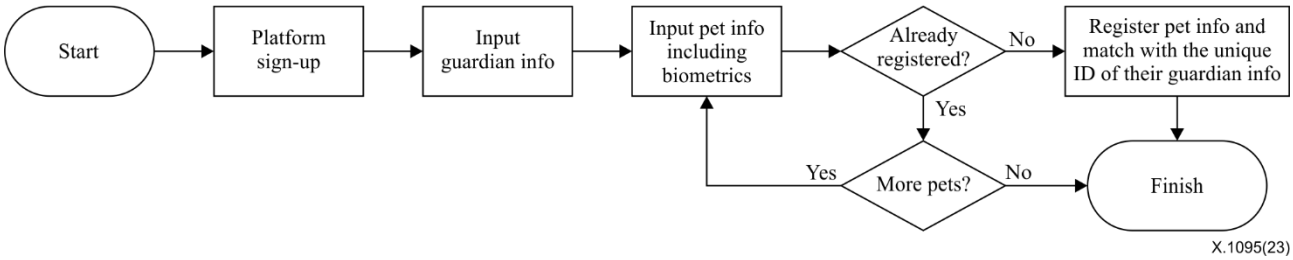

Figure II.2 – A flow chart of the sign-up and registration of the pet entity authentication platform

II.1.3 Authentication

The platform can set up the entity authentication process as a pre-requisite for providing the services such as delivering sensitive information about the pet animals and their guardians (see Figure II.3). When the guardians send a request to use a specific service, the platform retrieves the request to authenticate their pet animals. If the authentication results are output successfully, the guardians can use the service, but if the results fail to be output, the platform can refuse to provide the services to the guardians.

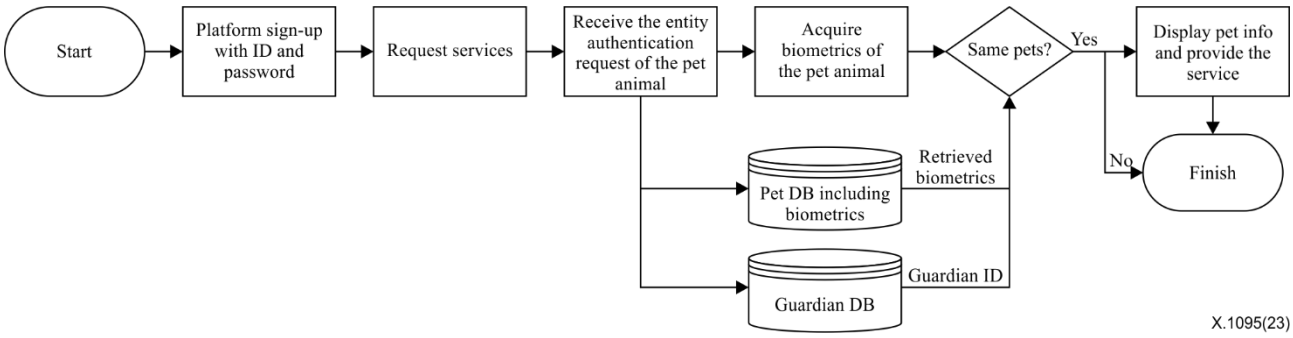

Figure II.3 – A flow chart of the sign-in and authentication of the pet entity authentication platform

In the case of the guardian failing to authenticate their pet animal more than *N* times with the same biometrics, access to the platform can be blocked (see Figure II.4). To rearrange the pet animal to the platform after the block, the guardian should verify that the pet animal is the same as the previously registered one by submitting the other biometrics. A manager of the platform can determine whether the pet animal can be re-registered or not based on the submitted biometrics.

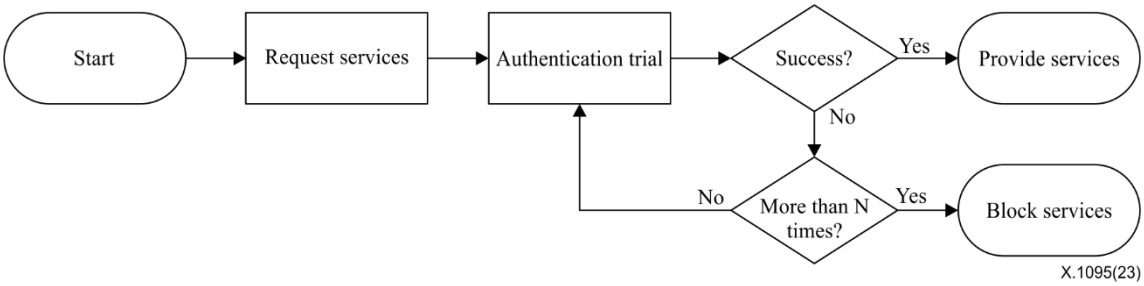

Figure II.4 – A flow chart of the failure case of the authentication

Bibliography

[b-ISO 6196-7] ISO 6196-7:1992, *Micrographics – Vocabulary – Part 7: Computer micrographics*.
<https://www.iso.org/obp/ui/en/#iso:std:iso:6196:-7:ed-1:v1:en>

[b-ISO 20954-1] ISO 20954-1:2019, *Digital cameras – Measurement method for image stabilization performance – Part 1: Optical systems*.
<https://www.iso.org/obp/ui/#iso:std:iso:20954:-1:ed-1:v1:en>

[b-ISO 29301] ISO 29301:2017, *Microbeam analysis – Analytical electron microscopy – Methods for calibrating image magnification by using reference materials with periodic structures*.
<https://www.iso.org/obp/ui/#iso:std:iso:29301:ed-2:v1:en>

[b-ISO/IEC 19795-1] ISO/IEC 19795-1:2021, *Information technology – Biometric performance testing and reporting – Part 1: Principles and framework*.
<https://www.iso.org/obp/ui/en/#iso:std:iso-iec:19795:-1:ed-2:v1:en>

[b-ISO/IEC 2382-37] ISO/IEC 2382-37:2022, *Information technology – Vocabulary – Part 37: Biometrics*.
<https://www.iso.org/obp/ui/en/#iso:std:iso-iec:2382:-37:ed-3:v1:en>

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Published in Switzerland
Geneva, 2024