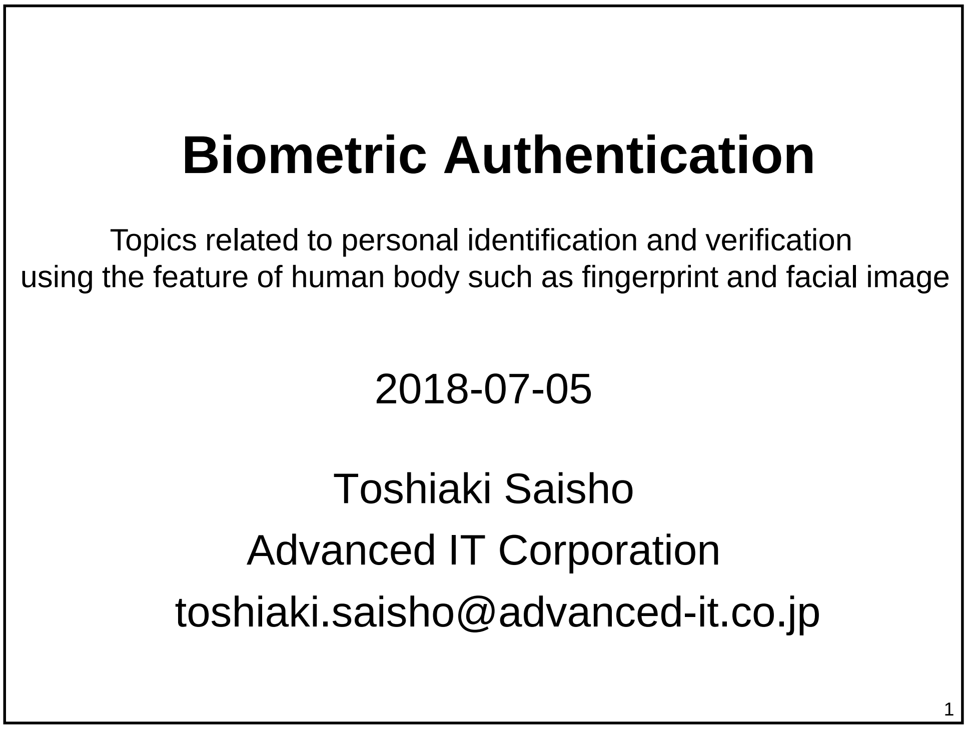
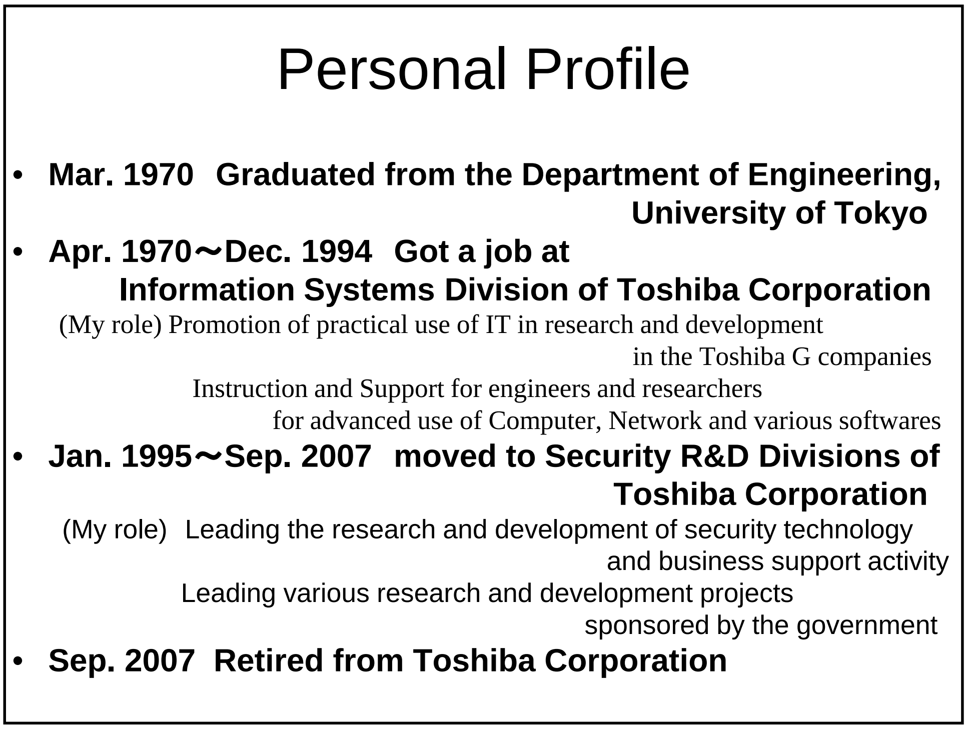


Biometric Authentication

Topics related to personal identification and verification
using the feature of human body such as fingerprint and facial image

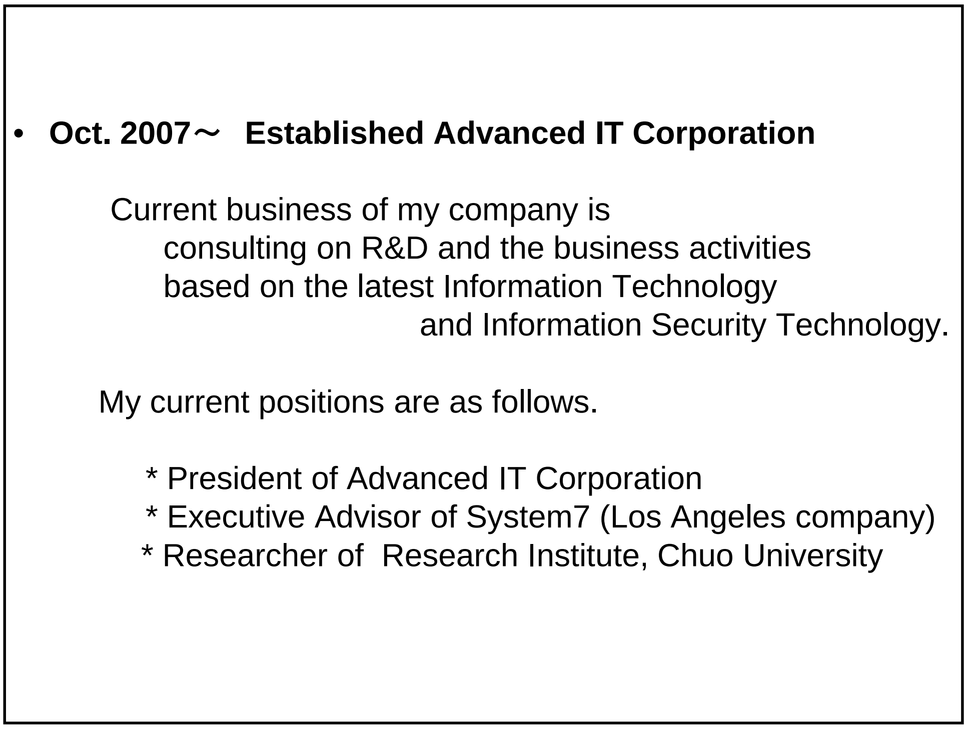
2018-07-05

Toshiaki Saisho
Advanced IT Corporation
toshiaki.saisho@advanced-it.co.jp



Personal Profile

- **Mar. 1970 Graduated from the Department of Engineering, University of Tokyo**
- **Apr. 1970～Dec. 1994 Got a job at Information Systems Division of Toshiba Corporation**
  (My role) Promotion of practical use of IT in research and development in the Toshiba G companies
  Instruction and Support for engineers and researchers for advanced use of Computer, Network and various softwares
- **Jan. 1995～Sep. 2007 moved to Security R&D Divisions of Toshiba Corporation**
  (My role) Leading the research and development of security technology and business support activity
  Leading various research and development projects sponsored by the government
- **Sep. 2007 Retired from Toshiba Corporation**

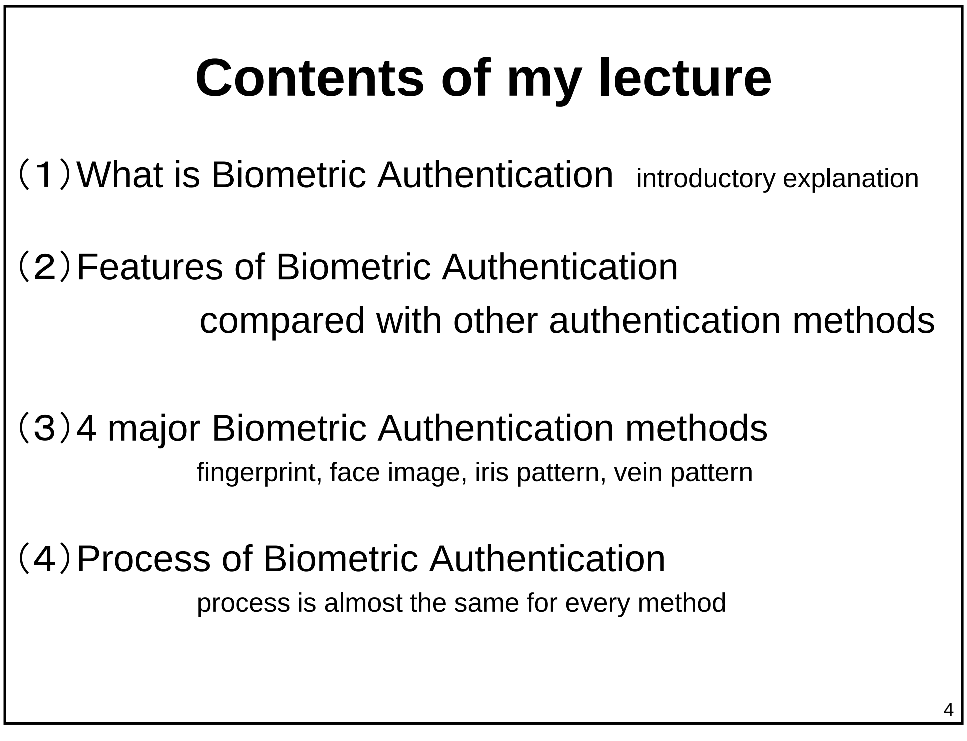


- **Oct. 2007～ Established Advanced IT Corporation**

Current business of my company is
consulting on R&D and the business activities
based on the latest Information Technology
and Information Security Technology.

My current positions are as follows.

* President of Advanced IT Corporation
* Executive Advisor of System7 (Los Angeles company)
* Researcher of Research Institute, Chuo University



Contents of my lecture

（1）What is Biometric Authentication introductory explanation

（2）Features of Biometric Authentication
compared with other authentication methods

（3）4 major Biometric Authentication methods
fingerprint, face image, iris pattern, vein pattern

（4）Process of Biometric Authentication
process is almost the same for every method

（1）

First part of my lecture is

“What is Biometric Authentication”

“Biometric Authentication is personal identification/verification method using human body features.”

Usually, people judge whether a person is someone they are familiar with or not, by the similarity of human body features (face image, voice feature, etc.) of a familiar person.

Biometric Authentication uses almost the same method as the one that people usually use.

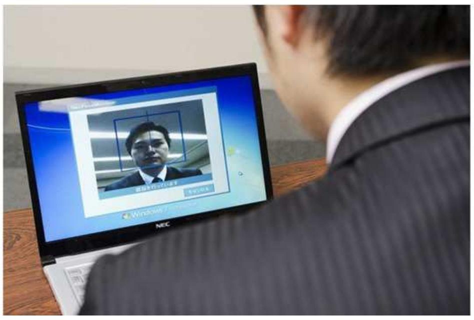
(1)the human body features of people who want to carry out personal identification/verification are registered beforehand

(2)the human body features of people who are going to be identified/verified are extracted

(3)two human body features are compared

(4)judges whether the person is a someone they know or not, according to the result of that comparison

Verification of PC Owner by Facial Authentication



Facial Authentication

http://www.gsd-inc.com/event/index.html

(1)PC stores owner’s facial feature in advance.

(2)PC gets facial feature of the person sitting down in front of PC.

(3)Comparing two facial features.

(4)Judge whether the person is owner or not based on that comparison result.

You don’t need to input user-id and password!

7

Summary of this part is …

Biometric Authentication is
a method using
human body features.

Biometric Authentication uses
almost the same method
as the one that people usually use.

（2）

Second part of my lecture is

"Features of Biometric Authentication compared with other authentication methods".

Three types of personal authentication methods

（1）Personal authentication by checking the information which only that person knows

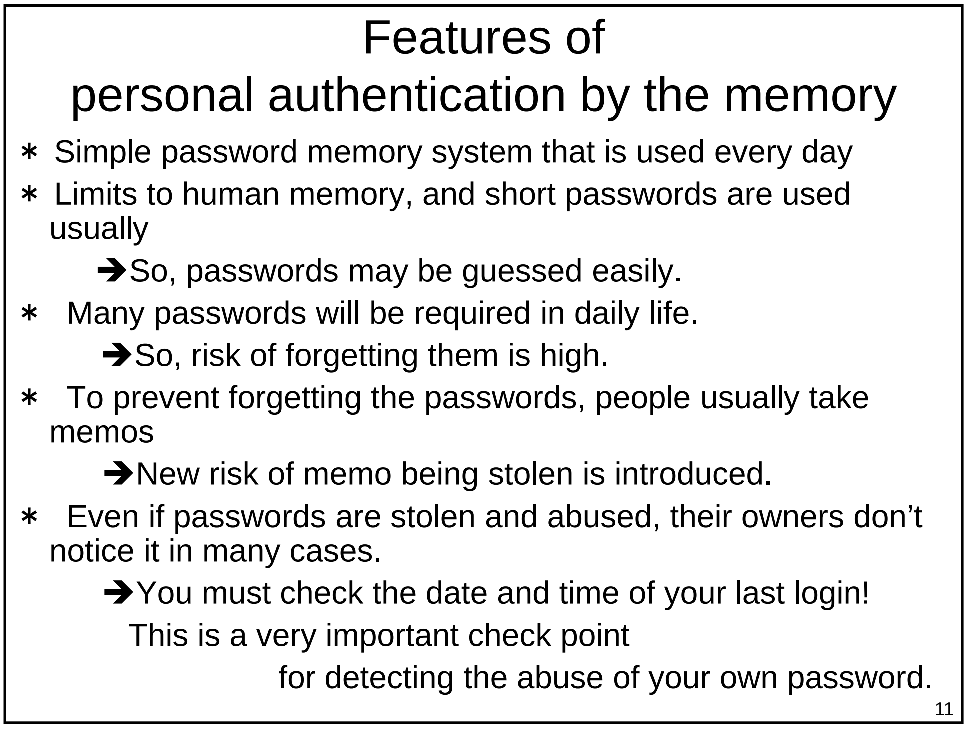
➔**Personal authentication by memory**

（2）Personal authentication by the thing which only that person has

➔**Personal authentication by the thing**

（3）Personal authentication by checking the human body feature which only that person has

➔**Personal authentication by the human body feature**
（**Biometric Authentication**）



Features of personal authentication by the memory

∗ Simple password memory system that is used every day

∗ Limits to human memory, and short passwords are used usually

➔So, passwords may be guessed easily.

∗ Many passwords will be required in daily life.

➔So, risk of forgetting them is high.

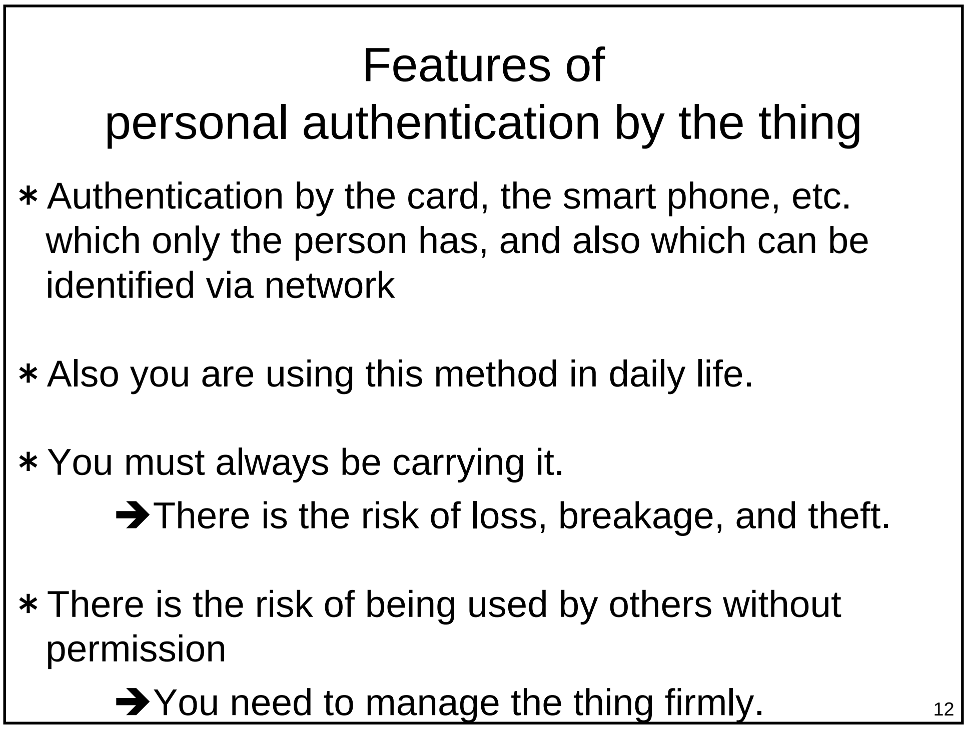
∗ To prevent forgetting the passwords, people usually take memos

➔New risk of memo being stolen is introduced.

∗ Even if passwords are stolen and abused, their owners don’t notice it in many cases.

➔You must check the date and time of your last login!
This is a very important check point
for detecting the abuse of your own password.

11



Features of personal authentication by the thing

∗ Authentication by the card, the smart phone, etc. which only the person has, and also which can be identified via network

∗ Also you are using this method in daily life.

∗ You must always be carrying it.

➔There is the risk of loss, breakage, and theft.

∗ There is the risk of being used by others without permission

➔You need to manage the thing firmly.

12

Features of personal authentication by the human body feature （Biometric Authentication）

∗ Forgery is difficult to make if compared with that of other systems.

∗ The personal authentication system, which doesn’t need any memory nor any thing, can be built by biometric authentication.

(But, it is used usually in combination with the memory or the thing.)

∗ This method sometimes requires a few times of scanning the human body feature.

(The reason is that the scanned images are often not of good quality. So, your human body feature must be scanned again.)

13

Summary of this part is …

Biometric Authentication is
an authentication method
using human body features.

Biometric Authentication is expected
to be a reliable authentication method.

(20m)

（3）

Third part of my lecture is

“Introduction of Major Biometric Authentication systems”

4 major authentication methods

＊Fingerprint Authentication（指紋認証）

Use the fact that fingerprint images and the presence / positional relationship of feature points are different for each individual

＊Facial Authentication（顔認証）

Use the fact that the positional relationships and shapes of facial images and facial parts are different for each individual

＊Iris Authentication（虹彩認証）

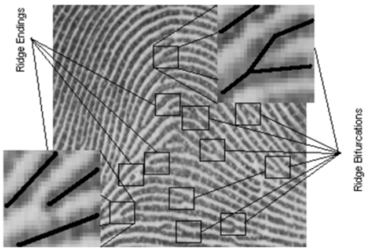
Use the fact that the iris pattern of the eyes is different for each individual

＊Vein Authentication（静脈認証）

Use that fact that the route of the venous blood vessels (pattern of blood flow) is different for each individual

Fingerprint（1）

- **Typical comparison method**
  - Typical methods use positions of the peculiar feature called “Minutiae”（マニューシャ） in the fingerprint pattern.
  - Typical “Minutiae” are Ridge（稜線） ending, Ridge bifurcation.



- **Accuracy**
  - Accuracy of fingerprint authentication is high in general.

  (The reason is that fingerprint authentication has been used for a long time for criminal investigation purposes.)

Fingerprint（2）

- **Features of usage**
  - Since an input sensor is usually a contact type, it can be miniaturized.
    - ➔ So, it can be embedded in equipment cheaply.
  - The data of required quality may not be obtained because of the dryness of the skin, perspiration（発汗）, crack（傷）, worn out（摩耗）, etc.
- **Places used**
  - It is used for registration of the candidate of social welfare etc. in the U.S.
  - It is being used without resistance in many situations where authentication is required.

Application to owner verification for personal device

Smartphone

PC

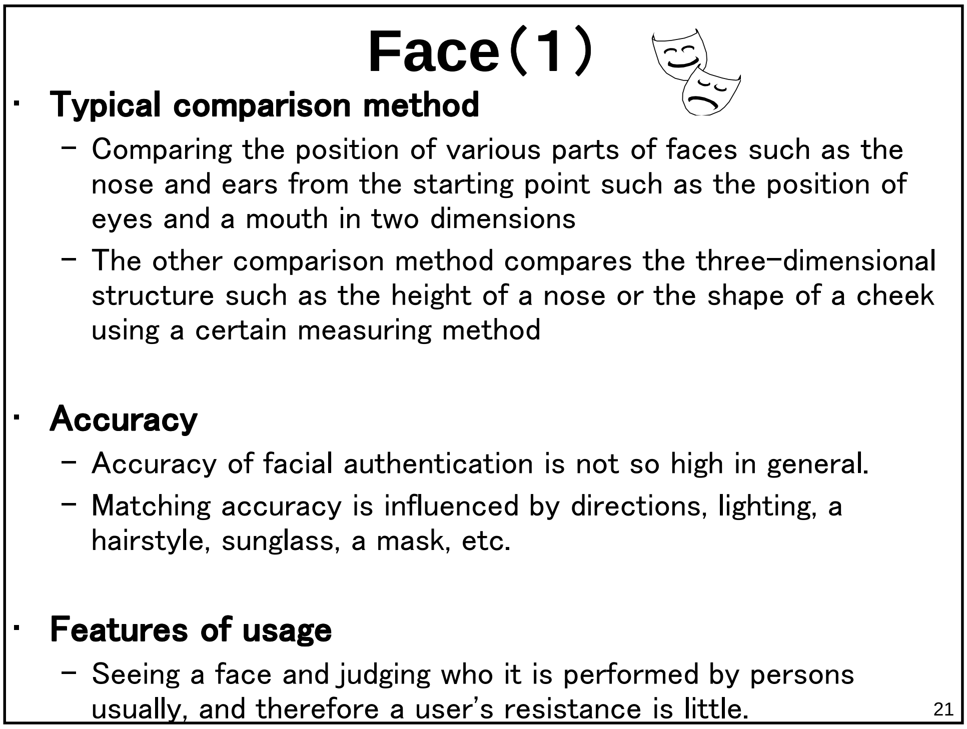
You can use it if the matching result between the scanned fingerprint and the owner's fingerprint registered in advance is good.

Application to authorization check of entering room/house

Server Room

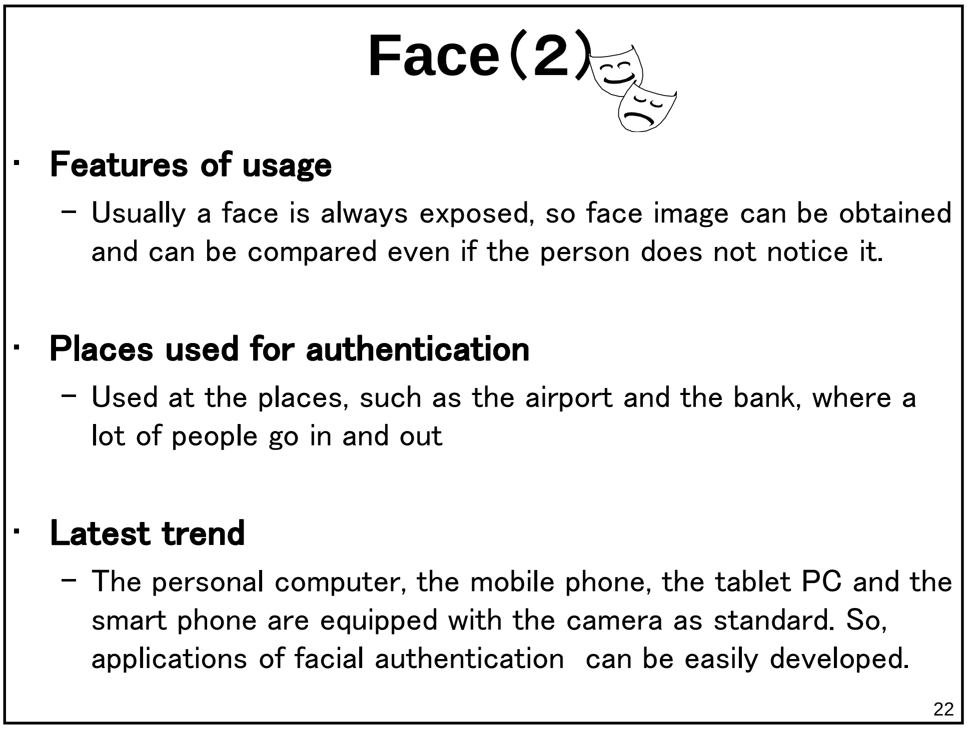
Home

You can enter in it if the matching result between the scanned fingerprint and one of the person’s fingerprint registered in advance is good.



Face(1)

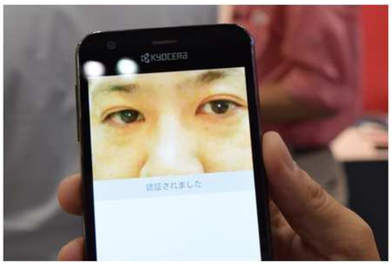
- **Typical comparison method**
  - Comparing the position of various parts of faces such as the nose and ears from the starting point such as the position of eyes and a mouth in two dimensions
  - The other comparison method compares the three-dimensional structure such as the height of a nose or the shape of a cheek using a certain measuring method
- **Accuracy**
  - Accuracy of facial authentication is not so high in general.
  - Matching accuracy is influenced by directions, lighting, a hairstyle, sunglass, a mask, etc.
- **Features of usage**
  - Seeing a face and judging who it is performed by persons usually, and therefore a user's resistance is little.



Face(2)

- **Features of usage**
  - Usually a face is always exposed, so face image can be obtained and can be compared even if the person does not notice it.
- **Places used for authentication**
  - Used at the places, such as the airport and the bank, where a lot of people go in and out
- **Latest trend**
  - The personal computer, the mobile phone, the tablet PC and the smart phone are equipped with the camera as standard. So, applications of facial authentication can be easily developed.

Application to owner verification for personal device

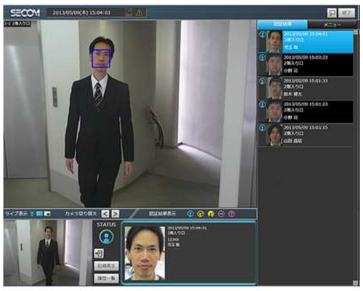


Smartphone

PC

You can use it if the matching result between the scanned face image and the owner's face image registered in advance is good.

Application to authorization check when entering and leaving



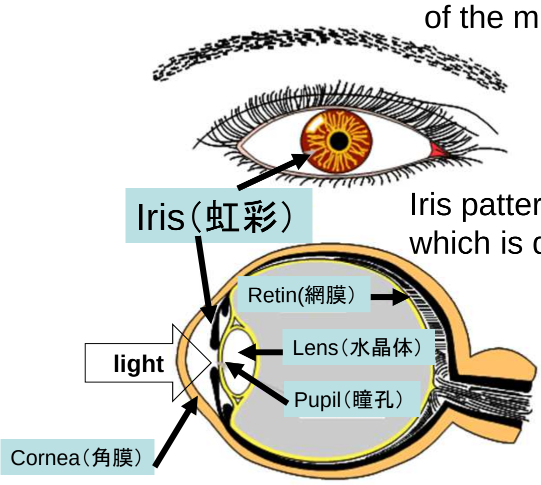
Office

Building

You can enter in it if the matching result between the scanned face image and one of the person’s face image registered in advance is good.

Iris（1）

Iris is a pattern on the surface of the muscles surrounding a pupil.



Iris pattern is this colored part which is different in each individual.

The muscles surrounding a pupil help regulate the amount of light entering the eye.

Iris（2）

- **Comparison method**
  - Comparing the iris pattern on the surface of the muscles surrounding a pupil
- **Accuracy**
  - Accuracy of iris authentication is high in general.
  - Iris pattern doesn’t change through lifetime.
- **Features of usage**
  - Iris is visible from the outside and the image can be obtained without contact.

Iris（3）

- **Latest trend**
  - The basic patent of iris authentication expired.
    New iris authentication algorithms are being developed
    so that cheap and compact implementation is possible.
  - It is expected that not only application with the conventional physical access security but also iris authentication will be utilized broadly from now on.

Application to owner verification for personal device

Smartphone

You can use it if the matching result between the scanned iris pattern and the owner's iris pattern registered in advance is good.

Application to authorization check when entering and leaving

Office

Mansion(Entrance)

You can enter in it if the matching result between the scanned iris pattern and one of the person’s iris pattern registered in advance is good.

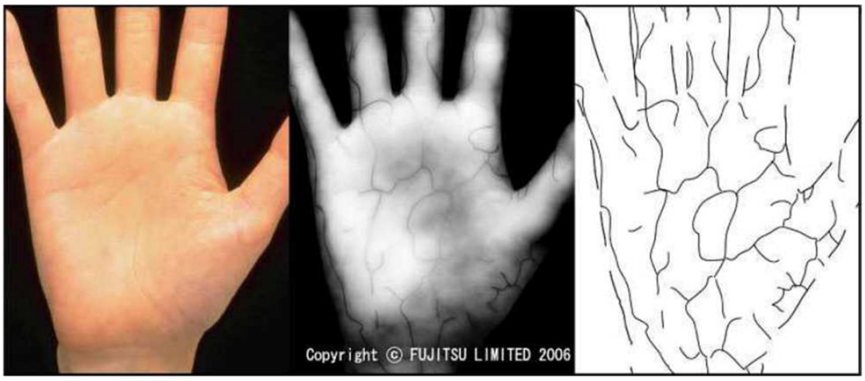
Vein（1）

- **Mechanism of vein authentication**
  - An artery（動脈） sends oxygenated hemoglobin into each bodily tissue, and supplies oxygen. A vein（静脈） returns the reduced hemoglobin（還元ヘモグロビン） which lost oxygen to the heart. The patterns of the blood flow are different among individuals.
  - Reduced hemoglobin absorbs light with a wavelength of about 760 nm of a near-infrared light domain（近赤外光領域）.
  - If near-infrared light is applied to a palm, only the vascular pattern（血管パターン） of a vein will be reflected darkly.
  - The vascular pattern of a vein gives a dark reflection.
- **Accuracy**
  - High accuracy comparable with that of the fingerprint and the iris is expectable.
  - There is almost no aging influence.

Vein (2)

- **Features of usage**
  - There are few contact portions and there is almost no resistance of a user.
- **Places used**
  - ATMs with Palm vein authentication developed by Fujitsu are installed in many banks such as Mitsubishi UFJ, Hiroshima, etc.
  - ATMs with Finger vein authentication developed by Hitachi are installed in many banks such as Sumitomo Mitsui, Yucho, and Mizuho, etc.
- **Technical feature**
  - The adaptation rate is good. (There are few people that can not use the vein authentication.)
  - Compared with other biometrics, forgery is difficult.

Palm vein pattern



(a) photograph of the palm by the ordinary camera

(b)photograph of the palm by the infrared camera

(c)outline and vein pattern of a palm

This vein pattern is different for each person.

Application to authorization check when entering and leaving

Office
<Palm vein>

出典：http://pr.fujitsu.com/jp/news/2005/08/18.html

Mansion(Entrance)
<Finger vein>

出典：http://www.kaji-gl.com/security/index.html

You can enter in it if the matching result between the scanned palm/finger vein pattern and one of the person’s palm/finger vein pattern registered in advance is good.

Application to account owner verification for ATM

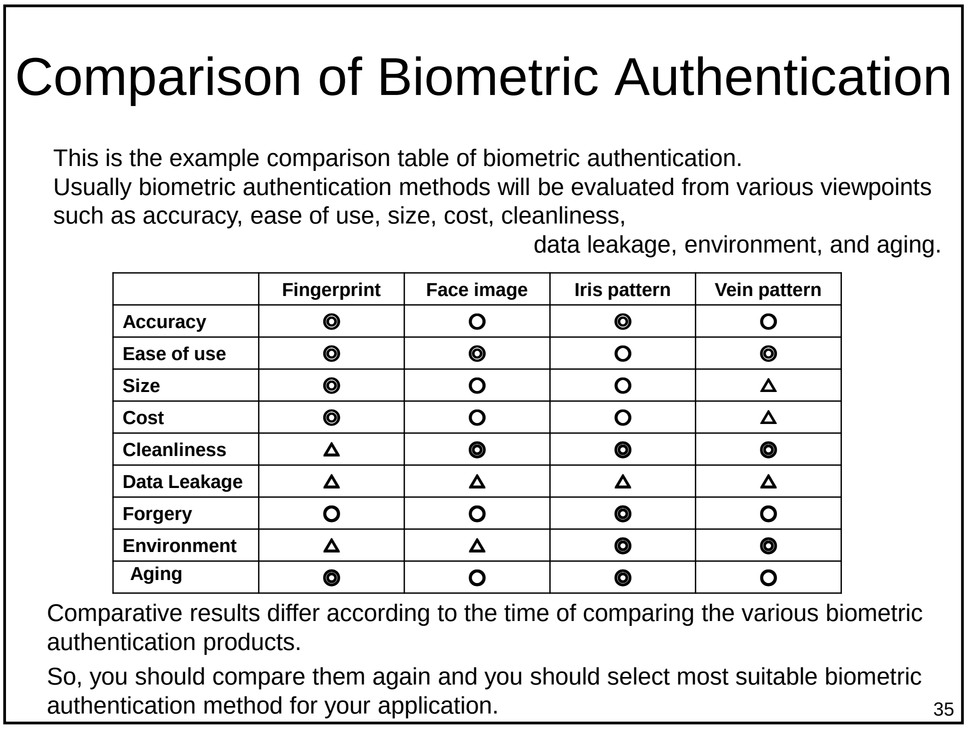
Finger vein

出典：http://www.itmedia.co.jp/mobile/articles/0410/01/news076.html

Palm vein

出典：http://jbpress.ismedia.jp/articles/-/42629

You can operate the ATM if the matching result between the scanned palm/finger vein pattern and the owner's palm/finger vein pattern stored in cash card is good.



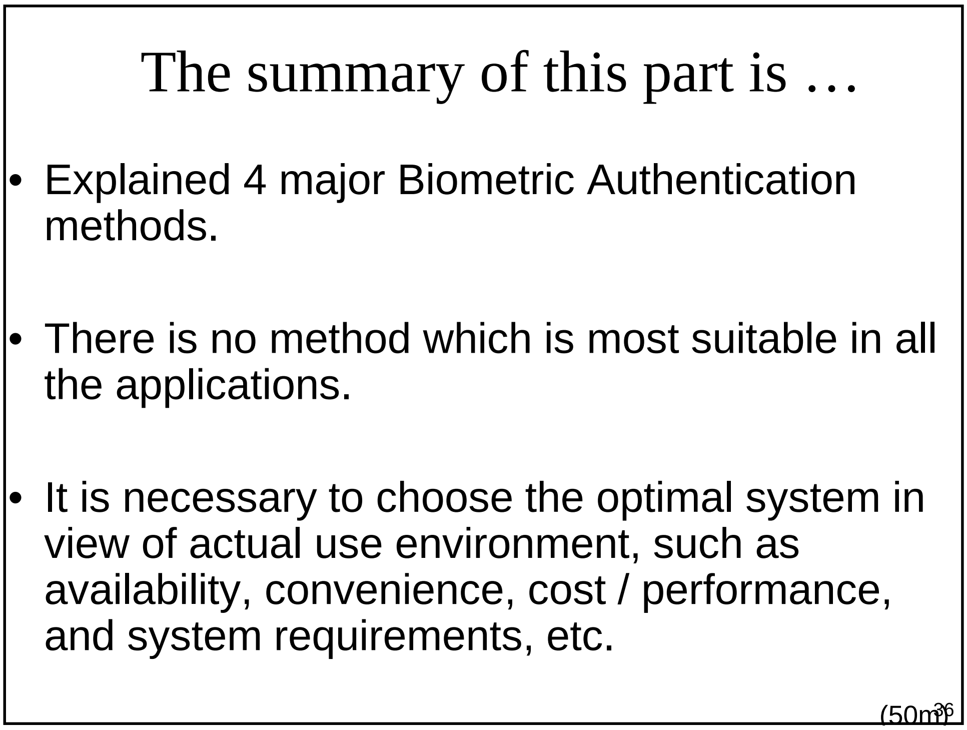
Comparison of Biometric Authentication

This is the example comparison table of biometric authentication.
Usually biometric authentication methods will be evaluated from various viewpoints such as accuracy, ease of use, size, cost, cleanliness, data leakage, environment, and aging.

	Fingerprint	Face image	Iris pattern	Vein pattern
Accuracy	◎	○	◎	○
Ease of use	◎	◎	○	◎
Size	◎	○	○	△
Cost	◎	○	○	△
Cleanliness	△	◎	◎	◎
Data Leakage	△	△	△	△
Forgery	○	○	◎	○
Environment	△	△	◎	◎
Aging	◎	○	◎	○

Comparative results differ according to the time of comparing the various biometric authentication products.

So, you should compare them again and you should select most suitable biometric authentication method for your application.



The summary of this part is …

- Explained 4 major Biometric Authentication methods.
- There is no method which is most suitable in all the applications.
- It is necessary to choose the optimal system in view of actual use environment, such as availability, convenience, cost / performance, and system requirements, etc.

(50m)

（4）

Fourth part of my lecture is

“Process of Biometric Authentication”

37

Procedure of Biometric Authentication

registration

Human body features extracted from people are registered with their names and personal information (template data)

feature extraction

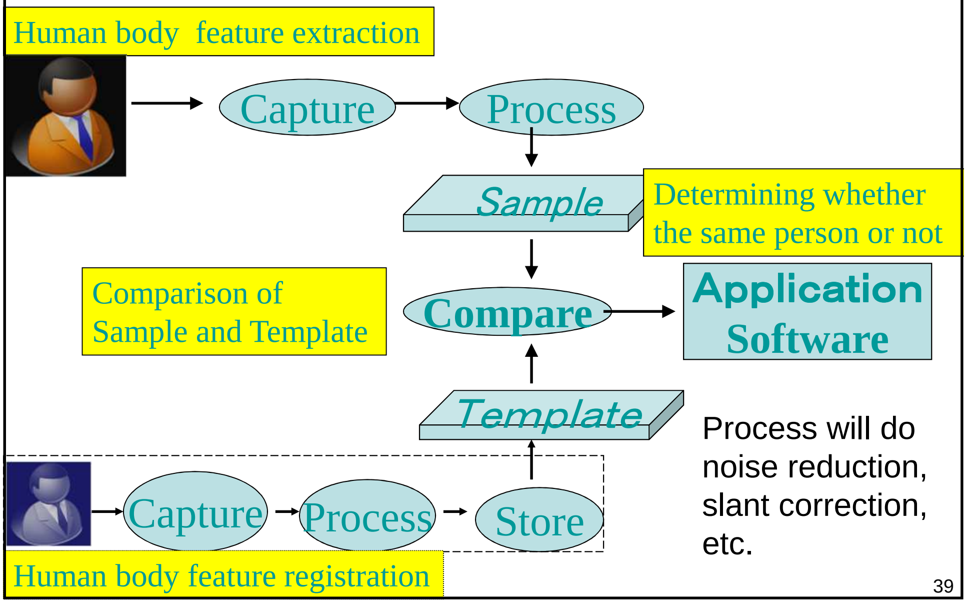
Human body features of a person who is going to be identified is extracted (sample data)

comparison and identification

By comparing the extracted feature from the person with the registered feature of all the candidate people, judge whether the person is identical with one of the people registered beforehand.

38

General Biometric Authentication Process



Human body feature extraction

Capture

Process

Sample

Determining whether the same person or not

Comparison of Sample and Template

Compare

Application Software

Template

Capture

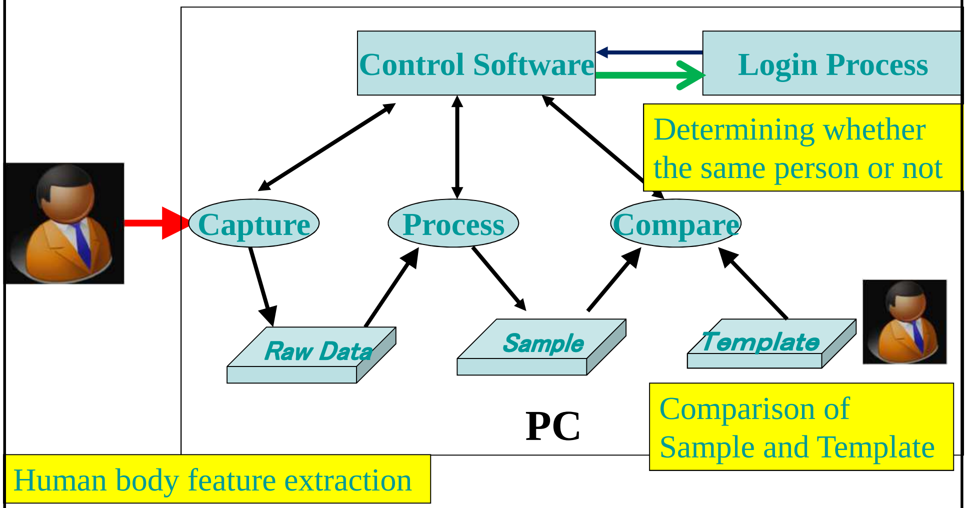
Process

Store

Human body feature registration

Process will do noise reduction, slant correction, etc.

Example Biometric Authentication Process — PC owner verification —



Control Software

Login Process

Determining whether the same person or not

Capture

Process

Compare

Raw Data

Sample

Template

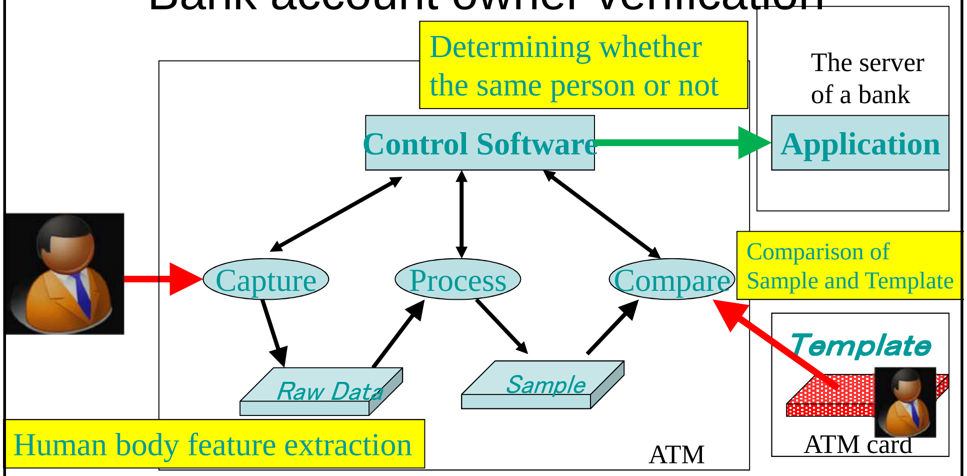
PC

Comparison of Sample and Template

Human body feature extraction

Template of PC owner is usually stored on PC hard disc.
Only the PC owner can login this PC.

Example Biometric Authentication Process
－ Bank account owner verification －


Determining whether the same person or not

The server of a bank

Control Software

Application

Capture

Process

Compare

Comparison of Sample and Template

Template

Raw Data

Sample

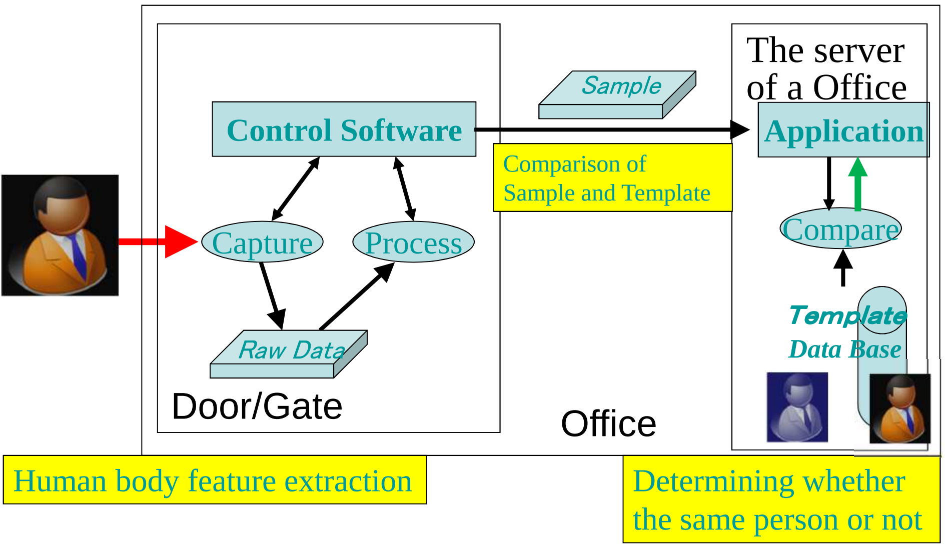
Human body feature extraction

ATM

ATM card

The important point of this system is that the user's template is being stored on the ATM card which the user itself is carrying.
Because template is the personal information which will pose a big problem if it leaks, the bank doesn't want to store user's template on their server.
Only the account owner can access his own account at ATM.

Example Biometric Authentication Process
－ Entrance authorization verification －


The server of a Office

Sample

Control Software

Application

Comparison of Sample and Template

Capture

Process

Compare

Template Data Base

Raw Data

Door/Gate

Office

Human body feature extraction

Determining whether the same person or not

Templates of registered people are usually stored on the server of office.
Only authorized person can pass the door/gate.

Summary of this part is

- Although there are various biometric authentication methods, the process is almost the same. And Biometric Authentication process uses almost the same method as the one that people usually use.
- Sensor captures the human body feature and processes it and stores it as the sample.
- And then, the sample will be compared with the template stored beforehand.
- And then, it judges that the person who has sample data is the same person whose human body feature was extracted as the template.
- Biometric data such as template and sample should be managed carefully due to sensitive personal data.

End

(60m)

Supplementary explanation on 3 Topics

(1)Classification of biometric authentication by the type of body feature

(2)Accuracy of biometric authentication

(3)Bio PKI

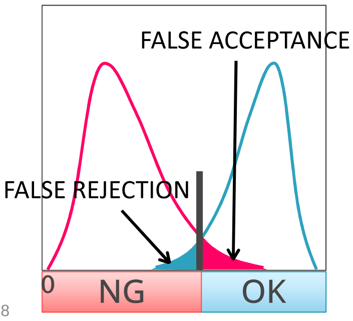
(1)Classification of biometric authentication by the type of body feature

- **Static feature of body（身体的特徴）によるもの）**
  - ❍ Face（顔）
  - ❍ Retina（網膜）
  - ❍ Iris（虹彩）
  - ❍ Fingerprint（指紋）
  - ❍ Finger vein（指静脈）
  - ❍ Palm vein（手のひら静脈）
  - ❍ DNA
- **Dynamic feature of body（行動的特徴によるもの）**
  - ❍ Voiceprint（声紋）
  - ❍ Sign（署名）
  - ❍ Keystroke（キーストローク）

(2)Accuracy of authentication

Biometrics

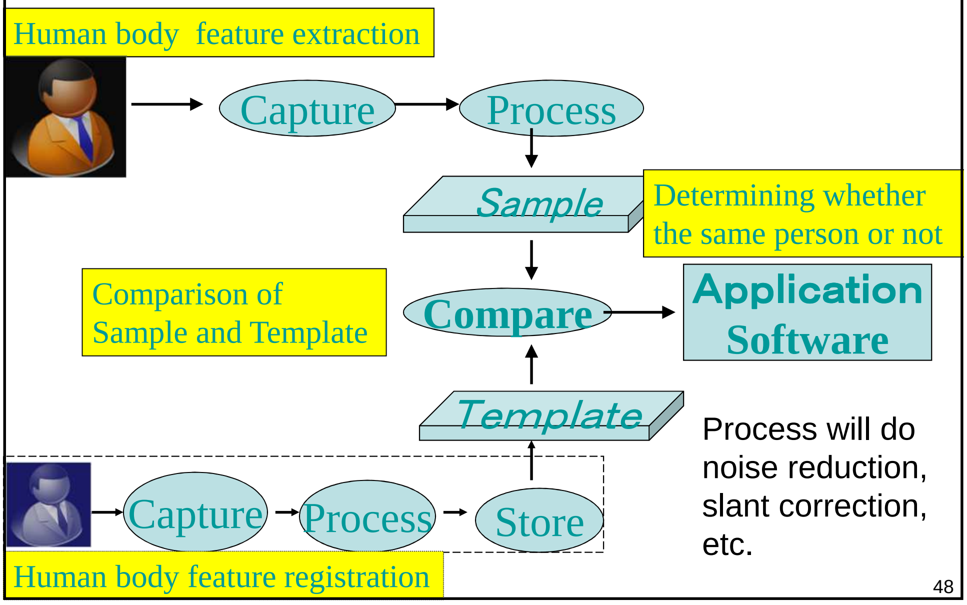
- Any modals have risk of false acceptance and false rejection.



Password

- If user input correct password, system surely accepts.

General Biometric Authentication Process



Human body feature extraction

Capture → Process → Sample → Compare → Application Software

Determining whether the same person or not

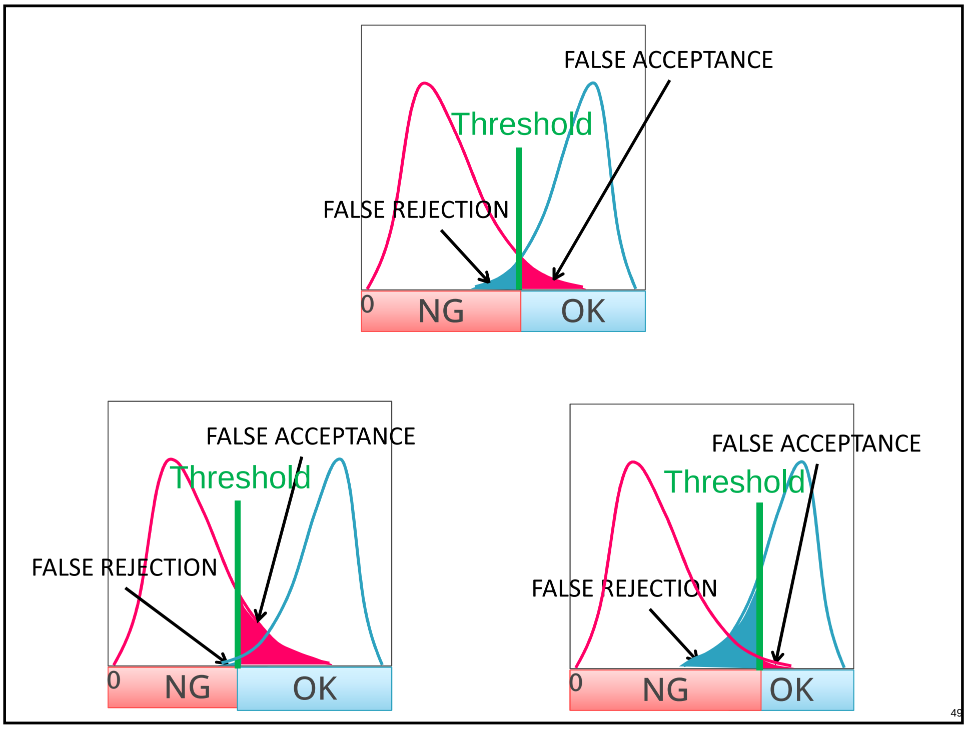
Comparison of Sample and Template

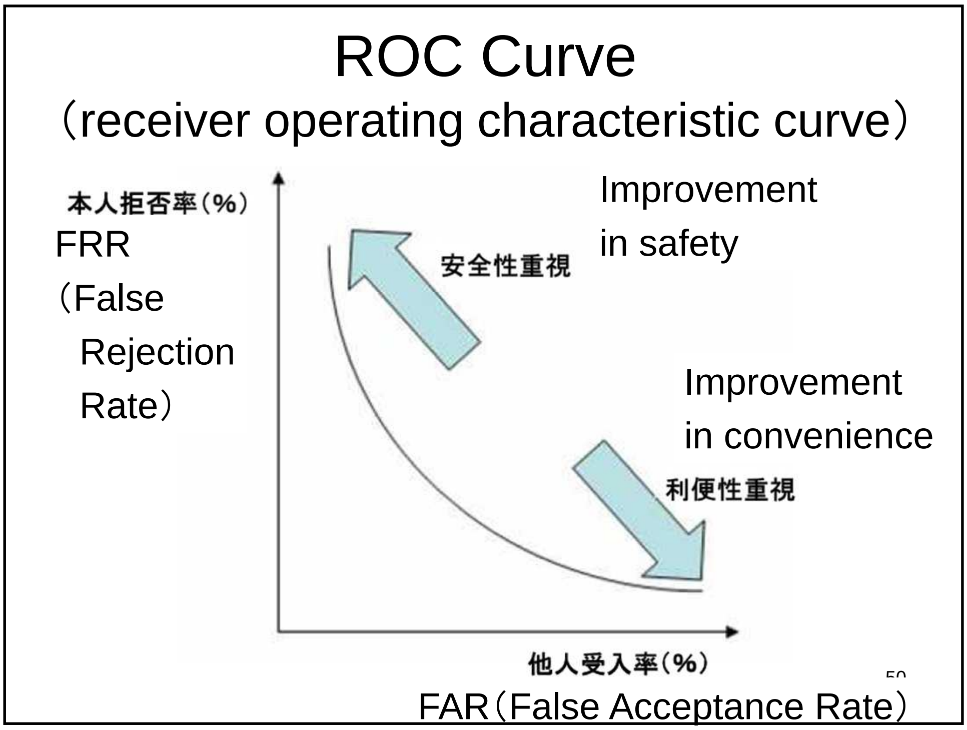
Template

Capture → Process → Store

Human body feature registration

Process will do noise reduction, slant correction, etc.





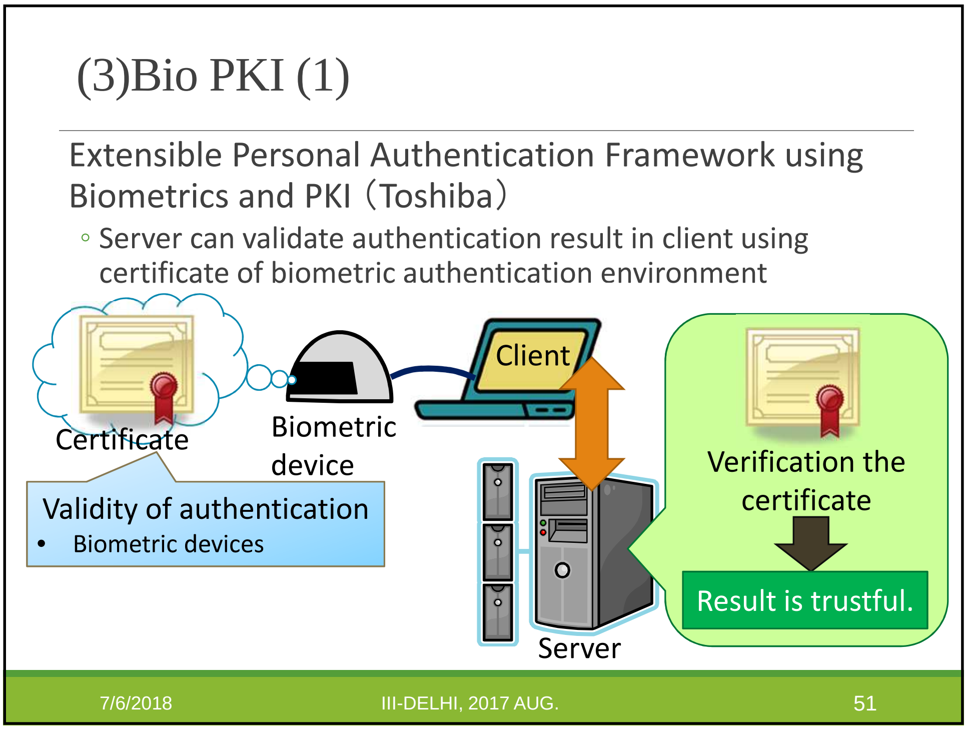
ROC Curve
（receiver operating characteristic curve）

FRR（False Rejection Rate）

Improvement in safety

Improvement in convenience

FAR（False Acceptance Rate）



(3)Bio PKI (1)

Extensible Personal Authentication Framework using Biometrics and PKI（Toshiba）

- Server can validate authentication result in client using certificate of biometric authentication environment

Certificate

Biometric device

Client

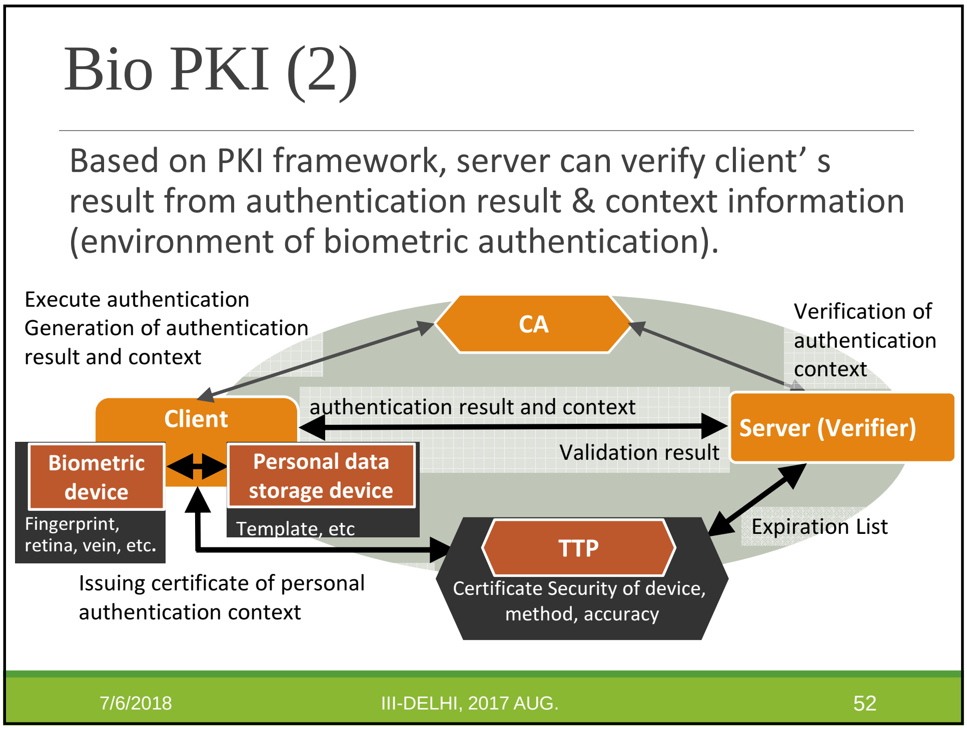
Validity of authentication

- Biometric devices

Server

Verification the certificate

Result is trustful.



Bio PKI (2)

Based on PKI framework, server can verify client’ s result from authentication result & context information (environment of biometric authentication).

Execute authentication
Generation of authentication result and context

CA

Verification of authentication context

Client

authentication result and context

Server (Verifier)

Validation result

Biometric device

Fingerprint, retina, vein, etc.

Personal data storage device

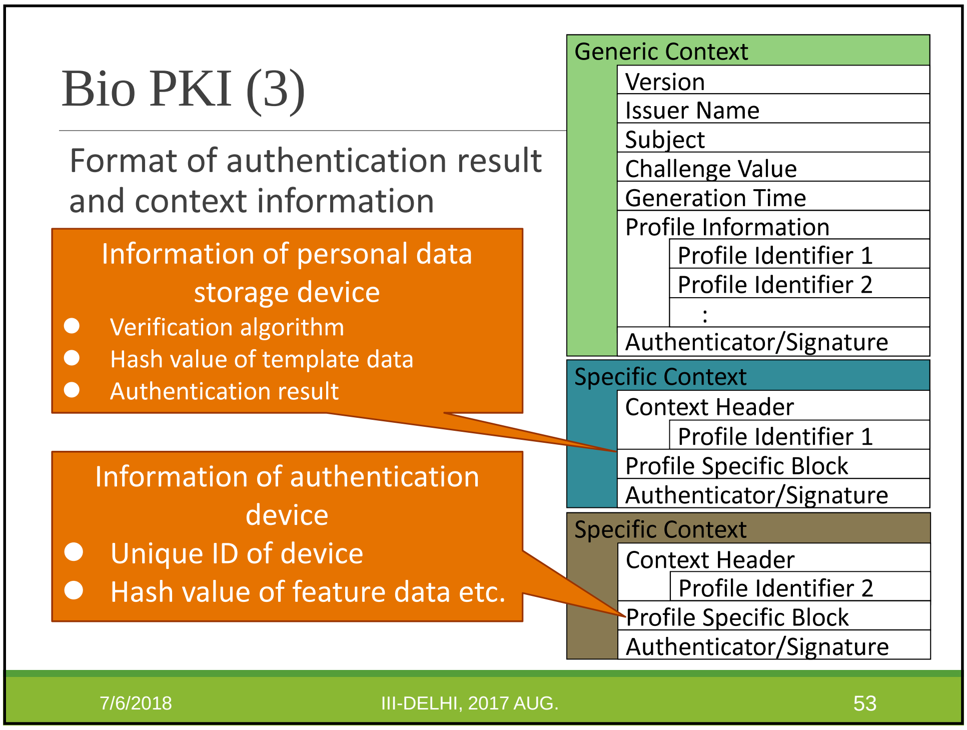
Template, etc

TTP

Certificate Security of device, method, accuracy

Expiration List

Issuing certificate of personal authentication context



Bio PKI (3)

Format of authentication result and context information

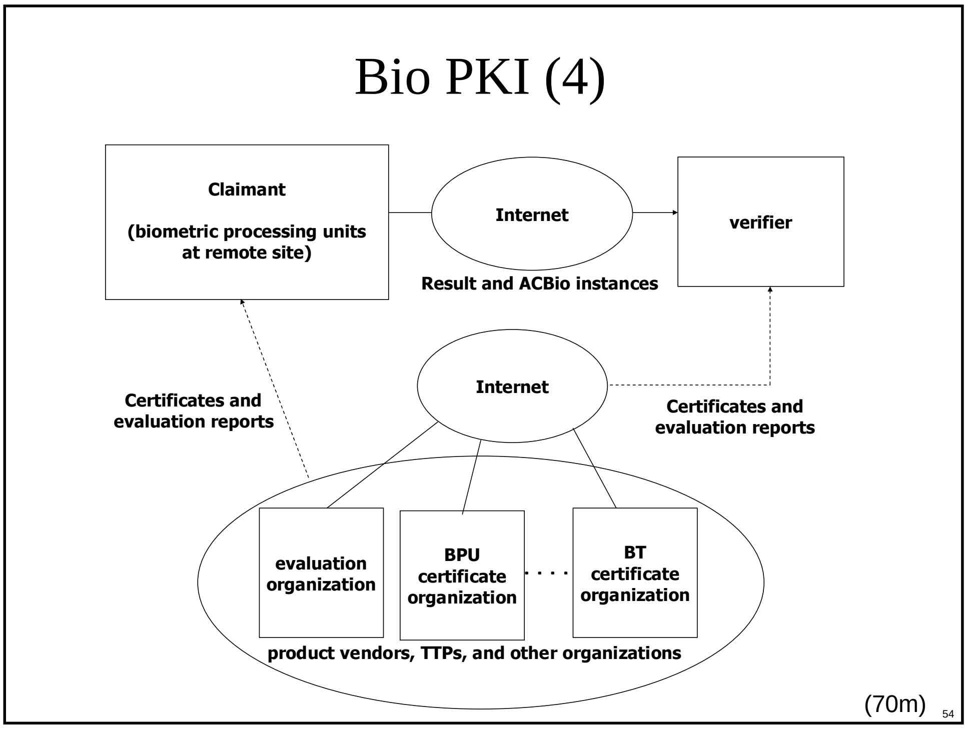
Information of personal data storage device

- Verification algorithm
- Hash value of template data
- Authentication result

Information of authentication device

- Unique ID of device
- Hash value of feature data etc.

- Generic Context
  - Version
  - Issuer Name
  - Subject
  - Challenge Value
  - Generation Time
  - Profile Information
    - Profile Identifier 1
    - Profile Identifier 2
    - :
  - Authenticator/Signature
- Specific Context
  - Context Header
    - Profile Identifier 1
  - Profile Specific Block
  - Authenticator/Signature
- Specific Context
  - Context Header
    - Profile Identifier 2
  - Profile Specific Block
  - Authenticator/Signature

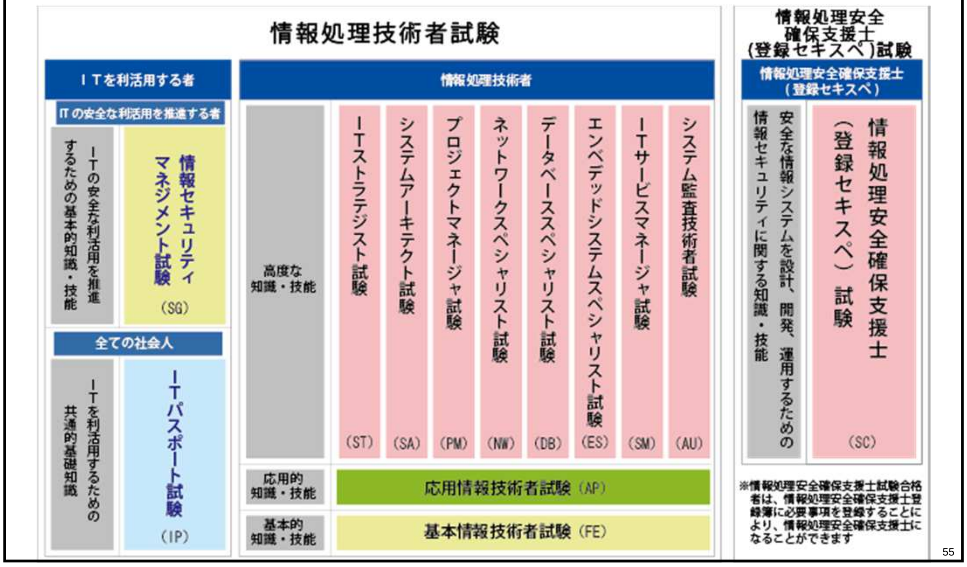


Bio PKI (4)

Claimant
(biometric processing units at remote site)
Internet
verifier
Result and ACBio instances
Internet
Certificates and evaluation reports
Certificates and evaluation reports
evaluation organization
BPU certificate organization
· · · ·
BT certificate organization
product vendors, TTPs, and other organizations

(70m)

Information Technology Engineers Examination



情報処理技術者試験

ＩＴを利活用する者

IT の安全な利活用を推進する者

ＩＴの安全な利活用を推進するための基本的知識・技能

情報セキュリティマネジメント試験 (SG)

全ての社会人

ＩＴを利活用するための共通的基礎知識

ＩＴパスポート試験 (IP)

情報処理技術者

高度な知識・技能

ＩＴストラテジスト試験 (ST)

システムアーキテクト試験 (SA)

プロジェクトマネージャ試験 (PM)

ネットワークスペシャリスト試験 (NW)

データベーススペシャリスト試験 (DB)

エンベデッドシステムスペシャリスト試験 (ES)

ＩＴサービスマネージャ試験 (SM)

システム監査技術者試験 (AU)

応用的知識・技能

応用情報技術者試験 (AP)

基本的知識・技能

基本情報技術者試験 (FE)

情報処理安全確保支援士(登録セキスペ)試験

情報処理安全確保支援士(登録セキスペ)

安全な情報システムを設計、開発、運用するための情報セキュリティに関する知識・技能

情報処理安全確保支援士（登録セキスペ）試験 (SC)

※情報処理安全確保支援士試験合格者は、情報処理安全確保支援士登録簿に必要事項を登録することにより、情報処理安全確保支援士になることができます

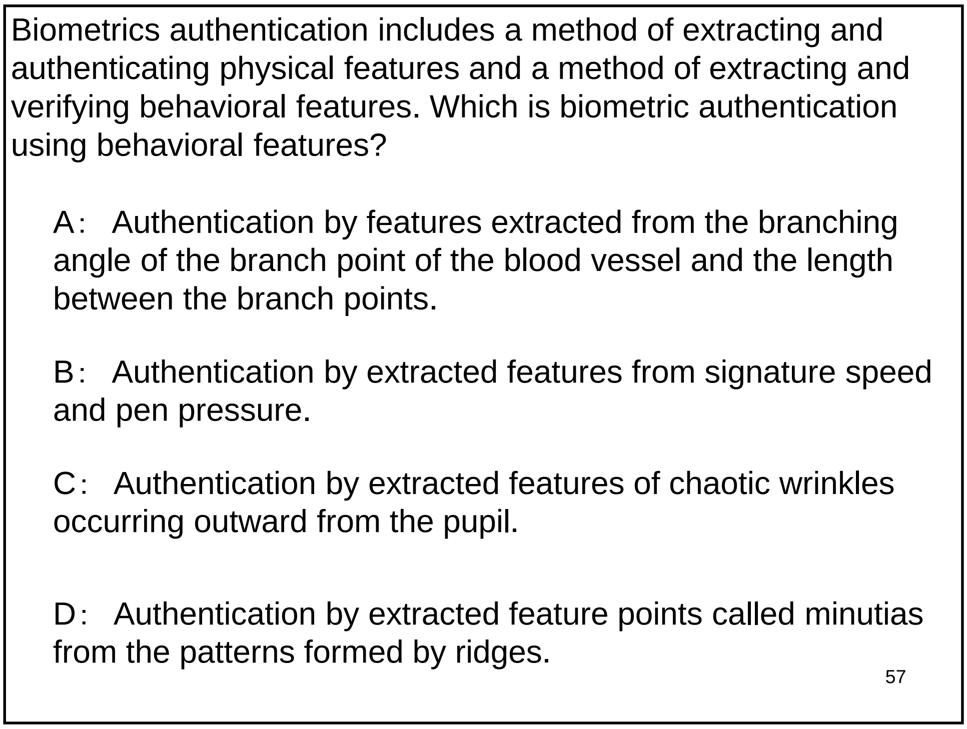
Which is biometric authentication that checks images input from compact optical sensors or thin electrostatic sensors by feature point extraction method or pattern matching?

A: Iris Authentication

B: Fingerprint Authentication

C: Voiceprint Authentication

D: Retina Authentication



Biometrics authentication includes a method of extracting and authenticating physical features and a method of extracting and verifying behavioral features. Which is biometric authentication using behavioral features?

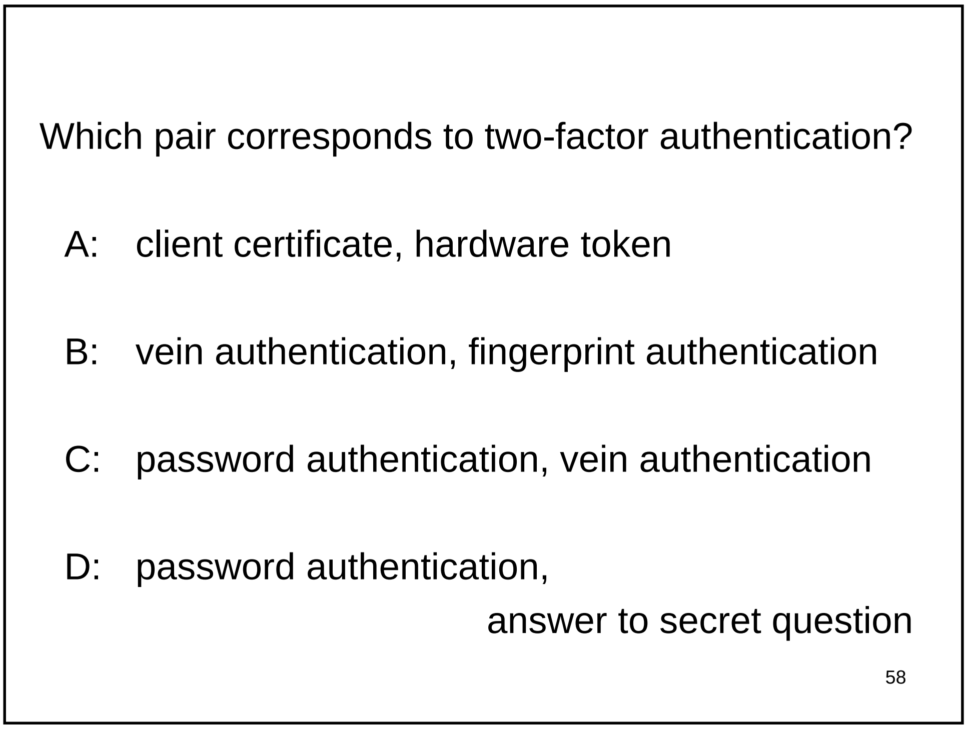
A: Authentication by features extracted from the branching angle of the branch point of the blood vessel and the length between the branch points.

B: Authentication by extracted features from signature speed and pen pressure.

C: Authentication by extracted features of chaotic wrinkles occurring outward from the pupil.

D: Authentication by extracted feature points called minutias from the patterns formed by ridges.

57



Which pair corresponds to two-factor authentication?

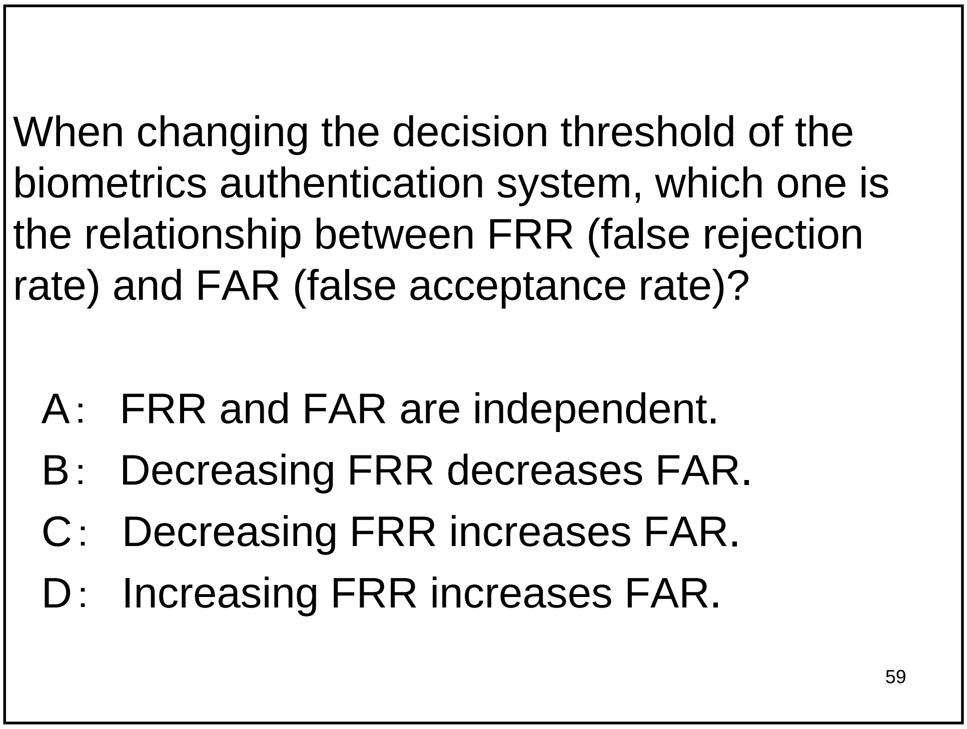
A: client certificate, hardware token

B: vein authentication, fingerprint authentication

C: password authentication, vein authentication

D: password authentication,
answer to secret question

58



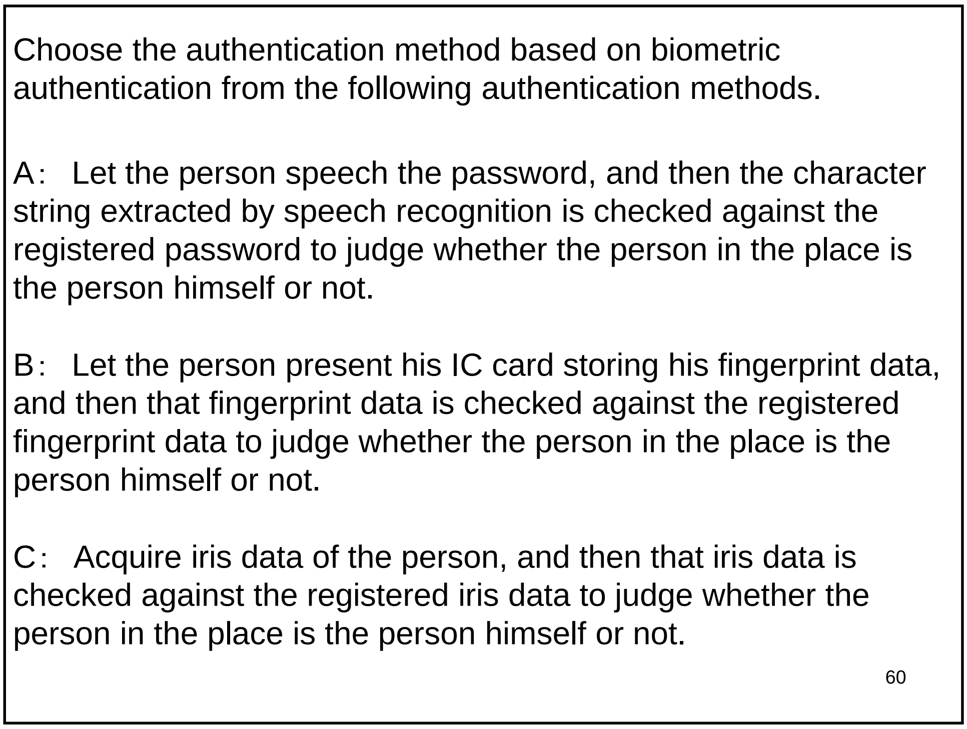
When changing the decision threshold of the biometrics authentication system, which one is the relationship between FRR (false rejection rate) and FAR (false acceptance rate)?

A: FRR and FAR are independent.

B: Decreasing FRR decreases FAR.

C: Decreasing FRR increases FAR.

D: Increasing FRR increases FAR.



Choose the authentication method based on biometric authentication from the following authentication methods.

A: Let the person speech the password, and then the character string extracted by speech recognition is checked against the registered password to judge whether the person in the place is the person himself or not.

B: Let the person present his IC card storing his fingerprint data, and then that fingerprint data is checked against the registered fingerprint data to judge whether the person in the place is the person himself or not.

C: Acquire iris data of the person, and then that iris data is checked against the registered iris data to judge whether the person in the place is the person himself or not.