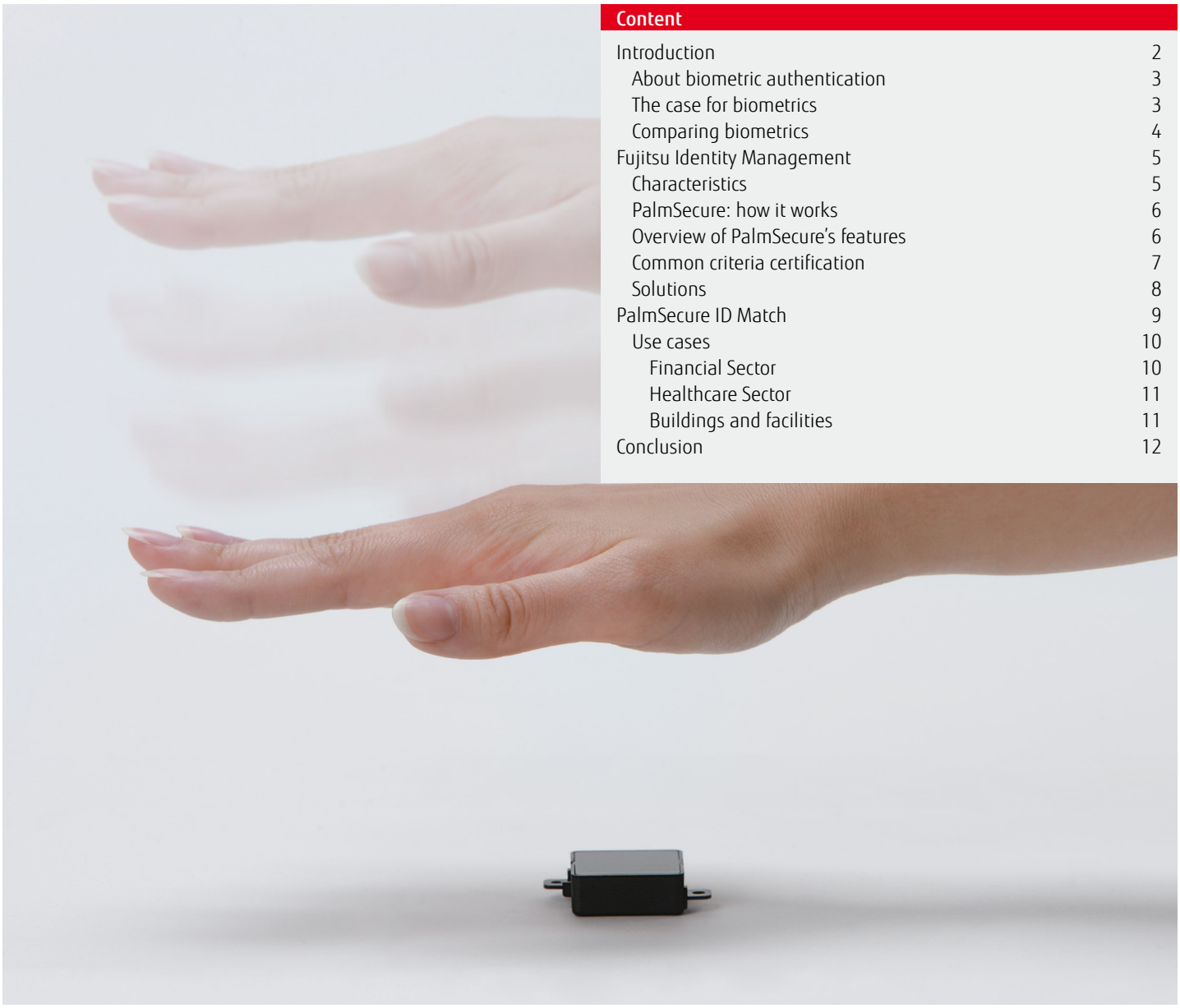
White paper
Fujitsu Identity Management and PalmSecure

To protect your business, it's critical that you can control who accesses your data, systems and premises. Today, many organizations rely on passwords or cards to confirm people's identity. But these are easily lost, stolen or copied. Biometric authentication is different. It uses a unique physical trait to recognize legitimate workers or registered customers. With technology like palm-vein pattern recognition, Fujitsu is at the forefront of using biometrics for effective identity management.

Content



Introduction

Traditional forms of identification usually involve something you know (like a password or PIN) or something you have (like an ID card). The problem is people can easily lose, steal, share or forget codes and cards.

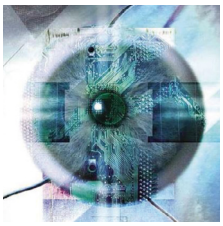
You can avoid this risk by using biometric authentication. Rather than presenting a card or remembering a password, people prove their identity with a unique biological characteristic. They will always have it with them. And they cannot transfer it to someone else.

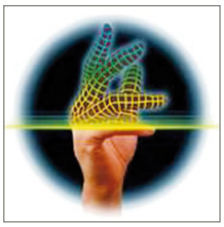
Fujitsu has developed several types of biometric authentication, including fingerprints, faces, voiceprints, and palm veins. The best one to use depends on the environment and the needs of your business.

In this white paper, you can take a closer look at our palm-vein recognition technology. Called PalmSecure, it is both accurate and hygienic. This has made it effective in public places and in the financial and health sectors. Read on to learn how it works, and how organizations are using it for better identity management.

About biometric authentication

Biometric characteristics are unique biological traits like iris patterns, fingerprints or palm-vein patterns. New technologies measure, capture and then match these characteristics to confirm someone's identity.





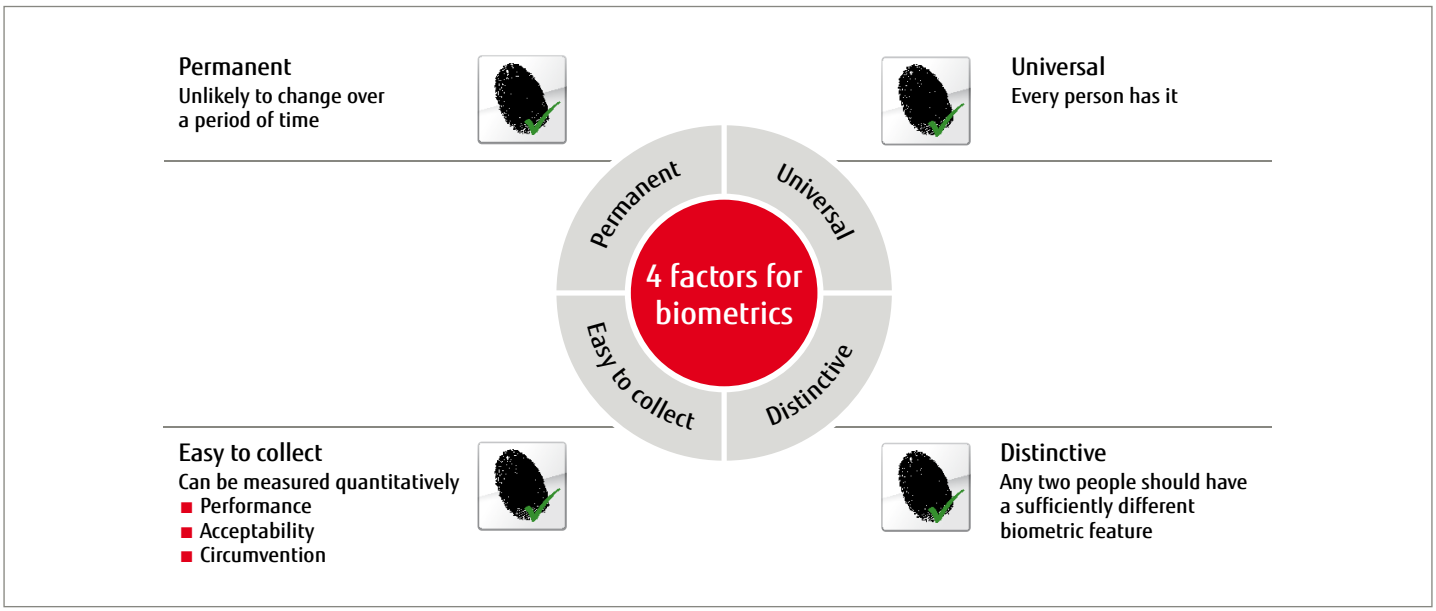
Unlike tokens, passwords and smart cards, biometric features are incredibly hard to steal. This helps to combat identity and data theft, hacking and skimming.

Various biometric technologies have been developed and launched to the market. To select the right one, you must consider carefully the needs of your organization. Before introducing a biometric method, you will analyze factors like the environment, cost, speed, accuracy and acceptance by users.

The case for biometrics

An effective method of biometric authentication will be:

- **Permanent**
  Ideally, the biometric feature will not change during someone's lifetime. This removes the need to re-enroll, saving time and money.
- **Universal**
  Each person should have this feature and be able to use the chosen technology.
- **Easy to collect**
  It should be easy for the biometric authentication technology to measure the biometric feature.
- **Distinctive**
  The feature has to be unique to each individual.



Furthermore, biometric technologies should also fulfil the following criteria:

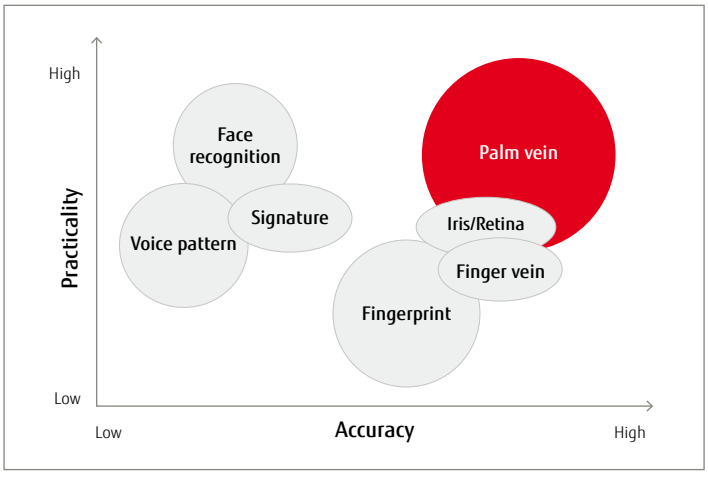
- **Safe:** it is important to test the biometric sensor and its algorithm using methods specified by the appropriate ISO standard – so that international authorities, institutes or organizations approve the technology.
- **Easy to use:** each person should be able to use the specific biometric application regardless of age, gender, ethnic origin or profession. Nor should the following factors prevent people using it: wearing glasses, contact lenses or a beard; using a wheelchair; high or low blood pressure; illness; use of oil or cream on skin; external injuries.
- **Right for the environment:** when choosing a biometric technology, take in to account conditions such as quality of light and weather.
- **Right for your budget:** compare the cost of installing and operating the biometric application to the increased security, and enhanced experience for the people using it. If you will spend less time maintaining the authentication method, this will also contribute to a return on investment.

In order to enhance security, organizations often combine a biometric and a traditional method to create 'two-factor' authentication. Financial services firms typically use this approach for tasks like making transactions.

It is also possible to store the biometric template created during enrollment on a smart card or debit card, which remains in the possession of the individual. This prevents the storage of biometric data in a central location.

Comparing biometrics

As already mentioned, choosing the right biometric technology depends on a wide range of factors. In the graph below, we compare some of the most common technologies by the criteria "accuracy" and "practicality".



Fujitsu's PalmSecure technology uses a biometric pattern inside the body. It is certified by ISO and approved by the German Ministry of IT Security.

The following table ranks biometric methods on their False Acceptance Rate (FAR) and False Rejection Rate (FRR). These indicators define the security level of a biometric system (FAR) and the usability of a biometric system (FRR).

False Acceptance Rate (FAR) and False Rejection Rate Comparison (FRR)

Authentication method	FAR (%)	If FRR (%)
Face recognition	≈ 1.3	≈ 2.6
Voice pattern	≈ 0.01	≈ 0.3
Fingerprint	≈ 0.001	≈ 0.1
Finger vein	≈ 0.0001	≈ 0.01
Iris/Retina	≈ 0.0001	≈ 0.01
Fujitsu Palm vein	< 0.00001	≈ 0.01

FAR = false acceptance rate: The probability that the system incorrectly matches the input pattern to a non-matching template in the database. It measures the percentage of invalid inputs which are incorrectly accepted.

FRR = false rejection rate: The probability that the system fails to detect a match between the input pattern and a matching template in the database. It measures the percentage of valid inputs which are incorrectly rejected.

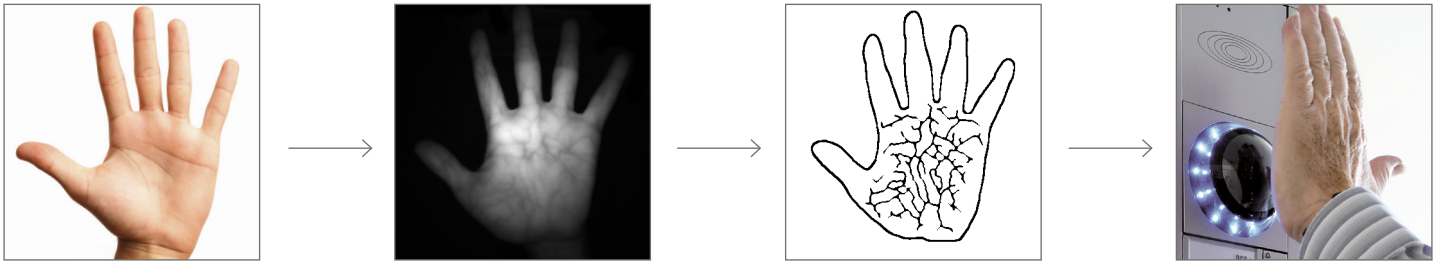
In the case of PalmSecure, the probability of an unauthorized person falsely gaining access (FAR case) is about 0.00001%. And the probability of an authorized person being incorrectly denied access is about 0.01% (valid for 1:1 verification)

Fujitsu
Identity Management

Fujitsu has developed a contactless palm-vein pattern recognition technology, called Fujitsu PalmSecure. It accurately identifies an individual using the complex vein pattern in the palm of their hand. The technology is incredibly secure – only granting access if blood is flowing through the circulatory system.

Characteristics

The PalmSecure sensor captures more than five million reference points from someone's palm-vein pattern to confirm their identity. The image capture and matching processes work without the need to touch the sensor's surface, making it very hygienic. A person's palm-vein pattern remains the same throughout their life. Every palm-vein pattern is also unique. Individuals have different patterns in their left and their right hands, and even twins have different patterns.



a) Visible ray image

b) Infrared ray image

c) Extracted vein pattern

Principles of vascular pattern authentication

Hemoglobin in the blood is oxygenated in the lungs and carries that oxygen to the tissues of the body through the arteries. After it releases its oxygen to the tissues, the deoxidized hemoglobin returns to the heart through the veins. These two types of hemoglobin have different rates of absorbency. Deoxidized hemoglobin absorbs light at a wavelength of about 760 nm, in the near-infrared range. When the near-infrared light illuminates the palm, unlike the image seen by the human eye [Figure a], the deoxidized hemoglobin in the palm veins absorbs this light. This reduces the reflection rate and causes the veins to appear as a black pattern [Figure b]. This pattern is photographed with near-infrared light, extracted by image processing [Figure c] and registered.

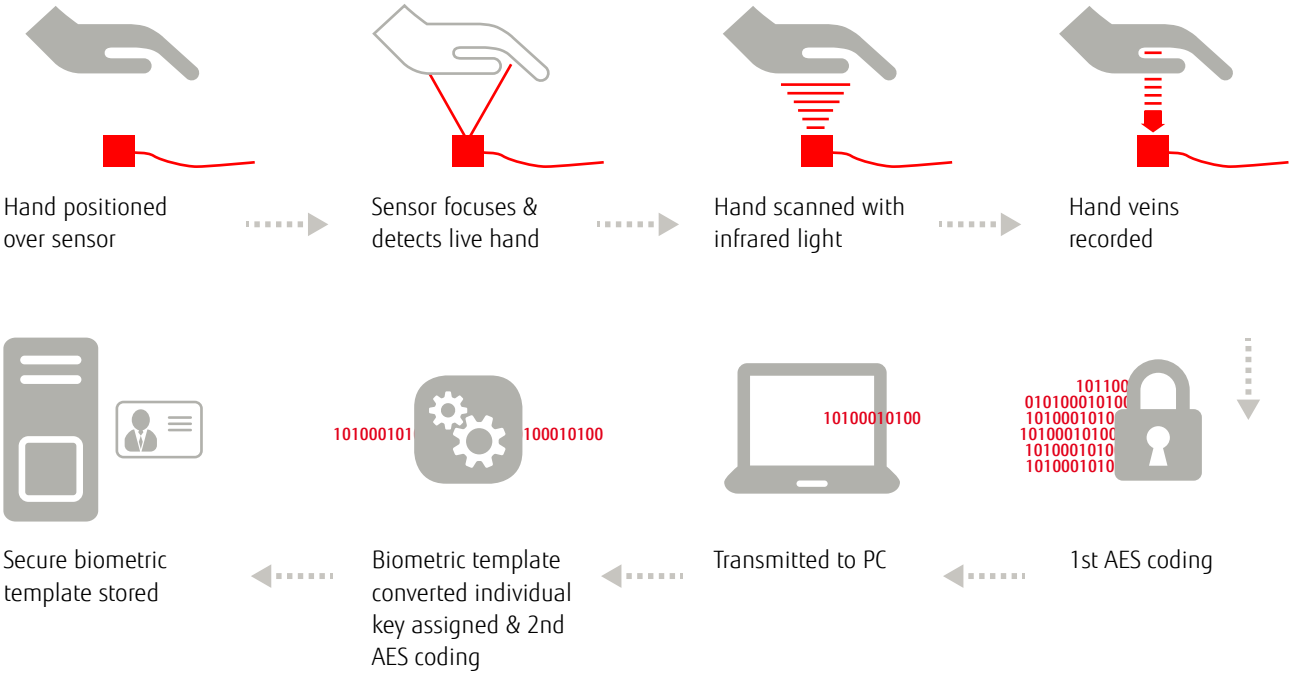
Benefits of palm vein technology

- **Contactless operation**
  - Hygienic
  - Less resistance from users
  - Suitable for public use
  - Quick recognition
- **Applicability rate**
  - Almost everyone can register (even with fingerprints, two percent to three percent cannot register)
  - More complex: with more reference points, there are fewer failures
- **Uses information from inside the body**
  - Difficult to copy (blood is always flowing)
  - Palm veins are unique and permanent
- **High performance, high security**
  - FRR = 0.01 percent (rejection rate for authorized users)
  - FAR = 0.00001 percent (acceptance rate of unauthorized users)

PalmSecure: how it works

The following chart shows PalmSecure in action. When a person places their hand above the PalmSecure sensor, it emits a near-infrared light. The near-infrared light records the palm vein pattern and the sensor encrypts the received data. After transferring the encrypted data to the PC, the software converts it to a biometric template and assigns it an individual key.

It is possible to store the protected biometric template on a PC, device or chip. We agree the best way to match and store the data with you, based on your organization's individual requirements.



A brief overview of PalmSecure's features

Highly accurate

PalmSecure has a proven false rejection rate of 0.01 percent and a false acceptance rate of less than 0.00001 percent. No other system in the world can match this performance.

Easy to use

Using PalmSecure is effortless. Scanning is intuitive and people feel no mental resistance to it.

Hygienic and non-invasive

Because the system is contactless, it is completely hygienic. This is useful in most situations, but especially in hospitals and other medical settings. In addition, PalmSecure is non-invasive. The near-infrared rays used in the scanner have no effect on the body.

Easy to integrate

We can embed the PalmSecure system in all kinds of flat products, including laptops copiers, printers, fax machines, access systems, and eventually even mobile phones.

Value propostion

Fujitsu PalmSecure's value proposition is based on three factors: 'ease of use', 'cost' and 'security'.

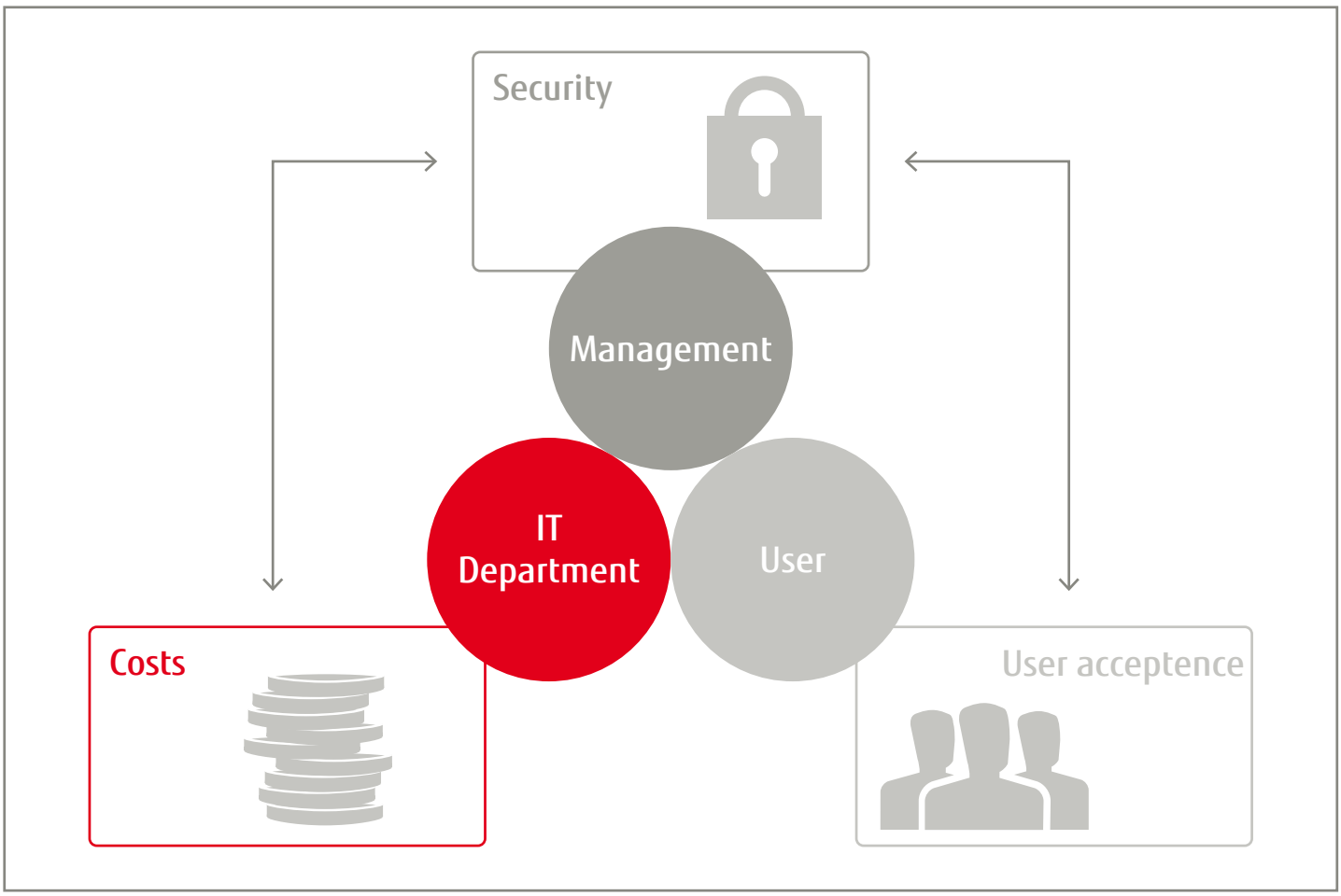
- **Ease of use**
  - PalmSecure is easy and intuitive to use
  - People do not need to remember an ID card, token or PIN
  - PalmSecure sensors are contactless and hygienic
- **Cost**
  - Reduce running costs like IT administration, IT helpdesk time
  - Reduce replacement costs for stolen or lost cards and tokens
  - Reduce investment costs for smart cards and smart card readers
- **Security**
  - No fraudulent use of smart cards or passwords
  - You can track logins
  - Certified technology

Common criteria certification

ISO has approved the PalmSecure technology and its algorithm, based on thecommon criteria certification for security, EAL 2. This includes tests and approvals for life detection, intruding the interface, accuracy, FAR/FRR/FTE specification, and the secure manufacturing and R&D process.

About Common Criteria (ISO/IEC 15408)

The Common Criteria for Information Technology Security Evaluation (abbreviated as Common Criteria or CC) is an international standard (ISO/IEC 15408) for computer security certification. Common Criteria is used as the basis for a Government driven certification scheme and typically evaluations are conducted for the use of Government agencies and critical infrastructure. It provides assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous and repeatable manner at a level that is appropriate for the situation in which it will be used. A certification according to the Common Criteria is recognized internationally.



Solutions

Fujitsu PalmSecure technology has been deployed worldwide in a wide range of vertical markets, including security, financial/banking, healthcare, commercial enterprises, and educational facilities. Other applications include physical access control, logical access control, retail POS systems, ATMs, kiosks, time and attendance management systems, visitor ID management, and other industry-specific biometric applications. Businesses also choose PalmSecure for their login and single sign-on applications.

ISVs and OEMs can develop their own solutions. The Fujitsu PalmSecure PS OEM Sensor/Software Developer Kit is available to selected OEMs/SIs that want to develop their own PS-based solutions and applications. Suppliers in the vertical market can integrate PalmSecure into their own products.

PalmSecure Time & Attendance Terminal & Software is available for all enterprises that are seeking secured time-management solutions for controlling and monitoring employee attendance for wage or insurance purposes. It is perfect for advanced systems like cardless employee time recorders and for cardless, keyless access to doors, computers, printers, copiers, and other office equipment.

Appropriate for environments with:

- Hygienic requirements, for example, hospitals
- Frequently changing staff, including restaurants and hotels
- On-call staff with part-time contracts, such as weekend/ summer/ winter employees
- Private schools

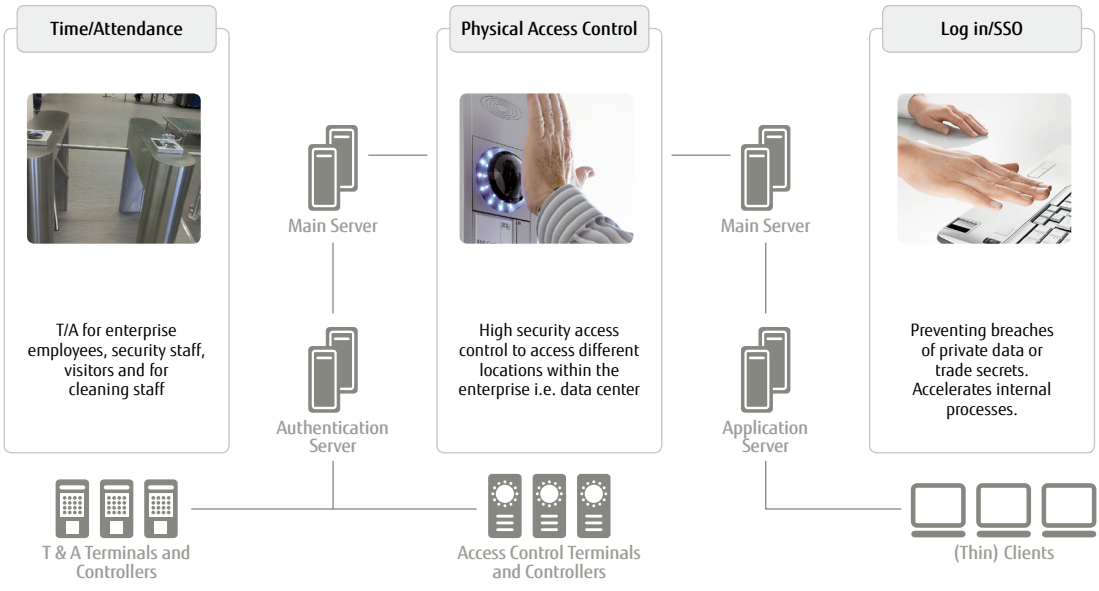
PalmSecure Physical Access Control Terminal/Controller/Software is available for all enterprises that are looking for secured solutions to allow, control, and monitor the access of authorized individuals to secured areas in buildings, facilities, data centers, and control centers.

- Company employees; guests and members of hotels and sport and fitness centers; business people in VIP areas/lounges
- Access control management for secured areas
- Sensitive areas like control centers, airports, and research and development
- Data centers or rack access management
- Parking bays or underground tenants parking

PalmSecure software is available to all enterprises that are looking for secured solutions for accessing workplaces and OS/applications, and that want to replace inconvenient and unsecured passwords, smart cards, or tokens. Typical scenarios include:

- Login/single sign-on security
- Infrastructure access management
- Secured managed printing/scanning
- Secured cloud access
- Digital signature

PalmSecure has many uses. These include monitoring time and attendance, controlling physical access and logging on to devices.



PalmSecure ID Match

Whether you're safeguarding data, a physical location or financial transactions, Fujitsu PalmSecure ID Match adds a new level of security to smartcards.

Registered users store their biometric identity on a chip contained in a smartcard. They keep possession of the smartcard. To access a system or service, the user presents both their palm and the card. If a match is found, they gain entry.

This solution does not require the storage of personal biometric data on a server or in the cloud. The comparison of the biometric template on the card – which is just 1 KB to 2 KB in size – with the user's palm takes place in the Fujitsu PalmSecure ID Match terminal.

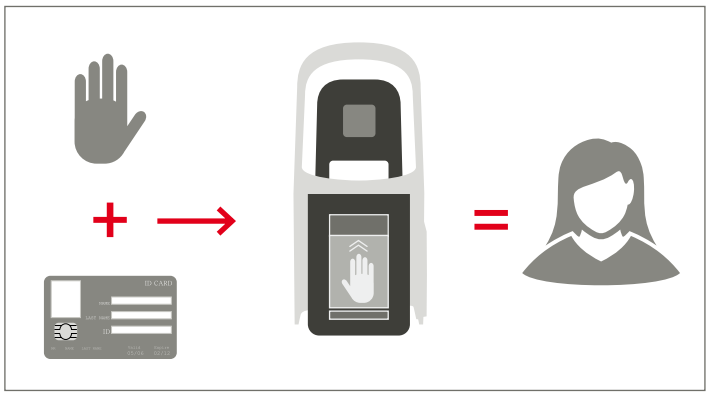
It's possible to incorporate PalmSecure ID Match in a wide range of places. Fujitsu also provides a Software Developer Kit (SDK) to enable fast integration in Identity Access Management applications developed by OEMs and integrators.

Potential uses of PalmSecure ID Match include:

- payment terminals
- physical access controls (without a central biometric database) or
- other IT access systems.

The business logic is defined within the overall solution; the SDK applies no restrictions. The partitioning of the logic is flexible: it can be based at the back end or on a server; or run on the ID Match device itself.

- **A complete solution**
  PalmSecure ID Match includes all the hardware, software and services you need to optimize your existing security.
- **Instant security**
  The ID Match terminal includes highly effective ARM technology, advanced security features and all the interfaces you need for security applications. The high-quality, tamper-proof device with integrated PalmSecure sensor provides touch-free, two-factor authentication.
- **Flexible integration**
  The software is based on Linux. An SDK allows partners and customers to use the application as part of their complete security solution. We also provide demo applications.
- **Advice and support**
  Fujitsu provides supports consulting and training to support partners and customers.



FUJITSU PalmSecure ID Match supports very secure, ergonomic and convenient multifactor authentication. The solution can also be used instead of passwords for all processes in critical infrastructures that require stringent identification control procedures.

PalmSecure and the financial sector

Financial services companies worldwide use PalmSecure to complete transactions securely. The technology works because it combines accuracy, contactless sensors and a high rate of acceptance by customers. The technology is already used with debit cards for withdrawals from automated teller machines (ATMs). Finance firms are also considering a role for PalmSecure in online banking and cashless transactions in retail stores.

Here are some examples of how banks in different countries are using PalmSecure.

Japan

Japan's biggest bank has embedded PalmSecure in its 9,000 ATMs. To withdraw money, customers scan their palms using a built-in sensor. Their palm-vein pattern is then compared to the biometric template stored on their bank card. Daily, customers complete one million transactions using this technology.

Brazil

Brazil's biggest bank originally used fingerprint sensors in ATMs. However, dirty sensors prevented successful withdrawals. For two years, the bank has been transitioning to PalmSecure sensors.

Like in Japan, these sensors are used in combination with bank cards. So far, the bank has equipped 48,000 ATMs with PalmSecure sensors. 70 million customers have completed 700 million transactions across 4,600 branches with no incidents of fraud.

Russia

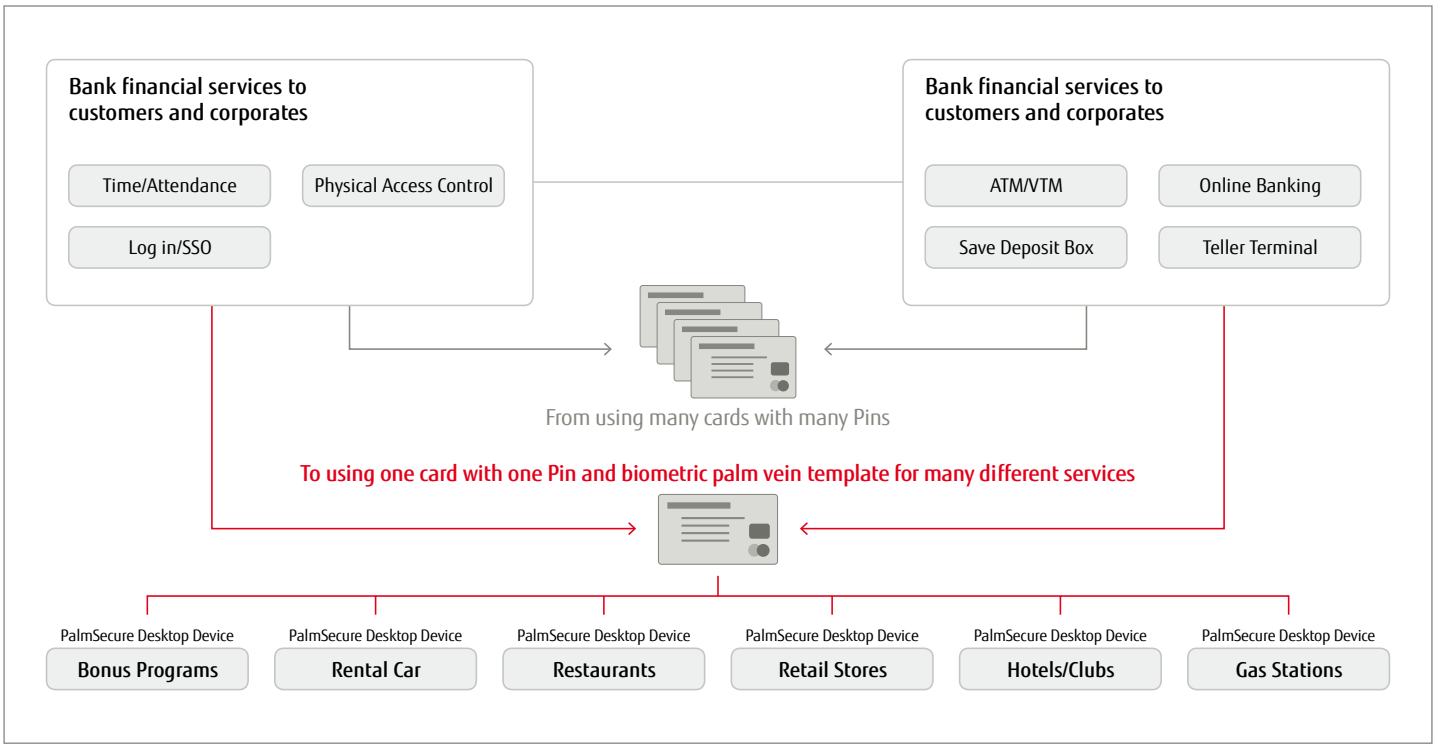
The largest bank in Russia also uses palm vein sensors in its ATMs and for governmental transactions. The high level of security is very popular with customers.

Turkey

One of Turkey's biggest state banks uses PalmSecure to quickly and accurately confirm the identity of customers. It has also embedded the biometric authentication system in its 1,500 ATMS and its video teller machines (VTMs). Customers can even make cardless transactions using PalmSecure.

India

The Reserve Bank of India uses PalmSecure to control physical access to its facilities. The bank required the highest security level, including live detection. It also wanted a fast, intuitive system to grant access to legitimate staff and visitors.



PalmSecure and the healthcare sector

Patient identification in Turkey
Turkey is using PalmSecure for their social insurance system. Patients identify themselves in hospitals by scanning their palm veins and presenting their social insurance card. This has stopped invoice fraud. PalmSecure was installed as an end-to-end solution with secured client workstations in each hospital.

Private hospital in the US
A private hospital uses PalmSecure to register and recognize patients. It has enrolled more than 5 million patients. The hospital has reduced both its costs and cases of insurance and medical record fraud.

Drug stores in Austria
Drug stores in Austria are using PalmSecure as a tamper-proof business process. To work with medicines, staff must authenticate themselves. PalmSecure also tracks the activity. The company chose this technology because it is secure and easy to use.

PalmSecure in buildings and facilities

Automated access for a large gym
A large gym in the UK is using PalmSecure to control who enters. The company wanted to ensure that only members have access – not people who have borrowed cards from friends. Members can join, pay, enroll, and gain access to the gym without involvement from staff.

Protecting datacenters in Germany
A German service provider uses PalmSecure to fulfil its security obligations to customers. The biometric access control gives staff quick, easy access to its datacenters. But it also offers a high degree of protection to these security-critical zones.

Monitoring attendance in India
A large steel company and a large pharmaceutical company in India are using PalmSecure in their plants to track when employees are at work. This has solved the problem of ghost workers. Workers can easily move between plants.

Recording time and attendance in Malaysia
A leading fast food company is using PalmSecure to record employees' hours. PalmSecure is hygienic and fits best in food areas. Through easy enrollment, new and time based workers can immediately be staffed and payment is correctly without any clearance effort.

Major advantages of PalmSecure

- Nearly everyone can use their vein pattern to prove their identity
- It offers extremely high security
- It can form part of a convenient, safe payment process
- As part of a cashless payment process, it can reduce costs for retailers
- It provides greater protection against fraud than a PIN number
- PalmSecure information is hidden in the body. It is almost impossible to copy the complex vein pattern
- It is hygienic
- Leading banks use PalmSecure in their ATMs
- Customers respond positively to PalmSecure (it does not have the same associations as fingerprints or national ID cards)
- It is possible to store biometric information on a card rather than a central archive

Conclusion

PalmSecure is a highly accurate, easy-to-use biometric system for checking people are who they claim to be. Using a complex pattern hidden inside the body, it provides a permanent identifier. Because it is detected by near-infrared light, no contact is needed with the sensor.

This offers many advantages to companies who need a secure way to identify multiple customers or workers, quickly. So far, many organizations in the finance and healthcare sectors have made good use of the technology. We are continuing to find new ways to put PalmSecure to work for our customers. If you are looking for a more secure, more stable way to control access to your systems and premises, talk to us. We work with you to create the ideal approach to identity management.

www.fujitsu.com/palmsecure

Published by
Fujitsu Limited

www.fujitsu.com/