White paper
Fujitsu Identity Management

Security and control becomes more important. Identification technologies based on – smart-cards or passwords are not protected against loss, fraud or copy. Unique identification is only given through biometrics of the person. Identity Management with palm vein identification is one of the most efficient technologies in use scenarios.

Content

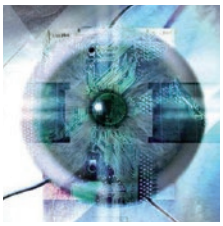
Introduction

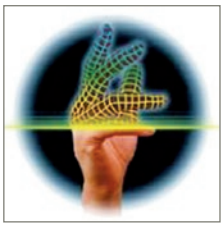
Passwords, Personal Identification Numbers (4-digit PIN numbers) or identification cards are actually used for personal identification. However cards can be stolen, passwords and numbers can be guessed or forgotten. To solve these problems biometric authentication technology which identifies people by their unique biological information is attracting attention. In biometric authentication an account holder's body characteristics or behaviors (habits) are registered in a database.

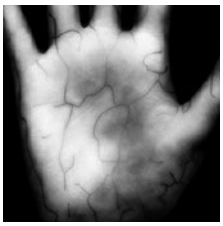
These datas will be compared with others who may try to access an account to see if the attempt is legitimate. Fujitsu is researching and developing biometric authentication technology focusing on four methods: fingerprints, faces, voiceprints, and palm veins. Among these technologies contactless palm vein authentication technology is being incorporated into various financial solution products and for use in public places because of it's high accuracy and hygienic usage. This whitepaper introduces palm vein authentication technology (PalmSecure) and some examples of its fields of application. Fujitsu developed PalmSecure for the general market. The company's key milestone is to standardize Identity Mangement with PalmSecure for biometric authentication.

About biometrics

Fundamental view Biometric technology is used to measure, to capture and to match physiological or behavior characteristics in areas of the human's body to authenticate a person's identity. To achieve this various biometric principles have been developed and launched to the market.







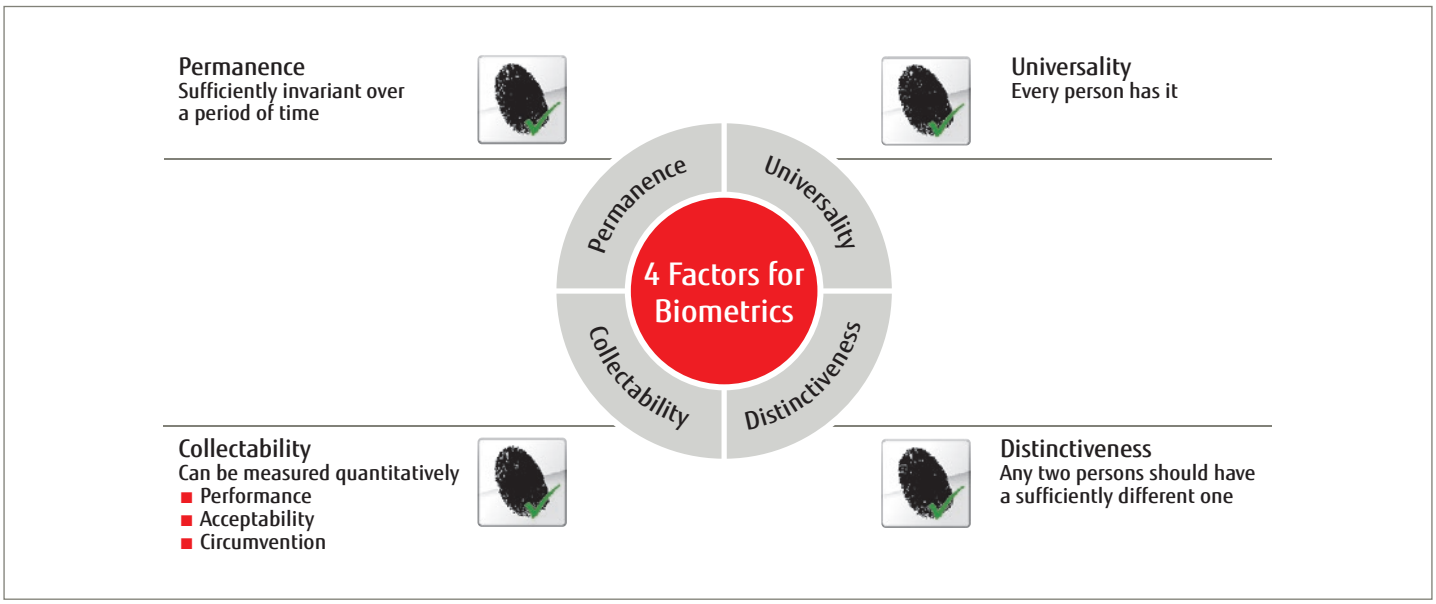
Biometric authentication impedes data and identy theft, hacking and skimming. While passwords, tokens and smart cards can be stolen or hacked biometric data achieves the highest security level.

Selecting the feasible biometric technology for a specific security application will definitely drastically increase the application's safety and the comfort for its' user. Security level and the level of comfort vary between the different biometric technologies. Therefore it is mandatory to carefully analyze which biometric principle fits best for a specific application in advance. Environmental-, social-, applicability- and performance factors need to be taken under consideration, before a biometric application project can be realized.

Claim of biometrics

Biometric authentication technologie should base on the following four factors of biometric:

- **Permanence**
  The biometric factor should be immutabil for a long period of time or even for the whole life.
- **Universailty**
  Each person should have this factor and be able to use the chosen biometric authentication.
- **Collectablity**
  The biometic authentication technology should be based on criterias which are qualitatively measureable.
- **Distinctiveness**
  The factor has to be different bweteen every person even between twins.



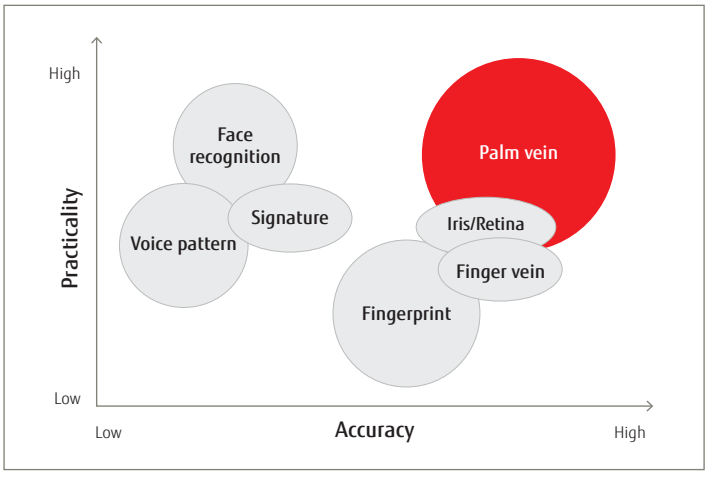
Furthermore biometric technologies should also full fill the following criterias:

- **Safety:** the biometric sensor and its algorithm has to be approved against fraud- and intruding attacks by international authorized authorities, institutes or organizations by using test methods specified within the related ISO standard
- **Applicability:** each person should be able to use the specific biometric application independently from its age, from its gender, from its ethnic origin, from its profession. Personal influencing factors like wearing glasses, contact lenses, beard, or the necessary of using a wheelchair, impacts at the skin, less/high blood pressure, having cancer, having oily/painted or skin injured hands/fingers, or using moistures crèmes should not have any influence using the specific biometric application
- **Non changeability:** to save further costs and to avoid user inconveniences due to new enrolment procedures based on changing biometric patterns after a certain time, the specific biometric pattern needs to be constant for the whole life time way
- **Environmental:** selection of a biometric technology for a specific biometric application needs also to take in account environmental conditions, such as influences by light and weather
- **Costs:** the whole costs for installation and operation of the specific biometric application should be considered by taken in account the added value and the added security and the higher convenience for the user with regards to the ROI.

Due to privacy issues and due to further increase the security level it is most common to use "two factor methods" – especially in the financial transaction segment. In this case the biometric template is most often stored in a chip of a smartcard, or debit card or credit card.

Comparison of biometrics

As already mentioned it is very important to select the best fitting biometric technology for a specific biometric application. The figure below compares the most common technologies by the criterias "accuracy" and "practicability!



Fujitsu's PalmSecure technology is a biometric technology which uses biometric pattern inside the body and which is approved by German Ministry of IT Security accordingly to ISO based common criteria security certification.

The following table shows the most common technologies and ranks them on their FAR and FRR. These indicators are used to define the security level of a biometric system (False Acceptance Rate – FAR) and to define the usability of a biometric system (False Rejection Rate - FRR).

False Acception 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	< 0.00008	≈ 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 percent of invalid inputs which are incorrectly accepted.

FFR = 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 percent of valid inputs which are incorrectly rejected.

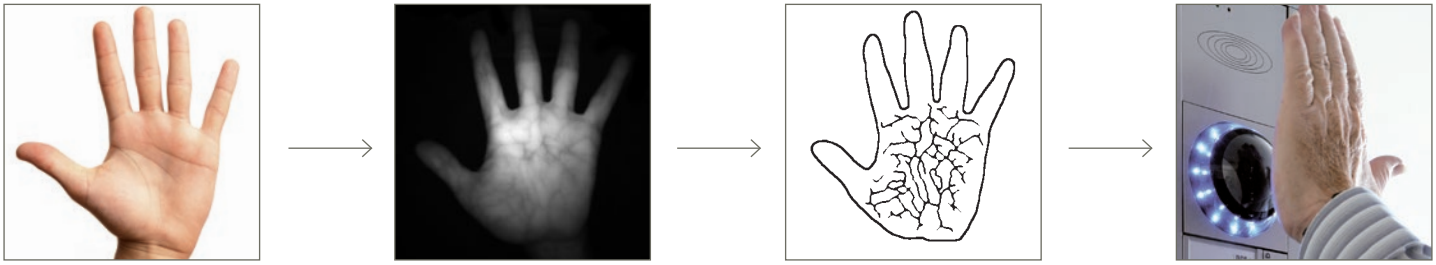
In the case of PalmSecure, the probability of an unauthorized person falsely gaining access (FAR case) is about 0.00008%. And the probability of an authorized person being incorrectly denied access is about 0.01% (valid for 1:1 verification)

Fujitsu
Identity Management

Fujitsu developed a biometric authentication technologiy based on palm veins – PalmSecure. More than 5 miollion reference points are used to measure humans palm veins. The measurement of the exact position and order is only able while blood is flowing. So the usage and identification is only possible with persons alive.

Characteristics

PalmSecure technology is using the very complex vein pattern inside the palm of the hand. More than 5 millions reference points of the vein pattern will be captured by the PalmSecure sensor for highest accuracy. The capturing- and the matching process works contactless without contact to the sensor's surface for most hygienic usage. The palm vein pattern remains the same for the whole life time and it is different at the left and at the right hand, and even twins have different palm vein 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 palm is illuminated with near-infrared light, unlike the image seen by the human eye [Figure a], the deoxidized hemoglobin in the palm veins absorbs this light, which reduces the reflection rate and causes the veins to appear as a black pattern [Figure b]. In vein authentication based on this principle, the region used for authentication is photographed with near-infrared light and the vein pattern is extracted by image processing [Figure c] and registered.

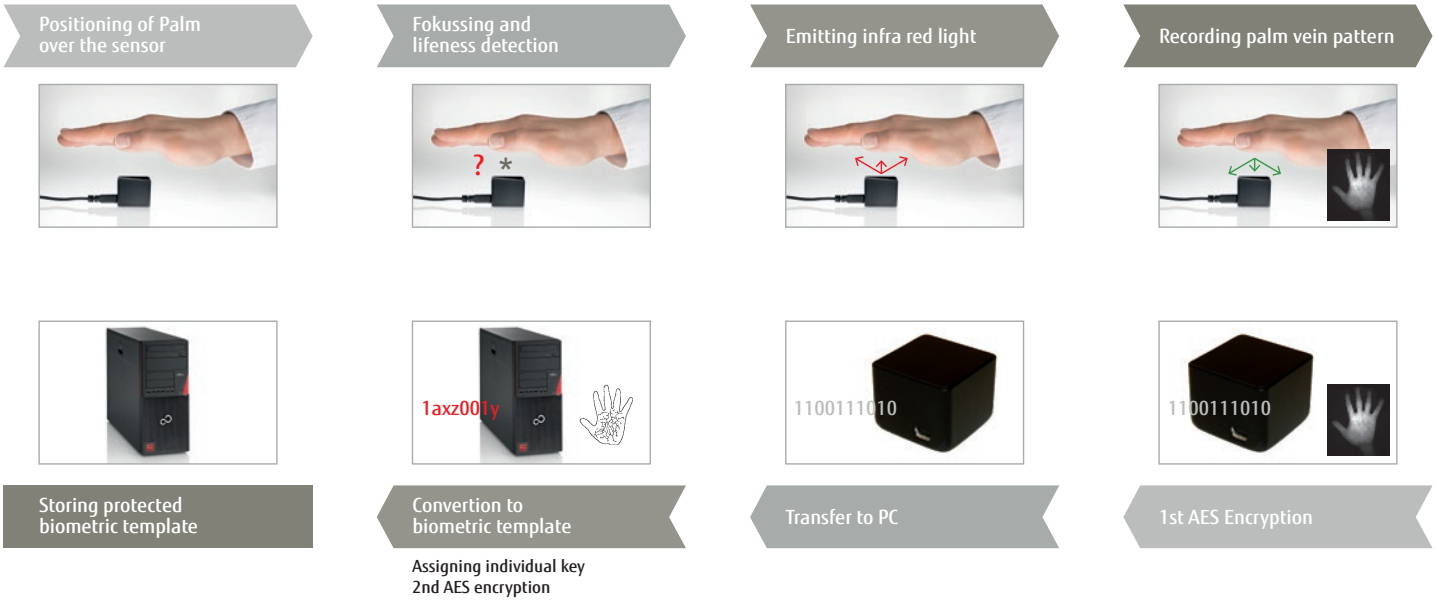
Benefits of palm vein technology

- Contactless operation
  - Hygienic
  - Less resistance from users
  - Suitable for public use
  - Quick recognition
- Applicability rate
  - Almost everyone can register (fingerprints: two to three percent cannot register)
  - More complex: There are more factors to be differentiated in order to avoid failures
- Uses information from inside the body
  - Difficult to forge palm vein data (blood is always flowing)
  - Palm veins are unique and permanent throughout our lives
- High performance, high security
  - FRR = 0.01 percent (rejection rate for authorized users)
  - FAR = 0.000008 percent (rejection rate for unauthorized users)

Functional principle

The following chart shows the fuctional principle of PalmSecure. Once a hand is placed in the right position above the PalmSecure sensor emitting infra red light emblazed the hand. The infra red light redords the palm vein patterns and the sensor encypts th received datas. After transfering the encrypted data to the PC the software converts it to a biometric template and assignes an individual key.

The protected biometric templates can be stored on a PC, device or chip. Fujitsu evaluates the best way to match and store the data together with the customer and its individual requirements.



Advantages

A brief overview of PalmSecure's features in

Highly accurate

PalmSecure has a proven false rejection rate of 0.01 percent and a false acceptance rate of less than 0.00008 percent. No other system in the world can match this performance.

Easy to use

PalmSecure is effortless to use. The scanning process is conducted in a simple and natural way that is not awkward for the user or difficult in any way. Users intuitively sense the natural quality of the system and feel no psychological resistance to it.

Hygienic and non-invasive

Because the system is contactless, it is completely hygienic – a consideration of significant importance to everyone, but especially to those in hospitals and other medical settings. In addition, PalmSecure is non-invasive: The near-infrared rays used in the scanner have no effect whatsoever on the body.

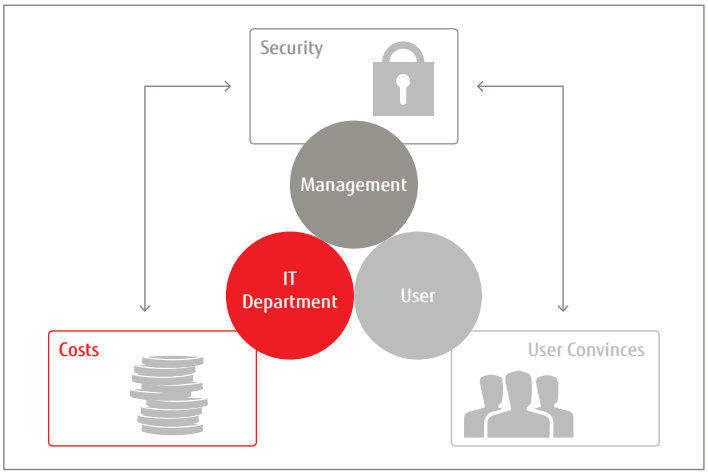
Can be embedded

The PalmSecure system can be embedded in all kinds of flat type products, including laptop computers, copiers, printers, fax machines, wall-mounted room access systems, and eventually even mobile phones.

Value proposition

Fujitsu PalmSecure value proposition combines the 3 factors "user convinces", "costs" and "security".

- User convinces
  - PalmSecure is easy and intuitively to use.
  - No worries about forgotten ID cards, tokens or PIN codes
  - Hygenic usage of contactless PalmSecure sensors
- Costs
  - Reducing running costs like IT-administration, IT service desk, helpdesk
  - Reducing replacement costs for stolen or lost smart cards and tokens - Reducing investment costs for smart cards and smart card readers
- Security
  - No impersonation by smart cards or passwords
  - Monitoring function for Login
  - Certified technology



Common criteria certification

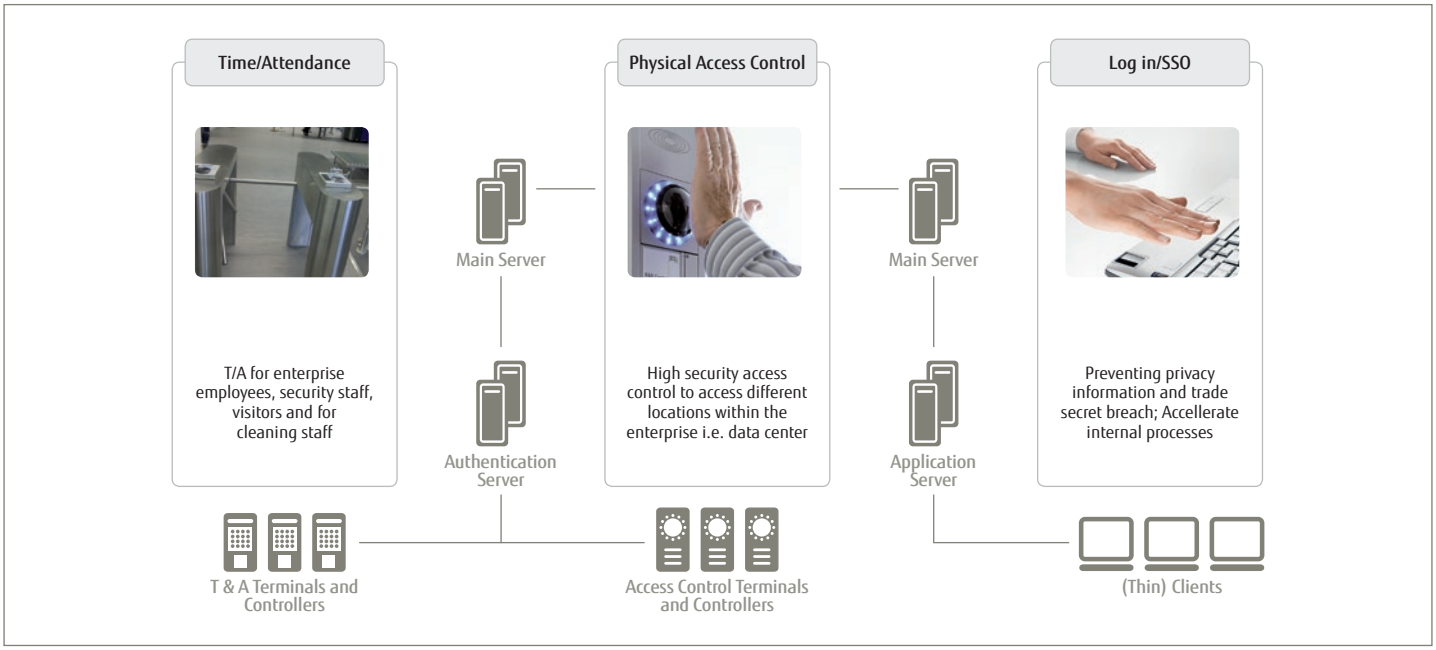
The PalmSecure sensor technology and its algorithm has been approved by ISO based common criteria certification for security – EAL 2. This includes also tests and approvals for life detection, intruding the interface, accuracy, FAR/FRR/FTE specification, and the whole secured manufacturing and R&D process.

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 Federal 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 standard and repeatable manner at a level that is commensurate with the target environment for use. A certification according to the Common Criteria is recognized internationally mutually.

Solutions

The technology of PalmSecure can be used for various solutions. Following the interaction between the most common solutions like time & attendance, physical access control and single sign on are shown.



Fields of application

Wide range of application

PalmSecure is used as a fundamental element for several biometric security solutions.

Target Groups

- **Datacenter**
  Datacenters using PalmSecure to secure the access to their facilities and racks. The technology is also used to secure the IT infrastructure.
- **Retail**
  The retail sector uses PalmSecure to secure their cash register. Furthermore PalmSecure grants the possibility for secured cashless payment. Also the time & attendance management is done via PalmSecure due to the high hygienic standard.
- **Financial Sector**
  The financial sector is one of the biggest sectors using PalmSecure. To grant customers the highest security level ATMs are equipped with PalmSecure. This technology is also used for customer ID management, customer service security and network transaction. Banks also offer safe deposit boxes with PalmSecure for their customers.
- **Government**
  PalmSecure is used for personal ID cards and social insurance cards as a biometric identification method on the ID cards chip. The government and public authorities using PalmSecure based technology also for their IT infrastructure and compliant archiving.
- **Automotive**
  PalmSecure in the automotive area is used e.g. for ID management with rental cars. Besides this PalmSecure is also used for time & attendance, network support services and access management.
- **Healthcare**
  The healthcare sector uses PalmSecure for patient identification (compared with social ID cards). Furthermore PalmSecure is used for access security, IT infrastructure security and time & attendance. PalmSecure is a good solution due to it's contactless usage and the high hygienic standard.
- **Utility**
  Utility companies need a high level of security. Actual this target groups uses PalmSecure for their IT infrastructure & network security, access security and time & attendance recording.
- **Enterprises**
  Enterprises all sizes using PalmSecure to secure their infrastructure and physical access control. Futhermore big enterprises combining PalmSecure time & attendance with their HR system.
- **Industry**
  The industrial sector uses PalmSecure to secure special areas like R&D departments. Furthermore PalmSecure is used generally for access security and time and attendane. Besides also cloud access is secured with PalmSecure.
- **Entertainment**
  The entertainment sector uses PalmSecure to identify their customers and to grant their members a comfortable access e.g. in fitness studios or casions

Use cases

Fujitsu's PalmSecure technology has been already approved in various applications for more than 6 years. Following some sectors are shown with the actual fields of application.

Financial Sector

PalmSecure technology has been selected already by a couple of banks to be used for withdrawing money from automated teller machines (ATMs) in combination with debit-/credit cards. Since five years this biometric concept has been approved to fulfill the security criteria required by the financial market, as well as it has approved the high acceptance rate by the persons using this technology in the daily life. As next step projects have been started to use this technology also for online banking, but also at the point of sales to pay cashless at retail shops.

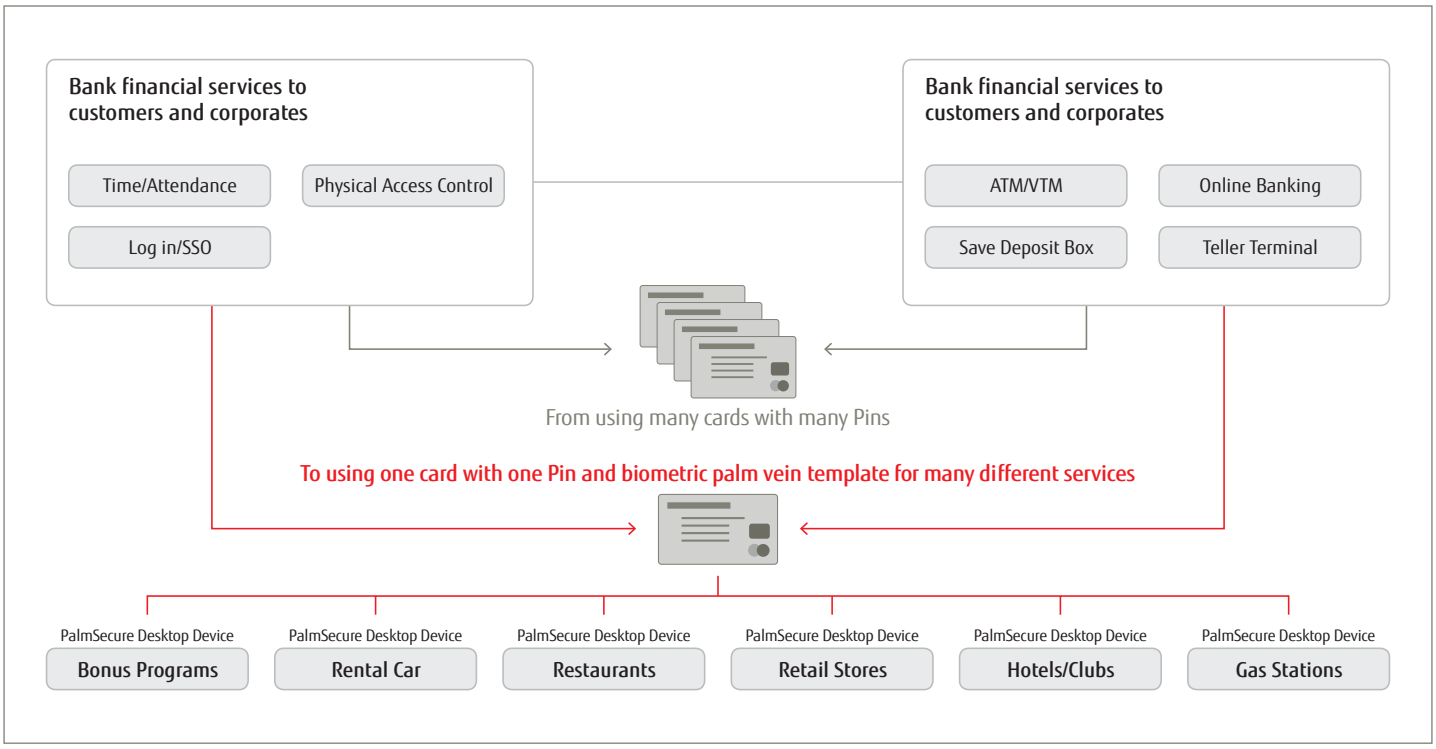
In Japan – beside many others – the biggest bank uses PalmSecure inside the ATMs. A bank customer can withdraw money from the ATM using his credit card on which the biometric template is stored in the credit card chip. By scanning his palm vein data via the built in PalmSecure sensor, the scanned data is compared with the biometric template stored in the chip of his credit card. In this one bank case ca, 9.000 ATMs are equipped with PalmSecure, and daily there are done almost 1 million transactions using this technology.

In Brazil, the biggest bank has gone away from fingerprint sensors integrated in its ATMs, due to many problems with dirty fingers and sensors. A couple of years ago they have started to replace the fingerprint sensors by PalmSecure sensors to allow secured money withdrawing in combination with credit cards. Currently ca.12.000 of total 30.000 ATMs of this bank are equipped with PalmSecure sensors to withdraw money. In more than 3.000 branches of this bank, there have been done more than 33 Million transactions, by more than 1 Million users.

In Russia, the largest bank is using PalmSecure within their ATM transaction service. PalmSecure is used for identification of the customers and furthermore also for supporting governmental transactions. The high level of security is treasured by the customers of the bank.

In Turkey, the biggest state bank also uses Palm Secure for their ATM and VTM services. Almost more than 1.500 ATMs are actually enrolled with PalmSecure. The biometric authentication system enables cardless transaction and is also used as an identification system for the customers.

In India, the Reserve Bank uses PalmSecure as a physical access control solution to grant access to their facilities. The bank requires the highest security standard compared with live detection. Furthermore a contactless usage such as an intuitive usage for the user was required. All this claim are fixed with PalmSecure.



Healthcare Sector

Patient identification Turkey

Turkey is using PalmSecure for their social insurance system. Patient have to identify themselves in hospitals via social insurance card and palm veins. The purpose was to eliminate fraud causes on invoices. PalmSecure was installed as an end-to-end solution with secured client workstations in each hospital.

Private hospital in USA

A private hospital uses PalmSecure as a patient registration and identification tool. Actually more than 5 million patients are registert and using PalmSecure. The hospital prevents insurance and medical record fraud. Though costs have been reduced.

Pharmacy Austria

Pharmacies in Austria using PalmSecure as a tamper proof business process. Documents and evidences of any acting with medicine are secured with PalmSecure. The request was using a highly secure technology which is easy to use for the employees.

Buildings and facilities

A large gym in UK is using PalmSecure for physical access control. Professional access control is essential for a large number of members. It is necessary to ensure that only authorized persons have access, not persons with borrowed cards from friends. Membership is automated via INTERNET offering and paying, enrollment and access authentication is realized without service staff.

Datacenters

The authentication of persons in security-critical zones like data centers requires procedures that are easy to use and at the same time offer a very high degree of protection against forgery. A German service provider protected his data centers, archives and control areas with PalmSecure authentication and fulfills security requirements of his customers.

Time attendance in India

A large steal company and a large pharmaceutical company in India are using PalmSecure in their plants for time attendance. Working time is now transparent and without the possibility of spoofing through ghost workers. Workers can easy move to other plants.

Time attendance in Malaysia

A word wide leading fast food company is using PalmSecure for time attendance in their branches. 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 clearance effort.

Advantages

The major advantages to use the PalmSecure technology application/transaction area are:

- Almost each person can pay by using its palm vein pattern
- PalmSecure technology offers extremely high security and it is a fraud and forgery approved system until today.
- The payment process is convenient, safe and fast
- It can reduce the costs for retailer for the cashless payment process
- In combination with a smartcard, debit card or credit card there can be offered multiple services (only one card is necessary to use different payment applications/bonus program services at different POSs)
- In the case of using a PIN number, PalmSecure protects the card additionally against fraud, skimming and usage by thefts
- PalmSecure information is hidden in the body. It is almost impossible to get access to the complex vein pattern to copy it.
- Hygienic, contactless operation method
- Already approved at ATMs for years
- High acceptance rate by customers, as there is no criminal association like at finger prints (used for crime detection and in some national id cards
- No central archiving of the biometric templates necessary due to either template on card or match on card solutions

Conclusion

This paper introduces palm vein authentication. This technology is highly secure because it uses information contained within the body and is also highly accurate because the pattern of veins in the palm is complex and unique to each individual. Moreover, its contactless feature gives it a hygienic advantage over other biometric authentication technologies. This paper also describes some examples of financial solutions and product applications for the general market that have been developed based on this technology.

Many of our customers have favorably evaluated this technology and have experienced no psychological resistance to using it. This has encouraged us to start development of new products for various applications, beginning with financial solutions and followed by access control units and login units.

Published by
Fujitsu Limited

www.fujitsu.com/