Fujitsu PalmSecure

The solution for user-friendly and reliable authentication – more secure than the competition.

A guideline for biometric authentication.

shaping tomorrow with you

FUJITSU

The Challenge:
Authenticate people, not passwords

In our society of ubiquitous networks, where individuals can easily access their information anytime and anywhere, we are also faced with the risk that others can easily access the same information – anytime and anywhere. Because of this risk, personal identification technology that can distinguish between registered, legitimate users and imposters is generating increasing interest.

Today passwords, personal identification numbers (PINs), and ID cards are commonly used to confirm people's identities. However, cards can be stolen and passwords and numbers can be guessed or forgotten.

Another issue is how to handle the growing number of passwords. The management of many passwords – including refreshing a web page after a given period of time, or maintaining a high level of protection by using a long password – is asking too much of many users. Passwords are typically recorded in places that are not safe or on paper, which results in passwords being lost, copied, stolen, or forgotten. And then there's the potential damage and extra administration that is necessary to create new passwords or cards.

The Solution: Fujitsu PalmSecure

Fujitsu has developed a contactless palm vein pattern authentication technology: Fujitsu PalmSecure. Fujitsu PalmSecure technology uses the very complex vein pattern in the palm of your hand to ensure the safety of your information.

Fujitsu, the leader in biometric palm vein recognition offers a wide range of individual solutions that include hardware, software, and services. Fujitsu Financial Services helps you acquire tomorrow's technology today. With our unique and customized financial solutions, we are addressing shrinking budgets, transferring technology risks, and dispersing financial risk.

Fujitsu supports its own and multivendor products. We also deliver maintenance services for heterogeneous infrastructures from a single source – from installing new products to providing fast and uncomplicated hardware and software support for individual products as well as complete infrastructures.

Biometric authentication:
You are the key

Biometric authentication technology, which identifies people by their unique biological information, is attracting more and more attention. In biometric authentication, an account-holder's body characteristics or behaviors are registered in a database. When they access their account, their features are compared with those in the database to make sure that the attempt is legitimate. The advantages are:

- **Permanence** – sufficiently invariant over a long period of time
- **Collectability** – the following can be quantitatively measured:
  - Performance
  - Acceptability
  - Circumvention
- **Universality** – every person has biometric features
- **Distinctiveness** – any two people have sufficiently different features

Biometric technology offers an enormous increase in security for many different applications, further simplifies procedures, and reduces costs.

There is a wide range of biometric methods and technologies: fingerprint recognition, face recognition, iris recognition, voice recognition, and vein pattern recognition. Fingerprint recognition is the most widely used application. The goal of all biometric authentication methods is to identify everyone by their physical or behavioral features, which are unique for each person, invariant over time, and almost impossible to copy. These features make biometric methods appropriate for areas that require high security. The question is, which biometric technology should be used? Each technology has specific attributes and must be mapped to individual requirements.

Important attributes to consider include the:

- Time needed for recognition
- Quality of recognition and fraud rejection
- Sensitivity to environmental influences like temperature, dust, and water
- Price of the infrastructure and maintenance/operation
- Effort required to integrate the technology in existing applications and systems
- Acceptance by users

Quality of biometric systems

The false acceptance rate (FAR) is used to identify the security level of a biometric system, and the false rejection rate (FRR) is the benchmark for describing the usability of a biometric system. The chart to the right provides an overview of the precision of the various technologies:

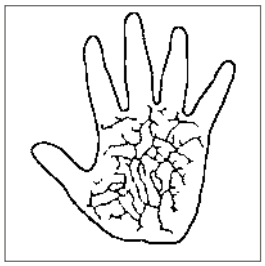
Authentication Method	FAR (%)	FRR (%)
Face recognition	~ 1.3	~ 2.6
Voice pattern recognition	~ 0.01	~ 0.3
Fingerprint recognition	~ 0.001	~ 0.1
Finger vein recognition	~ 0.0001	~ 0.01
Iris/retina recognition	~ 0.0001	~ 0.01
Fujitsu palm vein recognition	~0.00001	~ 0.01

Fujitsu PalmSecure

Fujitsu has developed a contactless palm vein pattern authentication technology, called Fujitsu PalmSecure. Fujitsu PalmSecure technology uses the very complex vein pattern in the palm of your hand to identify you with great precision. More than five million reference points of the vein pattern are captured by the highly accurate PalmSecure sensor. The capturing and matching process is contactless – the sensor's surface is never touched, for hygienic reasons. Your palm vein pattern remains the same for your entire lifetime and is different on your left and right hands. Even twins have different palm vein patterns. Vein recognition technology is extremely secure, because the authentication data is inside your body in your circulatory system, making it very difficult to forge.

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. It then carries that oxygen to the tissues of the body through the arteries. After it releases its oxygen to the tissues, thedeoxidized hemoglobin returns to the heart through the veins. These two types of hemoglobin have different rates of absorbency. Deoxidized hemoglobin absorbs lightat 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
- More complex: there are more factors to be differentiated which avoids 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 = ~0.00001 percent (acceptance rate for unauthorized users)

PalmSecure
How it works

First, it is necessary to save a person's biometric palm vein pattern during initial registration as a biometric template. This takes place during an enrollment process. The template, created by a sensor, is compressed to three to five kilobytes and encrypted internally in the sensor using an AES key. Once externally transferred to the PalmSecure software, the template is converted to a biometric template and after a second AES encryption it is assigned an individual key.

During this enrollment process, two images are made for each hand and their quality is then tested by means of subsequent verification. Each individual biometric template is also provided with an individual encryption key, which is known only to the company performing the enrollment process.

The quality of enrollment is of decisive importance in determining how well the biometric identification/verification process can be performed in practice.

PalmSecure sensors can be used for
- Physical access control
- Logical access control
- Device access control

Depending on the biometric application, it is very important to select the right method to store and operate the biometric template. The template can be stored on a central storage system, on a SmartCard, or on the device.

When the template is stored on a SmartCard, verification is performed inside the card's chip. This happens very quickly and at a high security level. For this type of verification, users need their hand and their SmartCard, which means that it is a so-called two-factor method. This is typically used by ATM devices in banks.

Keeping the templates on the device's board (match on device) is almost the same. In these devices, a security module is installed for decryption. The number of users is limited by the capacity of the device, and the devices can interact with other devices. A typical example of this is single-access control, like member entry to a fitness center.

When the template is stored centrally on a storage system, the infrastructure must be protected. This method is used when there is a large number of users and many authentication requests.

Fujitsu PalmSecure's authentication process is extremely fast:

Enrollment processing time (two images + verification)	= ca. 10 sec.
Verification processing time (1:1)	= ca. 0.8 sec.
Identification processing time (1:10.000)	= ca. 1-2 sec.

A brief overview of PalmSecure's advantages

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 easy for the user. People intuitively sense the natural quality of the system and feel no psychological resistance when using 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 devices, including Fujitsu notebooks, desktop PCs and tablets. It can also be part of solutions for copiers, printers, fax machines and wall-mounted room access systems.

Client Computing Devices featuring PalmSecure sensors

Fujitsu has always been eager to help customers protect their business-critical information and privacy, long before newspapers broke stories about massive online surveillance almost every day. To this end, we have developed or adopted a fair share of technologies and solutions, ranging from fingerprint or palm vein sensors to TPM chips and from web privacy enhancements to the Advanced Theft Protection suite.

As a result, Fujitsu Client Computing Devices are as prominent for their comprehensive security features as they are for outstanding functionality.

Fujitsu has developed the world's smallest and slimmest palm vein authentication sensor that is capable of being employed in mobile devices. By upgrading the technology's design with new image sensors and other optical components, Fujitsu Laboratories has successfully slimmed down the new sensor to a thickness of 5 mm. The new sensor delivers the same authentication performance as existing technology while halving the thickness of current models. With this development, we can embed the sensor in tablets and notebooks, which are becoming slimmer. We can also build the sensor into Mini PCs. This helps to expand the range of application scenarios for palm vein authentication. More customers will now be able to perform secure authentication using simple operations.

LIFEBOOK U7 family

The FUJITSU Notebook LIFEBOOK U7 family is a slim, light and stylish ultra-mobile notebook for business professionals. Being only 19 mm thin and weighing only from 1.15 kg (2.5 lbs.) it provides excellent mobility. Ergonomic viewing is guaranteed with the anti-glare HD, FHD or optional FHD touch display options and the embedded palm vein or finger print sensor provide outstanding security. The common port replicator of the LIFEBOOK U family facilitates workplace sharing within today's modern workstyle.

LIFEBOOK S936

The FUJITSU Notebook LIFEBOOK S936 is a touch-enabled notebook for frequent travelers with highest demands. Lightweight from 1.19 kg (2.62 lbs), with a battery runtime up to 21 hours, a crystal clear 33.8 cm (13.3-inch) WQHD or FHD anti-glare display option and unique palm vein sensor option empower you to work with confidence wherever you are.

STYLISTIC Q736

The FUJITSU Tablet STYLISTIC Q736 is the perfect companion for professionals who require ultimate security and a large screen. The optional palm vein sensor combined with PalmSecure™ technology provides an unrivaled security level. Everywhere connectivity is ensured with embedded 4G/LTE, GPS and NFC. A cradle shared with other STYLISTIC models enables best-in-class comfort in the office.

LIFEBOOK P727

The FUJITSU Tablet LIFEBOOK P727 is an ultra-light, portable 2-in-1 device with a day-long battery that enables an agile multi-mode working style. The device can handle demanding design- and illustration-based applications with ease using latest Intel processors. It ships with the Windows 10 Pro operating system and offers industry-leading palm vein authentication technology for your enterprise security needs.

CELSIUS H760

If you are looking for workstation power on-the-go packed in a 39.6 cm (15.6-inch) stylish form factor, then the FUJITSU CELSIUS H760 mobile workstation is the right choice. Its port replicator is compatible with seven LIFEBOOK devices and thus ideal for a shared desk environment. Maximum data security is guaranteed by the unique PalmSecure™ technology.

ESPRIMO Q956

Save space, cut noise, and reduce power consumption. The FUJITSU ESPRIMO Q956 mini PC is easy to use, energy efficient and provides excellent performance. It has a Low Power Active Mode, to save energy when not in use. But you can still respond instantly to communications. The flexible bay allows you to use a range of devices, including a SmartCard reader and PalmSecure™ sensor. With a Zero Noise function and small footprint, the FUJITSU ESPRIMO Q956 gives you a cleaner, quieter workplace.

How to manage: Authentication with Workplace Protect

Workplace Protect is best described as a security suite consisting of several authentication modules designed for different working environments and security levels. It relies on biometrics as well as more “traditional” authentication methods, which may be used alone or in combination with each other. More specifically, these methods include:

- User authentication for Microsoft Windows
- Pre-boot authentication at BIOS level
- Single sign on (SSO) for Microsoft Windows
- Password Safe, for storing secret login details needed to access protected websites
- Encrypted container, virtual disk encryption for safeguarding important user data

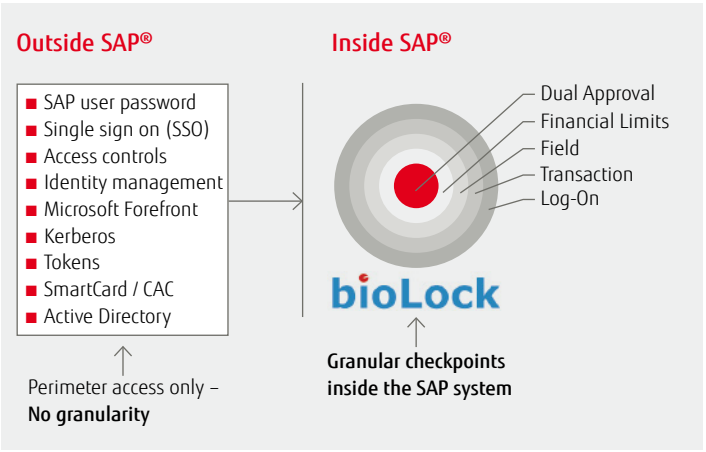
PalmSecure software solutions

realtime bioLock™ for use with SAP® ERP - powered by Fujitsu PalmSecure™

Traditional SAP security approaches have relied on knowledge-based (password) security, which can be circumvented by password misuse or fraud, since they do not identify the human being behind the password. New access points such as kiosks, POS/cash registers, tablets, ATMs and more require stronger protection. Current SAP security levels can easily be enhanced by moving to two-factor security with biometrics.

Realtime bioLockTM software, powered by Fujitsu PalmSecure adds biometric security and is integrated for use with SAP and HANA.

realtime bioLockTM for use with SAP ERP – powered by Fujitsu PalmSecure works with the most advanced palm vein recognition technology to securely, privately and swiftly identify the user requesting an SAP action. This solution authenticates not only the user log-on, but continuously checks user credentials at granular "checkpoints", validating users' credentials for specific activities in the SAP system on a re-authentication basis. For example, if an employee is transferring a large sum of money, setting up a new vendor account, or opening a customer's file containing personally identifiable information (PII) these activities are critical enough to require the operator to re-authenticate via biometrics.



This has a number of key advantages:

- Prevent a user from violating Segregation of Duties policies by hiding behind a generic log-on or shared password
- Create true accountability for users' actions with multi-factor security, including biometric identification by Fujitsu PalmSecure
- Enforce any segregation of duties, or checks and balances
- Set checkpoints at detailed levels such as menu items, tables, transactions, info types, fields, field threshold values, buttons, or dual approval. Control actions such as exporting, printing, changing or viewing data
- Generate a robust audit trail of user activities, with silent e-mail alerts of violations
- Obtain legal evidence to pursue rogue employees

Existing SAP security, roles, authorizations, GRC and SSO are unaffected – realtime bioLock for use with SAP – powered by Fujitsu PalmSecure complements and reinforces existing SAP security.

PalmSecure ID Match

FUJITSU PalmSecure ID Match offers two-factor authentication that combines unique PalmSecure technology with ID cards and badges. The solution is based on a compact multifunction device comprised of a touch screen, the latest generation embedded ARM processor board, a multicard reader, NFC read/write module and Fujitsu's high security PalmSecure technology for personal identification and verification based on palm vein patterns. PalmSecure ID Match is suited for implementation in a wide range of application scenarios and environments. Fujitsu also provides a Software Developer Kit (SDK) for OEMs and integrators to support fast integration in Identity Access Management applications.

Fujitsu offers a complete solution platform comprised of hardware, software and services for optimizing existing security solutions:

- The hardware, namely the ID Match terminal, includes highly effective ARM technology, advanced security features and all the interfaces needed for security applications. The high-quality, tamper-proof device housing with integrated PalmSecure sensor allows for intuitive, touch-free two-factor authentication, with ample flexibility for various types of installation or mounting.
- The software is based on Linux. An SDK enables partners and customers to implement the application as part of their complete security solution. Demo applications are also provided as a means of support.
- Fujitsu supports partners and customers with consulting and training programs when it comes to developing and realizing individual, customized security solutions.

Customers benefit from a flexible solution platform for implementation of match-on-device applications for POS payment terminals, physical access control systems (without a central biometric database) and other types of IT access systems. The business logic is defined within the overall solution, and the SDK imposes no restrictions. The partitioning of the logic is flexible and can be largely server/backend-based or have more orientation toward the ID Match

PalmSecure ID Access

Fujitsu PalmSecure is a robust biometric authentication system that uses vascular pattern technology for fast and convenient identification. Fujitsu PalmSecure is a hygienic, contactless solution that is user friendly and easily applicable to all users including children. ID Access provides enterprises with a superior authentication technology with highest convenience. Fujitsu ID Access is easy to integrate into existing hardware infrastructures – thus a perfect starting point for biometric authentication. Fujitsu PalmSecure ID Access covers all requirements for access control and time attendance.

The support of interfaces like Wiegand 26/34 and Electric Lock/Exit Button/Alarm positions this offering as the technology of choice for fast and easy-to-deploy biometric approaches.

Benefits of PalmSecure ID Match

- Fast and easy introduction of biometrics – by easy and convenient integration in existing infrastructure.
- High security - as vein patterns are hidden under the skin, they never change and are detectable only when blood is flowing.
- High accuracy - as the palm vein patterns are very complex and provide up to more than 5 million reference points and they are insensitive to external factors like cold temperatures and skin scratches.
- High acceptance - as palm vein recognition is fast, easy and intuitive to use and very hygienic as it is contactless.

To meet multi-factor authentication requirements, the system can be integrated with other technologies to satisfy two-factor authentication. The system can be integrated with e.g. pin pad, proximity card and smart card technologies.

OpenLimit truedentity® - powered by Fujitsu PalmSecure

OpenLimit truedentity® - powered by Fujitsu PalmSecure supports the mutual authentication of service providers and users. The ultimate control over the identity remains with the user. The basic principle ensures that customer data does not reside with a service provider. Data is transmitted over secure communication channels only on request. The so-called Identity Provider is integrated as an additional service and acts as the mediator for mutual authentication.

How it works:
The Identity Provider confirms the identity of the service provider to the user and oversees the identification of the user in the direction of the service provider. Thus a service provider only needs to be registered once with the Identity Provider. The service provider is allocated an authorization certificate that can subsequently be used for any requests to the Identity Provider. Only registered providers can request a user identity via the Identity Provider. The user's identity data is securely stored locally on a chip card. The identification data is requested from the Identity Provider, and users decide whether or not to release the data by giving the OK through their authentication.

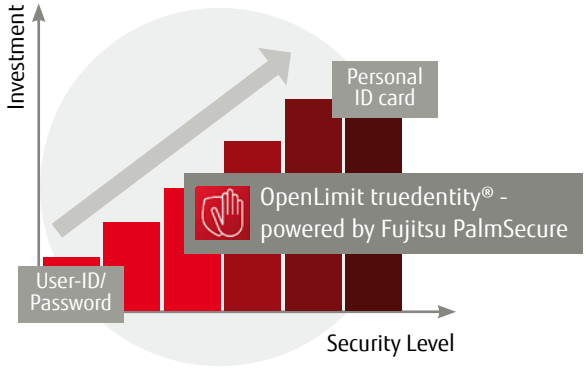
In short, a truedentity server verifies the authenticity of the identities of both partners in order to set up a connection and permit access to the identity data. The Identity Provider is based on multitenancy and can serve multiple service providers.

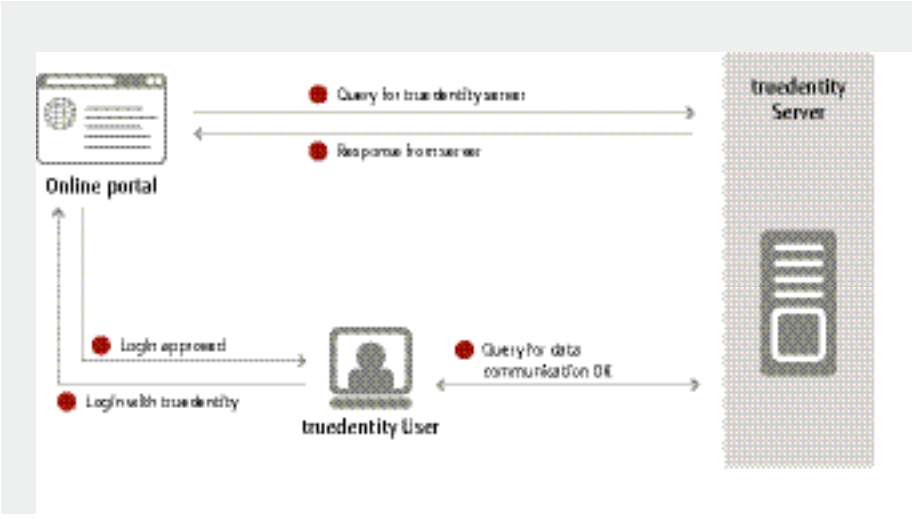
All communication between browsers, the truedentity client, web server and truedentity server is encoded, and in this instance, the transport layer security (TLS) and the transferred data are encoded as well. The communication between truedentity clients and truedentity servers is based on protocols which are used in the area of sovereign documents.

The information is stored on a chip card in order to safeguard the identity data of the user. To prevent loss, theft or forgery of the user's personal and unique biometric palm vein pattern, this is also stored on the card to take advantage of the extremely secure Fujitsu PalmSecure technology.

The palm vein pattern is compared 1:1 with the pattern stored on the chip card before the identity data is selected. This confirms that the user of the card is indeed the owner of the card – only then can the identity data be released to the service making a request. Stolen cards, for example, are detected immediately so that misuse can be prevented well in advance.

OpenLimit truedentity® - powered by Fujitsu PalmSecure supports the implementation of highly secure infrastructures in a wide range of scenarios and, with user-centric authentication, leads the trend toward making silo authentication architectures obsolete.





PalmSecure MultiModal Biometric Authentication Solution

Fujitsu PalmSecure MultiModal middleware delivers a high level of authentication security. Biometric identity based on three fingerprints combined with the inside palm vein pattern satisfies high security requirements. The result is a very low False Acceptance Rate (FAR) of < 10^{-14} %. Even if some of the identity data is subject to some variations, the other biometric data will compensate through fusion scores. Furthermore using pre-selection reduces the authentication processing time to just a few seconds.

A wide range of applications

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 that 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.

Approved security

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

General enterprise solutions

The PS Sensor Guide Kit + Client/Client-Server 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, SmartCards, or tokens. Typical scenarios include:

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

Retail solutions

Fujitsu's ID Match terminal in combination with a Fujitsu tablet can be used for customer authentication in retail stores.

- Self-authentication kiosks
- Self-registration kiosks
- Cashless payment (for example, cafeterias, dining halls)
- At any point of sale as a match on device

Finance solutions

Identity fraud and card fraud are major challenges in the finance sector. Fujitsu offers banks throughout the world a system that combines palm vein authentication with the use of a SmartCard.

Fujitsu PalmSecure offers:

- Secured financial (online) transactions via PC
- Building security. For example, locker rooms
- ATM or safe deposit-box integration
- The most secure front-end devices to protect sensitive customer data

Office and company solutions

PS 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

Facility, building, and data center solutions

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




Healthcare solutions

PalmSecure can be integrated into an existing medical records system to unfailingly guarantee patient identity. PalmSecure stops the wrong medicines or medical services from being provided to patients, prevents medical identity theft/insurance fraud, and eliminates duplicate medical records. In addition, PalmSecure systems can greatly accelerate registration efficiency and convenience and foster the development of patient services.

The PalmSecure option for selected mobile devices can be used in hospitals and other medical venues. Because it uses a hygienic, contactless interface, it is ideal for:

- Patient identification
- Mobile visits

Public-sector solutions

Fujitsu's PalmSecure multi-modal middleware can provide highly secure authentication for large segments of the population:

- National ID cards
- Social security/welfare applications
- Immigration/visa services
- Public library systems
- Airport security




choosepeopleoverpasswords.global.fujitsu.com

CONTACT US

Published by
Fujitsu Technology Solutions GmbH
Mies-van-der-Rohe-Strasse 8, 80807 Munich, Germany