



# 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 (four-digit PIN numbers), and ID cards are used for personal identification. However, cards can be stolen and passwords and numbers can be guessed or forgotten. Another issue is how to handle growing numbers of passwords. This results in a security risk, because three out of four users share their online banking password with a nonfinancial Website: 47 percent share both ID and password. 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 saved or on paper, which results in passwords being lost, copied, stolen, or forgotten. Not to mention the potential damage and extra administration effort that is necessary to create new passwords or cards.

### The Solution: 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 ensure the safety of your information.

Fujitsu, the leader in biometric palm vein security, 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 also supports its own and multivendor products and delivers 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 only 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 (habits) 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 biometrics methods and technologies: fingerprint recognition, face recognition, iris recognition, voice recognition, and vein pattern recognition. Fingerprint recognition is the most widely used application. Face recognition is one of the developing biometric methods. The goal of these 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 methods should be implemented in most of the areas that require high security. The question is which biometric technology should be used: Each technology has specific attributes and must be mapped for individual requirements.

Important attributes are:

- Time needed for recognition
- Quality of recognition and fraud rejection
- Sensitive to environmental influences like temperature, dust, and water
- Price for infrastructure and maintenance/operation
- Implementation effort in applications and systems
- Social acceptance

## Quality of biometric systems

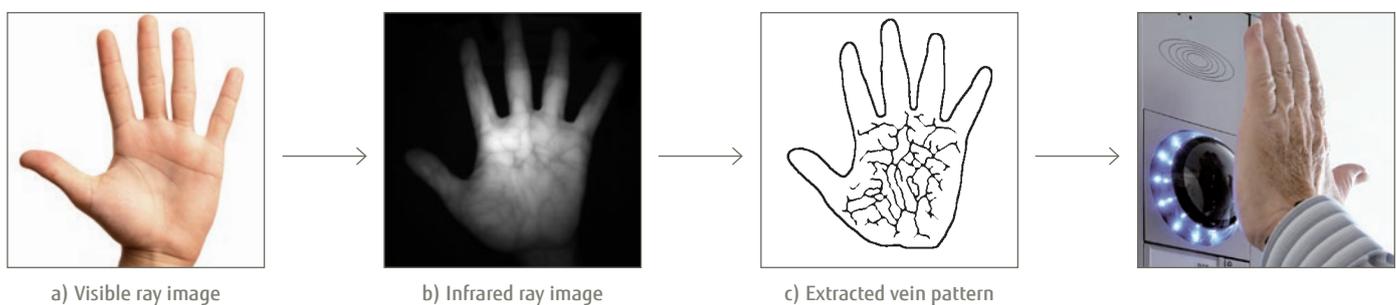
The false acceptance rate (FAR) is used to identify the security level of a biometric system, and the false rejection rate (FRR) is the benchmark for describing the usability of a biometric system. The chart below provides an overview of the precision of the various technologies:

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 PalmVein	< 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 secure, because the authentication data is inside your body in your circulatory system, making it very difficult to forge.



## 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 1(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 1(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 1(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 = 0.00001 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 enrolment 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 enrolment 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 enrolment process.

The quality of enrolment 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 solutions
- Logical access control solutions
- Device access control solutions

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 smart card, or on the device.

When the template is stored on a smart card, verification is performed inside the smart-card chip. This happens very quickly and at a high security level. For this type of verification, users need their hand and their smart card, 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 members 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 features in

#### 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

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.

# Workplace systems with PalmSecure sensors for universal usage cases

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 workplace systems are as prominent for their comprehensive security features as they are for outstanding functionality.

Fujitsu develops the world's smallest and slimmest palm vein authentication sensor that is capable of being employed in tablet 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. This also enables easy deployment in mobile devices, such as tablets and slate PCs, which are becoming increasingly slimmer, and helps to expand the range of applications for palm vein authentication. More customers will now be able to perform secure authentication using simple operations.

## CELSIUS H730

If you are looking for a workstation providing high-end graphics and processor performance in a 39.6 cm (15.6-inch) mobile form factor, Fujitsu's CELSIUS H730 with an attractive slim design is the right choice. Thanks to comprehensive ISV certifications, you will enjoy smooth and hassle-free operation of all your applications. Its modular bay offers expandability and enhanced flexibility. For example, you can insert a second battery to increase mobile working time. High-speed network access from anywhere is guaranteed through embedded UMTS, WLAN or Bluetooth® connectivity. Peace of mind and data security are ensured by an optional palm vein sensor and Fujitsu's Advanced Theft Protection.



## STYLISTIC Q775



The FUJITSU Tablet STYLISTIC Q775 is the perfect companion for professionals who require ultimate security and a large screen span. Its 33.8 cm (13.3-inch) Full HD anti-glare display supports pen and touch input, while 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 U904



PalmSecure

If you are looking for an attractively slim but fully-featured business Ultrabook™, then the Fujitsu LIFEBOOK U904 is the perfect choice for business professionals. Its outstanding thin design of 15.5 mm combined with a low weight of only 1.39 kg allows you to travel in complete comfort, while its robust magnesium housing and aluminum palm rest ensure that your notebook stays protected at all times. The super-crisp 35.6 cm (14-inch)

frameless WQHD + IGZO display also supports touch input, thus providing you with the flexibility you desire for managing your tough and hectic business routine. What's more, an extended battery runtime, high responsiveness, backlit keyboard, ultimate security features and optional embedded 4G/LTE offer you the exceptional mobility you need when on the move. With the optional port replicator ultimate convenience is guaranteed in the office.

## 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

## Fujitsu PalmSecure and realtime bioLock™

Investing in biometric access and perimeter security can best protect an organization's data from financial fraud, industrial espionage or unauthorized access to intellectual property, while increasing regulatory compliance. SAP® is the business application of choice used in most enterprises today. The bioLock™ software from realtime AG is the only biometric security program available featuring seamless integration and certification for SAP since 2002.

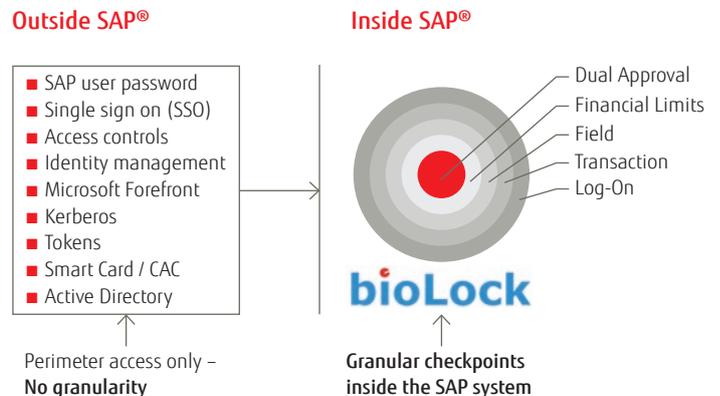
The combination of bioLock software and Fujitsu PalmSecure not only controls what happens within SAP at the moment of log-on, but also what goes on after the user is in the system. SAP users can easily make dramatic security improvements by implementing re-authentication at granular levels which become user-specific checkpoints. When those re-authentications are based on biometric identity management instead of passwords or devices, the results are indisputable audit trails and accountability. bioLock protects the entire SAP system against unauthorized activity by monitored users. This applies to any SAP function that is chosen for monitoring.



For example, if an employee is transferring a large sum of money, or 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:

- Absolutely prevent a user from gaining access to unauthorized areas.
- Create true accountability for each user's actions.



- Enforce any segregation of duties, or checks and balances deemed necessary by the organization's business management or regulatory requirements.
- Generate a robust audit trail of user activities, including failed access attempts.
- Provide employers with legal evidence to pursue rogue employees.

Existing SAP security, roles and authorizations are unchanged – bioLock software complements, reinforces and resides on top of existing SAP security and GRC.



## 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 multcard reader 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 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 device itself.



## PalmSecure truedentity®

Fujitsu PalmSecure truedentity® 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.

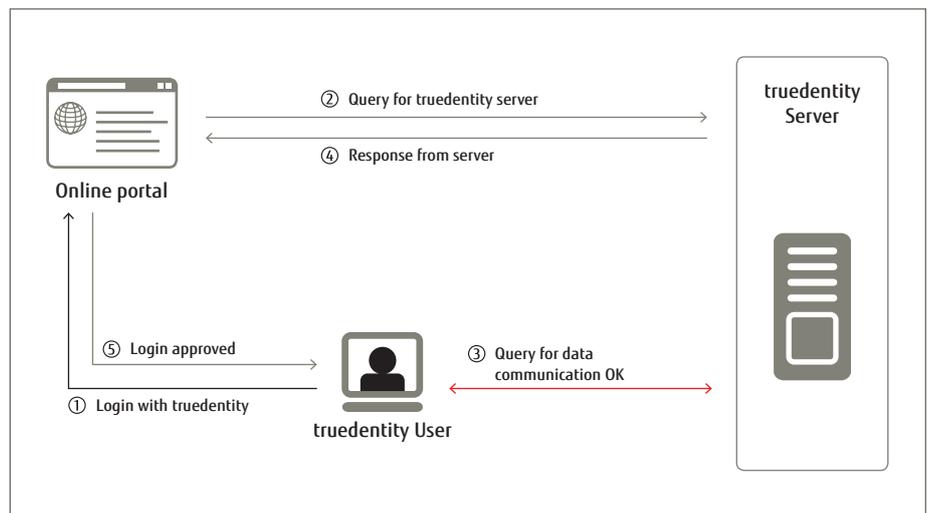
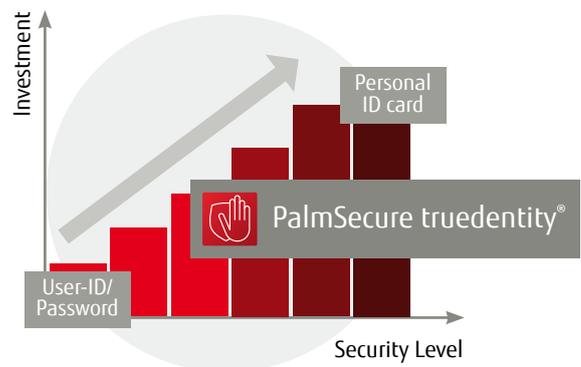
In short, a truedentity server verifies the authenticity of the identities of both partners in order to set up a connection and permit access to the identity data. The Identity Provider is based on multitenancy and can serve multiple service providers.

All communication between browsers, the truedentity client, web server and truedentity server is encoded, and in this instance, the TLS and the transferred data are also 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, the user's personal and unique biometric palm vein pattern 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.

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





# 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 liveness 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 work-places 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

## Retail solutions

PalmSecure “Jacket” option for the STYLISTIC Q775 tablet, used for customer authentication in retail stores (cashless payment) for B2B customers.

- 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 smart card.

Fujitsu PalmSecure enables:

- Secured financial (online) transactions via PC
- Building infrastructure security, for example, locker rooms
- ATM or safe deposit-box integration



### 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.

PalmSecure's option for the STYLISTIC Q775 tablet can be used in hospitals and other medical venues. A big advantage is the hygienic contactless user interface.

- For patient identification
- For mobile visits
- For treatment room and rehabilitation center access



### 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



[www.fujitsu.com/palmsecure](http://www.fujitsu.com/palmsecure)

Published by

**Fujitsu Technology Solutions GmbH**

Mies-van-der-Rohe-Strasse 8, 80807 Munich, Germany

Copyright: © Fujitsu Technology Solutions 2015

All rights reserved, including intellectual property rights. Technical data subject to modifications and delivery subject to availability. Any liability that the data and illustrations are complete, actual or correct is excluded. Designations may be trademarks and/or copyrights of the respective manufacturer, the use of which by third parties for their own purposes may infringe the rights of such owner.