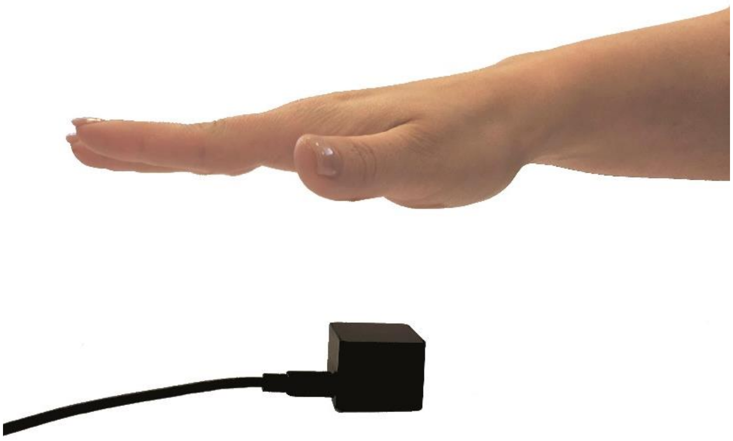
White paper
FUJITSU PalmSecure™ ID LifePass

Fujitsu Biometric Authentication PalmSecure™ ID LifePass is a biometric central authentication middleware. Based on the Fujitsu PalmSecure™ palm vein recognition technology, ID LifePass ensures secure personal authentication with the wave of the hand, which can be easily integrated into own third party system.

Content



Fujitsu PalmSecure™ ID LifePass
Personal authentication with the wave of a hand

Fujitsu PalmSecure™ - Your business easily secured

Personal authentication became a significant part of corporate live, from computer login to cash withdrawal, access control and online transactions just to mention a few. For this reason, a secure, fast, easy to use and reliable solution is essential to provide the adequate security level. ID LifePass is exactly offering this as it is based on Fujitsu PalmSecure™ palm vein recognition technology, one of the most unique physical biometric characteristics.

Important aspects for choosing the most suitable biometric system

- Universality

Everybody should be able to be identified: Most users have at least one hand.

- Uniqueness

The biometric pattern should be as unique as possible to ensure the maximum level of security: The palm vein recognition based system identifies the vein pattern under the skin of the palm, which is one of the most unique biometric IDs.

- Stability

The biometric ID should be stable: Palm veins remain stable statistically from the age of 16, therefore a person needs to be registered in one system in general only once in a lifetime.

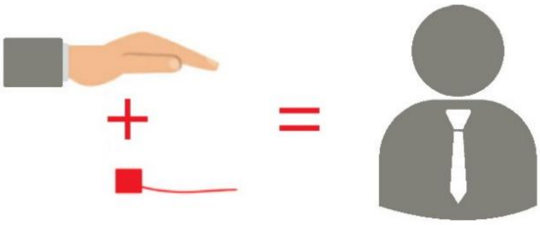
- Convenience

The biometric system should be easy to use: Fujitsu PalmSecure™ palm vein recognition is an intuitive and hygienic system.

ID LifePass – personal authentication with the wave of the hand

Based on the Fujitsu PalmSecure™ palm vein recognition technology, ID LifePass is a biometric central authentication middleware, which can be easily integrated into own third party hardware or software system via API. By using ID LifePass, the security of the palm vein recognition based technology can be integrated into existing system, thus replacing or completing low security identifiers (e.g. passwords, cards, etc.). Whether it is used for security or convenience reasons, ID LifePass can be deployed in a wide range of markets, from physical security to IT security solutions, including office buildings, educational facilities, financial institutions, healthcare, safe deposits, correctional facilities or theme parks, just to mention a few. Fujitsu PalmSecure™ ID LifePass ensures 1:n identification and 1:1 verification based on the customer´s requests.

ID LifePass is the central middleware module of all solutions based on Fujitsu PalmSecure™ including ID Access and ID Login. In case customers would like to integrate palm vein recognition into their own system replacing or extending the actual authentication module it can be realized via API. ID LifePass acts as a central base for all connected solutions and therefore they are combined to each other via ID LifePass and can use the same database, avoiding multiple user enrolments. By using ID LifePass a central corporate security concept can be created, which can be extended via API any time.



Main benefits of using ID LifePass

- FRR 0,01%, FAR 0,00001%
- Vein ID cannot be stolen, copied, reproduced
- No need for RFID cards, chips, bracelets, passwords (can be combined)
- Can be easily integrated into own 3rd party system via API
- Compatibility through standard interfaces
  Enables 1:n identification and 1:1 verification methods
- Ideal solution for large number of users
- template encryption (AES256), encrypted data flow (SSL/TLS 1.2)

Main fields of use of ID LifePass

- Office buildings
- IT data centres
- Healthcare, hospitals
- Schools, universities
- Justice buildings
- Sport venues
- Airports
- Correctional facilities
- Factories, oil refinieries
- Construction sites
- R&D centres
- Financial institutions
- Pharmaceutical and chemical industry
- State sector/critical infrastructure
- Military

Features and benefits

ID LifePass in a nutshell

Highly secure

Based on the Fujitsu PalmSecure™ technology, ID LifePass ensures the maximum level of security in personal authentication with the wave of the hand.

User-friendly

ID LifePass is just as convenient as using a card or token, but the client does not have to worry about lost or stolen credentials.

Cost-effective

By using ID LifePass, the costs of replacing stolen or lost RFID cards can be absolutely eliminated.

Simple to use

ID LifePass can be easily used by anyone by simply hovering one's hand above the sensor.

Easy to integrate

ID LifePass can be easily integrated into any 3rd party system via APIs.

Fast authentication

ID LifePass ensures ~1 second biometric authentication time, which is faster than almost any other solutions.

Main features

- Online, offline operation
- Unlimited numbers of users
- 1:1 or 1:n authentication
- 1:1 multifactor authentication is also possible
- Anonymous stored user data
- Encrypted communication
- ~1 second authentication time
- Can be used as primary or secondary identification/verification method

Benefits

- Highest security in biometrics, FAR 0.00001%, FRR 0.01%
- No need for physical cards, therefore cost effective solution
- Can be easily used by anyone, regardless of age (above 5) or abilities
- Easy to integrate
- Users need to be registered in one system in general only once in a lifetime
- ~1 second biometric authentication time
- RFID and biometric authentication can be combined
- Can be combined with ID Access, ID Login as a corporate security solution package
- Can be fully integrated into 3rd party solutions just as RFID based access control systems, software with password authentication etc.

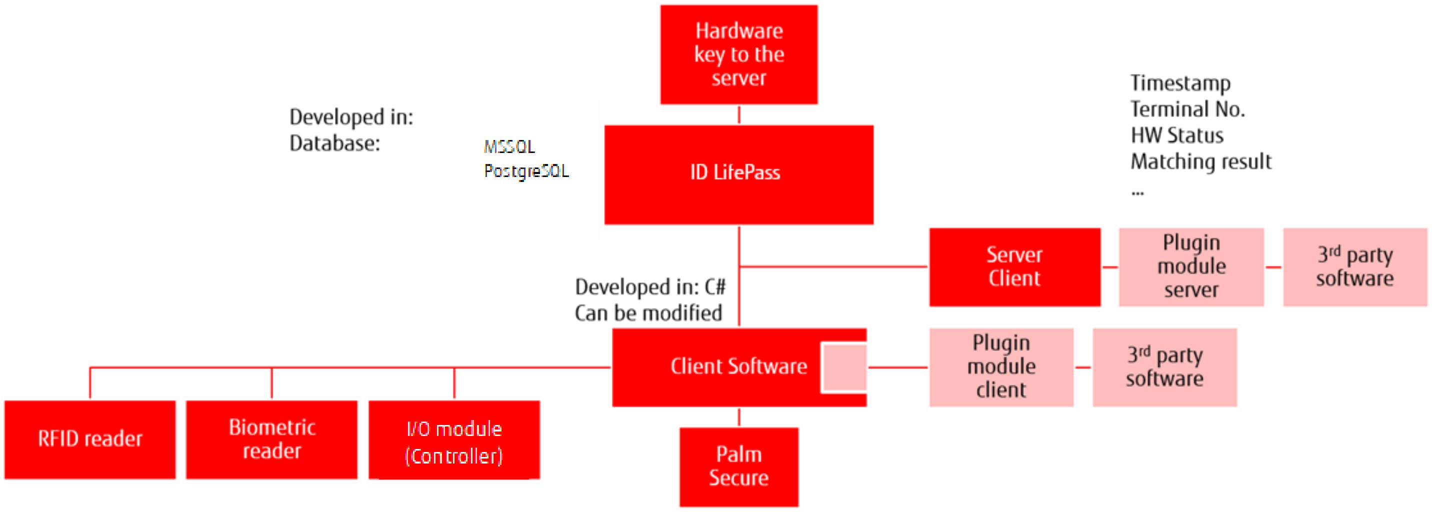
Security features

All components of ID LifePass are protected by state of the art technology security mechanisms. ID LifePass uses a three-level encryption (biometric template, communication, database). The system management software does not use passwords, it can be accessed only via palm vein recognition. The optional RFID reader device uses latest Mifare technology (please contact us for further information).

Technical Details

Client operating system	Windows 8, 8.1 (32 or 64 bit), Windows 10
Server operating system	Min. Microsoft Server 2012 R2, 64 bit
Database	Min. MS-SQL 2012 or higher, PostgreSQL 9.6
Necessary hardware	Desk terminal + 1 USB port
Possible authentication procedure	Identification (1:n), Verification (1:1)

System architecture



Main elements

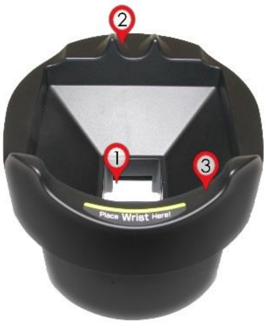
In case of using ID LifePass as authentication middleware for physical access projects when existing facility systems are continually used:

U Guide	Registration desk terminal
Triple1 / Triple1+ / TripleTime	Biometric reader terminal
Server	Any virtual or physical server operating on Microsoft Server platform
ID LifePass Server	Core module of ID LifePass as server software
Client device or Controller	Can be any Intel™ computing device operating on Microsoft platform
ID LifePass Client	Client software on the local computing device
Management and registration device	U Guide with additional F Pro OEM sensor connected via USB with any computing device operating on Microsoft platform
ID LifePass AdminSuite	System/user management, registration interface

Optional hardware

U Guide - biometric registration device

The U Guide is a biometric reader device, specialized in user enrolment processes. An additional F Pro OEM sensor is required for functionality. The intuitive design allows users to optimally position their hands for capturing. U Guide is perfect for high traffic locations, since hundreds of users have designed it for daily utilization and it is easy to install and maintain.



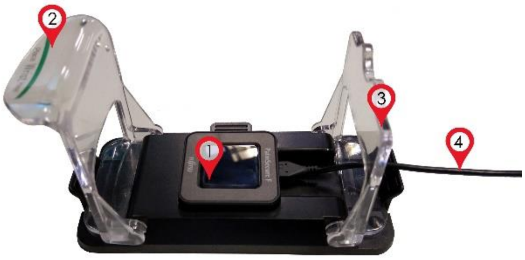
1) Place for additional Fujitsu PalmSecure™ F Pro OEM sensor

2) Finger rest (for optimal distance from sensor)

3) Hand rest (for the optimal hand positioning)

Foldable hand guide - biometric authentication device

The foldable hand guide provides simple, secure and fast biometric capturing. The excluded F Pro Standard sensor can be connected to the computing device via USB cable. The hand guide supports ideal hand positioning with finger and wrist guides, ensuring ease of use from the very first time. As it is small and easy portable, the hand guide provides an ideal solution for secure biometric authentication, computer login, access management or data protection in any place, where a maximum level of security solution is required.



1) Additional Fujitsu PalmSecure™ F Pro Standard sensor

2) Hand rest (for optimal distance from sensor)

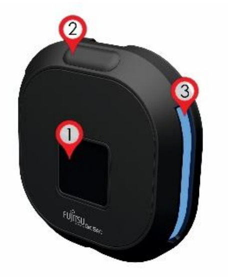
3) Finger guide (for optimal distance from sensor)

4) USB cable

Hardware for ID LifePass combined with an access control system

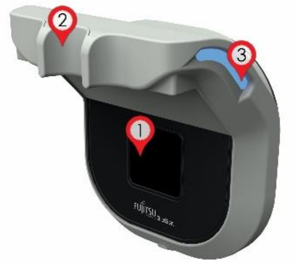
Triple1 - modular biometric reader terminal for indoor environment

The Triple1 terminal is the biometric PalmSecure™ sensor device specialized in 1:n identification. It contains a Fujitsu PalmSecure™ F Pro OEM sensor and is connected to the local ID Access GATEKEEPER controller via one USB and one CAT5 wire. The maximum distance between the Triple1 and controller is 5 meters but can be extended to 25 meters (requires additional hardware).
The Triple1 has a built-in sabotage protection. In case of an alarm, the terminal will be cut off automatically from the controller and there is no possibility to get into the controller via the terminal after that.
The unique feature of the Triple1 is that it can be installed in three versions: contactless, with finger rest or complete hand rest (all three options are provided within the package). The terminal can be surface mounted or sunk into the wall.



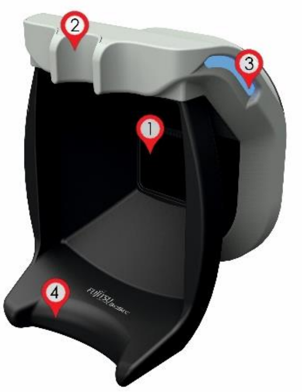
Triple1 - contactless

1) Fujitsu PalmSecure™ F Pro OEM sensor
2) Cover for connection slot to finger rest
3) RGB LED



Triple1 – finger rest

1) Fujitsu PalmSecure™ F Pro OEM sensor
2) Middle finger rest (for optimal distance from sensor)
3) RGB LED

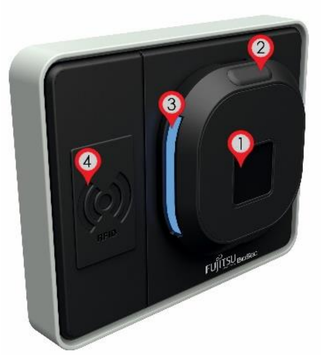


Triple1 – full hand rest

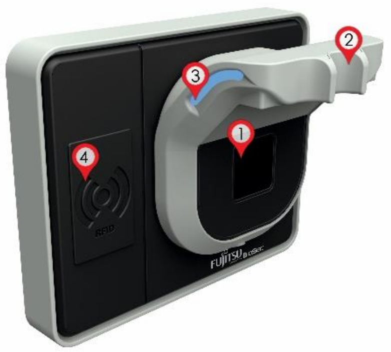
1) Fujitsu PalmSecure™ F Pro OEM sensor
2) Middle finger rest (for optimal distance from sensor)
3) RGB LED
4) Hand rest (for the optimal hand positioning)

Triple1+ - biometric terminal with RFID reader

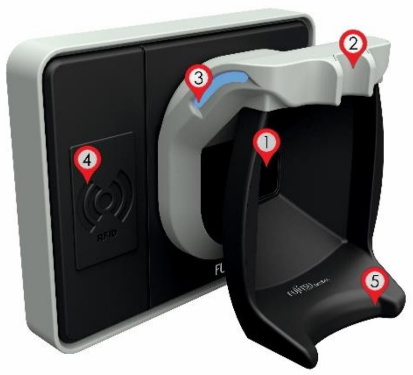
The Triple 1+ terminal is a biometric access control device, which was specially designed for indoor environments. The Triple1+ includes a Fujitsu PalmSecure™ F Pro OEM Sensor, a Triple1 biometric terminal and a RFID reader device in a single housing. By using palm vein recognition based biometric authentication, the maximum level of security can be provided, while the RFID reader enables further authentication options based on the customer´s requests.
The biometric terminal of the Triple1+ is connected to the local controller (ID Access GATEKEEPER Controller) via one USB and one CAT5 wire. The maximum distance between the terminal and the controller is 5 meters but can be extended to 25 meters (requires additional hardware).
The biometric authentication unit has a built-in sabotage protection. In case of an alarm, the terminal will be cut off automatically from the controller and there is no possibility to get into the controller via the terminal after that.
The unique feature of the Triple1+ is that the biometric terminal can be installed in three versions: contactless, with finger rest or complete hand rest (all three options are provided within the package). The terminal can be surface mounted or sunk into the wall.



1) Fujitsu PalmSecure™ F Pro OEM sensor
2) Cover for connection slot to finger rest
3) RGB LED
4) RFID reader



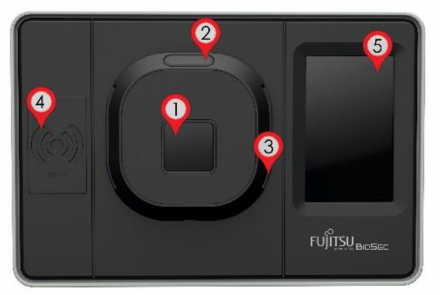
1) Fujitsu PalmSecure™ F Pro OEM sensor
2) Middle finger rest (for optimal distance from sensor)
3) RGB LED
4) RFID reader



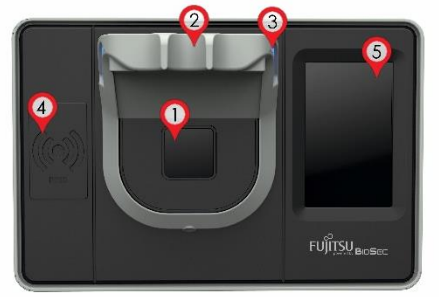
1) Fujitsu PalmSecure™ F Pro OEM sensor
2) Middle finger rest (for optimal distance from sensor)
3) RGB LED
4) RFID reader
5) Hand rest (for the optimal hand positioning)

TripleTime - biometric time and attendance terminal

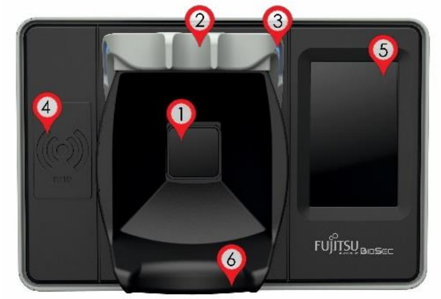
The TripleTime terminal is an indoor biometric PalmSecure™ sensor device for time and attendance solutions. The TripleTime terminal includes a PalmSecure™ F Pro OEM sensor, a Triple1 terminal, an RFID reader device and a 5-inch touchscreen for seamless clocking in and out. By using palm vein recognition based biometric authentication, employee monitoring becomes accurate, while identity abuses and buddy punching can be eliminated with the greatest certainty. Combined with an RFID reader, the TripleTime terminal enables 1:n and 1:1 authentication options based on customer´s requests. In addition, the 5-inch touchscreen supports ease of use and convenience.
The TripleTime biometric terminal is connected to the local controller (ID Access GATEKEEPER Controller) via one USB and one CAT5 wire. The maximum distance between the terminal and the controller is 5 meters but can be extended to 25 meters (requires additional hardware). The biometric authentication unit has a built-in sabotage protection. In case of an alarm, the terminal will be cut off automatically from the controller and there is no possibility to get into the controller via the terminal after that. The unique feature of the TripleTime is that the biometric terminal can be installed in three versions: contactless, with finger rest or complete hand rest (all three options are provided within the package). The terminal can be surface mounted or sunk into the wall.



1) Fujitsu PalmSecure™ F Pro OEM sensor
2) Cover for connection slot to finger rest
3) RGB LED
4) RFID reader
5) 5-inch touchscreen



1) Fujitsu PalmSecure™ F Pro OEM sensor
2) Middle finger rest (for optimal distance from sensor)
3) RGB LED
4) RFID reader
5) 5-inch touchscreen

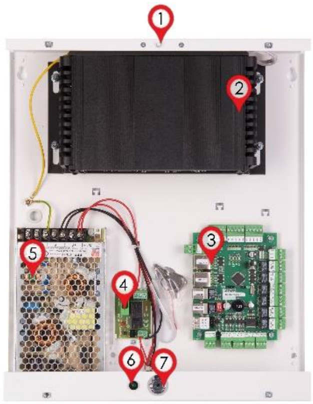


1) Fujitsu PalmSecure™ F Pro OEM sensor
2) Middle finger rest (for optimal distance from sensor)
3) RGB LED
4) RFID reader
5) 5-inch touchscreen
6) Hand rest (for the optimal hand positioning)

ID Access GATEKEEPER Controller

The controller unit manages maximum two biometric terminal devices and/or four RFID reader devices. The controller contains one Fujitsu OEM system board (D3544 S3) designed for constant operation and one I/O module for management of two access points. The controller is the link between the biometric terminals and the ID Access GATEKEEPER software installed onto the central server.

The local controllers are communicating with the servers via encrypted and certified TCP/IP protocol and minimum CAT5 network. The system can operate in offline modus in case the connection to the server is interrupted for any reason. In this case, the identification process will be taken over by the local computing device in the controller.



1) Sabotage tamper switch
2) Micro PC
3) I/O module
4) Central electric relay
5) Power supply
6) Power feedback relay
7) On-off key

ID LifePass server – the server software

The ID LifePass central identification software as a middleware on the server performs personal identification, contains logs and synchronizes all Controllers, also in redundancy.

The redundant server infrastructure is created as master/slave server combination. In case of server failure, the other server takes over the central role of the system automatically.

There is no need to license redundant server software instances (only the productive instance needs one license).

The system management software (ID LifePass AdminSuite) is connected directly to the server software. The ID LifePass AdminSuite can be installed onto as many workstations as licensed in the system but no sensitive data is stored in the software, direct online connection is needed to the server software.

Technical specifications of the ID LifePass server

Database	MS-SQL 2012 or higher, PostgreSQL 9.6
Server operating system	Min. Microsoft Server 2012 R2, 64bit
Server configuration for 1:1 authentication	Up to 1 million users, minimum requirement: Intel E3-1231v3 CPU, 8GB 1600MHz ECC RAM, 250GB SATA HDD
Redundancy	Master/slave combination, automatic failover

Contact
FUJITSU
Fujitsu Technology Solutions GmbH
Address: Mies-van-der-Rohe Str. 8,
80807 Munich, Germany
E-mail: palmsecure@ts.fujitsu.com
Website: http://www.fujitsu.com/palmsecure
2020/05/08

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.
For further information see:
https://www.fujitsu.com/global/about/resources/terms/
Copyright © 2020 Fujitsu Technology Solutions