PalmSecure™

U2PS-LA23-02ENZ3(3)

FUJITSU Biometric Authentication

PalmSecure™ SDK V02

System Development Guide

FUJITSU

◆ Revision History

Revision	Issued Date	Revised Page	Modification Details
			* For the revision history before Rev. 2.2, refer to the "◆ Previous Revision History" at the end of this document.
Rev 2.2	Nov 2022	Entire document	• Modified descriptions according to support for 200,000 R-format data items for identification by Enterprise Edition.
		Entire document	• Modified descriptions according to support for Linux(arm) by Sample interface module for Java and Sample application for Java.
		Page 18 to Page 24	• Modified the following descriptions in "2.2 Hardware and Software Requirements". ・OS in "2.2.1 Windows and Linux(x64)". ・OS and the tested CPU in "2.2.3 Android(Arm8-A)".
		Page 67	• Added "2.8.6 Palm Vein Data Group Thread Sharing Function" to "2.8 Designing Applications for Identification".
		Page 91	• Added descriptions concerning the Palm vein data group thread sharing function to "4.1.1 Features of PalmSecure SDK V02L03".
		Page 93 to 95	• Updated "4.2.1 Additional/Modified Functions in PalmSecure SDK V02L03".
		Page 125 to 126	• Modified tested OS for each software in "Appendix B Tested OSes".
Rev. 2.3	Jan 2023	Entire document	• Modified descriptions concerning supported OSes. ・Windows 8.1 is finished. ・Windows 11 is updated to Version 22H2..
		Entire document	• Deleted "for extended function" from the name of the Sensor driver.
		Entire document	• Modified to describe 64 bit versions first.
		Page 9	• Modified descriptions in "1.4.2 Sensor Driver " due to addition of the driver package type of Sensor driver.
		Page 18 to Page 20	• Modified the following descriptions in "2.2 Hardware and Software Requirements". ・Memory ・OS ・Sensor driver

Revision	Issued Date	Revised Page	Modification Details
Rev. 2.3	Jan 2023	Page 77	• Added “3.2.3 Developing Windows Applications”.
		Page 126	• Added descriptions for the driver package type of the Sensor driver to “Appendix A How to Confirm the Version Level Information”.

◆ Introduction

Thank you for purchasing PalmSecure™ SDK V02 (hereinafter called “this product”). This document provides an overview of this product and describes considerations when you develop and operate the Palm vein authentication system.

January 2023: Rev. 2.3

Caution for This Manual

You are required to use this product within the specification described in this document.

Regarding to High Safety Required Usage

This Product is designed, developed and manufactured as contemplated for general use, including without limitation, general office use, personal use, household use, and ordinary industrial use, but is not designed, developed and manufactured as contemplated for use accompanying fatal risks or dangers that, unless extremely high safety is secured, could lead directly to death, personal injury, severe physical damage or other loss (hereinafter "High Safety Required Use"), including without limitation, nuclear reaction control in nuclear facility, aircraft flight control, air traffic control, mass transport control, medical life support system, missile launch control in weapon system. You shall not use this Product without securing the sufficient safety required for the High Safety Required Use. If you wish to use this Product for High Safety Required Use, please consult with the sales representatives in charge before such use.

Cautions for Exporting This Product

When exporting or providing this product and this document to a foreign country, check relevant laws such as "Foreign Exchange and Foreign Trade Control Law", and regulations such as U.S. export control law, and follow the necessary procedures.

Warnings

- Reprinting or reproducing this document in part or in whole without permission is forbidden.
- Items described in this document are subject to change without prior notice.

PalmSecure is a trademark of Fujitsu Ltd.

Microsoft, Windows, Windows Server, and Visual Basic are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Android is a trademark or registered trademark of Google Inc. in the U.S. and other countries.

Intel and Intel Core are trademarks of Intel Corporation or its subsidiaries in the U.S. and/or other countries.

Arm is a trademark or registered trademark of Arm Limited (or its subsidiaries) in the US and/or elsewhere.

Java is a registered trademark of Oracle and/or its affiliates.

VMware vSphere is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions.

Other company names and product names described in this document are trademarks or registered trademarks of each company.

◆ Composition of This Document

This document consists of the following four chapters and the appendix.

Chapter Title	Description
Chapter 1 Introduction to This Product	Provides an overview of this product.
Chapter 2 Developing the Palm Vein Authentication System	Describes development of the Palm vein authentication system.
Chapter 3 Considerations for Developing the Palm Vein Authentication System	Describes the issues to be considered when you develop the Palm vein authentication system.
Chapter 4 When You Are Using Previous Versions	Describes PalmSecure SDK V02L03, additional/modified functions made in each version level and the issues to be considered when you are migrating.
Appendix	
Appendix A How to Confirm the Version Level Information	Describes how to confirm the version level information of software, documents, and firmware in the Sensor unit that are provided with this product.
Appendix B Tested OSes	Displays a list of software provided with this product and OSes with which operations of the given software are confirmed.
Appendix C Updating the Firmware on the Sensor Unit	Describes two methods to update the firmware on the Sensor unit.
Appendix D Checking the Sensor Type	Describes how to check the sensor type.
Appendix E Consideration on the Palm Guide	Describes the concept of using the Palm guide.
Appendix F Power Saving Function of the Sensor Unit	Describes the power saving function of the Sensor unit.
Appendix G Comparison of Functions in Each Format Type	Lists functional differences between the R-format type, I33-format type, and I-format type.
Appendix H Comparison of Functions of Each Authentication Library	Lists functional differences between each Authentication library.

◆ Abbreviations and Common Terms

Abbreviations and common terms used in this document are as follows.

Abbreviations/ Common Term	Description
This product	Abbreviation for “PalmSecure™ SDK V02”.
Sensor	Common term for “PalmSecure Sensor V2” and “PalmSecure-F Pro”.
SDK	Abbreviation for “PalmSecure™ SDK”.
Windows 10	Abbreviation for “Microsoft® Windows® 10”.
Windows 11	Abbreviation for “Microsoft® Windows® 11”.
Windows Server 2012 R2	Abbreviation for “Microsoft® Windows Server® 2012 R2”.
Windows Server 2016	Abbreviation for “Microsoft® Windows Server® 2016”.
Windows Server 2019	Abbreviation for “Microsoft® Windows Server® 2019”.
Windows Server 2022	Abbreviation for “Microsoft® Windows Server® 2022”.
Windows	Common term for “Windows 10”, “Windows 11”, “Windows Server 2012 R2”, “Windows Server 2016”, “Windows Server 2019”, and “Windows Server 2022”.
VB .NET	Abbreviation for “Microsoft® Visual Basic® .NET”.
VMware vSphere	Abbreviation for “VMware vSphere®”.
Authentication library	Abbreviation for “Authentication library V34”.
Windows version of Authentication library	Common term for “Windows(x86) Authentication library” and “Windows(x64) Authentication library”.
Linux version of Authentication library	Common term for “Linux(x64) Authentication library”, “Linux(armhf) Authentication library”, and “Linux(arm64) Authentication library”.
Authentication library for Android	Abbreviation for “Android(Armv8-A) Authentication library”.
Authentication library for Arm	Common term for “Linux(armhf) Authentication library”、“Linux(arm64) Authentication library”, and “Android(Armv8-A) Authentication library”.
ABI	Abbreviation for “Application Binary Interface”.
Android NDK	Abbreviation for “Android Native Development Kit”.
“Sensor Instruction Manual”	Common term for “Sensor Instruction Manual for PalmSecure Sensor V2” and “Sensor Instruction Manual for PalmSecure-F Pro”.
“Hardware Drawings”	Common term for “Hardware Drawings for PalmSecure Sensor V2” and “Hardware Drawings for PalmSecure-F Pro”.

◆ Notations

The following symbols are used in this document.

Symbol	Description
!Caution	Describes things that you have to look out for. You must read it.
★Tip	Provides reference information. Read it as necessary.
>See>	Indicates an item to be referred.

Also, the “PalmSecure-F Pro” is called “PalmSecure-F Pro sensor” in this document.

◆ Table of Contents

Chapter1 Introduction to This Product ····· 1

1.1 Overview 2

1.2 Features 3

1.3 Hardware Overview 4

1.4 Software Overview 5

1.4.1 Authentication Library 6
1.4.2 Sensor Driver 9
1.4.3 Sample Interface 11
1.4.4 Sample Application 12
1.4.5 Tools to Help You 14

Chapter2 Developing the Palm Vein Authentication System ····· 15

2.1 System Configuration 16

2.1.1 Stand-alone Configuration 16
2.1.2 Client/Server Configuration 17

2.2 Hardware and Software Requirements 18

2.2.1 Windows and Linux(x64) 18
2.2.2 Linux(arm64) and Linux(armhf) 22
2.2.3 Android(Armv8-A) 24

2.3 Enrollment of Palm Vein Data and Authentication 25

2.3.1 Enrollment of Palm Vein Data 25
2.3.2 Authentication 25
2.3.3 Authentication Accuracy 27

2.4 Authentication Library Type and Mode 28

2.4.1 Format Type 28
2.4.2 Using the Palm Guide (Guide Mode) 31

2.5 Extended Functions of the Sensor 35

2.5.1 Continuous Capture Function 35

2.5.2 Image Compression Function (I33-format type and I-format type only) 36
2.5.3 High-Power Function (PalmSecure-F Pro Sensor Only) 37

2.6 Designing Applications to Enroll Palm Vein Data 38
2.6.1 Data Format for Palm Vein Data for Enrollment....38
2.6.2 Palm Vein Data Enrollment Sequence 43
2.6.3 Other Considerations 49

2.7 Designing Applications for Verification 50
2.7.1 Data Format for Palm Vein Data for Authentication....50
2.7.2 Verification Sequence 51

2.8 Designing Applications for Identification 55
2.8.1 Data Format for Palm Vein Data for Authentication....55
2.8.2 Identification Method of Palm Vein Data....56
2.8.3 Risk of False Acceptance 58
2.8.4 Identification Sequence 63
2.8.5 Speeding Up the Identification Process 65
2.8.6 Palm Vein Data Group Thread Sharing Function....67
2.8.7 Other Consideration 68

Chapter3 Considerations for Developing the Palm Vein Authentication System ……69

3.1 Considerations for Designing an Application 70
3.1.1 Changing the Angle of the Hand against the Sensor....70
3.1.2 Connecting Multiple Sensors....72
3.1.3 Supporting Multiple Clients....74

3.2 Considerations for Developing an Application 76
3.2.1 Developing in C/C++....76
3.2.2 Developing in Other Languages....76
3.2.3 Developing Windows Applications....77

3.3 Security Countermeasures When Managing Vein Data.... 78

3.4 Considerations for Operating the Palm Vein Authentication System 80
3.4.1 Considerations for Enrollment of Palm Vein Data and Authentication 80
3.4.2 Consideration for the Use by Children.....83

3.5 Other Considerations..... 86

Chapter4 When You Are Using Previous Versions ·····89

4.1 Release of PalmSecure SDK V02L03..... 90
4.1.1 Features of PalmSecure SDK V02L03.....90
4.1.2 Migrating to PalmSecure SDK V02L03.....92

4.2 Additional/Modified Functions and Notes for PalmSecure SDK V02L03..... 93
4.2.1 Additional/Modified Functions in PalmSecure SDK V02L03.....93
4.2.2 Notes on Migrating to PalmSecure SDK V02L03 97

4.3 Additional/Modified Functions and Notes for PalmSecure SDK V02L02..... 106
4.3.1 Features of PalmSecure SDK V02L02.....106
4.3.2 Additional/Modified Functions in PalmSecure SDK V02L02.....108
4.3.3 Notes on Migrating to PalmSecure SDK V02L02 111

4.4 Additional/Modified Functions and Notes for PalmSecure SDK V02L01..... 118
4.4.1 Features of PalmSecure SDK V02L01 118
4.4.2 Additional/Modified Functions in PalmSecure SDK V02L01.....119
4.4.3 Notes on Migrating to PalmSecure SDK V02L01 122

Appendix ……123

Appendix A How to Confirm the Version Level Information 124

Appendix B Tested OSes 126

Appendix C Updating the Firmware on the Sensor Unit 128

Appendix D Checking the Sensor Type 130

D.1 Checking from the Base of the Sensor 130

D.2 Checking with the Sensor Maintenance Tool 130

D.3 Checking the Sensor Type from an Application 130

Appendix E Consideration on the Palm Guide..... 131

E.1 Use of the Palm Guide in Authentication 131

E.2 Use of the Palm Guide in Enrollment 133

Appendix F Power Saving Function of the Sensor Unit..... 135

Appendix G Comparison of Functions in Each Format Type 136

Appendix H Comparison of Each Authentication Library 138

Chapter1 Introduction to This Product

1.1 Overview

1.2 Features

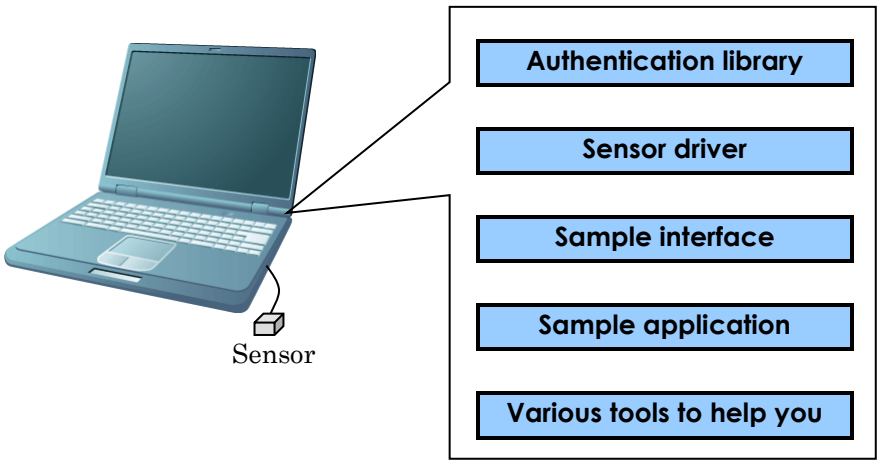
1.3 Hardware Overview

1.4 Software Overview

1.1 Overview

This product is a group of products that helps you develop the Palm vein authentication system. It consists of the Sensor set and software including the Authentication library, Sensor driver, Sample interface, Sample application, and various tools to help you develop an application.
This product allows you to develop the Palm vein authentication system for Windows, Linux, or Android operating systems, according to your business operation.

The following diagram provides an overview of this product.



1.2 Features

The features of this product are as follows:

- **Contactless**

  The Sensor is a piece of equipment that uses near-infrared light to capture palm veins without contacting the palm.

  Therefore, this system can be used hygienically even in places where unspecified numbers of people share the equipment.

- **Higher authentication accuracy**

  Very high authentication accuracy can be expected because the palm has a large number of veins, and each of them crosses intricately.

- **Difficult to counterfeit**

  Because palm veins are information that you have inside your body, there is little chance being stolen and more difficult to be forged.

1.3 Hardware Overview

The Sensor is a piece of equipment that uses near-infrared light to capture palm veins without contacting the palm.

PalmSecure SDK V02L03 supports the following two sensors.

- **PalmSecure Sensor V2**

  The PalmSecure Sensor V2 is the previous model that was included in PalmSecure SDK V02. The sales of this sensor were discontinued in 2020.

- **PalmSecure-F Pro sensor**

  The PalmSecure-F Pro sensor is the successor of the above and currently included in PalmSecure SDK V02.

  This Sensor is supported by the Authentication library V33Lxx-B25 or later.

>See> For information on how to check the sensor type, refer to “Appendix D Checking the Sensor Type”.

★Tip **The PalmSecure Sensor**
The PalmSecure Sensor that was discontinued before PalmSecure Sensor V2 is no longer supported.

The hardware parts included in the PalmSecure SDK V02 are different depending on the shipping date. Refer to the “Confirmation of Contents” for details.

>See> For information on how to use the Sensor, refer to the “Sensor Instruction Manual”.

>See> For information on drawings of the Sensor, refer to the “Hardware Drawings”.

★Tip **Integrating the Sensor into hardware**
The Sensor can be integrated into hardware such as an information provision terminal (Kiosk) by referring to the “Hardware Drawings”.

★Tip **Creating your own Holder, USB Interface cable, and Palm guide**
You can create your own Holder, USB Interface cable, and Palm guide by referring to the “Hardware Drawings”.

1.4 Software Overview

This product provides the following software to help you develop the Palm vein authentication system. You can download the latest version of software from SDK V02L03 in the SDK V02 Support Website.

- Authentication library
- Sensor driver
- Sample interface
- Sample application
- Tools to help you
  - Sensor maintenance tool
  - Firmware update tool

★Tip **When software is updated**
In addition to the update announcement on the SDK V02 Support Website, we will send you update information by e-mail.
Check version level information of the software that you are using and update to the latest version by downloading it from SDK V02L03 in the SDK V02 Support Website accordingly.

>See> For information on how to confirm the version level information, refer to "Appendix A How to Confirm the Version Level Information".

>See> For information on how to update the software to the latest version, refer to the manual for each software.

★Tip **Confirmed OSes for each software**
Confirmed OSes vary by the software..

>See> For information on confirmed OSes, refer to "Appendix B Tested OSes".

1.4.1 Authentication Library

The Authentication library is a program in a library format that enrolls vein data and authenticates a person.
You can use the Authentication library to develop an application for the Palm vein authentication system that runs on Windows, Linux, or Android, according to your needs.

◆ Editions of the Authentication library

There are two editions of Authentication libraries as follows.

- **Professional Edition**

  This library allows you to enroll, capture, verify, and identify palm vein data.
  The Professional Edition supports only calls from a single thread.

- **Enterprise Edition**

  This library is designed for servers.
  With this edition, your application can call functions for verification or identification in multi-threads.
  However, you cannot enroll or capture palm vein data with the Enterprise Edition.

◆ 64-bit and 32-bit Versions of Authentication Libraries

There are 64-bit and 32-bit versions of Authentication libraries.

- **64-bit versions**

  These Authentication libraries operate on 64-bit OSes.

  64-bit versions of Authentication libraries are as follows.

  ・Windows(x64) Authentication library Professional Edition

  ・Windows(x64) Authentication library Enterprise Edition

  ・Linux(x64) Authentication library Professional Edition

  ・Linux(x64) Authentication library Enterprise Edition

  ・Linux(arm64) Authentication library Professional Edition (Note 1)

  ・Android(Armv8-A) Authentication library Professional Edition (Note 2)

- **32-bit version**

  This Authentication library operates on 32-bit OSes.

  32-bit version of Authentication library is as follows.

  ・Windows(x86) Authentication library Professional Edition

  ・Linux(armhf) Authentication library Professional Edition (Note 3)

Note 1) Target of the Linux(arm64) Authentication library is 64-bit (AArch64 mode) Linux(Armv8-A).

Note 2) Target of the Android(Armv8-A) Authentication library is 64 bit (AArch64). Also, it provides Java interface.

Note 3) Target of the Linux(armhf) Authentication library is 32-bit Linux(Armv7-A). This Authentication library is for armhf: the library's floating-point ABI is "hard floating-point".

> **★Tip　Authentication library for armel**
> We do not provide Authentication library for armel: the library's floating-point ABI is "soft floating-point".

>See> For information on the Windows version or Linux version of Authentication library, refer to the "Authentication Library Reference Guide",

>See> For information on the Android version of Authentication library, refer to the "Authentication Library for Android Reference Guide".

>See> For the comparison of the functions of each Authentication library, refer to "Appendix H　Comparison of Each Authentication Library".

!Caution **License authentication of the Authentication library**

License authentication for the given edition is required when using the Authentication library.
Acquire the license file and authenticate the license.

>See> For information on how to acquire the license file, refer to the "How to Acquire the License File".

>See> For information on how to carry out the license authentication, refer to the "Authentication Library Reference Guide" or "Authentication Library for Android Reference Guide".

!Caution **Application keys**

The "application key" described in the "License agreement" is required to use the Authentication library.

>See> For information on how to use an application key, refer to one of the following manuals.

- "Authentication Library Reference Guide"
- "Authentication Library for Android Reference Guide"
- "Sample Application for Microsoft .NET Framework Manual Professional Edition"
- "Sample Application for Microsoft .NET Framework Manual Enterprise Edition"
- "Sample Application for Java Manual Professional Edition"
- "Sample Application for Java Manual Enterprise Edition"
- "Sample Application for Android Manual"
- "Sample Source for C Language Manual Professional Edition"

1.4.2 Sensor Driver

The Sensor driver enables operations on the Sensor.

There are two types of Sensor drivers as follows.

- Sensor driver for Windows
- Sensor driver for Linux

★Tip **About conventional Sensor driver for Windows**
The support for the conventional Sensor driver for Windows (V11 and V20) that was provided since the launch of PalmSecure SDK V01 is discontinued.
Also, note that in this document, naming of the "Sensor driver for extended functions" has been changed to "Sensor driver".

Note that the Android version of Sensor driver is not provided because it is not necessary.

◆ Sensor Driver (Windows Version)

The following Sensor drivers are available for Windows..

- **Installer type**

This Sensor driver is provided in the installer format (MSI package).

The following are the installer type of the Sensor.

・Windows(x64) Sensor Driver V31

・Windows(x86) Sensor Driver V31

Note that this driver does not support the Windows 11 Smart App Control. If the Smart App Control support is required, use the Driver package type of Sensor driver V32.

- **Driver package type**

This Sensor driver is provided in the driver package.

The following is the driver package type of the Sensor.

・Windows(x64) Sensor driver V32

>See> For information on the Sensor driver (Windows version), refer to the “Sensor Driver Installation Guide”.

◆ Sensor Driver (Linux Version)

This is the Sensor driver for Linux.

The Sensor driver for Linux is provided as source code.

!Caution **About Sensor driver for Linux**
Operations of the Sensor driver for Linux are not guaranteed in customers' environments. It is customers' responsibility to verify the operations.

>See> For information on the Sensor driver (Linux version), refer to the "Sensor Driver Installation Guide".

1.4.3 Sample Interface

This product provides the following Sample interface.

- **Sample interface library for Microsoft .NET Framework (Windows(x86)/Windows(x64))**

  This library allows you to call functions in the authentication library from .NET Framework applications. You can use this library when developing applications in VB.NET and C#. The Sample interface library for .NET 6 is also provided for Windows(x64) version.

- **Sample interface module for Java (Windows(x86)/Windows(x64)/Linux(x64)/Linux(armhf)/Linux(arm64))**

  This module allows you to call functions in the authentication library from Java applications. You can use this library when developing applications in Java.

  Note that only build environment such as Makefile is available for the Interface Native module for Arm.

  Also, the Windows 11 Smart App Control is not supported,

!Caution **Developing applications using the Sample interface**
The Sample interface is intended to help customers in developing applications; however, its operations are not guaranteed in the customer's operational environment. Therefore, it is customer's responsibility to fully verify the operations when developing applications using the Sample interface.

>See> For information on the Sample interface library for Microsoft .NET Framework, refer to "Sample Interface Library for Microsoft .NET Framework Manual".

>See> For information on the Sample interface module for Java, refer to "Sample Interface Module for Java Manual".

1.4.4 Sample Application

The following Sample applications and Sample source are provided to show how to use the Sample interfaces or the Authentication library.

- **Sample application for Microsoft .NET Framework (Windows(x86)/Windows(x64))**

  This application operates on .NET Framework and calls functions in the Authentication library via the Sample interface library for Microsoft .NET Framework. You can use this library when developing applications in VB.NET and C#.

  There are the Professional Edition and Enterprise Edition of the Sample application for Microsoft .NET Framework. The Sample application for .NET 6 is also provided for Windows(x64) Professional Edition. For Enterprise Edition, the Sample application for .NET 6 is provided in C#.

- **Sample application for Java (Windows(x86)/Windows(x64)/Linux(x64)/Linux(armhf)/Linux(arm64))**

  This application operates on Java virtual machine (JVM) and calls functions in the Authentication library via the Sample interface module for Java. You can use this library when developing applications in Java.

  There are the Professional Edition and Enterprise Edition of the Sample application for Java. Only Professional Edition supports the Arm.

  Note that the Windows 11 Smart App Control is not supported,

- **Sample application for Android (Armv8-A)**

  This application calls methods in the Authentication library for Android. This application is developed in Java.

- **Sample source for C language**

  This sample source shows how to call basic functions of Windows version and Linux version of the Authentication library. You can refer to this sample source when developing applications in C/C++.

  Note that application module is not provided.

!Caution **Developing applications using the Sample application**
The Sample application is intended to help customers develop applications; however, its operations are not guaranteed in the customer's operational environment. Therefore, it is customers' responsibility to fully verify the operations when developing applications using the Sample application.

>See> For information on the Sample application for Microsoft .NET Framework, refer to the "Sample Application for Microsoft .NET Framework Manual Professional Edition" or "Sample Application for Microsoft .NET Framework Manual Enterprise Edition".

>See> For information on the Sample application for Java, refer to the "Sample Application for Java Manual Professional Edition" or "Sample Application for Java Manual Enterprise Edition".

>See> For information on the Sample application for Android, refer to the "Sample Application for Android Manual".

>See> For information on the Sample source for C language, refer to the "Sample Source for C Language Manual Professional Edition".

1.4.5 Tools to Help You

This product provides the following tools to help you:

- Sensor maintenance tool
- Firmware update tool

1.4.5.1 Sensor Maintenance Tool

You can use the Sensor maintenance tool to troubleshoot by diagnosing Sensor's internal components and the internal camera. You can also check the Sensor Information.

>See> For information on the Sensor maintenance tool, refer to the "Sensor Maintenance Tool Operation Guide".

1.4.5.2 Firmware Update Tool

The firmware on the Sensor unit can be updated easily with the Firmware update tool.

Note that the Windows 11 Smart App Control is not supported,

★Tip **Updating the firmware**
The firmware can be updated using the Firmware update tool as well as using the Authentication library firmware update function.

>See> For information on the two firmware update methods, refer to "Appendix C Updating the Firmware on the Sensor Unit".

>See> For information on the Authentication library firmware update function, refer to the "Authentication Library Reference Guide".

>See> For information on the Firmware update tool, refer to the "Firmware Update Tool Operation Guide".

Chapter2 Developing the Palm Vein Authentication System

2.1 System Configuration

2.2 Hardware and Software Requirements

2.3 Enrollment of Palm Vein Data and Authentication

2.4 Authentication Library Type and Mode

2.5 Extended Functions of the Sensor

2.6 Designing Applications to Enroll Palm Vein Data

2.7 Designing Applications for Verification

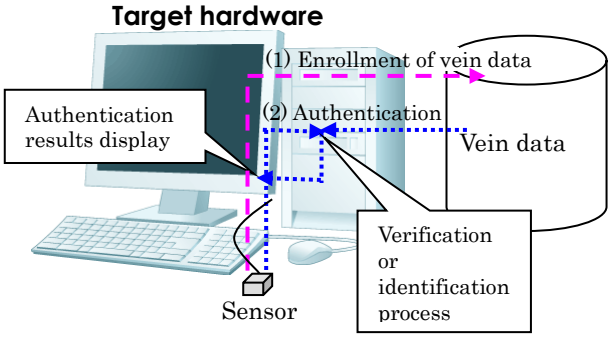
2.8 Designing Applications for Identification

2.1 System Configuration

When you develop the Palm vein authentication system, the system configuration should be determined according to your business operation.
Many system configurations are possible when using the Palm vein authentication system, such as a stand-alone configuration, a client/server configuration, and the combination of a stand-alone configuration and an administrative personal computer.
In this document, we will use a stand-alone configuration, and a client/server configuration, as examples.

2.1.1 Stand-alone Configuration

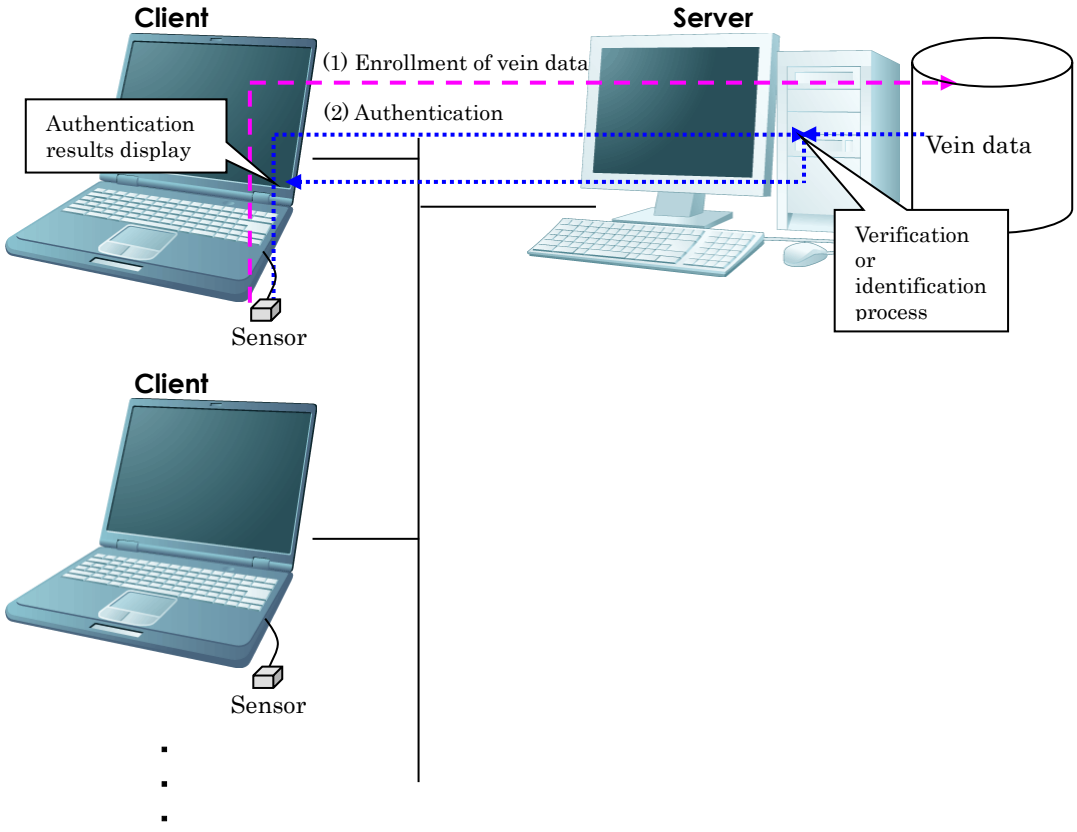
In this configuration, all procedures, from the enrollment of vein data and authentication to management of vein data, can be performed on one target hardware.
The following diagram illustrates an example of a stand-alone configuration.



!Caution Using the Sensor from multiple applications (processes)
A Sensor cannot be accessed simultaneously from multiple applications (processes).

2.1.2 Client/Server Configuration

In this configuration, all procedures (from the enrollment of vein data and authentication to management of vein data) can be performed separately by the client and the server. For example, operations such as the enrollment of vein data and authentication are performed by the client, and the management of vein data and verification and identification processes are performed by the server.
The following diagram illustrates an example of a client/server configuration.



!Caution Using the Sensor from multiple applications (processes)
A Sensor cannot be accessed simultaneously from multiple applications (processes).

2.2 Hardware and Software Requirements

2.2.1 Windows and Linux(x64)

◆ Professional Edition

Hardware and Software Requirements		Description
Hardware Requirement	CPU	Intel® Core™2 Duo 2.40GHz or more (Note 1) (must also comply with the recommended value for the given OS) CPUs with SSE4.2/AES-NI are recommended.
	Memory	64-bit version : 4 GB or more 32-bit version : 2 GB or more (must also comply with the recommended value for the given OS)
	USB port	< PalmSecure Sensor V2 > ・ USB 2.0 < PalmSecure-F Pro sensor > ・ USB 2.0, USB 3.0 (Note 2)
	HDD space (Note 3)	231 MB or more
	Sensor	・PalmSecure Sensor V2 ・PalmSecure-F Pro sensor
		Use the following version level of firmware for the Sensor. ・PalmSecure Sensor V2 : V50L225 or later ・PalmSecure-F Pro sensor : V56L022 or later
Software Requirement	OS (Note 4)	・Windows 10 Version 21H2 (x86 and x64)) ・Windows 11 Version 22H2 (x64) ・Linux(x64) (CentOS 7.9-2009 and Rocky 8.4)
	Sensor driver (Note 5)	< Windows> ■Installer type ・Windows(x64) Sensor driver V31L47 ・Windows(x86) Sensor driver V31L37 ■Driver package type ・Windows(x64) Sensor driver V32L01
		< Linux> ・Linux Sensor driver V31L04 or later Contact the sales representatives for the availability.
	Authentication library (Note 5)	・Windows(x64) Authentication library Professional Edition ・Windows(x86) Authentication library Professional Edition ・Linux(x64) Authentication library Professional Edition Download the latest version from SDK V02L03 in the SDK V02 Support Website.

!Caution **Downloading the Authentication library**
Check the version and edition of the Authentication library that is written in the "License agreement" of the Authentication library, and download the correct library.

Note 1) When using a CPU that is not described in this requirement, please verify the operations yourself. (The Authentication library does not work if SSE3/SSSE3 instructions are not implemented on the CPU.)
When performing identification, CPUs with SSE4.2/AES-NI are required.

Note 2) When using high-power function, PalmSecure-F Pro sensor draws 900 mA of power from a USB port. Therefore, be sure to connect the Sensor to a USB 3.0 port.
If you use the high-power function on a USB 2.0 port, a device failure may occur on the target hardware.

>See> For information on the high-power function, refer to "2.5.3 High-Power Function (PalmSecure-F Pro Sensor Only)".

Note that even when the Sensor is connected to the USB 3.0 port, the transfer speed is the same as that of USB 2.0.

Note 3) Minimum required hard disk space for the Authentication library and the Sensor driver.

>See> For detailed information on the required hard disk space, refer to the "Authentication Library Reference Guide" and the "Sensor Driver Installation Guide".

Additional space to store palm vein data is also required. Be sure to secure enough space.

Note 4) Operations of the Authentication library and Sensor driver are confirmed in the following environments.

Windows 10 : Pro
Windows 11 : Pro
Linux : CentOS 7.9-2009 [kernel: 3.10.0-1160.el7.x86_64, glibc: 2.17]
Rocky 8.4-2105 [kernel: 4.18.0-305.3.1.el8_4.x86_64, glibc: 2.28]

Operations have not been tested in virtual environments.
Also, some of the software products does not support the Smart App Control for Windows 11. Refer to the "1.4 Software Overview" for the details.

Note 5) The downloaded Sensor driver and Authentication library are compressed.
You must decompress the folder using an extraction tool.

◆ Enterprise Edition

Hardware and Software Requirements		Description
Hardware Requirement	CPU (Note 1)	Intel® Core™2 Duo 2.40GHz or faster multi-core CPU (must also comply with the recommended value for the given OS) CPUs with SSE4.2/AES-NI are recommended.
	Memory	4 GB or more (must also comply with the recommended value for the given OS)
	HDD space (Note 2)	222 MB or more
Software Requirement	OS (Note 3)	・Windows Server 2012 R2 Update (x64) ・Windows Server 2016 (x64) ・Windows Server 2019 (x64) ・Windows Server 2022 (x64) ・Linux(x64) (CentOS 7.9-2009 and Rocky 8.4)
	Authentication library (Note 4)	・Windows(x64) Authentication library Enterprise Edition ・Linux(x64) Authentication library Enterprise Edition Download the latest version from SDK V02L03 in the SDK V02 Support Website.

!Caution **Downloading the Authentication library**
Check the version and edition of the Authentication library that is written in the "License agreement" of the Authentication library, and download the correct library.

Note 1) When using a CPU that is not described in this requirement, please verify the operations yourself. (The Authentication library does not work if SSE3/SSSE3 instructions are not implemented on the CPU.)
When performing identification, CPUs with SSE4.2/AES-NI are required.
Also, when performing identification against a palm vein data group of over 10,000 hands, use the CPUs with 4 or more cores.

Note 2) Minimum required space for the Authentication library alone.
>See> For detailed information on the required hard disk space, refer to the "Authentication Library Reference Guide".
Additional space to store palm vein data is also required. Be sure to secure enough space.

Note 3) Operations of the Authentication library are confirmed in the following environments.

Windows Server 2012 R2 : Standard Edition
Windows Server 2016 : Standard Edition
Windows Server 2019 : Standard Edition
Windows Server 2022 : Standard Edition
Linux : CentOS 7.9-2009 [kernel: 3.10.0-1160.el7.x86_64, glibc: 2.17]
Rocky 8.4-2105 [kernel: 4.18.0-305.3.1.el8_4.x86_64, glibc: 2.28]

Operations in virtual environments are verified using VMware vSphere 6 with the above OSes. However, the virtual environments may require more processing time and memory than the physical environments.

Note 4) The downloaded Authentication library are compressed.
You must decompress the folder using an extraction tool.

2.2.2 Linux(arm64) and Linux(armhf)

Hardware and Software Requirements			Description
Hardware Requirement	CPU architecture (Note 1)		<64-bit version> Armv8-A <32-bit version> Armv7-A
	Required CPU option		NEON, VFP (CRYPTO is recommended for 64-bit version)
	Supported CPU		<64-bit version (Armv8-A)> ・Cortex-A72: Broadcom BCM2711 <32-bit version (Armv7-A)> ・Cortex-A15: RZ/G1M (Renesas)
	Memory		<64-bit version> 1 GB or more <32-bit version> 256 MB or more (must also comply with the recommended value for the given OS)
	USB		・USB 2.0, USB 3.0 (Note 2)
	Sensor		・PalmSecure-F Pro sensor (Mouse type sensor is not supported) The firmware must be V56L022 or later.
Software Requirement	OS (Note 3)	Type	Linux (kernel: 3.10.0 or later)
		Endian	Little
		GNU C Library	2.10 or more
	Sensor driver		・Linux Sensor driver V31L04 or later Contact the sales representatives for the availability.
	Authentication library for the Arm processor		・Linux(arm64) Professional Edition ・Linux(armhf) Professional Edition (Note 4) Download the latest version from SDK V02L03 in the SDK V02 Support Website.

Note 1) The use of the multi-core processor is recommended for identification.

Note 2) When using high-power function, PalmSecure-F Pro sensor draws 900 mA of power from a USB port. Therefore, be sure to connect the Sensor to a USB 3.0 port.

If you use the high-power function on a USB 2.0 port, a device failure may occur on the target hardware.

Note that even when the Sensor is connected to the USB 3.0 port, the transfer speed is the same as that of USB 2.0.

>See> For information on the high-power function, refer to “2.5.3 High-Power Function (PalmSecure-F Pro Sensor Only)”.

Note 3) Operations have not been tested in virtual environments.

Note 4) The 32-bit version of Authentication library for armhf is available when floating-point ABI is “hard floating-point”.
This library is not available when floating-point ABI is “soft floating-point”.

2.2.3 Android(Armv8-A)

Hardware and Software Requirements		Description
Hardware Requirements	CPU architecture	Armv8-A (64 bit)
	Required CPU option	NEON, VFP (CRYPTO is recommended)
	Tested CPU	Cortex-A72: Broadcom BCM2711
	Memory	3 GB or more
	USB	USB 2.0 * Host function must be enabled
	Sensor	PalmSecure-F Pro sensor (Mouse type sensor is not supported) Use the firmware V56L022 or later.
Software Requirements	OS (Note)	Android 11 (64 bit) * 64 bit Native Library must be available
	Authentication library	Android(Armv8-A) Authentication library Professional Edition (Download the latest version from SDK V02L03 in the SDK V02 Support Website.)
	Software for development	Android Studio 4.0.1
		Android NDK LTS r21e

Note) The Authentication library for Android is confirmed to work with Android 11. If you upgrade to Android 12 or higher, it may become inoperable. For this reason, do not upgrade your Android-OS.
When upgrading the Android-OS, please verify the operation yourself thoroughly.

>See> For information on the installation and setting procedure of Android Studio and so on, refer to the website for Android Developers.

2.3 Enrollment of Palm Vein Data and Authentication

2.3.1 Enrollment of Palm Vein Data

You must first capture palm veins to be compared against, and enroll them as palm vein data before carrying out authentication.
This palm vein data, used for comparison, is called “palm vein data for enrollment”.

>See> For information on how to design applications to enroll palm vein data, refer to “2.6 Designing Applications to Enroll Palm Vein Data”.

2.3.2 Authentication

The following two methods are available for authentication.

- **Verification (1 to 1 authentication)**

  Authenticates a person by matching the captured palm veins against the enrolled palm vein data under the corresponding user identification information such as the ID. This method is generally called “1 to 1 authentication”.

  >See> For information on how to design applications to authenticate using the verification, refer to “2.7 Designing Applications for Verification”.

- **Identification (1 to many authentication)**

  Authenticates a person by searching through the entire enrolled palm vein data for one which is similar to the captured palm veins. This method is generally called “1 to many authentication”.

  The Authentication library returns the vein data item which is similar to the captured palm veins as the candidate.

!Caution **Authentication with identification**
Identification has higher risks of false acceptance compared to verification. Therefore, when deploying the identification for authentication, carefully consider measures against false acceptance when designing an application.
Note that the identification by un-enrolled users is not supported because the risk of false acceptance is significantly high. Do not use identification in an environment where un-enrolled users can easily attempt authentication (such as the gate outside of the facility).

>See> For information on how to design applications to authenticate using the identification, refer to “2.8 Designing Applications for Identification”.

!Caution **Palm vein data of both hands are enrolled for one user to authenticate the given user**
Repeat verification (1 to 1 authentication) twice for such cases.

>See> For information on how to authenticate using palm vein data for both hands, refer to “2.7.2 Verification Sequence”.

When the authentication method is determined, the advantages and disadvantages of each method should be considered.

The following table describes the advantages and disadvantages of each method:

○: Advantages, △: Disadvantages

Authentication Method	Operability	Authentication Time	Authentication Accuracy
Verification	△ Takes time to enter user identification information (such as ID, etc.).	○ Does not take time to obtain the authentication results.	○ High authentication accuracy.
Identification	○ Authentication can be performed merely by placing the hand. There is no need to enter user identification information.	△ The authentication time becomes longer as the number of enrolled palm vein data items increases.	△ The authentication accuracy is lower compared to verification.

>See> For information on the authentication duration, refer to the “Authentication Library Reference Guide”.

2.3.3 Authentication Accuracy

The authentication accuracy of the Sensor is generally represented by the false rejection rate (FRR) and false acceptance rate (FAR).

- **False Rejection Rate (FRR)**

  FRR represents the ratio of false rejections as a result of verifying a person with his/her own palm vein data.

- **False Acceptance Rate (FAR)**

  FAR represents the ratio of false acceptances as a result of verifying a person with another person's palm vein data.

The false rejection rate (FRR) is deemed to be the indicator of the convenience and the false acceptance rate (FAR) to be the indicator of the safety in the live operations.

The authentication accuracy varies depending on the authentication method, operating environment, and the way of placing hands. Also, it is largely influenced by the quality of enrolled palm vein data.

>See> For information on the authentication accuracy, refer to the “Authentication Accuracy Data Sheet”.

2.4 Authentication Library Type and Mode

The following type and mode can be specified to the Authentication library.

- Format type
- Guide mode

2.4.1 Format Type

You can switch the Authentication library V34 between the following three format types.

- **R-format type**

  R-format type is new from the Authentication library V34 and accelerates the identification process while maintaining high accuracy with high definition data. You can perform identification faster with higher accuracy than I33-format type using this type.

  Use this type basically from the Authentication library V34.

- **I33-format type (V33 compatible type)**

  I33-format type is from the Authentication library V33 and Palm vein data is stored as high definition data. High authentication accuracy can be achieved with high definition data.

  Note that this mode is not supported by the Authentication library for Arm.

  Use this type only in the following case.

  ・When using palm vein data that was enrolled with older versions because re-enrollment of the palm vein data is difficult.

  >See> For information on migrating from older versions, refer to “Chapter4 When You Are Using Previous Versions”.

- **I-format type (V32 compatible type)**

  Palm vein data is not stored as high definition data but in the same way as the Authentication library V32 in this type. Since high definition data is not used, the authentication accuracy and authentication duration in this type is the same as that of the Authentication library V32.

  Note that this mode is not supported by the Authentication library for Arm.

  Use this type only in the following cases.

  ・When specifying “compressed format” for “Enrollment format of palm vein data” in order to make the size of palm vein data smaller in cases such as storing the palm vein data on a smart card.

  ・When using palm vein data that was enrolled with older versions because re-enrollment of the palm vein data is difficult.

  >See> For information on the enrollment format of palm vein data, refer to “2.6.1.1 Enrollment Format of Palm Vein Data”.

  >See> For information on migrating from older versions, refer to “Chapter4 When You Are Using Previous Versions”.

Be sure to use the same format type at enrollment of palm vein data and at authentication of the user because palm vein data is not compatible between the different format types.

The following describes advantages and disadvantages of each format types.

○: Advantages, △: Disadvantages

Type	Palm vein data size	Authentication accuracy	Max number of items for identification	Identification Authentication duration
R-format type (default)	△ The size of palm vein data is large because the data is stored in high definition.	○ FRR: 1.00% (No retry) FAR: 0.000001% [Capture 2 times] The authentication accuracy for FAR is high.	○ [Enterprise Edition] Max. 200,000 items (200,000 hands for 100,000 people). (Note) [Professional Edition] Max. 5,000 items (5,000 hands for 2,500 people) can be identified.	○ Identification duration is the shortest. You can perform identification of high definition data at high speed.
I33-format type	△ The size of palm vein data is large because the data is stored in high definition.	○ FRR: 1.00% (No retry) FAR: 0.00001% [Capture 2 times] The authentication accuracy for FAR is high. The authentication accuracy is the same as that of the Authentication library V33.	○ [Enterprise Edition] Max. 10,000 items (10,000 hands for 5,000 people) can be identified. [Professional Edition] Max. 5,000 items (5,000 hands for 2,500 people) can be identified.	△ Identification duration is long because of the high definition data.
I-format type	○ The size of palm vein data is the smallest.	△ FRR: 1.00% (No retry) FAR: 0.00008% [Capture 1 time, non-compressed format] The authentication accuracy is the same as that of the Authentication library V32.	△ Max. 1,000 items (1,000 hands for 500 people) can be identified.	- * Not comparable because the Max number of items for identification is 1,000.

Note) Operations of the Sample interface module for Java and Sample application for Java are not confirmed with over 10,000 items for identification.

>See> For information on the palm vein data size, maximum number of items for identification refer to the “Authentication Library Reference Guide” or “Authentication Library for Android Reference Guide”.

>See> For authentication duration, refer to the “Authentication Library Reference Guide”.

>See> For information on the authentication accuracy, refer to the “Authentication Accuracy Data Sheet”.

>See> For information on functional differences of each format type, refer to “Appendix G Comparison of Functions in Each Format Type”.

2.4.2 Using the Palm Guide (Guide Mode)

While it is generally recommended to install the Palm guide with the Sensor, it is not always possible depending on the installation environment of the Sensor. Therefore, the Authentication library offers “Guide mode” which enables operations with or without the Palm guide.
The guide mode can be one of the following.

- **Without guide mode**

  A mode for environments where a Palm guide cannot be installed for authentication.

  However, this mode can be used in general from the Authentication library V33 onwards even when you are using the following palm guides.

  ・Folding guide (In case of PalmSecure-F Pro sensor, “Standard” is required)

  ・The guide attached to the Mouse or Mouse type sensor

  ・Your own palm guide

  >See> For information on the Palm guide included in this product, refer to the “Sensor Instruction Manual”.

  >See> For information on the “Standard”, refer to the “Standard Instruction Manual”.

  >See> For information on the Mouse, refer to the “Mouse Instruction Manual”.

  >See> For information on the mouse type Sensor, refer to “Mouse Type Sensor Instruction Manual”.

  However, be sure to install a Palm guide when enrolling palm vein data for identification. Even when enrolling palm vein data for verification, it is recommended to install a Palm guide.

  In the operation where the Palm guide is not installed, the users may have difficulty holding their hand in the correct position above the Sensor and the capture fails. Therefore, some measures such as instructing the user how to place the hand will be required when not installing the Palm guide.

- **With guide mode**

  A mode for environments where a Palm guide is used.

  As described above, Without guide mode can be used regardless of the installation of the Palm guide from the Authentication library V33 onwards; however, if you install the Palm guide for both enrollment and authentication, it is recommended to use With guide mode.

  In addition, be sure to use the Palm guide and With guide mode in the following cases.

  ・When using the U guide.

  ・When using palm vein data that was enrolled with older Authentication library versions in With guide mode because re-enrollment of the palm vein data is difficult.

>See> For information on migrating from older versions, refer to "Chapter4 When You Are Using Previous Versions".

!Caution **Guide mode for enrollment of palm vein data and authentication**
Always use the same Guide mode for enrollment and authentication of palm vein data in I-format type.

!Caution **Changing guide mode**
Do not change the Guide mode after the system implementation if identifying in I-format type.
You need to re-enroll palm vein data if changing the guide mode.

>See> For information on I-format type, refer to "2.4.1 Format Type".

Consider application cases, and advantages and disadvantages of both options before determining whether to use the Palm guide.
The following describes application cases, and advantages and disadvantages in using and not using the Palm guide.

○: Advantages, △: Disadvantages

Using or not using the Palm guide	Application case	Sensor installation environment	Operability	Authentication Accuracy
Using the Palm guide	・Where one Sensor is shared between many users Frequency of authentication operations per user is probably low and the way the users place their hands may not be stable. Therefore, an implementation with the Palm guide is more suitable. Application example) ・Attendance system ・Lending system	△ The space to install the Palm guide is required.	○ It is easier for the user to capture with the Palm guide.	○ The difference in the posture between enrollment of the palm vein data and authentication can be reduced by using the Palm guide. Therefore, the authentication accuracy is higher than the cases without the Palm guide.
	・When using identification for authentication False acceptance is likely to occur if the hand is placed incorrectly. Therefore, an implementation with the Palm guide is more suitable. >See> For information on the risk of false acceptance, refer to "2.8.3 Risk of False Acceptance".			
Not using the Palm guide	・Where one Sensor is used by only one user Frequency of authentication operations per user is probably high and the way the user place his/her hand may be stable. Therefore, an implementation without the Palm guide is more suitable. Application example) ・Login authentication	○ The space to install the Palm guide is not required.	△ Capturing may fail because the users cannot hold the hand correctly above the Sensor. Therefore some measures such as instructing the user how to place the hand will be required.	△ The postures at enrollment of the palm vein data and authentication are more likely to be different without the Palm guide. Therefore, the authentication accuracy is lower than the cases with the Palm guide.

>See> For information on whether to use the Palm guide, refer to "Appendix E Consideration on the Palm Guide".

!Caution **Having problems in capturing palm veins without the Palm guide**

There may be problems in capturing palm veins for authentication without using the Palm guide.
Operate with the Palm guide in the following situations.

- Hand is shaking and user cannot stop it.
- User cannot open the fingers.
- User cannot flat the palm horizontally.
- Other.

However, do not attach the following shade to the Palm guide.
Palm veins cannot be captured if a shade like ones illustrated below is attached since the horizontal minimum view angle cannot be secured.

<View from the side>

<View from above>

>See> For information on minimum view angle, refer to the “Hardware Drawings”.

2.5 Extended Functions of the Sensor

The following functions are collectively called extended functions.

- Continuous capture function
- Image compression function
- High-power function (PalmSecure-F Pro sensor only)

2.5.1 Continuous Capture Function

The continuous capture function captures palm veins several times continuously when a user places a hand for authentication.

This function improves operability by incorporating retry authentication in cases where the user authentication fails because the palm veins are captured while the hand is still moving.

However, capture may be performed only once even when the continuous capture function is enabled in a bright environment.

★Tip **Number of captures**
BioAPI_Capture captures the number of times specified in the operational environment setting file for the Authentication library. Whereas BioAPI_Verify and BioAPI_Identify stop capturing when authentication is successful; therefore, the number of captures can be lower than the number specified in the operational environment setting file for the Authentication library.

>See> For information on the operational environment setting file for the Windows version and Linux version of the Authentication library, refer to the “Authentication Library Reference Guide”.

>See> For information on the operational environment setting file for the Android version of the Authentication library, refer to the “Authentication Library for Android Reference Guide”.

2.5.2 Image Compression Function (I33-format type and I-format type only)

The image compression function compresses the image data captured by the Sensor before transferring it over the USB path for authentication.

This function can compress the image data to be transferred down to approximately one-eighth to one-tenth of the original data size.

However, the time required for the capturing process is approximately 200 milliseconds longer per capture if this function is used. Also, the authentication rate is slightly lower due to the image data compression.
Therefore, use the image compression function only when the following conditions are met.

・Verification authentication (1 to 1 authentication) is used.
・Enrollment format of palm vein data is non-compressed format.
・The size of image data to be transferred via the USB cable needs reducing.
・The V2 mode function is disabled.

Do not use the image compression function for identification (1 to many authentication) because the identification process will take a long time and the risk of FAR will increase. Also, note that this function is not available in R-format type.

2.5.3 High-Power Function (PalmSecure-F Pro Sensor Only)

High-power function is a newly added feature for PalmSecure-F Pro sensor to improve the tolerance to the external light when capturing a hand.

This function is available only when the following conditions are met.

- PalmSecure-F Pro sensor is used.
- The Sensor is connected to a USB 3.0 port that can supply 900 mA.

  !Caution **Transfer speed of the Sensor**
  Even when the Sensor is connected to a USB 3.0 port, the transfer speed is the same as that of USB 2.0.

- Windows version or Linux version of Authentication library is used.
- The operation mode for Authentication library is set to "Use high-power function (high-power mode)".

  >See> For information on how to set the high-power mode, refer to the "Authentication Library Reference Guide".

!Caution **When connecting the Sensor to a USB 2.0 port**
Be sure to set the operation mode for Authentication library to "Not using high-power function (normal-power mode)" when connecting the Sensor to a USB 2.0 port.
If you continue to use the Sensor on the USB 2.0 port setting high-power mode by the Authentication library, a device failure may occur on the target hardware.

!Caution **When using the Authentication library for Android**
Do not use the high-power function with Authentication library for Android.

>See> For information on the tolerance to the external light when using high-power function, refer to the "Sensor Instruction Manual for PalmSecure-F Pro".

2.6 Designing Applications to Enroll Palm Vein Data

2.6.1 Data Format for Palm Vein Data for Enrollment

Palm vein data for enrollment has the following attributes.

- Enrollment format of palm vein data
- Internal format of palm vein data
- Index type
- Encryption method of palm vein data

2.6.1.1 Enrollment Format of Palm Vein Data (I-format type only)

The following two formats are available for enrollment format of palm vein data in I-format.

- **Non-compressed format**

  Palm vein data is stored without compression in this format.

  Use this format in general

- **Compressed format (Note)**

  Palm vein data is compressed before being stored in this format.

  This format can be used only in I-format type.

  >See> For information on I-format type, refer to "2.4.1 Format Type".

  Use this format when you have a limited storage for palm vein data (for example, when storing palm vein data on a smart card).

  However, the authentication accuracy is lower in the compressed format than the non-compressed format.

  Once palm vein data is enrolled in this format, it cannot be restored to the non-compressed format.

  Note) Authentication with the identification is not available with the "compressed format". The authentication result score notification function is also unavailable.

  >See> For information on authentication result score notification function, refer to "2.6.2.4 Authentication Result Score Notification Function".

!Caution **Using the compressed format for children**

The palm status is likely to differ by each capturing operation with children (approximately 5 to 12 years old) because they may not hold their hands correctly; this may result in compression of palm vein data to fail in some cases.
Therefore, the compressed format should not be used for children who are younger than approximately 13.

!Caution **Changing the enrollment format of palm vein data**

Do not change the enrollment format of palm vein data after the system implementation if identifying in I-format type.

2.6.1.2 Internal Format of Palm Vein Data

The following three internal format types are available for palm vein data.
There is no need to specify the internal format for palm vein data because it is automatically determined to one of the following formats according to the format type in use.

- **R-format**

  This format is new from the Authentication library V34 which is used in R-format type.

- **I33-format**

  This format is from the Authentication library V33 which is used in I33-format type.

- **I-format**

  This format is from the Authentication library V12 which is used in I-format type.

★Tip **About G-format**
The support for a format called "G-format" was discontinued from the Authentication library V30.

>See> For information on each format type, refer to "2.4.1 Format Type".

2.6.1.3 Index Type

Index is the data added on the palm vein data when its enrollment format is non-compressed format and is used for the identification process.
The following two index types are available.
There is no need to specify the index type for palm vein data because one of the following is automatically applied according to the format type in use.

- **R-Index**

  This index type is new from the Authentication library V34 and used when identifying with the R-method.
  This index type is applied in R-format type.

- **F33-Index**

  This index type is from the Authentication library V33 and used when identifying with the F33-method.
  This index type is applied in I33-format type.

- **F27-Index**

  This index type is from the Authentication library V30 and used when identifying with the F27-method.
  This index type is applied in I-format type.

★Tip **About F-Index**
The support for an index type called “F-index” was discontinued from the Authentication library V30.

>See> For information on the enrollment format of palm vein data, refer to “2.6.1.1 Enrollment Format of Palm Vein Data”.

>See> For information on each format type, refer to “2.4.1 Format Type”.

>See> For information on identification with each method, refer to “2.8.2 Identification Method of Palm Vein Data”.

2.6.1.4 Encryption Method of Palm Vein Data (I-format type only)

The following two formats are available for encryption method of palm vein data.

- **AES128 method**

  This method encrypts with AES128 bits.

- **AES256 method**

  This method encrypts with AES256 bits.

There is no need to specify the encryption method of palm vein data in R-format type or I33-format type because AES256 is automatically used.

2.6.1.5 Compatibility of Palm Vein Data Using Application Keys

An “application key” (described in the “License agreement”) is required when developing an application for the Palm vein authentication system which changes the information in the palm vein data. Therefore, when using different application keys in multiple applications, the palm vein data that has been created in each application is not compatible.

When the compatibility of vein data is required between multiple applications, please develop the application using the same application key.

>See> For information on how to use an application key, refer to one of the following manuals.

- “Authentication Library Reference Guide”
- “Authentication Library for Android Reference Guide”
- “Sample Application for Microsoft .NET Framework Manual Professional Edition”
- “Sample Application for Microsoft .NET Framework Manual Enterprise Edition”
- “Sample Application for Java Manual Professional Edition”
- “Sample Application for Java Manual Enterprise Edition”
- “Sample Application for Android Manual”
- ”Sample Source for C Language Manual Professional Edition”

2.6.2 Palm Vein Data Enrollment Sequence

Consider the following sequence when designing an application to enroll palm vein data.

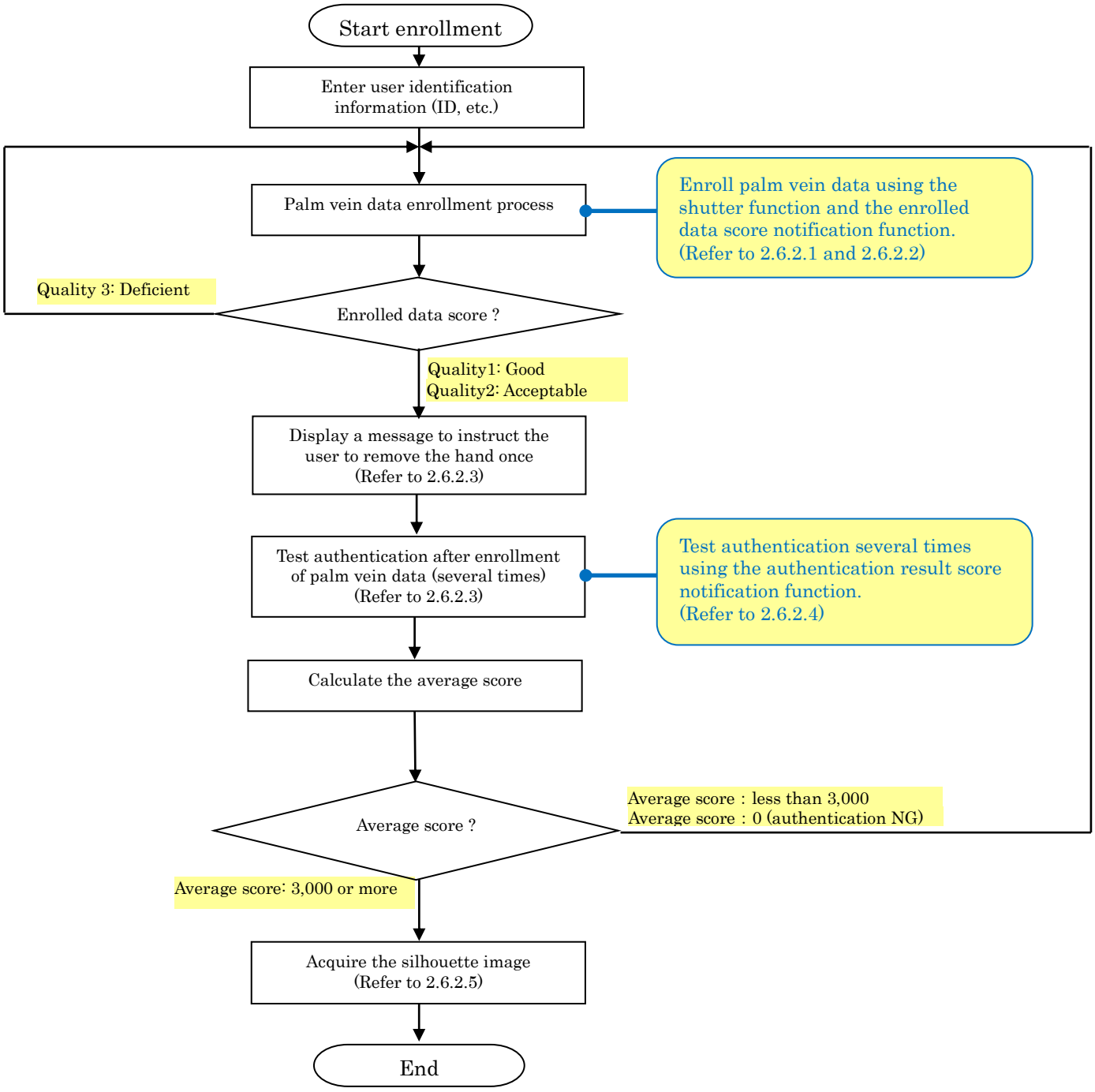
◆ When the Enrollment Format of Palm Vein Data is Non-compressed Format

[Notes on designing]

- **Design to improve quality of palm vein data to be enrolled**

  The following sequence repeats the enrollment process using the shutter function if Quality 3 (deficient) is returned from the enrolled data score notification function.

  Also the sequence instructs the user to remove the hand once, carries out test authentication several times using the authentication result score notification function, and repeats the enrollment process again if the average score of the tests is less than 3,000.


Start enrollment
Enter user identification information (ID, etc.)
Palm vein data enrollment process
Enroll palm vein data using the shutter function and the enrolled data score notification function. (Refer to 2.6.2.1 and 2.6.2.2)
Quality 3: Deficient
Enrolled data score ?
Quality1: Good
Quality2: Acceptable
Display a message to instruct the user to remove the hand once (Refer to 2.6.2.3)
Test authentication after enrollment of palm vein data (several times) (Refer to 2.6.2.3)
Test authentication several times using the authentication result score notification function. (Refer to 2.6.2.4)
Calculate the average score
Average score ?
Average score : less than 3,000
Average score : 0 (authentication NG)
Average score: 3,000 or more
Acquire the silhouette image (Refer to 2.6.2.5)
End

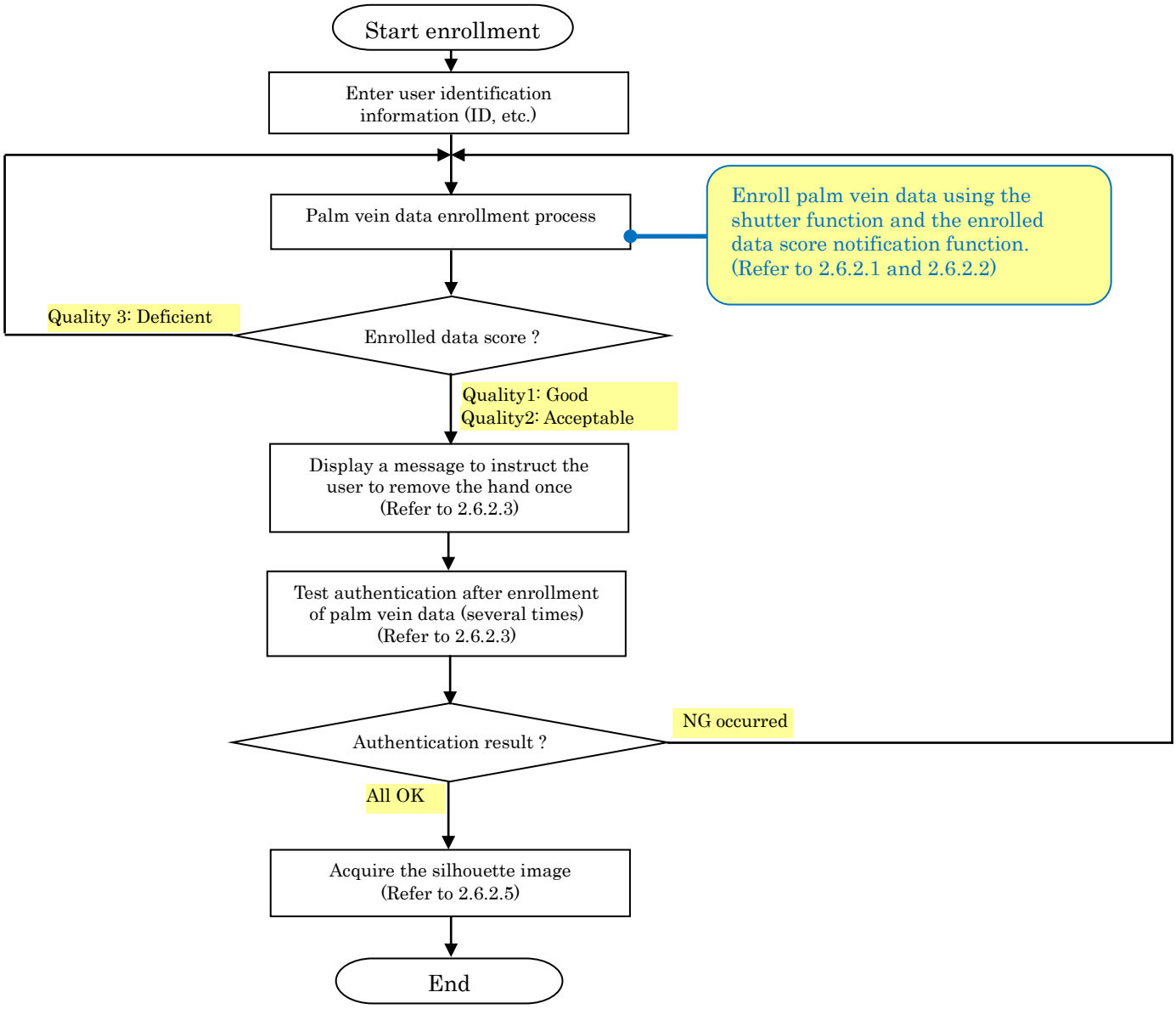
◆ When the Enrollment Format of Palm Vein Data is Compressed Format (I-format only)

[Notes on designing]

- **Design to improve quality of palm vein data to be enrolled**

  The following sequence repeats the enrollment process using the shutter function if Quality 3 (deficient) is returned from the enrolled data score notification function.

  Also the sequence instructs the user to remove the hand once, carries out test authentication several times, and repeats the enrollment process again if any test result is NG.



★Tip **Authentication result score notification function**
The authentication result score notification function is not available when the enrollment format of palm vein data is compressed format.

2.6.2.1 Shutter Function

The shutter function waits for the second capture until a user operation such as clicking the start capture button when enrolling vein data.
When using the shutter function the Authentication library will return the capture start callback message before capturing the palm veins for the second time.
This function is useful when you have an operator who can assist the user to place the hand.
This function allows you to confirm that the hand is placed properly before capturing. This enables enrollment of better-quality vein data.

2.6.2.2 Enrolled Data Score Notification Function

The enrolled data score notification function returns whether the quality of palm vein data for enrollment is “Quality 1: Good”, “Quality 2: Acceptable”, or “Quality 3: Deficient”. You can improve the quality of palm vein data for enrollment by designing the application to re-enroll the palm vein data if “Quality 3: Deficient” is returned.
However, for some users “Quality 3: Deficient” may be returned again for re-enrollment even if the hand was correctly placed. Therefore, it is recommended to design the application to be able to accept palm vein data in the case where “Quality 3: Deficient” is persistently returned to re-enrollment operations.

!Caution **Enrolled Data Score Notification Function**
The enrolled data score notification function does not always guarantee the enrollment environment of palm vein data, the way of placing hands, or the authentication accuracy (to guarantee that authentication NG does not occur).
Therefore, design the application to carry out a test authentication after enrolling palm vein data.

>See> For information on test authentication, refer to “2.6.2.3 Test Authentication after Enrolling of Palm Vein Data and the Hand Detection Function”.

2.6.2.3 Test Authentication after Enrolling of Palm Vein Data and the Hand Detection Function

◆ Test Authentication

The test authentication is a verification (1 to 1 authentication) process to confirm validity of the palm vein data to be enrolled.
It is recommended to carry out test authentication several times in the same environment as the operational environment (Note).

Note) For example, if the Palm guide is used for enrolling palm vein data but is not used in authentication in actual operation, it is recommended to carry out test authentication without the Palm guide.

◆ Hand Detection Function

The hand detection function detects whether the hand is placed above the Sensor before capturing palm veins for test authentication.
When the hand detection function is enabled, a callback message to instruct the user to remove the hand is returned from the Authentication library if the hand is already placed when starting to capture palm veins. Therefore, implementing the process to display a message to remove the hand is no longer required.

2.6.2.4 Authentication Result Score Notification Function

The authentication result score notification function returns the degree of similarity to the enrolled palm vein data in the range from 0 to 10,000 in 1,000 units. 0 indicates that the authentication result has been NG, and 1,000 to 10,000 indicates that the authentication result has been OK. The larger the value, the higher the similarity.

>See> For information on the settings necessary to use the authentication result score notification function, refer to the “Authentication Library Reference Guide or “Authentication Library for Android Reference Guide”.

Stable authentication can be expected in actual operation if the average score is 3,000 or larger over several attempts of test authentication; therefore, you can reduce the frequency of authentication resulting in NG.

However, if the average score is less than 3,000 or 0 (authentication NG), authentication will be unstable in actual operation and authentication NG may occur. Design the application to re-enroll the palm vein data in such a case.
For users whose average score is still less than 3,000 after the re-enrollments, select the palm vein data item which seems to be the most reliable for actual operation.

2.6.2.5 Acquire the Silhouette Image

It is recommended to acquire the silhouette image when capturing palm veins for enrollment. This allows you to confirm how the hand was placed when it was captured.

!Caution **Impact on processing speed by anti-virus software**
Some anti-virus software runs a check when storing silhouette images into files. This may slow down the application.

!Caution **Managing personal information**
The acquired silhouette image can be personal information.
Therefore, you should strictly control files that contain silhouette images.

2.6.3 Other Considerations

2.6.3.1 Enrollment of Palm Vein Data for Both Hands

It is recommended to design applications to enroll palm vein data for both hands. It will allow the user to use another hand for authentication even when the user injures one hand.

>See> For information on how to authenticate using palm vein data for both hands, refer to “2.7.2 Verification Sequence”.

2.6.3.2 Periodical Re-enrollment of Palm Vein Data

It is recommended to design applications to prompt users for periodical re-enrollment of palm vein data.
Re-enrollment of palm vein data leads to improvement of authentication accuracy.

2.6.3.3 Attach the Palm Guide

Be sure to attach the Palm guide when enrolling palm vein data for identification. The Palm guide helps the user to place the palm on the Sensor in the same manner each time. This enables enrollment of better-quality palm vein data and improves the authentication accuracy.
Note that even when enrolling palm vein data for verification, it is recommended to attach a Palm guide.

2.7 Designing Applications for Verification

2.7.1 Data Format for Palm Vein Data for Authentication

Palm vein data for authentication has the following attributes.

- Internal format of palm vein data
- Encryption method of palm vein data

>See> For information on internal format of palm vein data, refer to “2.6.1.2 Internal Format of Palm Vein Data”.

>See> For information on encryption method of palm vein data, refer to “2.6.1.4 Encryption Method of Palm Vein Data”.

2.7.2 Verification Sequence

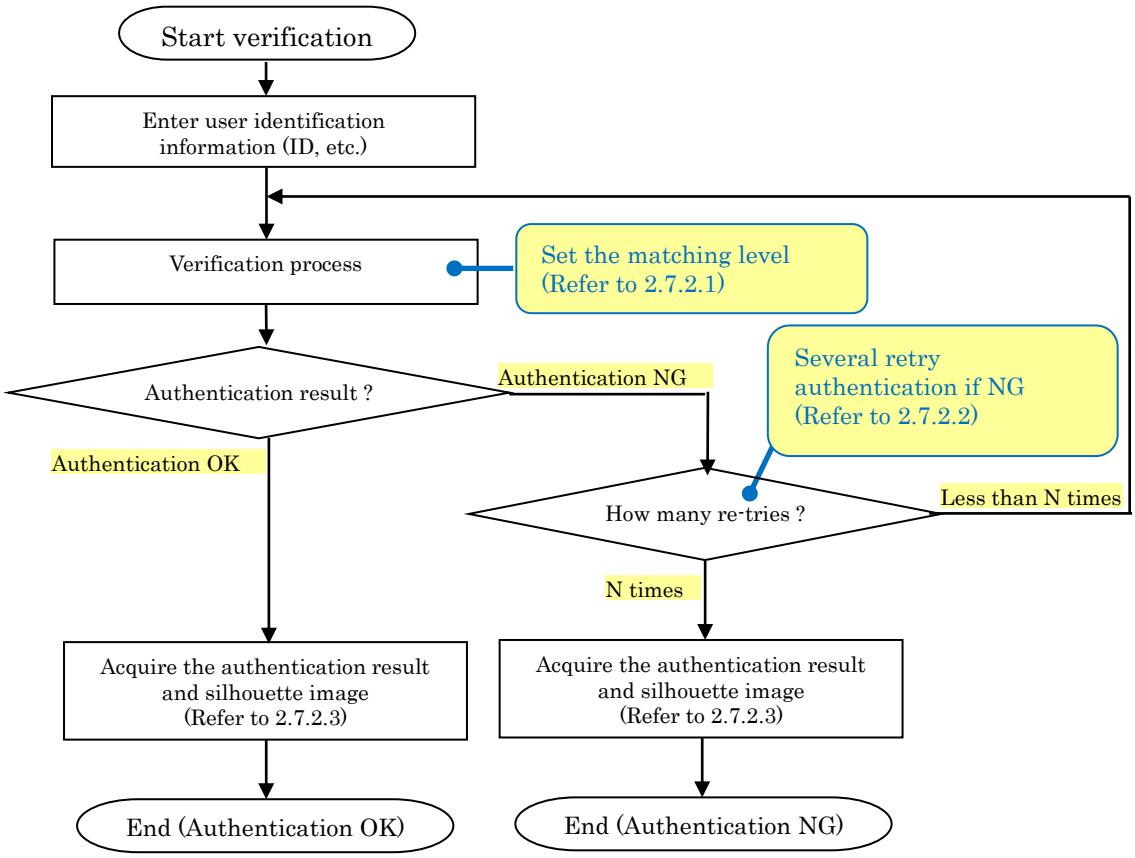
Consider the following sequence when designing an application to authenticate a person using the verification.

◆ When Palm Vein Data for One Hand per User is Enrolled

[Notes on designing]

- **Design to retry authentication for users who are unfamiliar with the hand placing operation**

  The following sequence repeats the authentication if the authentication results in NG.



!Caution Authentication result score notification function in I33-format type and I-format type

The time required for verification is slightly longer if authentication result score notification function is used in verification processes. Therefore, it is recommended not to use the authentication result score notification function in verification processes except for the test authentication.

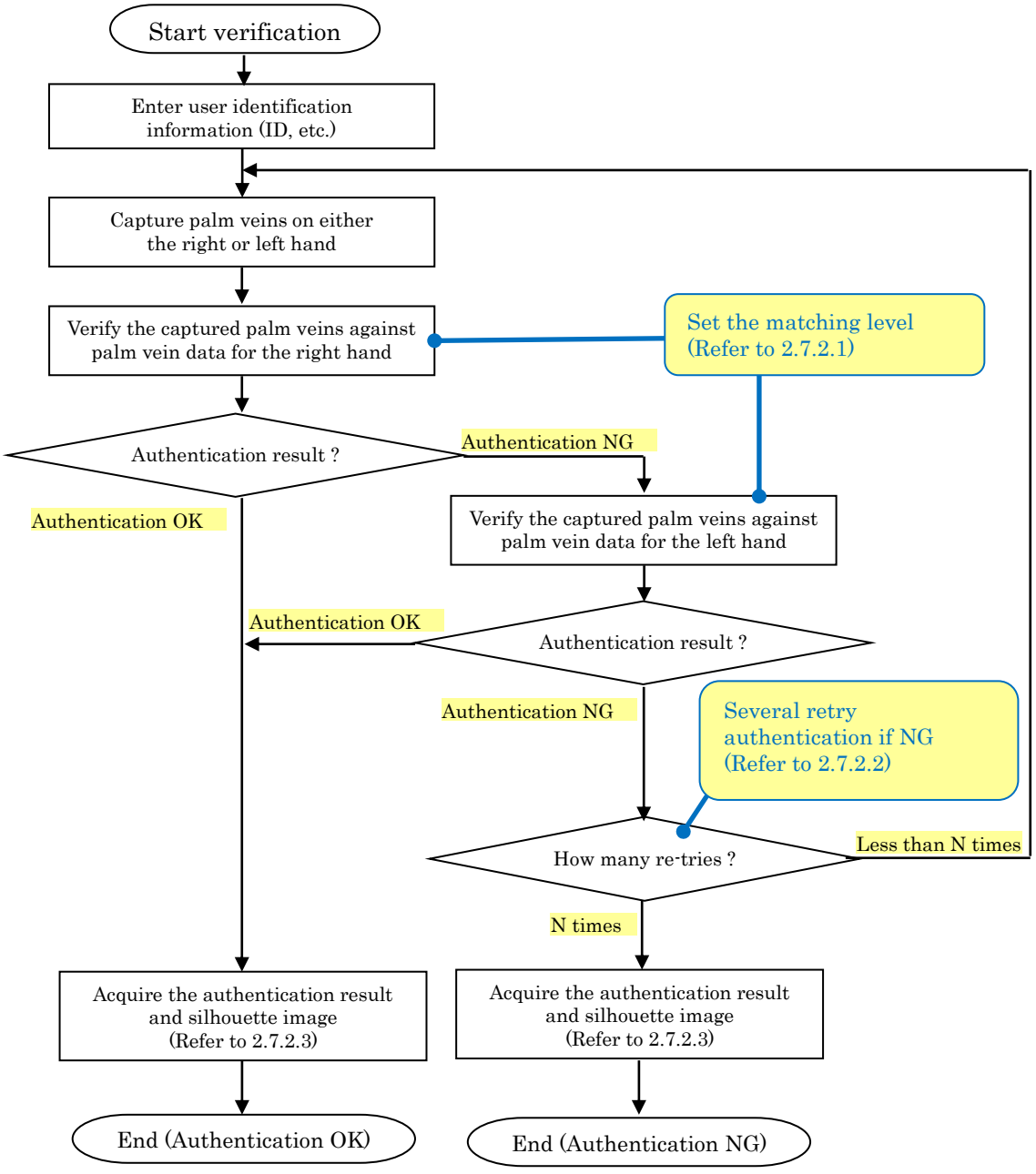
◆ When Palm Vein Data for Both Hands per User is Enrolled

[Notes on designing]

- **Build in a mechanism to be able to authenticate a person with either hand in case the user injures one hand**

  The following sequence captures palm veins on either right or left hand first. Then, it verifies the captured palm veins against the enrolled palm vein data for the right hand. If the authentication is NG, the sequence verifies it against the enrolled palm vein data for the left hand.

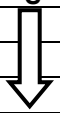
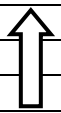
  Also, the sequence repeats retry authentication several times if the authentication results in NG again.



!Caution **Authentication result score notification function in I33-format type and I-format type**
The time required for verification is slightly longer if authentication result score notification function is used in verification processes. Therefore, it is recommended not to use the authentication result score notification function in verification processes except for the test authentication.

2.7.2.1 Matching Level

There are five matching levels as shown in the following table.
Changing this matching level setting can increase or decrease FRR (False Rejection Rate) and FAR (False Acceptance Rate).
Use the "Normal" matching level for day-to-day operations.

Matching Levels	FRR (False Rejection Rate)	FAR (False Acceptance Rate)
Highest	**High**	**Low**
High		
Normal		
Low		
Lowest	**Low**	**High**

>See> For information on the FRR (False Rejection Rate) and FAR (False Acceptance Rate), refer to "2.3.3 Authentication Accuracy".

2.7.2.2 Retry Authentication

The authentication result heavily depends on how the hands are placed at the authentication. Authentication NG may occur if the user is not familiar with the hand-placing operation.
Design the application to retry authentication several times without returning to the user identification information (ID, etc.) entry process if the authentication result is NG. The retry authentication improves the usability for unfamiliar users.

2.7.2.3 Acquire the Authentication Results and Silhouette Image

It is recommended to acquire the authentication results in order to manage the authentication status.
Information such as the authentication date, time, user identification information (ID, etc.) and authentication result can be acquired.
Managing the authentication status enables you to take measures such as instructing how to place the hand correctly to users with a poor authentication success rate.

Also, it is recommended to acquire the silhouette image when capturing palm veins for authentication. This allows you to confirm how the hand was placed when it was captured.

!Caution **Impact on processing speed by anti-virus software**
Some anti-virus software runs a check when storing authentication results and silhouette images into files. This may slow down the application.

!Caution **Managing personal information**
The acquired authentication results and silhouette image can be personal information.
Therefore, you should strictly control files that contain authentication results or silhouette images.

2.8 Designing Applications for Identification

2.8.1 Data Format for Palm Vein Data for Authentication

Palm vein data for authentication has the following attributes.

- Internal format of palm vein data
- Encryption method of palm vein data

>See> For information on internal format of palm vein data, refer to “2.6.1.2 Internal Format of Palm Vein Data”.

>See> For information on encryption method of palm vein data, refer to “2.6.1.4 Encryption Method of Palm Vein Data”.

2.8.2 Identification Method of Palm Vein Data

The following three identification methods are available for identifying palm vein data.

One of the following palm vein data identification methods is automatically used according to the index type applied to the palm vein data.

- **R-method**

  R-method is capable of identifying with palm vein data containing up to 200,000 items (200,000 hands for 100,000 people) (Note) at high speed, and is available from the Authentication library V34.

  This identification method applies when the index type is R-Index.

!Caution	**Palm vein data for identification using the R-method** Palm vein data must be enrolled in R-format type in order to perform identification in R-method. In case of Professional Edition, a palm vein data group containing up to 5,000 items (5,000 hands for 2,500 people) is available.
>See>	For information on internal format of palm vein data, and index type, refer to "2.6.1 Data Format for Palm Vein Data for Enrollment".

- **F33-method**

  F33-method is capable of identifying with palm vein data containing up to 10,000 items (10,000 hands for 5,000 people) (Note), and is available from the Authentication library V33.

  This identification method applies when the index type is F33-Index.

!Caution	**Palm vein data for identification using the F33-method** Palm vein data must be enrolled in I33-format type in order to perform identification in F33-method. In case of Professional Edition, palm vein data containing up to 5,000 items (5,000 hands for 2,500 people) is available.
>See>	For information on internal format of palm vein data, and index type, refer to "2.6.1 Data Format for Palm Vein Data for Enrollment".

- **F27-method**

  F27-method is capable of identifying with palm vein data containing up to 1,000 items (1,000 hands for 500 people) (Note), and is available from the Authentication library V30.

  This identification method applies when the index type is F27-Index.

  !Caution **Palm vein data for identification using the F27-method**
  Palm vein data must satisfy the following conditions for identification in F27-method.
  ・Enrollment format of palm vein data is non-compressed format
  ・Internal format of palm vein data is I-format
  ・Index type is F27-Index

  >See> For information on enrollment format of palm vein data, internal format of palm vein data, and index type, refer to “2.6.1 Data Format for Palm Vein Data for Enrollment”.

Note) Hereinafter called “max identification items”.

The more the number of items in palm vein data subject to identification, the higher the risk of false acceptance in identification. Therefore, keep the number of palm vein data items subject to identification within the max identification items.

Also, the more the number of items in palm vein data subject to identification, the longer the authentication process. Therefore, it is recommended to use a higher number of CPU cores when the number of items in palm vein data subject to identification exceeds 1,000 (1,000 hands for 500 people).

>See> For information on the case where the number of items in palm vein data subject to identification is high, refer to “2.8.3.1 Risk of False Acceptance Arising from the Number of Items in Palm Vein Data Subject to Identification, and Measures”.

★Tip **About F-method and S-method**
The support for identification methods called “F-method” and “S-method” was discontinued from the Authentication library V30.

2.8.3 Risk of False Acceptance

Identification has higher risks of false acceptance compared to verification. Therefore, when deploying the identification for authentication, carefully consider measures against false acceptance when designing an application.
The following describes the cases where the risk of false acceptance becomes high.

2.8.3.1 Risk of False Acceptance Arising from the Number of Items in Palm Vein Data Subject to Identification, and Measures

◆ Risk of False Acceptance

The false acceptance rate (FAR) in identification heavily depends on the number of items in palm vein data subject to identification. The more the number of items in palm vein data subject to identification, the higher the risk of false acceptance in general.

◆ Measures against False Acceptance

The following considerations are necessary in designing and operating applications in order to prevent unnecessary increase of the number of items in palm vein data subject to identification.

- Consider a mechanism like the following to keep the number of palm vein data items subject to identification within the limit in the environment where the number of items may exceed max identification items.

  ・Narrow down the palm vein data subject to identification by adding a second factor information such as date of birth, phone number, or department code.

  Note that the Authentication library returns an error when the number of items exceeds the max identification items for an additional 200 items.

  >See> For information on the max identification items, refer to “2.8.2 Identification Method of Palm Vein Data”.

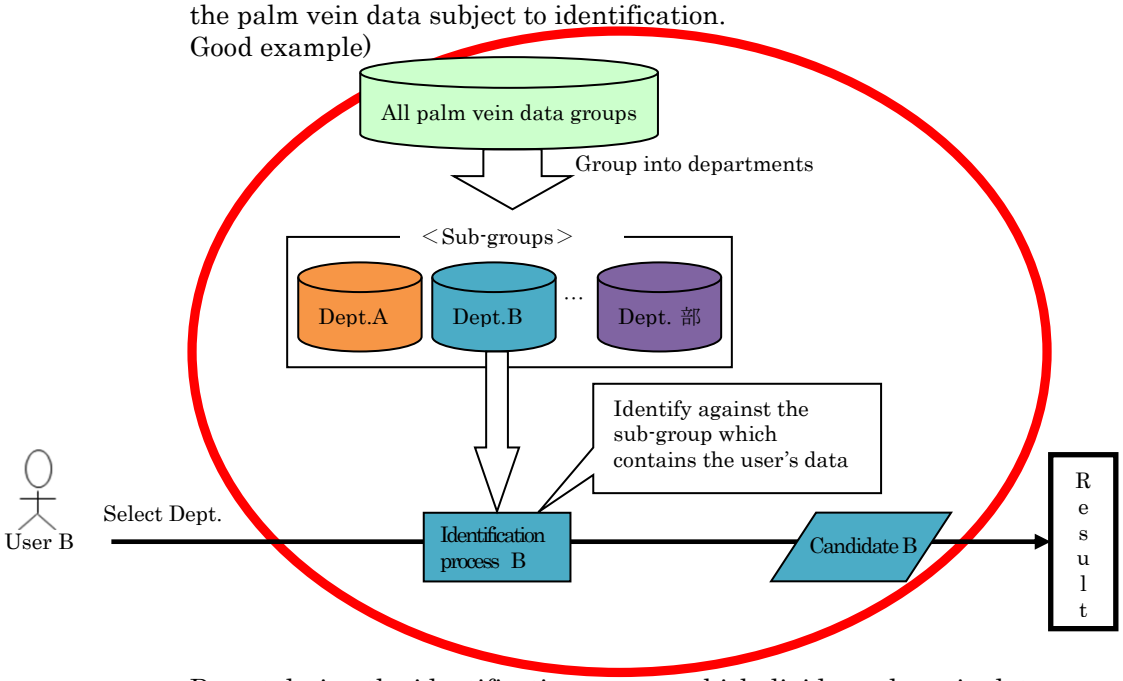
  >See> For information on how to reduce the palm vein data subject to identification, refer to “Caution Considerations for reducing palm vein data subject to identification” on the next page.

- Immediately delete unnecessary palm vein data as part of data management.

!Caution Considerations for reducing palm vein data subject to identification

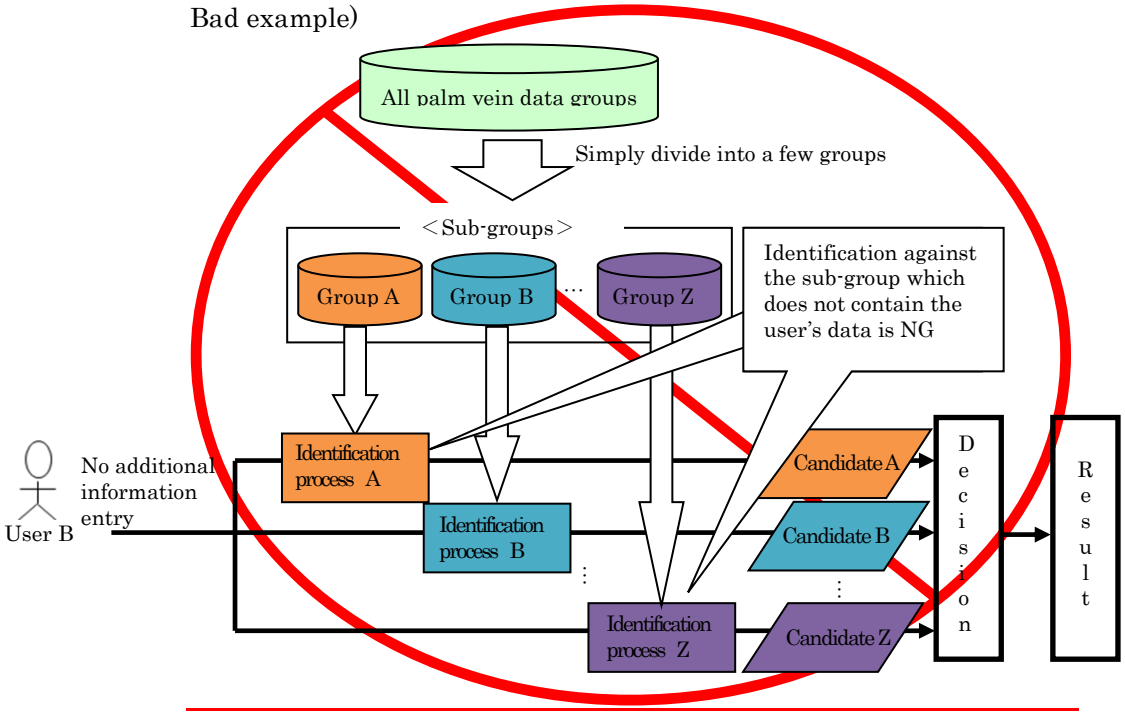
Design the application to carry out the identification process against the sub-group which contains the user's palm vein data when reducing the palm vein data subject to identification.

Good example)



Do not design the identification process which divides palm vein data subject to identification into groups and identifies against each group. The risk of false acceptance is very high when identifying against a group which does not contain the user's palm vein data.

Bad example)



>See> For information on identification against a group which does not contain the user's palm vein data, refer to "2.8.3.3 Identification by Un-enrolled Users".

2.8.3.2 Risk of False Acceptance Arising from Increased False Rejection, and Measures

◆ Risk of False Acceptance

Identification has a characteristic where the false acceptance rate (FAR) becomes generally high when the false rejection rate (FRR) is high as described below.

- False acceptance is likely to occur when the user's authentication fails (false rejection) while there is another item of palm vein data which may cause false acceptance; the latter item becomes the first candidate.

The following cause a higher false rejection rate (FRR).

- **Incorrect positioning of the hand at enrollment**
  Placing the hand incorrectly at enrollment of palm vein data, for example, placing the palm on the Wrist guide, may cause false rejection.

- **Use for children**
  False rejection may occur since children often cannot place the hand in the same manner.

- **Dirt on the palm or the sensor surface**
  False rejection and false acceptance may occur when the palm is extremely dirty or the sensor surface is dirty.

- **Use of your own palm guide which does not comply with the designing conditions in the "Hardware Drawings"**
  Some palm guides designed by users may cover part of the palm. If part of the palm is covered, the amount of captured palm veins information is reduced. Therefore, the ability to distinguish the user from others is compromised and this may cause false rejection or false acceptance.

- **Mixture of palm vein data enrolled by the current and previous versions of the Authentication library**
  The algorithm to capture and acquire palm veins may be improved when the Authentication library is updated. In such a case, a certain difference will occur between palm vein data enrolled by previous versions of Authentication library and ones enrolled by the latest version of Authentication library. This may cause false rejection to a small minority of users.

- **Using a different type of Sensor from the one used for Enrollment**

  There is a certain difference between palm vein data enrolled using PalmSecure Sensor V2 and the data enrolled using PalmSecure-F Pro sensor. This may cause false rejection to a small minority of users.

◆ Measures against False Acceptance

The following considerations are necessary in designing and operating applications in order to eliminate the cause which increases the false rejection rate (FRR).

- Place the hand correctly when enrolling palm vein data.

  (For example, instruct how to place the hand correctly to prevent the user from placing the palm on the Wrist guide.)

  >See> For information on correct hand positioning, refer to the "Sensor Instruction Manual".

- Use the identification only for approximately 13 years old or older if authenticating children.
- Wash hands if the palms are dirty.

  Wipe off the dirt if the Sensor surface is dirty.
- If designing your own palm guide, make sure that the palm guide complies with the designing conditions in the "Hardware Drawings".
- Re-enroll palm vein data where possible after an Authentication library update.
- Re-enroll palm vein data where possible when changing the Sensor type.

2.8.3.3 Identification by Un-enrolled Users

The operations are not guaranteed if un-enrolled users attempt identification. It is because the false acceptance is more likely to occur with un-enrolled users and the risk is much higher than with enrolled users. Therefore, take necessary considerations in designing and operating applications in order to prevent un-enrolled users from authenticating.

The following shows the comparison of the identification by enrolled users and un-enrolled users.

Enrolled users	Un-enrolled users
False acceptance is less likely even if there are items in palm vein data which may cause false acceptance because the user's own palm vein data generally has higher similarity to be the candidate.	False acceptance is more likely because any item in palm vein data which may cause false acceptance becomes the first candidate.

★Tip **Approximate false acceptance rate of un-enrolled users in identification**

The following is the approximation of the false acceptance rate (FAR) when un-enrolled users attempt identification.

FAR in identification by un-enrolled users
≒ FAR for verification × Number of items in palm vein data subject to identification

For example, if the FAR for verification (1 to 1 authentication) is 0.000001%, the approximate FAR in identification (1 to 200,000 authentication) by un-enrolled users is 0.000001% × 200,000 = 0.2%, showing a significantly high FAR.

An environment where un-enrolled users can easily attempt authentication is called an "open environment".

Example) An environment such as the physical access control device which uses identification is installed at the gate outside of the facility.

!Caution **Do not install a palm vein authentication system in an open environment**

For example, install the physical access control device within the facility after passing the gate rather than installing it at the gate outside the facility.

!Caution **Do not carry out an identification process (1 to many authentication) in order to determine whether the palm vein data for the user is enrolled or not**

For example, add user identification information (ID, etc.) to palm vein data to determine whether the user is already enrolled or not by an application.

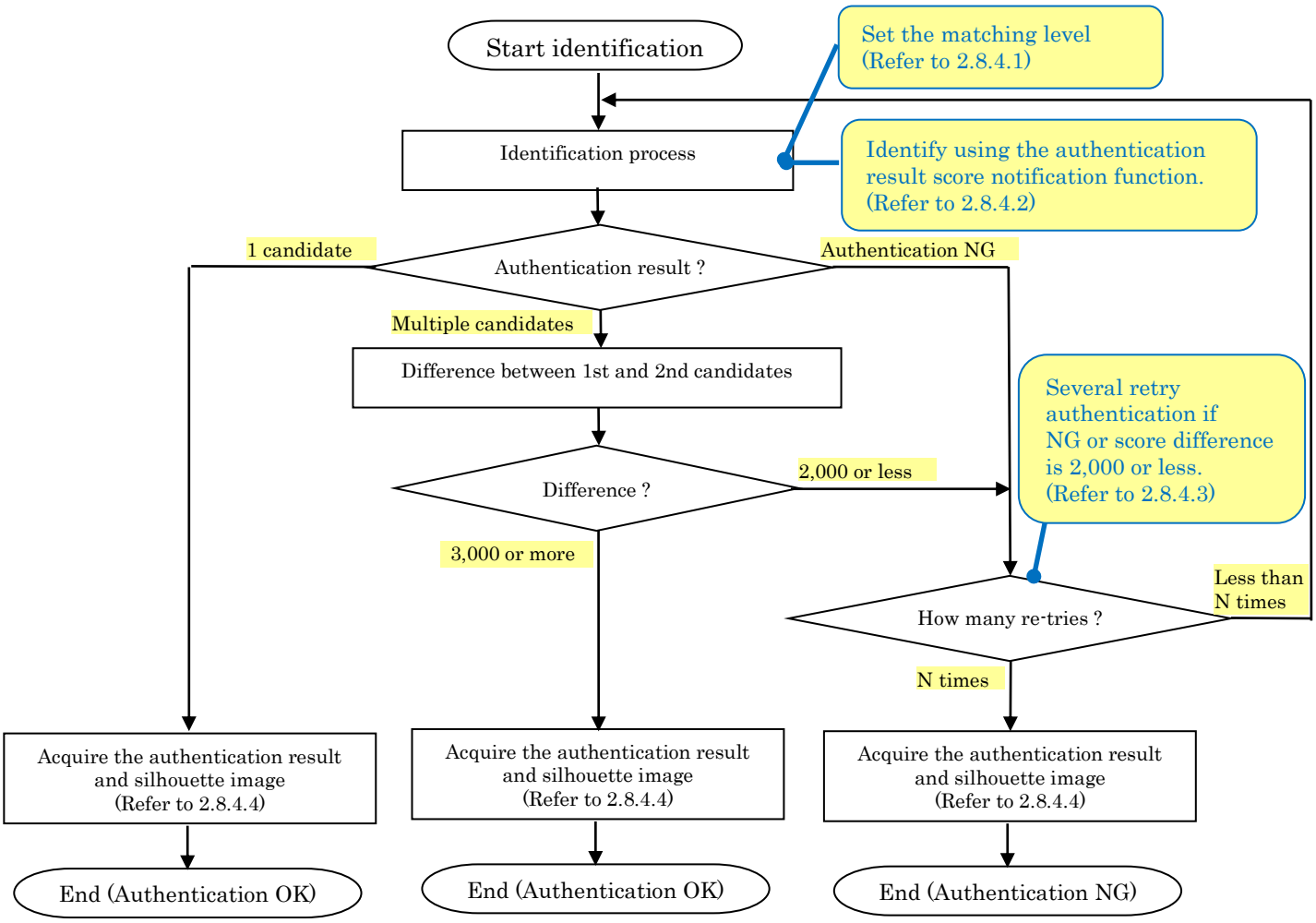
2.8.4 Identification Sequence

Consider the following sequence when designing an application to authenticate a person using the identification.

[Notes on designing]

- **Design to reduce the risk of false acceptance**

  The following sequence uses the authentication result score notification function and authenticates the user if the difference between the returned score value of the first candidate and that of the second is 3,000 or more.



★Tip **When multiple candidates are returned**

If multiple candidates are returned as a result of identification, apply the above method or use another means (password authentication, etc.) on those returned candidates to determine the authenticity.

2.8.4.1 Matching Level

>See> Refer to “2.7.2.1 Matching Level”.

!Caution **Matching level for identification in R-format type and I33-format type**
The matching level for identification in R-format type and I33-format type is “Normal”, “Low”, or “Lowest”. Note that “Normal” is applied if “High” or “Highest” is specified.

2.8.4.2 Authentication Result Score Notification Function

The authentication result score notification function returns the degree of similarity to the enrolled palm vein data in the range from 0 to 10,000 in 1,000 units. 0 indicates that the authentication result has been NG, and 1,000 to 10,000 indicates that the authentication result has been OK. The larger the value, the higher the similarity.

If multiple candidates are returned as a result of identification, first calculate the difference in the score values between the first and second candidates. Based on this difference, determine as follows.

- The difference is more than a certain value
  Determine that is the legitimate user and authentication OK.
- The difference is less than a certain value
  Retry authentication since it might be false acceptance.

This can reduce the risk of false acceptance.

2.8.4.3 Retry Authentication

>See> Refer to “2.7.2.2 Retry Authentication”.

2.8.4.4 Acquire the Authentication Results and Silhouette Image

>See> Refer to “2.7.2.3 Acquire the Authentication Results and Silhouette Image”.

2.8.5 Speeding Up the Identification Process

◆ Windows Power Options

Set “High performance” for Power Options in Windows if you are using Windows. This may reduce the time required for identification processes.

◆ Multiple Processing for Identification

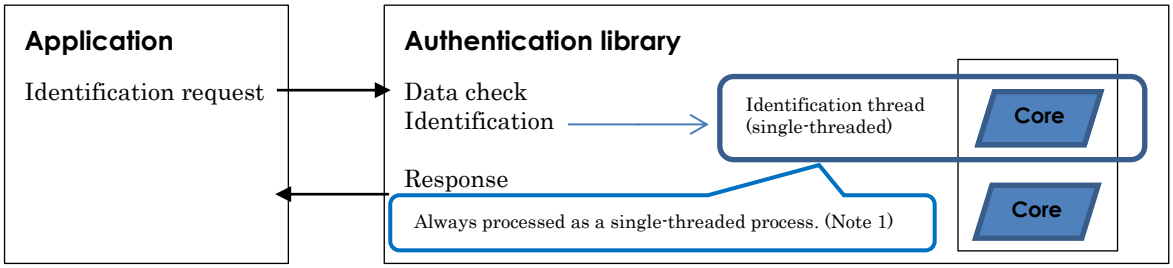
Multiple processing for identification is available if your CPU is a multi-core processor.
You can specify up to 128 threads for multi-processing, and you can reduce the time required for the identification process by increasing the number of threads.

However, the number of threads cannot exceed the number of CPU cores.

You can also use multi-threaded processes of Enterprise Edition and multiple processing for identification at the same time.
In this case, “the number of threads in multi-threaded processes × the number of threads for identification processes” cannot exceed the number of CPU cores.

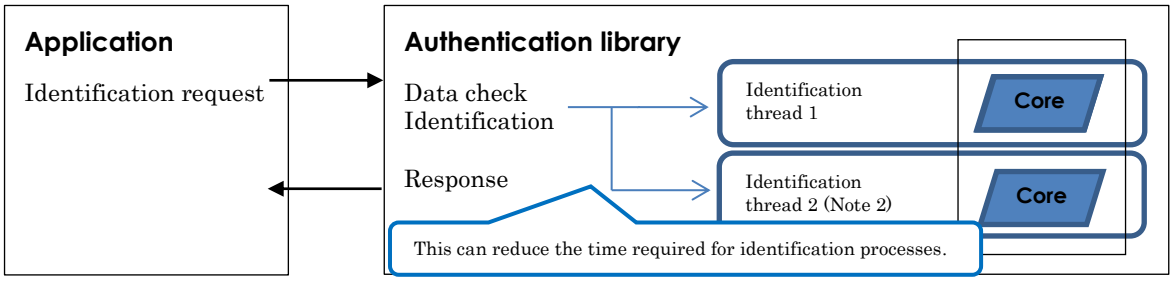
The following describes single-threaded and multi-threaded identification processes.

■Single-threaded identification process (number of identification threads = 1)



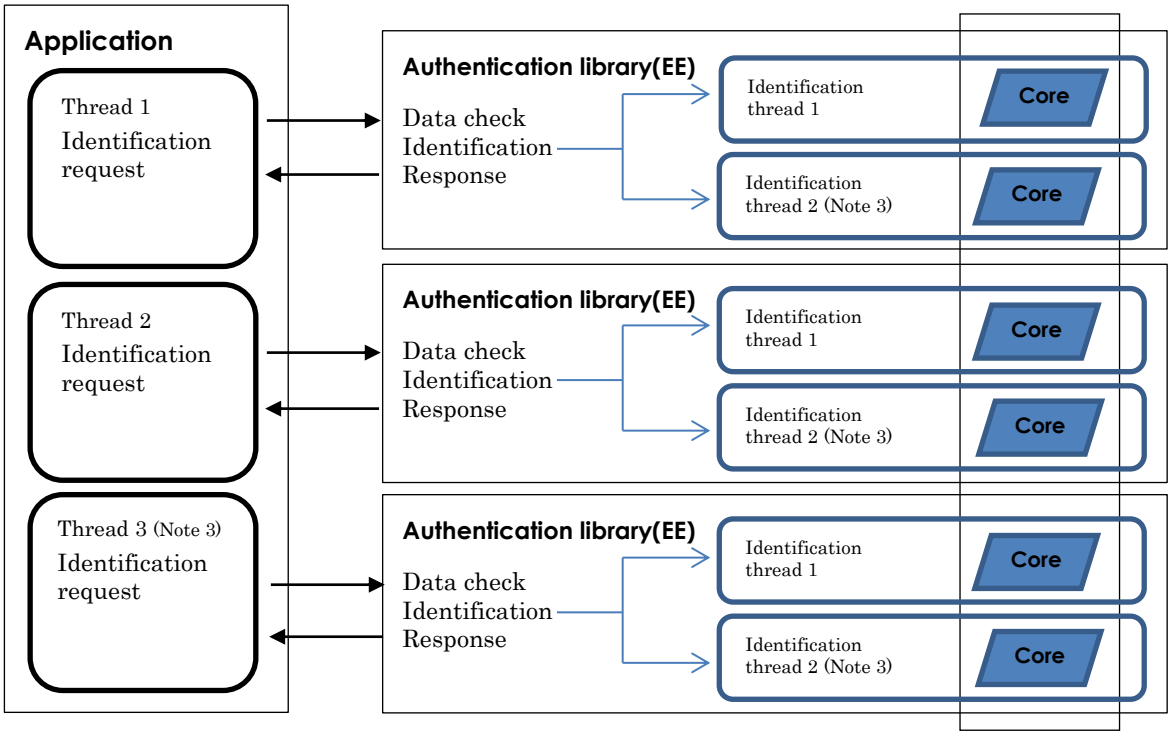
Note 1) Identification processes with previous versions of Authentication libraries are also always single-threaded.

■Identification using multiple processing (number of identification threads = 2)



Note 2) The number of threads cannot exceed the number of CPU cores.

■Identification using multiple processing combined with multiple threads of Enterprise Edition (numbers of threads = 3 and identification threads = 2)



EE: Enterprise Edition

Note 3) Multiplying “the number of threads in multiple threads” by “the number of identification threads”, ensure the value is not exceed the number of CPU cores.

2.8.6 Palm Vein Data Group Thread Sharing Function

This function enables all threads to share the pre-loaded palm vein data group for identification by executing the pre-loading processing of the vein data group that is normally required for each thread only from a specific thread.
This function is enabled by editing the setting for the operational environment setting file of the Authentication library.

>See> For information on palm vein data group pre-loading and operational environment setting file, refer to the “Authentication Library Reference Guide”.

This function is available only if the following conditions are met.

- Performing identification processing by the Authentication library Enterprise Edition.
- Using R-format vein data.

Note that the Sample interface and Sample application do not support this function.

2.8.7 Other Consideration

◆ Duplicate Enrollment of the Same User

Ensure that duplicate items of palm vein data for the same person are not enrolled under different IDs. Determining the user may become impossible if the same user enrolls multiple items of palm vein data under different IDs as described in “2.8.4 Identification Sequence”.

◆ Verifying the Identification Process of the Developed Application

Do not make copies of palm vein data or enroll palm vein data of the same person multiple times to increase the number of enrolled items in palm vein data. Processing speed and authentication capability cannot be verified correctly if you make copies of palm vein data or enroll multiple items from the same person.

Chapter3 Considerations for Developing the Palm Vein Authentication System

3.1 Considerations for Designing an Application

3.2 Considerations for Developing an Application

3.3 Security Countermeasures When Managing Vein Data

3.4 Considerations for Operating the Palm Vein Authentication System

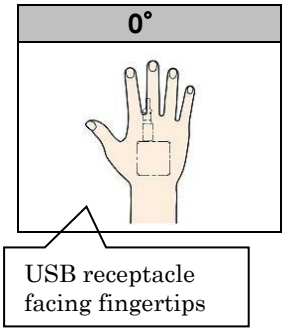
3.5 Other Considerations

3.1 Considerations for Designing an Application

3.1.1 Changing the Angle of the Hand against the Sensor

◆ When Using R-format type or I33-format Type

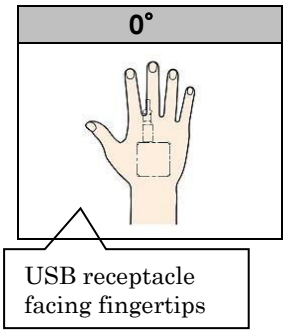
The angle of the hand against the Sensor (capturing angle) cannot be changed in R-format type and I33-format type. Always use 0° for the capturing angle.



>See> For information on R-format type and I33-format type, refer to “2.4.1 Format Type”.

◆ When Using Without Guide Mode in I-format Type

The angle of the hand against the Sensor (capturing angle) cannot be changed in I-format type with Without guide mode. Always use 0° for the capturing angle.



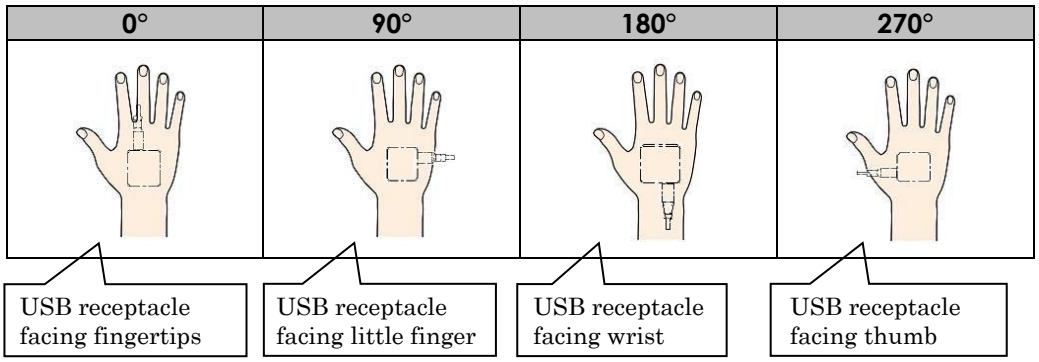
>See> For information on I-format type, refer to “2.4.1 Format Type”.

>See> For information on Without guide mode, refer to “2.4.2 Using the Palm Guide (Guide Mode)”.

◆ When Using With Guide Mode in I-format Type

The angle of the hand against the Sensor (capturing angle) can be changed in I-format type with guide mode.

The capturing angle can be one of the following.



★Tip **Capturing angle for enrollment of palm vein data and authentication**

It is recommended that the capturing angle for enrolling vein data be 0° and the same capturing angle should be used for authentication with the enrollment. If the capturing angle is different, it may result in lower authentication accuracy compared to the case in which the capturing angle is the same.

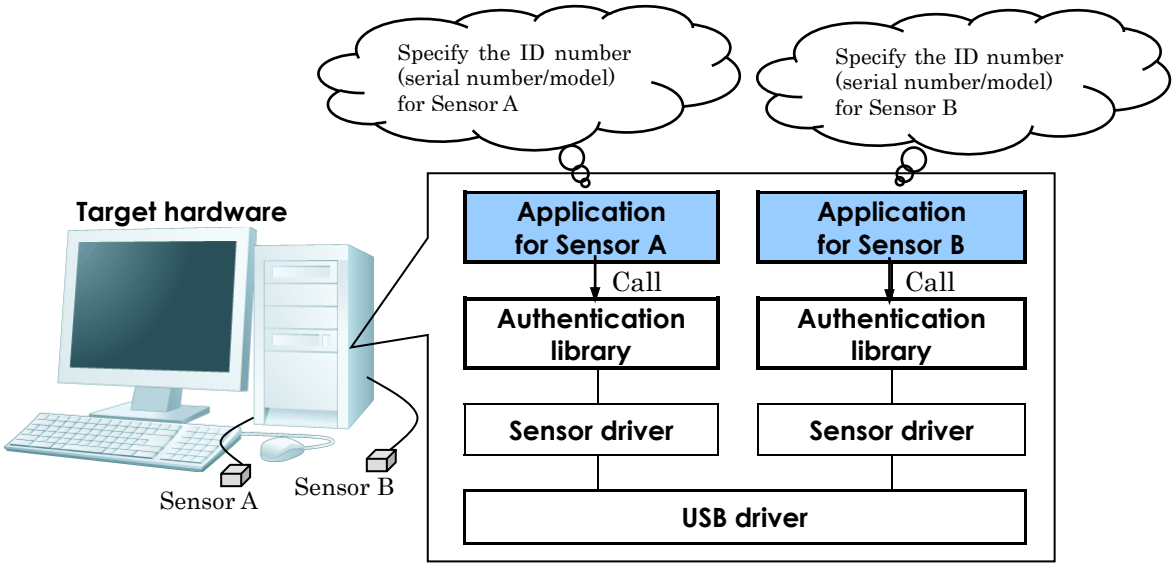
>See> For information on I-format type, refer to “2.4.1 Format Type”.

>See> For information on With guide mode, refer to “2.4.2 Using the Palm Guide (Guide Mode)”.

3.1.2 Connecting Multiple Sensors

When connecting multiple Sensors to a target hardware device to operate the palm vein authentication system, consider the following point in developing application. Note that the Authentication library for Android does not support multiple connection of the Sensors.

Only one Sensor can be connected per application (process).
Therefore, as shown in the following figure, create the same number of applications (multi-process) as the number of Sensors and call the Authentication library specifying the Sensor ID number (serial number/model) in each application.



★Tip **Sensor ID number (serial number/model)**
The ID number of the Sensor (serial number/model) can be confirmed using the Sensor maintenance tool.

>See> For information on the Sensor maintenance tool, refer to the "Sensor Maintenance Tool Operation Guide".

When connecting multiple Sensors, also keep the following points in mind.

◆ Number of connecting Sensors

Do not connect more than two Sensors. Operations are not guaranteed if three or more Sensors are connected.
While logically up to eight Sensors can be connected in a Windows environment, there is no guarantee on processing performance and operations.
The number of Sensors to be connected should be determined at the user's own risk on examination of the operational environment when developing palm vein authentication systems.

◆ Sensor Connection

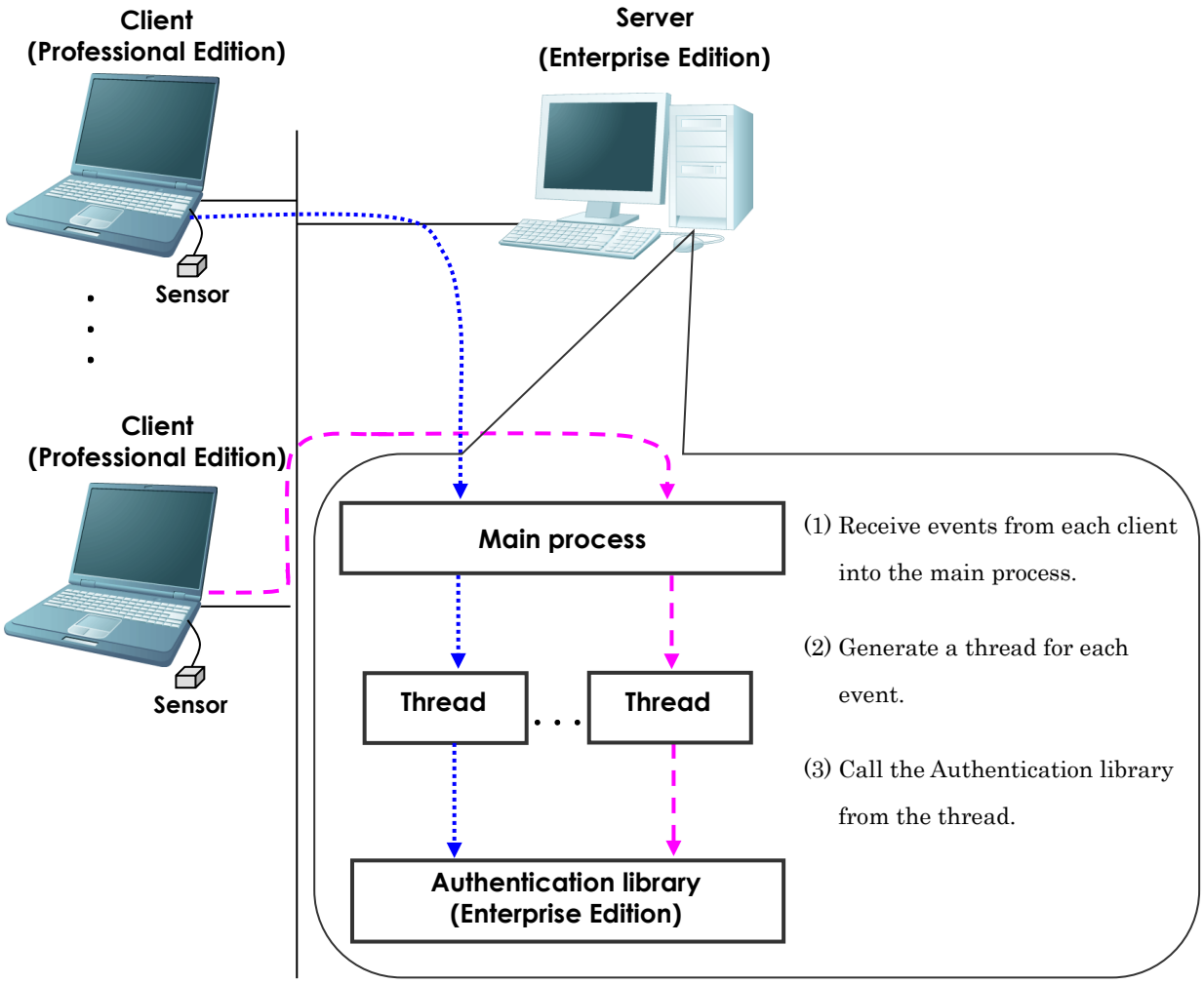
Generally, connect Sensors to the root hub when connecting multiple Sensors.

◆ Power Options in Windows

Set Windows Power Options to “High performance” when connecting multiple Sensors. Operations are not guaranteed if not set to “High Performance”.

3.1.3 Supporting Multiple Clients

When supporting multiple clients in a client/server configuration, the multi-threaded authentication process can be carried out by running the Enterprise Edition for the Authentication library on the server, generating multiple threads in the application on the server, and calling Authentication library functions from each thread as illustrated in the following figure.



!Caution Functions for generating threads

Use one of the following C standard functions.

<For Windows environment>

・_beginthread

・_beginthreadex

<For Linux environment>

・pthread_create()

!Caution **Number of threads in multi-threaded processes**

Up to 512 threads excluding cancellation threads can be called in multi-thread processes; however, this number is a logical value and there is no guarantee on issues such as processing speed and operation. The number of threads should be determined at the user's own risk on examination of the operational environment when developing palm vein authentication systems.
An error will be returned when the number of operational threads is exceeded.

3.2 Considerations for Developing an Application

An application for the Windows version and Linux version of the Palm vein authentication system can be developed in C/C++, VB .NET, C#, Java, etc.
As for an application for the Android version of the Palm vein authentication system, it can be developed in Java.

This section explains the issues to be considered when developing an application for the Windows version or Linux version of the Palm vein authentication system.

3.2.1 Developing in C/C++

Call the Authentication library functions from the application when developing in C or C++.

>See> For information on functions in the Authentication library, refer to the "Authentication Library Reference Guide".

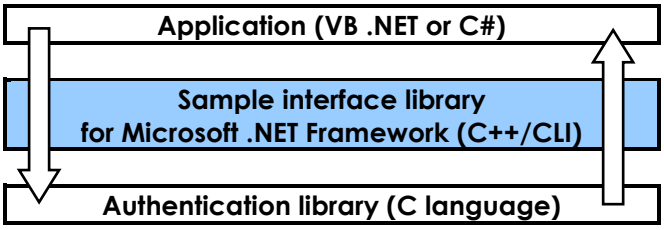
3.2.2 Developing in Other Languages

If you are developing applications with a language other than C or C++, you need an interface to exchange information since you are using a different language for development from the Authentication library.
This product provides the following Sample interfaces.

- Sample interface library for Microsoft .NET Framework
- Sample interface module for Java

◆ Developing Applications Using VB .NET or C#

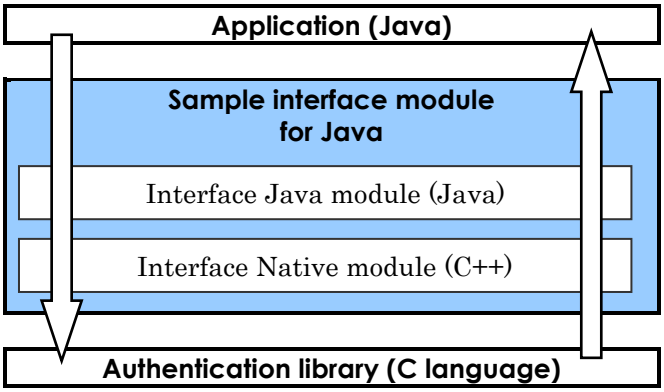
You can use the Sample interface library for Microsoft .NET Framework if you are developing Windows applications with VB .NET or C#.



>See> For information on the Sample interface library for Microsoft .NET Framework, refer to "Sample Interface Library for Microsoft .NET Framework Manual".

◆ Developing Applications Using Java

You can use the Sample interface module for Java if you are developing Windows or Linux applications with Java.



>See> For information on the Sample interface module for Java, refer to "Sample Interface Module for Java Manual".

3.2.3 Developing Windows Applications

In environments where the Smart App Control is turned on in Windows 11, applications without a valid signature are blocked.
If the Windows 11 Smart App Control support is required, you must sign your application yourself.
For information on signing applications, refer to the Microsoft website.

3.3 Security Countermeasures When Managing Vein Data

The vein data that is enrolled using the Palm vein authentication system can be personal information. Therefore, it is customer's responsibility to take security measures for handling of palm vein data in their Palm vein authentication systems.
Fujitsu Frontech Ltd will not be responsible for any damage caused by cracked security countermeasures such as leakage and counterfeit of vein data.

◆ Functions Administrator/Non-Administrator Are Allowed to Access

Security should be designed so that only the administrator can access the following functions:

- Enrollment/deletion of vein data
- Backup/restore of vein data

A non-administrator (user) is allowed to access basically his/her own authentication only.

◆ Management of Vein Data

The following security countermeasures are recommended for managing vein data:

- **Encryption of vein data/user identification information**
  Although vein data is encrypted in the Authentication library to enhance security, it is recommended that vein data and user identification information linked to vein data (e.g., ID) be further encrypted.

- **Indirect link between vein data/user identification information**
  It is recommended that vein data be linked indirectly to user identification information instead of using a direct link.
  It is also recommended that files containing vein data and user identification information be secured separately.

- **Splitting vein data for one hand**
  When you save vein data for one hand, data splitting is recommended.

◆ Sending/Receiving Vein Data on a Network

When you send and receive vein data on a network, ensure that adequate security countermeasures (such as encryption) are performed. Also, take network security countermeasures (such as VPN) for the traffic.

◆ Storing/Backing Up Vein Data

Please consider various methods to protect against theft and loss when storing vein data that is used.
Ensure that safety is secured. “The device to store vein data should be installed in a safe environment”. “If there are any safety concerns regarding the environment where the device is being installed, add the tamper resistant capability”. Security for backing up vein data should be treated in the same way as security for storing vein data.

★Tip **What is tamper resistant capability?**
This is a function to prevent vein data from being stolen or lost by physical, unauthorized access to vein data.
For example, the tamper resistant capability detects unauthorized access for the purpose of stealing vein data, such as the destruction and disassembly of the device that contains the vein data. When the tamper resistant capability detects an unauthorized access, vein data is deleted automatically.

◆ In the Case that Vein Data is Stored in a Smart Card

For enhanced security, each card should have a different individual encryption key, and vein data should be encrypted.

>See> For information on how to encrypt vein data by using a different individual encryption key for each smart card, refer to the “Authentication Library Reference Guide” or “Authentication Library for Android Reference Guide”.

3.4 Considerations for Operating the Palm Vein Authentication System

3.4.1 Considerations for Enrollment of Palm Vein Data and Authentication

There are a few issues to be considered for enrollment of palm vein data and authentication.

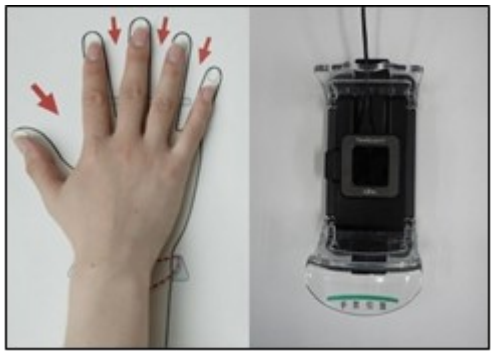
◆ Enrolling High Quality Palm Vein Data

Authentication accuracy of the Sensor is largely influenced by the quality of enrolled palm vein data. If the palm vein data is enrolled with incorrectly placed hands, it may result in false rejections. Therefore, good care should be taken for placing the hand correctly when capturing palm veins for enrollment.

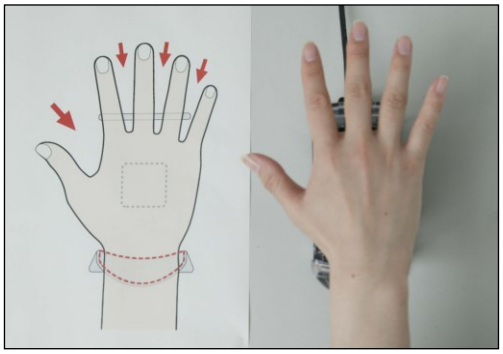
>See> For information on how to place the hand correctly, refer to the "Sensor Instruction Manual".

The SDK V02 Support Website provides a pdf file (HandPrintLeaflet_E.pdf) illustrating correct way to place the hand, in the Leaflet "Palm Vein Pattern Enrollment and Authentication Method".

To enroll high quality palm vein data, you can print this pdf file and use it as follows.



<Place the hand on the paper to check the correct way to place the hand>



<Place the hand on the Sensor>

◆ Installation Height of the Sensor and Palm Guide

When capturing the palm veins for enrollment or authentication, install the Sensor and Palm guide at an appropriate height for the prospective users' stature. For example, assuming the users to be Japanese adults, the recommended height for installation of the Sensor and Palm guide is at 85 cm or higher.
If the Sensor and Palm guide are installed too low and users have to perform enrollment of palm vein data or authentication while standing, authentication accuracy may decrease since the hand may be placed on top of the Wrist guide, or the palm may be lowered into the Palm guide.

<The hand is placed on top of the Wrist guide>

<The hand is lowered into the Palm guide>

◆ Posture When Enrolling Palm Vein Data and Authenticating

When capturing palm veins for authentication, give consideration that the user's posture should be as close as possible to that of the time of enrollment.
For example, if the enrolled palm vein data was captured while the user was seated, it is recommended to authenticate the user in the same sitting position.
The way a user places the hand are different when capturing palm veins while seated for enrollment and capturing palm veins while standing for authentication, and vice versa. In such cases, consider the height where the Sensor and Palm guide is installed, and train users to place their hands correctly.

◆ If Authentication Accuracy is Lower on Cold Mornings, etc.

Depending on the user's constitution (small blood vessels, low blood pressure, etc.), authentication accuracy may be lower in some situations, such as on cold mornings. In this case, warm up the hand for a while and retry the authentication.
If the false rejection persists, re-enroll the palm vein data. The re-enrollment of vein data improves the authentication accuracy.

3.4.2 Consideration for the Use by Children

There are several considerations which should be given when the Palm vein authentication system is used for children.

3.4.2.1 Characteristics of Children Aged between 5 and 12

Children aged between approximately 5 and 12 have the following characteristics. Therefore, an adult needs to carefully guide them on how to place the hand.

◆ Characteristics by Ages

- They are rather unsettled and tend to place their hands without checking the position of the hand when capturing the palm veins.
- They often do not understand the importance of correctly placing the hand when capturing the palm veins.
- When enrolling palm vein data, the hand needs to be placed twice in the same state. However, placing the hand in the same state is sometimes difficult.

◆ Characteristics of Placing the Hand

- Since children's hand-joints are very soft, fingers and the wrist tend to curve before placing the hand which curves the palm and subsequently prevents the palm being placed horizontally.
- There is a tendency that they cannot keep their hands still on the Palm guide when capturing palm veins. (Data cannot be captured correctly while the hand is moving.)
- They often close fingers when placing their hands. (Closed fingers may cause false rejection.)

3.4.2.2 Functional Restrictions by Ages

Children aged between approximately 5 and 12 often cannot place their hands correctly, or cannot hold their hands still.
Therefore, some Authentication library functions have their own age restrictions.
Also, the applicable age for the palm vein authentication system is at least approximately 5 years. (Not suitable for 4 years and younger)

The following describes the functions with age restrictions.

Function with age restrictions		Suitable age
enrollment format of palm vein data	Non-compressed format	5 years or older
	Compressed format	13 years or older
authentication method	Verification	5 years or older
	Identification	13 years or older

>See> For information on the enrollment format of palm vein data, refer to "2.6.1.1 Enrollment Format of Palm Vein Data".

>See> For information on authentication method, refer to "2.3.2 Authentication".

3.4.2.3 About Vein Data of Children

As they grow, children's palms change in size.
Therefore, it is recommended to periodically re-enroll palm vein data for children aged approximately 5 up to 18. The re-enrollment of vein data improves the authentication accuracy.

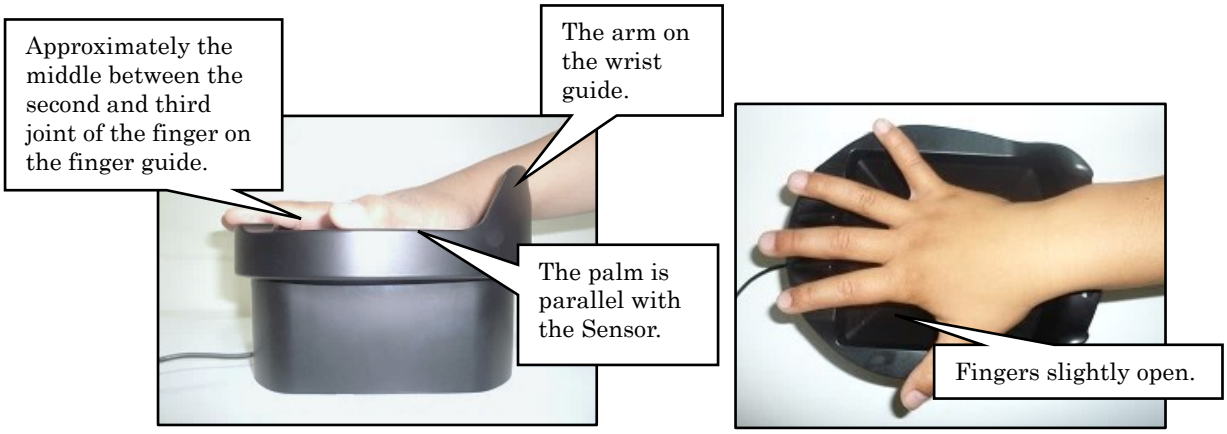
3.4.2.4 How to Place the Hand Over the Sensor

An adult needs to carefully guide the children aged between approximately 5 and 12 on how to place the hand.

★Tip **Applicable ages for the Palm guide included in this product**
The Palm guide included in this product is suitable for 7 years and older. It is recommended to make a Palm guide for children of 5 to 6 years designed for their palm size.
The Palm guide for children is not provided by Fujitsu Frontech Ltd.

◆ Using the Palm Guide Included in this Product

Since children's (aged between approximately 5 and 12) hands are small, place at approximately the middle between the second and third joint of fingers on the finger guide, and place the arm on the wrist guide. Ensure that the palm is parallel with the Sensor, and fingers slightly opened.
Following is an example of hand-placing using the U guide.



<View from the side> <View from above>

★Tip **If the wrist is placed on the wrist guide**
Palm veins may not be captured correctly when the fingertips are not reaching the finger guide; because in such a case, the gaps between fingers are included within the capturing range.

3.5 Other Considerations

◆ Removing and Re-inserting the USB Receptacle of the Sensor

Do not remove the USB receptacle of the Sensor during the use of applications.
If the USB receptacle of the Sensor is removed, further operations may not be guaranteed.
If any operational malfunctions occur after removing the USB receptacle of the Sensor,
terminate the application, re-insert the USB receptacle, and restart the application.

◆ Considerations for External Lights

The tolerance to external light is different depending on the Sensor type.
Install a sunshade where the amount of external light may affect the operation.

>See> For information on considerations for external light, refer to the "Hardware Drawings" and "Sensor Instruction Manual".

◆ Clearance Around the Sensor

Some clearance is required around the Sensor.

>See> For information on the required clearance around the Sensor, refer to the "Sensor Instruction Manual".

◆ Considerations for Using a USB Expansion Card

There are many kinds of USB expansion cards, so we cannot warrant that all USB expansion cards will work properly with the Sensor.
When you use a USB expansion card with the Sensor, please closely examine that it works properly with the Sensor.

◆ Considerations for Using a USB Hub

The Sensor can generally be connected via a USB hub. However, operations cannot be guaranteed for all USB hubs, since there are numerous types of USB hubs available. Therefore, Fujitsu Frontech Ltd. requests that customers fully examine operations in advance including tests on combinations with devices other than the Sensor when deploying a USB hub.
The following describes basic conditions on USB hubs when deploying with this product.

- It should be a self-powered hub which can supply 500 mA to the USB port where the Sensor is connected.
  (It must be able to supply 900 mA when using the high-power function.)
- The electricity supply from the USB hub to the USB port should be switched on and off at the same time as the target hardware.
- The electricity supply to the USB port should not be shut down.
  (The electricity supply to USB ports may be shut down on some USB hubs by an inrush current into the USB hub when powering on the target hardware or connecting the Sensor.)

The following describes issues to be considered when using a USB hub.

- Minimize the number of cascaded connections of USB hubs.
- Do not connect other devices to empty ports on the USB hub if possible.
- The auto-recovery function from the hibernation state and removal/re-insertion of the Sensor USB receptacle is not available when connecting the Sensor via a USB hub.

  >See> For information on the auto-recovery function for the hibernation state and removal/re-insertion of the Sensor USB receptacle, refer to the “Authentication Library Reference Guide”.

- Set Windows Power Options to “High Performance” when connecting a Sensor using a USB hub. Operations are not guaranteed if not set to “High Performance”.

◆ Considerations for Integrating a Sensor

There are a few issues to be considered when integrating a Sensor in hardware such as information terminals (Kiosk).

>See> For information on integrating a Sensor, refer to the “Hardware Drawings”.

◆ VDI (Virtual Desktop Infrastructure) and USB Redirection Environments

Operations on the VDI (Virtual Desktop Infrastructure) and USB redirection environments are not guaranteed.

Please carefully evaluate the operation and performance by taking the following points into consideration.

- Be sure to take necessary network security measures such as VPN since the image data captured by the Sensor will be transferred through the network.
- Be aware that the authentication process may slow down due to the increased network traffic, therefore, make sure to check the network capacity and authentication duration time.

Chapter4 When You Are Using Previous Versions

4.1 Release of PalmSecure SDK V02L03

4.2 Additional/Modified Functions and Notes for PalmSecure SDK V02L03

4.3 Additional/Modified Functions and Notes for PalmSecure SDK V02L02

4.4 Additional/Modified Functions and Notes for PalmSecure SDK V02L01

4.1 Release of PalmSecure SDK V02L03

PalmSecure SDK V02L03 has been released on the SDK V02 Support Website.

4.1.1 Features of PalmSecure SDK V02L03

PalmSecure SDK V02L03 has the following features.

- **Support for R-format type**

  R-format type is added in PalmSecure SDK V02L03 (Authentication library V34). In R-format type, you can perform accelerated identification while maintaining the authentication accuracy as high as that of I33-format type with high definition data. Also, by using the Authentication library Enterprise Edition in R-format type, you can perform identification against a palm vein data group of up to 200,000 items (200,000 hands for 100,000 people).

  >See> For information on the format-type, refer to “2.4.1 Format Type”.

  >See> For information on the approximate authentication duration, refer to the “Authentication Library Reference Guide”.

!Caution **When identifying against a palm vein data group of over 10,000 items**

When performing identification against a palm data group of over 10,000 items, you need to use the Authentication library Enterprise Edition V34Lxx-B27 or later, and the license file provided July 2021 or later. If you are using old library and license file, download the latest versions from the PalmSecure SDK Front Page and update them.

- **Added a function to help migration to R-format type**

  PalmSecure SDK V02L03 (Authentication library V34) provides multiple extraction function that extracts palm vein data in R-format and I33-format or R-format and I-format to help migration to the R-format type,

  >See> For information on the multiple extraction function, refer to “4.2.2.1 Notes on Migrating to the Authentication Library V34”.

- **Added the Authentication library for Arm**

  The Linux(armhf) Authentication library, Linux(arm64) Authentication library, and Android(Armv8-A) Authentication library are added as Authentication library for Arm.

  Note that the Authentication library for Arm supports only R-format type, and PalmSecure-F Pro sensor.

  >See> For information on the other function differences, refer to the "Appendix H　Comparison of Functions of Each Authentication Library".

  >See> For information of the Linux(armhf) and Linux(arm64) Authentication library, refer to the "Authentication Library Reference Guide".

  >See> For information of the Authentication library for Android, refer to the "Authentication Library for Android Reference Guide".

- **Added the palm vein data group thread sharing function (Authentication library Enterprise Edition)**

  This function enables all threads to share the pre-loaded palm vein data group for identification by executing the pre-loading processing of the vein data group that is normally required for each thread only from a specific thread.

  >See> For information on the palm vein data group thread sharing function, refer to "2.8.6 Palm Vein Data Group Thread Sharing Function".

4.1.2 Migrating to PalmSecure SDK V02L03

It is recommended for customers to check the version level of the current products and migrate to the latest PalmSecure SDK V02L03 products by download them from the SDK V02 Support Website.

>See> For information on how to check version level information, refer to "Appendix A How to Confirm the Version Level Information".

!Caution **Customers with previous products**

The following functions have been added to this product or modified in each version level of PalmSecure SDK V02.
V02L01: Support for the multiple processing for identification, manual shutter function, etc.
V02L02: Support for I33-format type, PalmSecure-F Pro sensor, etc.
V02L03: Support for R-format type, etc.

There are several considerations for migration to PalmSecure SDK V02L03 from previous products.

>See> For information on the migration to PalmSecure SDK V02L03, refer to "4.2 Additional/Modified Functions and Notes for PalmSecure SDK V02L03" through "4.4 Additional/Modified Functions and Notes for PalmSecure SDK V02L01" as needed depending on the version level of PalmSecure SDK V02 that you are currently using.

4.2 Additional/Modified Functions and Notes for PalmSecure SDK V02L03

4.2.1 Additional/Modified Functions in PalmSecure SDK V02L03

The following lists major additional/modified functions in PalmSecure SDK V02L03.

◆ Additional/Modified Functions for Software

Each software component in PalmSecure SDK V02L03		Additional/Modified Functions	Notes
Authentication library V34	Professional Edition Windows(x64) Windows(x86) Linux(x64) Linux(arm64) Linux(armhf) Android(Armv8-A)	Modified the tested OSes	For detailed information, refer to the "System Development Guide" (this document) and "Authentication Library Reference Guide" or "Authentication Library for Android Reference Guide". There are a few issues to be considered when migrating to the Authentication library V34. Refer to "4.2.2.1 Notes on Migrating to the Authentication Library V34".
		Added R-format type	
		Added multiple extraction function	
		Added Linux(arm64), Linux(armhf), Android(Armv8-A) versions	
	Enterprise Edition Windows(x64) Linux(x64)	Modified the tested OSes	
		Support for 1 to 200,000 identification in R-format type	
		Added palm vein data group thread sharing function	
Sensor driver	Windows(x64) V31L47 V32L01 Windows(x86) V31L37	Modified the tested OSes	For detailed information, refer to the "System Development Guide" (this document) and "Sensor Driver Installation Guide".
		Added V32L01 version	
	Linux(x64) Linux(arm64) Linux(armhf) V31L04	Modified the tested OSes	
		Support for Linux(arm64) and Linux(armhf)	

<table>
<tr><th colspan="2">Each software component in PalmSecure SDK V02L03</th><th>Additional/Modified Functions</th><th>Notes</th></tr>
<tr><td rowspan="3">Sample interface library for Microsoft .NET Framework V06</td><td rowspan="2">Professional Edition
Windows(x64)
Windows(x86)</td><td>Support for the Authentication library V34</td><td rowspan="3">For detailed information, refer to the “Sample Interface Library for Microsoft .NET Framework Manual”.
There are a few issues to be considered when migrating to the Sample interface library for Microsoft .NET Framework V06.
Refer to “4.2.2.2 Notes on Migrating to the Sample Interface V06 and Sample Application V06”.</td></tr>
<tr><td>Support for .NET 6 (x64 only)</td></tr>
<tr><td>Enterprise Edition
Windows(x64)</td><td>Support for the Authentication library V34</td></tr>
<tr><td rowspan="3">Sample application for Microsoft .NET Framework V06</td><td rowspan="2">Professional Edition
Windows(x64)
Windows(x86)</td><td>Support for the Authentication library V34</td><td rowspan="2">For detailed information, refer to the “Sample Application for Microsoft .NET Framework Manual Professional Edition”.
There are a few issues to be considered when migrating to the Sample application for Microsoft .NET Framework V06.
Refer to “4.2.2.2 Notes on Migrating to the Sample Interface V06 and Sample Application V06”.</td></tr>
<tr><td>Support for .NET 6 (x64 only)</td></tr>
<tr><td>Enterprise Edition
Windows(x64)</td><td>Support for the Authentication library V34</td><td>For detailed information, refer to the “Sample Application for Microsoft .NET Framework Manual Enterprise Edition”.
There are a few issues to be considered when migrating to the Sample application for Microsoft .NET Framework V06.
Refer to “4.2.2.2 Notes on Migrating to the Sample Interface V06 and Sample Application V06”.</td></tr>
</table>

<table>
<tr><th colspan="2">Each software component in PalmSecure SDK V02L03</th><th>Additional/Modified Functions</th><th>Notes</th></tr>
<tr><td rowspan="2">Sample interface module for Java V06</td><td>Professional Edition
Windows(x64)
Windows(x86)
Linux(x64)
Linux(arm64)
Linux(armhf)</td><td>Support for the Authentication library V34
Support for Arm</td><td rowspan="2">For detailed information, refer to the “Sample Interface Module for Java Manual”. There are a few issues to be considered when migrating to the Sample interface library for Java V06.
Refer to “4.2.2.2 Notes on Migrating to the Sample Interface V06 and Sample Application V06”.</td></tr>
<tr><td>Enterprise Edition
Windows(x64)
Linux(x64)</td><td>Support for the Authentication library V34</td></tr>
<tr><td rowspan="2">Sample application for Java V06</td><td>Professional Edition
Windows(x64)
Windows(x86)
Linux(x64)
Linux(arm64)
Linux(armhf)</td><td>Support for the Authentication library V34
Support for Arm</td><td>For detailed information, refer to the “Sample Application for Java Manual Professional Edition”. There are a few issues to be considered when migrating to the Sample application for Java V06.
Refer to “4.2.2.2 Notes on Migrating to the Sample Interface V06 and Sample Application V06”.</td></tr>
<tr><td>Enterprise Edition
Windows(x64)
Linux(x64)</td><td>Support for the Authentication library V34</td><td>For detailed information, refer to the “Sample Application for Java Manual Enterprise Edition”. There are a few issues to be considered when migrating to the Sample application for Java V06.
Refer to “4.2.2.2 Notes on Migrating to the Sample Interface V06 and Sample Application V06”.</td></tr>
<tr><td>Sample application for Android V02</td><td>Professional Edition
Android(Armv8-A)</td><td>New in PalmSecure SDK V02L03.</td><td>For detailed information, refer to the “Sample Application for Android Manual”.</td></tr>
<tr><td>Sample source for C language V01</td><td>Professional Edition
Windows(x64)
Windows(x86)
Linux(x64)
Linux(arm64)
Linux(armhf)</td><td>New in PalmSecure SDK V02L03.</td><td>For detailed information, refer to the “Sample Source for C Language Manual Professional Edition”.</td></tr>
</table>

Each software component in PalmSecure SDK V02L03		Additional/Modified Functions	Notes
Sensor maintenance tool V02L10	Windows(x64) Windows(x86)	Modified the tested OSes	For detailed information, refer to the “Sensor Maintenance Tool Operation Guide”.
Firmware update tool V03L03	Windows(x64) Windows(x86)	Modified the tested OSes	For detailed information, refer to the “Firmware Update Tool Operation Guide”.

◆ Additional/Modified Functions for Hardware

Each hardware component in PalmSecure SDK V02L03		Additional/Modified Functions	Notes
Sensor	PalmSecure Sensor V2		No modifications from PalmSecure SDK V02L02.
	PalmSecure-F Pro sensor		No modifications from PalmSecure SDK V02L02.
Firmware	For PalmSecure Sensor V2 V50L225		No modifications from PalmSecure SDK V02L02.
	For PalmSecure-F Pro sensor V56L022		No modifications from PalmSecure SDK V02L02.

4.2.2 Notes on Migrating to PalmSecure SDK V02L03

4.2.2.1 Notes on Migrating to the Authentication Library V34

There are several issues to be considered when migrating to the Authentication library V34.

!Caution **License authentication**
License authentication is required in order to use Authentication library V34. Purchase new license for V34 and acquire the license file because you cannot use the license files for older versions.

>See> For information on how to acquire the license file, refer to the “How to Acquire the License File”.

>See> For information on how to carry out the license authentication, refer to the “Authentication Library Reference Guide” or “Authentication Library Reference Guide for Android”.

!Caution **CPU requirements**
When migrating to the Authentication library V34, confirm that you are using a CPU that satisfies the hardware requirements.
Note that in Windows, if the SSE2 instructions are not implemented on the CPU, the OS will display an error message in a pop-up window when loading the Authentication library.

!Caution **About the Conventional Sensor driver for Windows**
The Conventional Sensor driver (V11 and V20) cannot be used from the Authentication library V34. Ensure that your sensor driver is V31 or later.
Note that if the Conventional Sensor driver is used on Windows, an error occurs in the Authentication library function "BioAPI_ModuleAttach".

◆ Changes in Tested OSes

Tested OSes for the Authentication library V34 are as follows.

<Professional Edition>

- Windows version
  - ・Windows 10 Pro Version 21H2 (x86 and x64)
  - ・Windows 11 Pro Version 22H2 (x64)
- Linux version
  - ・CentOS 7.9-2009 (x64)
  - ・Rocky 8.4 (x64)
  - ・Linux 4.9.51 64bit (arm64)
  - ・Linux-3.10.31-ltsi (armhf)
- Android version
  - ・Android 11 (Armv8-A)

<Enterprise Edition>

- Windows version
  - ・Windows Server 2012 R2 Update Standard (x64)
  - ・Windows Server 2016 Standard (x64)
  - ・Windows Server 2019 Standard (x64)
  - ・Windows Server 2022 Standard (x64)
- Linux version
  - ・CentOS 7.9-2009 (x64)
  - ・Rocky 8.4 (x64)

◆ About R-Format Type

This format type is provided from Authentication library V34 that enables fast identification processing while maintaining high authentication accuracy with high definition data.

Note that re-enrollment of palm vein data is required when migrating from a previous version to Authentication library V34 and using R-format type.

If re-enrollment of palm vein data is difficult and the palm vein data from the previous version should be used, use I33-format type (V33 compatible type) or I-format type (V32 compatible type) depending on the internal format of the enrolled palm vein data.

>See> For information on the format type, refer to “2.4.1 Format Type” and “Authentication Library Reference Guide” or “Authentication Library Reference Guide for Android”.

Keep the following points in mind in addition to the above when using R-format type.

- **Image compression function**

  This function is not available in R-format type.

  >See> For information on the image compression function, refer to “2.5.2 Image Compression Function”.

- **Capturing angle**

  The angle of the hand against the Sensor (capturing angle) cannot be changed in R-format type. Always use 0° for the capturing angle.

  Check the capturing angle setting in the Authentication library function “PvAPI_SetProfile” when migrating to the Authentication library V34 from a previous version and planning to use R-format type.

  >See> For information on the capturing angle, refer to “3.1.1 Changing the Angle of the Hand against the Sensor”.

  >See> For information on the Authentication library function “PvAPI_SetProfile”, refer to the “Authentication Library Reference Guide”.

◆ About Multiple Extraction Function

This function is intended to help migration of the palm vein data for enrollment to R-format.

When calling the Authentication library function “BioAPI_Capture”, the palm vein data for authentication is generated in multi-format of R-format and old-format (I33-format or I-format). This multi-format palm vein data can be used for both verification (1 to 1 authentication) with the palm vein data enrolled in R-format and verification with the palm vein data enrolled in old-format.

Note that this function is not supported by Authentication library for Android.

!Caution **Multi-format palm vein data in identification (1 to many authentication)**
The identification against a palm vein data group which does not contain the user’s palm vein data is not supported because the risk of false acceptance is very high. Therefore, do not design the migration procedure which attempts identification of multi-format palm vein data against each enrollment data group of the R-format and old-format.

>See> For information on the risk of false acceptance, refer to the “2.8.3 Risk of False Acceptance”.

When calling the Authentication library function “BioAPI_Verify”, the format is automatically switched to the internal format of the palm vein data for enrollment and processed.

This function is enabled by setting as follows.

・The format type is R-format type

・The multiple extraction mode is “Palm vein data in multi-format at BioAPI_Capture”.

Also, you can specify the following combination of internal formats of palm vein data by setting “multiple extraction data”.

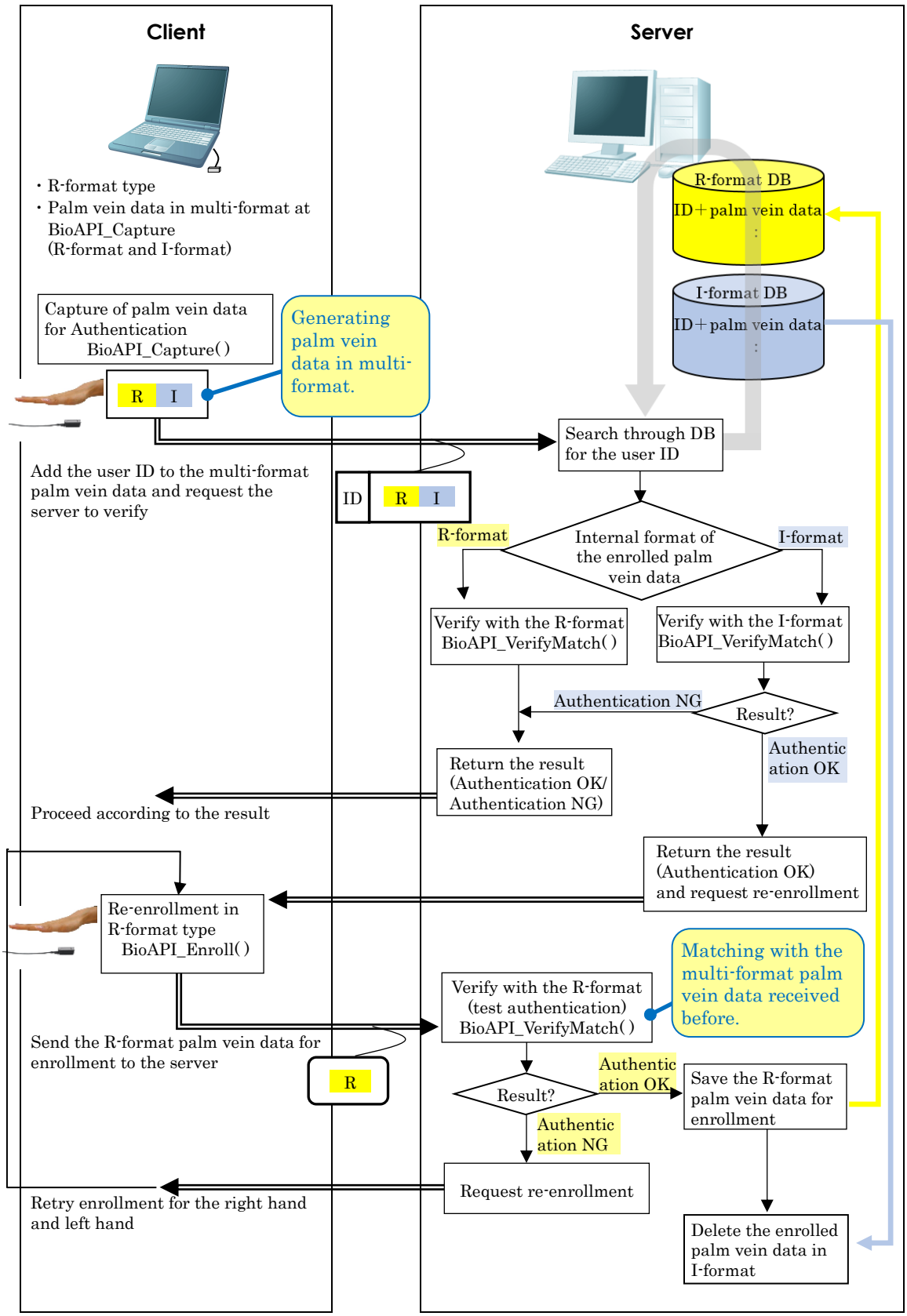
・R-format and I33-format

・R-format and I-format

>See> For information on how to set the format type, multiple extraction mode and multiple extraction data, refer to the “Authentication Library Reference Guide”.

!Caution **About the capturing duration**
The capturing duration becomes almost twice as long when this function is enabled. Therefore, set the multiple extraction mode back to the “Disable multiple extraction” after the migration of all palm vein data for enrollment is completed.

The following is an example of migration process using the multiple extraction function. (from I-format to R-format)



◆ Changes in the V2 Mode Function

The following modification is applied to the V2 mode function provided from the Authentication library V33.

>See> For information on the V2 mode function, refer to "4.3.3.1 Notes on Migrating to the Authentication Library V33".

- **Generating palm vein data for authentication**

  Palm vein data for authentication can also be generated by V2 mode function. However, do not use the image compression function while V2 mode function is enabled.

- **Available for identification**

  Palm vein data generated by V2 mode function can also be used for the identification (1 to many authentication).

The above changes allow the system in which the server remains running the Authentication library before V33Lxx-B25 to verify and identify the palm vein data as in <Example of a client/server configuration> on the following page.

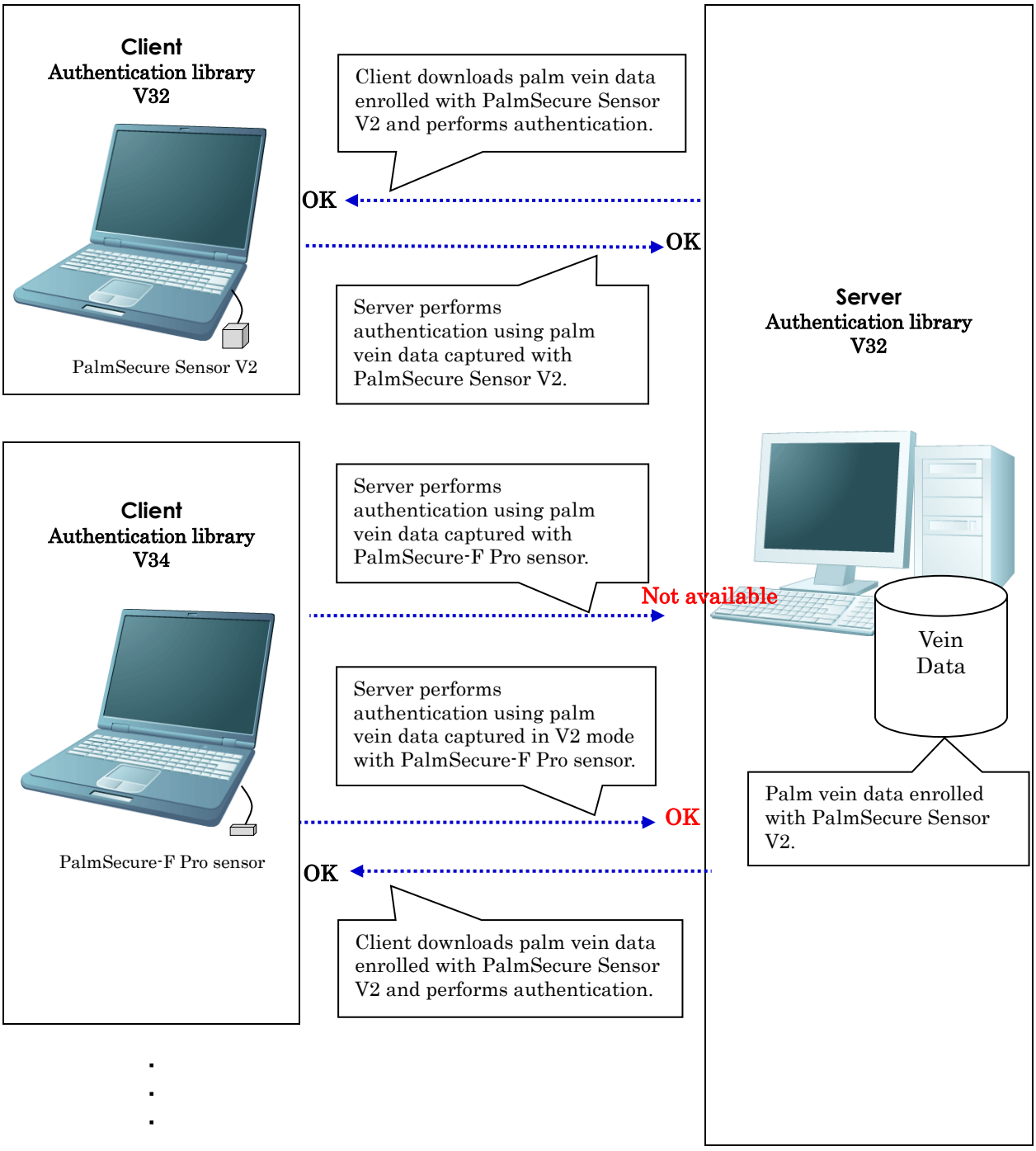
Use this function only when the following conditions are satisfied.

・PalmSecure-F Pro sensor is used for generating the palm vein data.
・I-format type (V32 compatible type) is used.
・Non-compressed format is specified for enrollment format of palm vein data.
・Not using image compression function.

!Caution **Risk of False Acceptance**
If the V2 mode function is used, the false rejection rate (FRR) becomes worse approximately two to three times than the case normal data form is used.
Also, the FRR becomes even worse when authenticating by Authentication library before V31.

!Caution **When migration to the Authentication library V34 is completed**
The V2 mode function is intended to be used temporarily for migration to the Authentication library V34. Therefore, disable the V2 mode function after the migration is completed.

<Example of a client/server configuration>



.
.
.

◆ Availability of Palm Vein Data enrolled by older versions of Authentication library

The following explains whether palm vein data enrolled by older versions of Authentication library can be used for the Authentication library V34.

- **Palm vein data enrolled by Authentication library V33**

  The palm vein data enrolled by the Authentication library V33 can be used in the same format type as the one used for enrolling the palm vein data.

  However, there are several points to note on data format when the JAVA/VB Interface library V01L04 or earlier was used.

  >See> For details on the data format, refer to the "Sample Interface Module for Java Manual".

- **Palm vein data enrolled by Authentication library V32, V31, or V30**

  The palm vein data enrolled by the Authentication library V32, V31, or V30 can be used as it is in I-format type.

  However, there are several points to note on data format when the JAVA/VB Interface library V01L04 or earlier was used.

  >See> For details on the data format, refer to the "Sample Interface Module for Java Manual".

- **Palm vein data enrolled by Authentication library V24 or earlier**

  The palm vein data enrolled by the Authentication library V24 or earlier cannot be used.

  You must re-enroll the palm vein data by Authentication library V34.

4.2.2.2 Notes on Migrating to the Sample Interface V06 and Sample Application V06

When migrating to the Sample application V06, you must migrate to the Sample Interface V06. Also, when migrating to the Sample Interface V06, you must migrate to the Authentication library V34.
The Sample interface V06 and Sample application V06 cannot operate properly without the Authentication library V34.

Note that operations of the Sample interface module for Java and Java Sample application are not confirmed with over 10,000 items for identification when using Enterprise Edition and R-format vein data.

4.3 Additional/Modified Functions and Notes for PalmSecure SDK V02L02

4.3.1 Features of PalmSecure SDK V02L02

PalmSecure SDK V02L02 has the following features.

- **Support for the PalmSecure-F Pro sensor**

  PalmSecure SDK V02L02 supports the PalmSecure-F Pro sensor.

- **Support for I33-format type**

  I33-format type that stores palm vein data as high definition data is added from PalmSecure SDK V02L02 (Authentication library V33) in addition to I-format type (V32 compatible type).

  The authentication accuracy as high as false acceptance 0.00001% can be achieved with high definition data.

  Also, the max identification items have significantly increased by supporting I33-format type.

  The following indicates the max identification items in each format type.

	Max identification items		
	PalmSecure SDK V02L01 (Authentication library V32)	PalmSecure SDK V02L02 (Authentication library V33)	
		Professional Edition	Enterprise Edition
I33-format type (Identification with F33-method)		Max 5,000 items (5,000 hands for 2,500 people)	Max 10,000 items (10,000 hands for 5,000 people)
I-format type (Identification with F27-method)	Max 1,000 items (1,000 hands for 500 people)	Max 1,000 items (1,000 hands for 500 people)	

>See> For information on I33-format type and I-format type, refer to "2.4.1 Format Type" and "Authentication Library Reference Guide".

>See> For information on identification and max identification items with F33-method and F27-method, refer to "2.8.2 Identification Method of Palm Vein Data".

>See> For information on the authentication accuracy, refer to the "Authentication Accuracy Data Sheet".

- **Support for the palm vein data acquisition function**

  PalmSecure SDK V02L02 (Authentication library V33) supports the following function to acquire palm vein data.

  ・PvAPI_GetTemplateInfoEx

  >See> For information on PvAPI_GetTemplateInfoEx, refer to the "Authentication Library Reference Guide".

- **Support for Windows(x64) WOW64**

  PalmSecure SDK V02L02 (Authentication library V33) can run on Windows(x64) WOW64 when using the Windows sensor driver for extended function.

4.3.2 Additional/Modified Functions in PalmSecure SDK V02L02

The following lists major additional/modified functions in PalmSecure SDK V02L02.

◆ Additional/Modified Functions for Software

Each software component in PalmSecure SDK V02L02		Additional/Modified Functions	Notes
Authentication library V33	Professional Edition Windows(x86) Windows(x64) Linux(x64)	Discontinued the Linux(x86) version	For detailed information, refer to the "System Development Guide" (this document) and "Authentication Library Reference Guide". There are a few issues to be considered when migrating to the Authentication library V33. Refer to "4.3.3.1 Notes on Migrating to the Authentication Library V33".
		Added the Linux(x64) version	
		Modified the supported OSes	
		Support for I33-format type	
		Support for the sensor connection retry process	
		Support for the hand detection function at test authentication	
		Support for the palm vein data acquisition function	
		Reviewed error information	
		Support for PalmSecure-F Pro sensor (V33Lxx-B25 or later)	
		Discontinued the support for PalmSecure Sensor	
		Discontinued the support for Conventional Sensor driver for Windows	
		Discontinued providing the enrolled data conversion library	
	Enterprise Edition Windows(x64) Linux(x64)	Modified the supported OSes	
		Support for the palm vein data acquisition function	
		Reviewed error information	
		Support for PalmSecure-F Pro sensor (V33Lxx-B25 or later)	
		Discontinued providing the enrolled data conversion library	

Each software component in PalmSecure SDK V02L02			Additional/Modified Functions	Notes
Sensor driver	Conventional	Windows(x86) V11L04 Windows(x64) V20L02		Not provided from PalmSecure SDK V02L02.
	For extended function	Windows(x86) V31L37 Windows(x64) V31L47	Modified the supported OSes	For detailed information, refer to the "System Development Guide" (this document) and "Sensor Driver Installation Guide".
			Support for Windows(x64) WOW64	
			Support for PalmSecure-F Pro sensor	
		Linux(x64) V31L04	Modified the supported OSes from Linux(x86) to Linux(x64)	
			Modified the supported OSes	
			Support for PalmSecure-F Pro sensor	
			Discontinued the support for PalmSecure Sensor	
Sample interface library for Microsoft .NET Framework V05		Professional Edition Windows(x86) Windows(x64)	Support for the Authentication library V33	For detailed information, refer to the "Sample Interface Library for Microsoft .NET Framework Manual".
		Enterprise Edition Windows(x64)		
Sample application for Microsoft .NET Framework V05		Professional Edition Windows(x86) Windows(x64)	Support for the Authentication library V33	For detailed information, refer to the "Sample Application for Microsoft .NET Framework Manual Professional Edition".".
Sample application for Microsoft .NET Framework V05		Enterprise Edition Windows(x64)	Support for the Authentication library V33	For detailed information, refer to the "Sample Application for Microsoft .NET Framework Manual Enterprise Edition".
Sample interface module for Java V05		Professional Edition Windows(x86) Windows(x64) Linux(x64)	Discontinued the Linux(x86) version	For detailed information, refer to the "Sample Interface Module for Java Manual".
			Added the Linux(x64) version	
			Support for the Authentication library V33	
		Enterprise Edition Windows(x64) Linux(x64)	Support for the Authentication library V33	
Sample application for Java V05		Professional Edition Windows(x86) Windows(x64) Linux(x64)	Discontinued the Linux(x86) version	For detailed information, refer to the "Sample Application for Java Manual Professional Edition".
			Added the Linux(x64) version	
			Support for the Authentication library V33	
Sample application for Java V05		Enterprise Edition Windows(x64) Linux(x64)	Support for the Authentication library V33	For detailed information, refer to the "Sample Application for Java Manual Enterprise Edition".

Each software component in PalmSecure SDK V02L02		Additional/Modified Functions	Notes
Sensor maintenance tool V02L09	Windows(x86) Windows(x64)	Modified the supported OSes	For detailed information, refer to the “Sensor Maintenance Tool Operation Guide”.
		Improved internal processes	
		Support for PalmSecure-F Pro sensor	
		Discontinued the support for PalmSecure Sensor	
		Discontinued the support for Conventional Sensor driver	
Firmware update tool V03L03	Windows(x86) Windows(x64)	Modified the supported OSes	For detailed information, refer to the “Firmware Update Tool Operation Guide”.
		Support for PalmSecure-F Pro sensor	
		Discontinued the support for PalmSecure Sensor	
		Discontinued the support for Conventional Sensor driver	

◆ Additional/Modified Functions for Hardware

Each hardware component in PalmSecure SDK V02L02		Additional/Modified Functions	Notes
Sensor	~~PalmSecure Sensor~~		Not supported from PalmSecure SDK V02L02.
	PalmSecure Sensor V2		No modifications from PalmSecure SDK V02L01.
	PalmSecure-F Pro sensor	New in PalmSecure SDK V02L02	
Firmware	~~For PalmSecure Sensor V00L203~~		Not provided from PalmSecure SDK V02L02.
	For PalmSecure Sensor V2 V50L225		No modifications from PalmSecure SDK V02L01.
	For PalmSecure-F Pro sensor V56L022	New in PalmSecure SDK V02L02	

4.3.3 Notes on Migrating to PalmSecure SDK V02L02

4.3.3.1 Notes on Migrating to the Authentication Library V33

◆ About I33-format type

This format type is new from the Authentication library V33 and Palm vein data can be stored as high definition data.
Re-enrollment of palm vein data in I33-format type is required when migrating from a previous version to the Authentication library V33 and using this type.
Use I-format type (V32 compatible type) if re-enrollment of palm vein data is difficult and the palm vein data from the previous version should be used.

>See> For information on I33-format type and I-format type, refer to “2.4.1 Format Type” and “Authentication Library Reference Guide”.

!Caution **Enrolled data conversion library**
The enrolled data conversion library can add F27-Index on uncompressed palm vein data in I-format that was enrolled with the Authentication library V21 or V24 to enable identification with F27-method.
However, this library cannot add F33-Index on uncompressed palm vein data in I-format to enable identification with F33-method.
Also, the enrolled data conversion library cannot convert palm vein data in I33-format.

>See> For information on the enrolled data conversion library, refer to the “Enrolled Data Conversion Library Reference Guide”.

>See> For information on the enrollment format of palm vein data (non-compressed format), refer to “2.6.1.1 Enrollment Format of Palm Vein Data”.

>See> For information on the internal format of palm vein data (I-format), refer to “2.6.1.2 Internal Format of Palm Vein Data”.

Keep the following points in mind in addition to the above when using this type.

- **Image compression function**

  The image compression function can also be used in I33-format type.

  Use this function only when performing verification authentication (1 to 1 authentication).

  >See> For information on the image compression function, refer to "2.5.2 Image Compression Function".

- **Capturing angle**

  The angle of the hand against the Sensor (capturing angle) cannot be changed in I33-format type. Always use 0° for the capturing angle.

  Check the capturing angle setting in the Authentication library function "PvAPI_SetProfile" when migrating to the Authentication library V33 from a previous version and planning to use this type.

  >See> For information on the capturing angle, refer to "3.1.1 Changing the Angle of the Hand against the Sensor".

  >See> For information on the Authentication library function "PvAPI_SetProfile", refer to the "Authentication Library Reference Guide".

◆ Support for Windows(x64) WOW64

Use Sensor driver for extended function V31L47 or later for Windows(x64) when migrating to the Authentication library V33 if you want to run the Authentication library Windows(x86) version on Windows(x64) WOW64.
The Authentication library V33 Windows(x86) version does not function properly without the Sensor driver for extended function V31L47 or later for Windows(x64) on Windows(x64) WOW64.

◆ Support for the Sensor Connection Retry Process

The Authentication library V33 Professional Edition supports the sensor connection retry process.
Therefore, if the Authentication library function “BioAPI_ModuleAttach” or “PvAPI_GetConnectSensorInfoEx” is called while the Sensor is not connected, a delay for the retry process occurs before returning from the function.

>See> For information on Authentication library functions “BioAPI_Module Attach” and “PvAPI_GetConnectSensorInfoEx”, refer to the “Authentication Library Reference Guide”.

◆ Guide Mode

Without guide mode can be used regardless of the use of the palm guide with the Authentication library V33.
However, use the palm guide and With guide mode in the following cases.

- When using the U guide
- When using palm vein data that was enrolled with older versions in With guide mode because re-enrollment of the palm vein data is difficult.
- When changing the angle of the hand against the Sensor (Only in I-format type).

>See> For information on guide mode, refer to “2.4.2 Using the Palm Guide (Guide Mode) ”.

◆ Newly added support for PalmSecure-F Pro sensor

The Authentication library V33Lxx-B25 or later supports the PalmSecure-F Pro sensor.

There are several considerations which should be given if the customer is using PalmSecure-F Pro sensor when migrating to the Authentication library V33 from previous products.

- When using old palm vein data
  The palm vein data that is enrolled by the Authentication library V30 or later can be used as it is. In this case, use I-format type (V32 compatible type).
  If the palm vein data is enrolled before the Authentication library V30, it is necessary to re-enroll the palm vein data.

  !Caution **The palm vein data enrolled before the Authentication library V30**
  Note that the PalmSecure-F Pro sensor does not support the palm vein data enrolled before the Authentication library V30.

- When using the Authentication library function “PvAPI_Sense”
  The recommended parameter value is different from PalmSecure Sensor V2. Review the setting value referring to the recommended value for the PalmSecure-F Pro sensor.
  Also, note that when using PalmSecure-F Pro sensor, basically, there is no need to use this function.

- When using palm vein data enrolled with PalmSecure-F Pro sensor
  An error occurs when older version of Authentication library performs authentication using palm vein data enrolled with PalmSecure-F Pro sensor. Therefore, in the system that is running older version of Authentication library, when only a partial group of target hardware is migrating to or newly using the PalmSecure-F Pro sensor, use Authentication library V33 (Note) for authentication.
  Also, in a client/server configuration, if some of the clients remain running older version of Authentication library in the system (see the following example), the authentication using palm vein data enrolled with PalmSecure-F Pro sensor cannot be performed. Therefore, use Authentication library V33 (Note) in the clients.

Use “V2 mode function” which is described later if migrating to the Authentication library V33 in client is difficult.

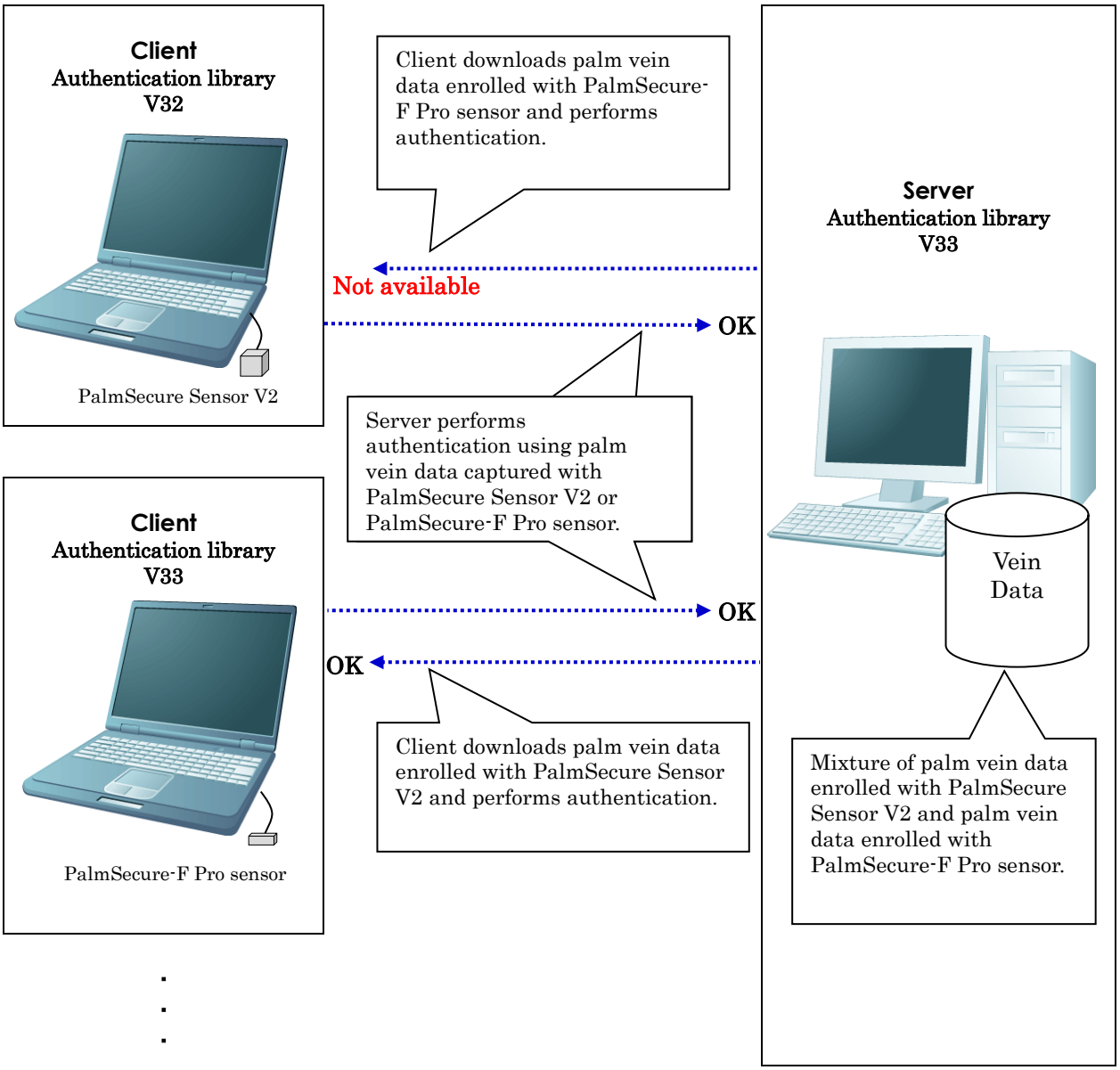
Note) Use the following Authentication library V33

Professional Edition Windows(x86): V33L10-B25 or later

Professional Edition Windows(x64): V33L60-B25 or later

Professional Edition Linux(x64) : V33L77-B25 or later

<Example of a client/server configuration>



.
.
.

◆ V2 Mode Function for PalmSecure-F Pro sensor

V2 mode function is provided by the Authentication library V33Lxx-B36 or later. This function is intended to help customers who are having difficulty migrating to Authentication library V33 and should only be used as a temporary measure until the migration completes.

This function generates palm vein data for enrollment in the data form of PalmSecure Sensor V2 when using the PalmSecure-F Pro sensor.

The palm vein data that is enrolled with this function can be used for verification (1 to 1 authentication) in the Authentication library earlier than V33Lxx-B25. This allows the system to perform verification even when some of the clients remain running older version of Authentication library as in <Example of a client/server configuration> on the previous page.

Use this function only when the following conditions are satisfied.

- PalmSecure-F Pro sensor is used for enrollment of palm vein data.
- The above enrolled palm vein data is to be used for verification (1 to 1 authentication) in older version of Authentication library.
- I-format type (V32 compatible type) is used.
- Non-compressed format is specified for enrollment format of palm vein data.

!Caution **Risk of False Acceptance**
When this V2 mode function is used, the false rejection rate (FRR) becomes worse approximately two to three times than the case normal data form is used.
Therefore, do not use this function for identification (1 to many authentication) since the risk of false acceptance becomes higher.

!Caution **Target palm vein data**
Only the palm vein data for enrollment can be created by this function.
The palm vein data for authentication remains in the data form of PalmSecure-F Pro sensor.

◆ Discontinued the support for PalmSecure Sensor and Conventional Sensor Driver for Windows

The Authentication library V33 discontinued the support for PalmSecure Sensor and Conventional Sensor driver for Windows.

◆ About Enrolled Data Conversion Library

The Authentication library V33 discontinued providing the enrolled data conversion library.

★Tip **Enrolled data conversion library**
The enrolled data conversion library converts the non-compressed I-format vein data enrolled by Authentication library V24 or V21 into the format with F27-Index that can be used for identification by the F27-method.

If using palm vein data enrolled by the Authentication library V24 or V21 for identification, consider to re-enroll the palm vein data when migrating to the Authentication library V33.
When conversion of the palm vein data is necessary, you can download only the enrolled data conversion library from SDK V02L02 in the SDK V02 Support Website and use it.
Note that the palm vein data converted from V24 or V21 is unable to use for PalmSecure-F Pro sensor. Use PalmSecure Sensor V2 for the converted data.

4.4 Additional/Modified Functions and Notes for PalmSecure SDK V02L01

4.4.1 Features of PalmSecure SDK V02L01

PalmSecure SDKV02L01 has the following features.

- **Support for the multiple processing for identification function**

  The multiple processing for identification function has been added from PalmSecure SDK V02L01.

  This function enables multi-processing of identification if your CPU is a multi-core processor. This can reduce the time required for identification processes.

  >See> For information on the multiple processing for identification, refer to "2.8.5 Speeding Up the Identification Process" and the "Authentication Library Reference Guide".

- **Support for the shutter function**

  The shutter function has been added from PalmSecure SDK V02L01.

  The shutter function waits for the second capture until a user operation such as clicking the start capture button when enrolling vein data.

  When using the shutter function the Authentication library will return the capture start calls back message before capturing the palm veins for the second time.

  This function is useful when you have an operator who can assist the user to place the hand.

  This function allows you to confirm that the hand is placed properly before capturing. This enables enrollment of better-quality vein data.

  >See> For information on the shutter function, refer to "2.6.2 Palm Vein Data Enrollment Sequence" and the "Authentication Library Reference Guide".

- **Newly added Sample interface module for Java and Sample application for Java**

  The Sample interface module for Java and Sample application for Java have been added from PalmSecure SDK V02L01.

  You can use them when developing applications in Java.

  >See> For information on the Sample interface module for Java, refer to "1.4.3 Sample Interface" and "Sample Interface Module for Java Manual".

  >See> For information on the Sample application for Java, refer to "1.4.4 Sample Application" and, "Sample Application for Java Manual Professional Edition" or "Sample Application for Java Manual Enterprise Edition".

4.4.2 Additional/Modified Functions in PalmSecure SDK V02L01

The following lists major additional/modified functions in PalmSecure SDK V02L01.

◆ Additional/Modified Functions for Software

Each software component in PalmSecure SDK V02L01		Additional/Modified Functions	Notes
Authentication library V32	Windows(x86) Windows(x64) Linux(x86) Linux(x64)	Discontinued Basic Edition	For detailed information, refer to the "System Development Guide" (this document) and "Authentication Library Reference Guide". There are a few issues to be considered when migrating to the Authentication library V32. Refer to "4.4.3.1 Notes on Migrating to the Authentication Library V32".
		Added Professional Edition	
		Discontinued Enterprise Edition Linux(x86) version	
		Added a file to the Linux version (f3bc4dmi)	
		Modified the supported OSes	
		Support for the multiple processing for identification function	
		Support for the shutter function	
		Removed "BioAPI_GetHeaderFromHandle" and "BioAPI_Process" functions	
		Modified the maximum number of vein data items for identification	
		Reviewed error information	

<table>
<tr><th colspan="3">Each software component in PalmSecure SDK V02L01</th><th>Additional/Modified Functions</th><th>Notes</th></tr>
<tr><td rowspan="3">Sensor driver</td><td rowspan="1">Conventional</td><td>Windows(x86)
V11L04
Windows(x64)
V20L02</td><td>Modified the supported OSes to Windows 7</td><td rowspan="3">For detailed information, refer to the “Sensor Driver Installation Guide”.</td></tr>
<tr><td rowspan="2">For extended</td><td>Windows(x86)
V31L35
Windows(x64)
V31L45</td><td>Modified the supported OSes to Windows 7 / 8.1 / 10</td></tr>
<tr><td>Linux
V31L02</td><td>Support for multiple Sensor connections (up to 2 Sensors)</td></tr>
<tr><td colspan="2" rowspan="2">Sample interface library for Microsoft .NET Framework V04</td><td rowspan="2">Windows(x86)
Windows(x64)</td><td>Support for the Authentication library V32</td><td rowspan="2">For detailed information, refer to the “Sample Interface Library for Microsoft .NET Framework Manual”.</td></tr>
<tr><td>Added the Interface library for the Authentication library Enterprise Edition</td></tr>
<tr><td colspan="2" rowspan="3">Sample application for Microsoft .NET Framework V04</td><td rowspan="3">Professional Edition
Windows(x86)
Windows(x64)</td><td>Support for the Authentication library V32</td><td rowspan="3">For detailed information, refer to the “Sample Application for Microsoft .NET Framework Manual Professional Edition”.</td></tr>
<tr><td>Modified the method to specify the application key</td></tr>
<tr><td>Added the capturing function</td></tr>
<tr><td colspan="2">Enterprise Edition
Windows(x64)</td><td>New in PalmSecure SDK V02L01</td><td>For detailed information, refer to the “Sample Application for Microsoft .NET Framework Manual Enterprise Edition”.</td></tr>
</table>

Each software component in PalmSecure SDK V02L01		Additional/Modified Functions	Notes
Sample interface module for Java V04	Windows(x86) Windows(x64) Linux(x86) Linux(x64)	New in PalmSecure SDK V02L01	For detailed information, refer to the “Sample Interface Module for Java Manual”.
Sample application for Java V04	Professional Edition Windows(x86) Windows(x64) Linux(x86)	New in PalmSecure SDK V02L01	For detailed information, refer to the “Sample Application for Java Manual Professional Edition”.
	Enterprise Edition Windows(x64) Linux(x64)	New in PalmSecure SDK V02L01	For detailed information, refer to the “Sample Application for Java Manual Enterprise Edition”.
Sensor maintenance tool V02L03	Windows(x86) Windows(x64)	Modified the supported OSes to Windows 7 / 8.1 / 10	For detailed information, refer to the “Sensor Maintenance Tool Operation Guide”.
		Added a Sensor error message	
Firmware update tool V03L02	Windows(x86) Windows(x64)	Modified the supported OSes to Windows 7 / 8.1 / 10	For detailed information, refer to the “Firmware Update Tool Operation Guide”.
		Improved internal processes	

◆ Additional/Modified Functions for Hardware

Each hardware component in PalmSecure SDK V02L01		Additional/Modified Functions	Notes
Sensor	PalmSecure Sensor		No modifications from PalmSecure SDK V01L08.
	PalmSecure Sensor V2		
Firmware	For PalmSecure Sensor V00L203		No modifications from PalmSecure SDK V01L08.
	For PalmSecure Sensor V2 V50L225	Improved internal processes	

4.4.3 Notes on Migrating to PalmSecure SDK V02L01

4.4.3.1 Notes on Migrating to the Authentication Library V32

◆ Removal of "BioAPI_GetHeaderFromHandle" and "BioAPI_Process" Functions

The Authentication library V32 discontinued providing the following functions.

・BioAPI_GetHeaderFromHandle

・BioAPI_Process

These functions were generally not used even in the older versions of Authentication libraries; however, be sure that these functions are not used in your applications.

◆ Change in the Maximum Number of Vein Data Items for Identification

Identification by the F27-method can handle up to 1,000 hands of vein data; meanwhile, the Authentication library V32 is capable of interfacing up to 1,200 hands though it was up to 4,000 hands till the Authentication library V31.
The more the number of items in vein data subject to identification, the higher the risk of false acceptance in general. Therefore, keep the number of vein data items subject to identification within 1,000 hands.

Appendix

Appendix A How to Confirm the Version Level Information

This appendix shows how to confirm version level information of software, documents, and the firmware in the Sensor unit provided with this product (PalmSecure SDK V02L03).

Type			How to Confirm the Version Information
Software	Authentication library		Display “pvfwvl.txt” or “pvfwvlSV.txt” in the folder where the Authentication library is stored by the text editor.
	Sensor driver	Windows version Installer type	(1) Select [Programs and Features] from Control Panel. (2) Select [FUJITSU PalmSecure Sensor Driver] from the displayed screen. (3) Check the [Version]. (Note) To make the version number displayed in the [Version] column correspond to the version information on the SDK V02 Support Website, translate the version number as follows. ・The first two digits correspond to V (Version) ・The 2nd and 4th digits of the last 4 digits correspond to L (Level). Example: When the version number is displayed as "3.1.0407", it is V31L47. Note) If [Version] is not displayed, right-click the [Name] column and select [Version] from the displayed menu.
		Windows version Driver package type	(1) Start Device Manager. (2) Right-click the device name under “PalmSecure ” and select“ Properties ” from the menu that appears. (3) From the properties screen that appears, select the “Driver” tab. (4) Confirm the version. To make the displayed version number correspond to the version information on the SDK V02 Support Website, translate the version number as follows. ・The first two digits correspond to V (Version) ・The last two digits correspond to L (Level). Example: When the version number is displayed as "3.2.0.1 ", it is V32L01.
		Linux version	(There is no means to check version level information)

Type		How to Confirm the Version Information
Software	Sample application for Microsoft .NET Framework	Right click each program (.exe) from Explorer and display Properties. See the Details tab in Properties.
	Sample interface for Java	(There is no means to check version level information)
	Sample application for Java	
	Sample application for Android	
	Sample source for C language	
	Sensor maintenance tool	Right click the program (.exe) from Explorer and display Properties. See the Details tab in Properties.
	Firmware update tool	Right click the program (.exe) from Explorer and display Properties. See the Details tab in Properties.
Documents (Manual)		Open each manual (pdf) and find the version number in "Revision History" or "Introduction".
Firmware in the Sensor		Version information can be confirmed using the maintenance function of the Sensor maintenance tool. >See> For information on the Sensor maintenance tool, refer to the "Sensor Maintenance Tool Operation Guide".

Appendix B Tested OSes

The following list shows OSes whose operations are confirmed with each software item provided with this product (PalmSecure SDK V02L03).

◆ Windows(x64) / Windows(x86) / Linux(x64)

Software type		OS type				
		Windows(x64)		Windows(x86)	Linux(x64)	
		10/11	Server2012 R2 /Server 2016 /Server 2019 /Server 2022	10	CentOS7.9	Rocky 8.4
Authentication library	PE	○	×	○	○	○
	EE	×	○	×	○	○
Sensor Driver	For Windows	○	×	○		
	For Linux				○	○
Sample interface library for Microsoft.NET Framework		○	○	○		
Sample application for Microsoft.NET Framework	PE	○	×	○		
	EE	×	○	×		
Sample interface module for Java		○	○	○	○	○
Sample application for Java	PE	○	×	○	○	○
	EE	×	○	×	○	○
Sample source for C language	PE	○	×	○	○	○
Sensor maintenance tool		○	×	○		
Firmware update tool		○	×	○		

○: Operations confirmed ×: Operations not confirmed

PE: Professional Edition EE: Enterprise Edition

[Legend for the OS type]

10	: Windows 10 Pro
11	: Windows 11 Pro (Note)
Server 2012 R2	: Windows Server 2012 R2 Standard Edition
Server 2016	: Windows Server 2016 Standard Edition
Server 2019	: Windows Server 2019 Standard Edition
Server 2022	: Windows Server 2022 Standard Edition

Note) The Sensor driver V31, Firmware update tool, and Java sample software do not support the Smart App Control for Windows 11.

◆ Linux(arm64) / Linux(armhf)

Software type		OS type	
		Linux(arm64)	Linux(armhf)
		Linux 4.9.51 64bit	Linux-3.10.31-ltsi
Authentication library	PE	○	○
Sensor driver	For Linux	○	○
Sample interface module for Java (Note)		○	○
Sample application for Java	PE	○	○
	EE	×	×
Sample source for C language	PE	○	○

PE : Professional Edition EE: Enterprise Edition

Note) Only build environment such as Makefile is available for the Interface Native module for Arm.

◆ Android(Armv8-A)

Software type		OS type
		Android 11 (Armv8-A)
Authentication library	PE	○
Sample application for Android	PE	○

PE : Professional Edition

Appendix C Updating the Firmware on the Sensor Unit

The firmware is stored on the Sensor unit.

In addition to publishing information on the SDK V02 Support Website, we will send you update information by e-mail when the firmware is updated.

Check the type and firmware version level of your sensor and update to the latest version by downloading it from SDK V02L03 in the SDK V02 Support Website as necessary.

>See> For information on how to check the sensor type, refer to “Appendix D Checking the Sensor Type”.

>See> For information on how to check the version level information of the firmware, refer to the “Sensor Maintenance Tool Operation Guide”.

The following two methods are available for updating the firmware on the Sensor unit.

- Using the Firmware update tool
- Using the Authentication library firmware update function (Note)

  Note) Unavailable in Authentication library for Android.

There are the following differences between the above 2 methods.

		Firmware update tool	Authentication library firmware update function
Sensor operating environment	OS	Windows 10 (x86 and x64) Windows 11 (x64)	OSes which are supported by the Windows version or Linux version of Authentication library.
	Others	The following must be installed ・Sensor driver	The following must be installed ・Authentication library ・Sensor driver ・An application which uses the Authentication library and Sensor.
Required items		The latest version of the Firmware update tool	The latest version of the firmware One of the following operational environment setting files. ・F3BC4FRM.INI (Windows environment) ・f3bc4frm.ini (Linux environment)
Note		Use this method in general.	Use this method only when you cannot use the Firmware update tool. Example) An entry-exit device with an embedded Sensor
Caution		Never operate any other applications while the firmware is being updated. Also note, the following events must not occur. ・Removing and re-inserting of the USB receptacle and cable ・Resetting the system ・Rebooting the OS ・Shutting down ・Power cut	

★Tip **The Firmware update tool programs (.exe)**

The Firmware update tool consists of the program file (.exe), operational environment setting file (.ini), and the update firmware (.arc). These 3 files form a set and are available from SDK V02L03 in the SDK V02 Support Website as the Firmware update tool.
Firmware update tools are named according to the version level of the contained firmware. File names of the Firmware update tool are "FWUpdate64_03XX_VxxLxxx.zip" (Windows(x64)) or "FWUpdate_03XX_VxxLxxx.zip"(Windows(x86)) ; the "03XX" section indicates the
tool version, and "VxxLxxx" indicates the version level of the firmware. "Vxx" in the firmware version varies as follows depending on the Sensor type.

・PalmSecure Sensor V2: V50
・PalmSecure-F Pro sensor: V56

The firmware in the Sensor will not be updated if you apply the firmware for a different sensor type.

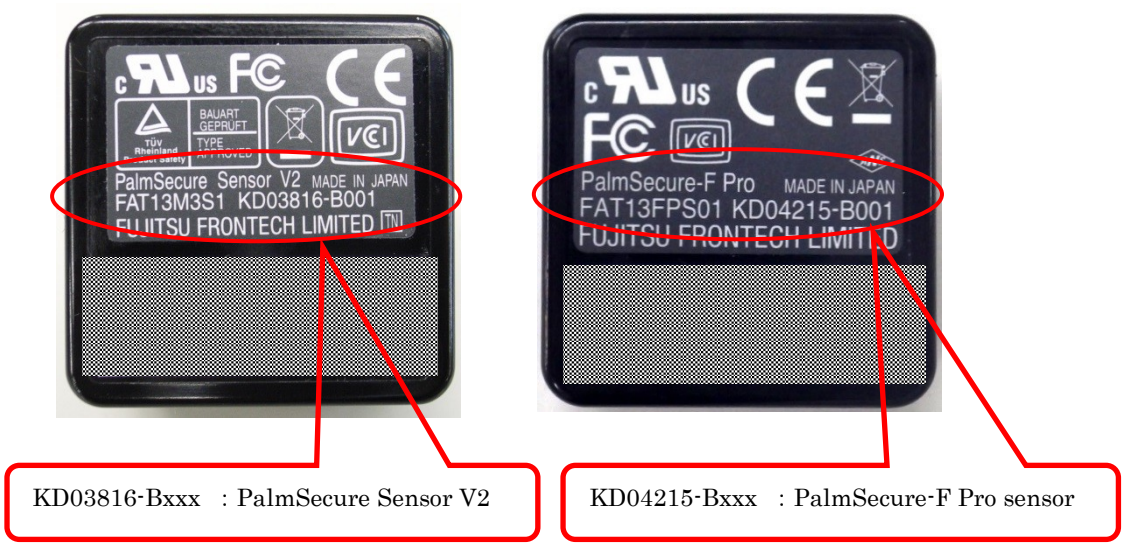
>See> For information on the Authentication library firmware update function, refer to the "Authentication Library Reference Guide".

>See> For information on the Firmware update tool, refer to the "Firmware Update Tool Operation Guide".

Appendix D Checking the Sensor Type

D.1 Checking from the Base of the Sensor

You can check the sensor type from the Model at the base of the sensor.



D.2 Checking with the Sensor Maintenance Tool

You can check the sensor type from the Model displayed by the maintenance function of the Sensor maintenance tool.

>See> For information on the Sensor maintenance tool, refer to the "Sensor Maintenance Tool Operation Guide".

D.3 Checking the Sensor Type from an Application

You can confirm the Sensor type using the following Authentication library function.

- PvAPI_GetLibraryInfo

When using Authentication library for Android, call the following method.

- Java_PvAPI_GetLibraryInfo

>See> For information on PvAPI_GetLibraryInfo, refer to the "Authentication Library Reference Guide".

>See> For information on Java_PvAPI_GetLibraryInfo of Authentication library for Android, refer to the "Authentication Library for Android Reference Guide".

Appendix E Consideration on the Palm Guide

E.1 Use of the Palm Guide in Authentication

Whether or not to use the Palm guide in authentication (live environment) and what type of Palm guide should be used depends on the available installation space, the provided hand-placing instruction, and the authentication frequency. They are summarized in the following table.

You can create your own palm guide based on the "Hardware Drawings"; however, users' own palm guides are not discussed in this document.

<table>
<tr><td colspan="2"></td><td colspan="2">＜Provided hand-placing instruction＞
Little ◄——► Detailed
＜Frequency of authentication operations＞
Infrequent ◄——► Frequent</td></tr>
<tr><td rowspan="3">Palm guide installation space</td><td>Unavailable</td><td>(Consider hand-placing training and practice at the beginning of the operation)</td><td>(1) (Note 1)
  </td></tr>
<tr><td>Available</td><td>(Consider hand-placing training at the beginning of the operation)</td><td>(2) (Note 2)
  </td></tr>
<tr><td>Plenty available</td><td>(3) (Note 3)
  </td><td></td></tr>
</table>

Note 1) Use Without guide mode for the Guide mode.

Note 2) Use With guide mode for the Guide mode.

Without guide mode is also available from the Authentication library V33.

However, if you use the Palm guide for both enrollment and authentication, it is recommended to use With guide mode.

Note 3) Use With guide mode for the Guide mode.

>See> For information on guide mode, refer to “2.4.2 Using the Palm Guide (Guide Mode)”.

(1) Not using Palm guide

Operations without the Palm guide may be possible where thorough instructions on hand-placing can be provided, or users are experienced in hand-placing due to frequent authentication.

Refer to the “Sensor Instruction Manual” or “Leaflet” when giving hand-placing instructions to users.

(2) Using the Folding guide

The Folding guide requires more attention than with the U guide when placing the hand. Therefore, hand-placing instructions are necessary when using the Palm guide.

Refer to the “Sensor Instruction Manual” or “Leaflet” when giving hand-placing instructions to users.

Note that when using Folding guide on PalmSecure-F Pro sensor, the “Standard” is required,

>See> For information on the “Standard”, refer to the “Standard Instruction Manual”.

(3) Using the U Guide

The U guide is devised to help the user place the hand correctly. Therefore, this is recommended in an environment where detailed hand-placing instructions are not possible or where users are not used to placing the hand due to the infrequent use of the product.

E.2 Use of the Palm Guide in Enrollment

Whether to use the Palm guide at enrollment depends on whether a Palm guide is used for authentication (live environment).

◆ Using the Palm Guide for Authentication in With guide mode

If you are using the Palm guide for authentication (operating environment), it is recommended to use **the same Palm guide as authentication** when enrolling palm vein data.

However, it is possible to use a different Palm guide as shown in the following table.

		Palm guide for authentication			
		No Palm guide	Folding guide (Note 1)	U guide (Note 2)	Your own palm guide (Note 1)
Palm guide for enrollment	No Palm guide				
	Folding guide		◎	○	△
	U guide		○	◎	△
	Your own palm guide (Note)		△	△	◎

◎ : Recommended ○ : Possible

△ : Possible (test the authentication accuracy in advance)

Note 1) Use With guide mode for the Guide mode.

Without guide mode is also available from the Authentication library V33.

However, if you use the Palm guide for both enrollment and authentication, it is recommended to use With guide mode.

Note 2) Use With guide mode for the Guide mode.

>See> For information on guide mode, refer to "2.4.2 Using the Palm Guide (Guide Mode)".

◆ Not Using the Palm Guide for Authentication in Without guide mode

If you are not using the Palm guide for authentication (operating environment), it is recommended to use the Folding guide when enrolling palm vein data.
However, it is possible to use a different Palm guide as shown in the following table.

		Palm guide for authentication			
		No Palm guide	Folding guide	U guide	Your own palm guide
Palm guide for enrollment	No Palm guide	△ (Note 1)			
	Folding guide	◎	○ (Note 2)		
	U guide				
	Your own palm guide	○			○ (Note 2)

◎ : Recommended ○ : Possible

△ : Possible only when using verification for authentication

Note 1) When using identification for authentication, be sure to use a Palm guide when enrolling palm vein data. Even when enrolling palm vein data for verification, it is recommended to use a Palm guide.

Note 2) Use only when you have difficulties in capturing palm veins (when authentication fails).

>See> For information on Without guide mode, refer to "2.4.2 Using the Palm Guide (Guide Mode)".

Appendix F Power Saving Function of the Sensor Unit

The Sensor is equipped with the power saving function.
The PalmSecure-F Pro sensor enters power saving mode immediately after completing the required processing.
On the other hand, PalmSecure Sensor V2 enters power saving mode when it has not received any processing request for 10 seconds.

Appendix G Comparison of Functions in Each Format Type

The following lists functional differences between each format type.

<table>
<tr><th colspan="4"></th><th>R-format type</th><th>I33-format type</th><th>I-format type</th></tr>
<tr><td colspan="2" rowspan="2">Enrollment format of palm vein data</td><td colspan="2">Non-compressed</td><td>Supported</td><td>Supported</td><td>Supported</td></tr>
<tr><td colspan="2">Compressed</td><td>Not supported</td><td>Not supported</td><td>Supported</td></tr>
<tr><td rowspan="3">Palm vein data size</td><td rowspan="2">For enrollment</td><td>Non-compressed</td><td>16,384 bytes</td><td>15,000 bytes</td><td>3,072 bytes</td></tr>
<tr><td>Compressed</td><td></td><td></td><td>832 bytes</td></tr>
<tr><td colspan="2">For authentication</td><td>8,192 bytes</td><td>8,192 bytes</td><td>4,096 bytes</td></tr>
<tr><td colspan="3">Encryption method</td><td>AES256</td><td>AES256</td><td>AES128 or AES256</td></tr>
<tr><td rowspan="2">Capturing angle</td><td colspan="2">Without guide mode</td><td rowspan="2">0°</td><td rowspan="2">0°</td><td>0°</td></tr>
<tr><td colspan="2">With guide mode</td><td>0°, 90°, 180°, or 270°</td></tr>
<tr><td rowspan="2">Max identification items</td><td colspan="2">Professional Edition</td><td>Up to 5,000 items (5,000 hands for 2,500 people)</td><td>Up to 5,000 items (5,000 hands for 2,500 people)</td><td rowspan="2">Up to 1,000 items (1,000 hands for 500 people)</td></tr>
<tr><td colspan="2">Enterprise Edition</td><td>Up to 200,000 items (200,000 hands for 100,000 people)</td><td>Up to 10,000 items (10,000 hands for 5,000 people)</td></tr>
<tr><td rowspan="2">Matching level</td><td colspan="2">Verification</td><td>5 levels (Highest, High, Normal, Low, Lowest)</td><td>5 levels (Highest, High, Normal, Low, Lowest)</td><td rowspan="2">5 levels (Highest, High, Normal, Low, Lowest)</td></tr>
<tr><td colspan="2">Identification</td><td>3 levels (Normal, Low, Lowest)</td><td>3 levels (Normal, Low, Lowest)</td></tr>
<tr><td colspan="3">Image compression function</td><td>Not supported</td><td>Supported (1 to 1 authentication only)</td><td>Supported (1 to 1 authentication only)</td></tr>
<tr><td colspan="3">Guidance notification message in guide modes</td><td>No difference between With and Without guide modes (Messages for Without guide mode is returned in With guide mode)</td><td>No difference between With and Without guide modes (Messages for Without guide mode is returned in With guide mode)</td><td>Different for With and Without guide modes</td></tr>
<tr><td rowspan="2">Authentication accuracy (for verification)</td><td colspan="2">False rejection rate (FRR)</td><td>1.00% (No retry)</td><td>1.00% (No retry)</td><td>1.00% (No retry)</td></tr>
<tr><td colspan="2">False acceptance rate (FAR)</td><td>0.000001%</td><td>0.00001%</td><td>0.00008%</td></tr>
</table>

	R-format type	I33-format type	I-format type
Approximate verification duration (capture 2 times/Authentication OK at capture 1 time) (Intel® Core i5 3.60GHz) Excluding capturing time	0.15 sec.	0.15 sec.	0.03 sec.
Approximate identification duration (capture 2 times/Authentication OK at capture 1 time/Multi-processing is "2") (Intel® Core i5 3.60GHz) Excluding capturing time	0.4 sec. (10,000 hands)	6.2 sec. (10,000 hands)	0.4 sec. (1,000 hands)
Remark	I33-format or I-format of palm vein data cannot be authenticated with R-format.	R-format or I-format of palm vein data cannot be authenticated with I33-format.	R-format or I33-format of palm vein data cannot be authenticated with I-format.

Appendix H Comparison of Each Authentication Library

The following lists the functional differences between each Authentication library (Professional Edition).

Function	Authentication library for Windows(x64) Windows(x86) Linux(x64)	Authentication library for Linux(arm64) Linux(armhf)	Authentication library for Android(Armv8-A)
Sensor	・PalmSecure-F Pro sensor ・PalmSecure Sensor V2	・PalmSecure-F Pro sensor *Excluding mouse type sensor	・PalmSecure-F Pro sensor *Excluding mouse type sensor
Format type	・R-format type ・I33-format type ・I-format type	・R-format type	・R-format type
Connecting multiple sensors	Supported	Supported	Not supported
Default number of continuous capturing time at authentication	Capture 2 times	Capture 1 time	Capture 1 time
High-power mode	Supported	Supported	Not supported
Number of identification threads for multiple processing	Default: 2 thread Max: 128 thread	Default: 1 thread Max: 8 thread	Default: 1 thread Max: 8 thread
Provided functions (methods)	—	PvAPI_Sense is not supported	PvAPI_Sense is not supported
Authentication library firmware update function	Available	Available	Not available
Auto-recovery function from the hibernation state	Available	Available	Not available

◆ Previous Revision History

Revision	Issued Date	Revised Page	Modification Details
Rev. 1	Jul 2020	Entire document	Newly created
Rev. 1.1	Oct 2020	Entire document	• Added descriptions concerning the Sample source for C language.
Rev. 2	Jul 2021	Entire document	• Modified descriptions according to support for 100,000 items for identification when using Enterprise Edition in R-format type.
		Entire document	• Added descriptions concerning Authentication library for Arm (Linux(armhf) / Linux(arm64) / Android(Armv8-A)).
		Page 10 to 11	• Added descriptions concerning support for .NET 5 in “1.4.3 Sample Interface” and “1.4.4 Sample Application”.
		Page 18 to 21	• Modified the following descriptions in “2.2.1 Windows and Linux(x64)” in “2.2 Hardware and Software Requirement”. ・Explanation in CPU (Note 1). ・Version of CentOS in OS (Note 4).
		Page 30	• Modified the following descriptions for R-format type in “2.4.1 Format Type”. ・Max identification items ・Authentication accuracy
		Page 51 Page 53	• Modified cautions for authentication result score notification function in “2.7.2 Verification Sequence”.
		Page 62	• Modified the example for approximate false acceptance rate of un-enrolled users in identification in “2.8.3 3 Identification by Un-enrolled Users”.
		Page 94	• Added descriptions concerning support for .NET 5 in “4.2.1 Additional/Modified Functions in PalmSecure SDK V02L03”
		Page 98	• Modified the tested OSes in “4.2.2.1 Notes on Migrating to the Authentication Library V34”.
		Page 125	• Modified the tested OSes in “◆ Windows(x86) / Windows(x64) / Linux(x64)” in “Appendix B Tested OSes”.
		Page 135 to 136	• Modified the following descriptions for R-format type in “Appendix G Comparison of Functions in Each Format Type”. ・Max identification items ・Authentication accuracy ・Approximate identification duration

Revision	Issued Date	Revised Page	Modification Details
Rev. 2	Jul 2021	Page 137	• Added “Appendix H Comparison of Each Authentication Library”.
Rev. 2.1	Mar 2022	Page 18 to 21 Page 98 Page 125	• Added Windows 11 and Windows Server 2022 to tested OS.


PalmSecure