

SDK/J Authentication Package v1.0 ユーザーズガイド

SDK/J Authentication Package Version:1.0



重要

Copyright © 2011 Ricoh Co., Ltd.

ご注意

1. 本書の内容に関しては、将来予告無しに変更することがあります。
2. 本書の一部または全部を無断で複写、複製、改変、引用、転載、配布することはできません。
3. 本書および本書の対象となるサンプルコードについて、当社は、何らの保証もいたしません。
本書および本書の対象となるサンプルコードを使用したことにより生じるお客様の損害、逸失利益、または第三者からのいかなる請求につきましても、当社は一切その責任を負いかねますので、予めご了承下さい。
4. 商標について
PostScript、Acrobatは、アドビシステムズ社の各国での登録商標または商標です。
Windowsは、米国Microsoft Corporationの米国及びその他の国における登録商標です。
UNIXは、X/Openカンパニーリミテッドがライセンスしている米国ならびに他の国における登録商標です。
Red Hatは、Red Hat, Inc.の米国およびその他の国における商標または登録商標です。
Java、JVM (CVM)、CDCは、すべてOracle Corporation 及びその子会社、関連会社の米国及びその他の国における登録商標です。
Eclipseは、eclipse.orgの米国およびその他の国における商標または登録商標です。
OSGi (TM)は、The Open Services Gateway Initiativeの米国およびその他の国における商標または登録商標です。
Apacheは、The Apache Software Foundationの米国およびその他の国における商標または登録商標です。
その他の製品名、名称は、各社の商標または登録商標です。

目次

1. 本書の目的	2
2. 対象読者	3
3. 動作環境	4
4. アーキテクチャ	5
5. Authentication Packageの機能.....	7
5.1. Smart Card Access	7
5.2. Device Access	7
5.3. Network Authentication	8
5.4. Panel Service	8
5.5. Authentication Service	8
6. カードを利用した認証について.....	9
6.1. カードリーダードライバの対応	10
6.2. その他の対応	10
6.3. カードのみ対応	11
7. カードによるユーザ認証対応.....	12
7.1. 拡張認証対応	13
7.2. 拡張認証 + カスタム認証対応	15
8. サポートしているカードリーダーについて	17
8.1. PC/SC準拠のスマートカードリーダー.....	17
8.2. その他のカードリーダー	18
変更履歴	19

1. 本書の目的

「SDK/J Authentication Package v1.0 ユーザーズガイド」はスマートカードなどの外部デバイスや外部サーバーを使用した認証処理を簡素化するために開発されたフレームワークであるSDK/J Authentication Package v1.0を使用するためのガイドです。

SDK/J Authentication Package v1.0は、スマートカードなどの外部デバイスへのアクセスやデータの取得、外部サーバーとの認証機能、SDK/Jからユーザ認証を利用する機能を提供します。このガイドには、これらの技術に関する説明と、SDK/J Authentication Package v1.0を用いたアプリケーションを作成する上で開発者が準拠すべきプロセスの詳細が述べられています。

2. 対象読者

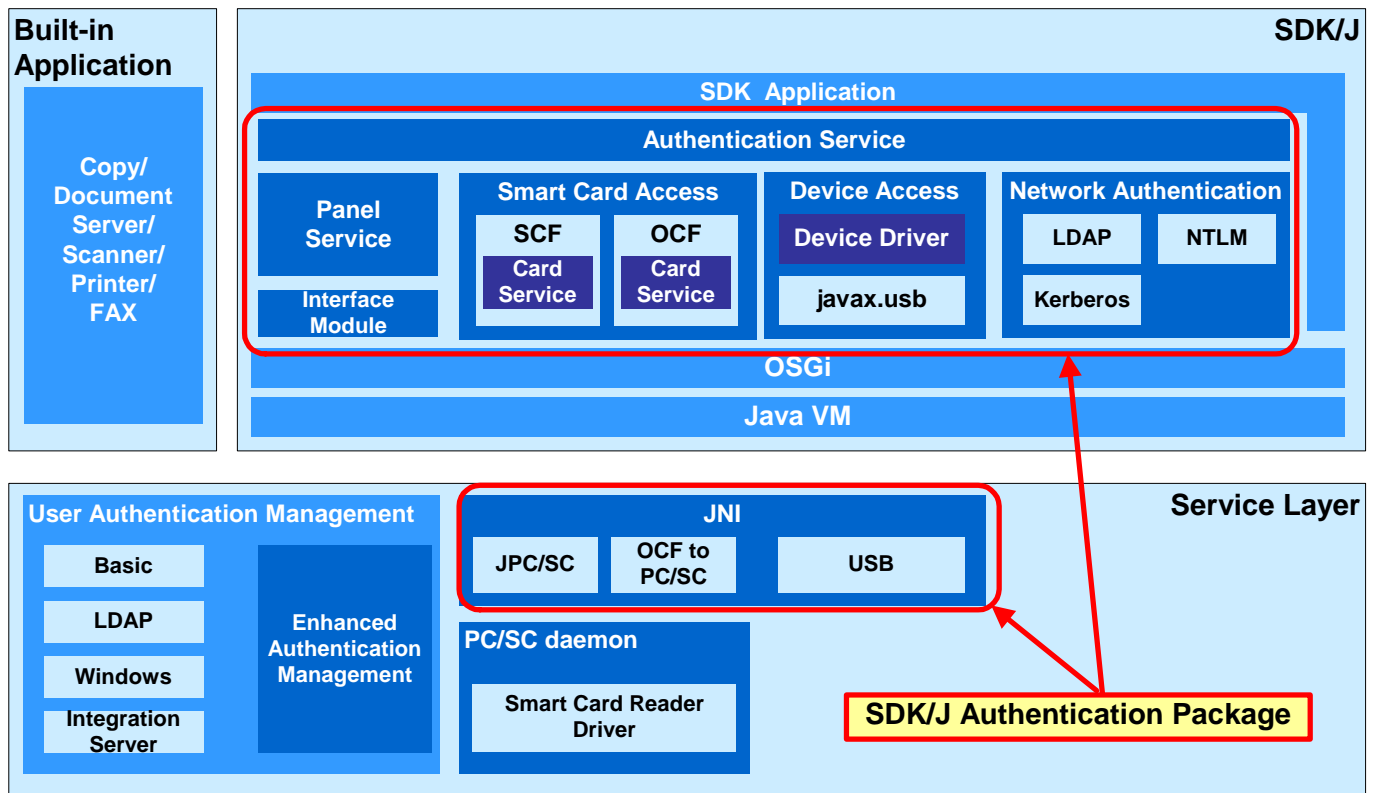
『SDK/J Authentication Package v1.0 ユーザーズガイド』には、SDK/J Authentication Packageを利用したアプリケーションの開発者向けの情報が掲載されています。したがって、プログラマ、サービスの導入担当者はこのガイドを読む必要があります。このガイドでは、次の知識を必要とします。

- Javaプログラミング言語の基礎知識
- SDK/Jの基礎知識

3. 動作環境

- SDK/J がインストール済みで、正常に動作していること
 - SDK/J Authentication Package を使用するための設定がされていること
- 設定に関しては、「SDK/J Authentication Package 設定ガイド」を参照してください

4. アーキテクチャ



Service Layer

JNI

以下の3つのJNIを提供します。

JPC/SC

当JNIはPC/SC daemonの提供するスマートカードへのアクセス機能をSDK/Jから使用するためのインターフェースです。SDK/JのSCF(SmartCardFramework)を使用する場合、当JNIを使用します。

OCFtoPCSC

当JNIはPC/SC daemonの提供するスマートカードへのアクセス機能をSDK/Jで使用するためのインターフェースです。SDK/JのOCF(OpenCardFramework)を使用する場合、当JNIを使用します。

USB

SDK/JからUSBポートへのアクセスを行うJNIです。JSR80に準拠したjavax.usbをサポートしています。

PC/SC daemon

スマートカードへのアクセス機能および、スマートカードリーダーのドライバを提供します。

User Authentication Management

本体システムのユーザ認証を管理しているモジュールです。Basic認証、LDAP認証、Windows認証、統合サーバー認証を提供します。

Enhanced Authentication Management

SDK/J Authentication PackageのPanelServiceから、本体システムのユーザ認証へのログイン/ログアウトを行うためのI/Fとなるモジュールです。

Built-in Application

コピー、スキャナ、FAX、プリンタ、ドキュメントボックスなどの本体のアプリケーションを表します。

SDK/J

JavaVM, OSGi

SDK/Jで標準サポートしているSDK/J Platformを表します。

Authentication Package

SDK/Jで提供する認証ライブラリを表します。これはオプションパッケージとして提供されます。

Smart Card Access

スマートカードへアクセスするためのライブラリを表します。PC/SC準拠のUSBカードリーダーが使用できます。

Device Access

USBデバイスへアクセスするためのライブラリを表します。USBデバイスへのアクセスを行うには、javax.usbを使用してDevice Driverを実装する必要があります。

Network Authentication

LDAP、Kerberos、NTLMの認証を提供します。

Panel Service

Enhanced Authentication Managementの提供するI/Fを利用して、SDK/JアプリケーションからUser Authentication Managementへのログイン/ログアウトを行う機能を提供します。

InterfaceModule

Panel ServiceとEnhanced Authentication ManagementのI/Fとなるモジュールです。

Authentication Service

SDK Applicationへ提供する抽象的なサービスを表します。Card Access、Network Authentication、Panel Serviceを自由に組み合わせてSDK Applicationに認証機能を提供します。

5. Authentication Packageの機能

5.1. Smart Card Access

スマートカードへアクセスするためのライブラリを表します。

SCF(SmartCard Framework)

PC/SCをJavaで使えるようにしたインターフェースであるJPC/SC上で動作する、スマートカードアクセスのためのFrameworkです。ISO 7816、ISO 14443に準拠したスマートカードをサポートします。

詳細は「SmartCard Framework開発者ガイド」を参照してください。

OCF(OpenCard Framework)

The OpenCard Consortiumが提供するFrameworkです。ISO 7816、ISO 14443に準拠したスマートカードをサポートします。

詳細は「OpenCard Framework開発者ガイド」を参照してください。

5.2. Device Access

USBデバイスへアクセスするためのライブラリを表します。使用するUSBデバイスのドライバを、javax.usbを使用して実装してください。

AuthenticationPackage では、javax.usbのサンプルとしていくつかのUSBカードリーダーのサンプルドライバを提供しています。

上記 Smart Card Access 、Device Access のどちらを使用するかは、使用するUSBデバイスに依存します。詳細は、「8. サポートしているカードリーダーについて」を参照ください。

USBデバイスのタイプ	実装方法	備考
PC/SC準拠USBカードリーダー	SCFまたはOCFを使用します。	SCFとOCFの併用は不可
上記以外	javax.usbでDriverを実装する必要があります。	

5.3. Network Authentication

LDAP、KerberosはSDK/JのOptionPackageとしてSunMicrosystemsから提供しているパッケージと同様のインターフェースを提供します。LDAPを使用する場合、JAAS、JNDIが必要になります。またKerberosを使用する場合はJCEが必要です。これらのライブラリは、SDK/Jに同梱されます。各パッケージに関する詳細はSunMicrosystemsのサイトを参照してください。

また、NTLMはJCIFS(<http://jcifs.samba.org>)のオープンソースを利用することが可能です。NTLMを使用する場合、JCIFSのサイトからダウンロードして使用してください。

5.4. Panel Service

本体側でUser Authentication Manegement,Enhanced Authentication Manegementを有効にした場合、当機能が利用可能です。操作パネルのアンロック/ロックを行います。

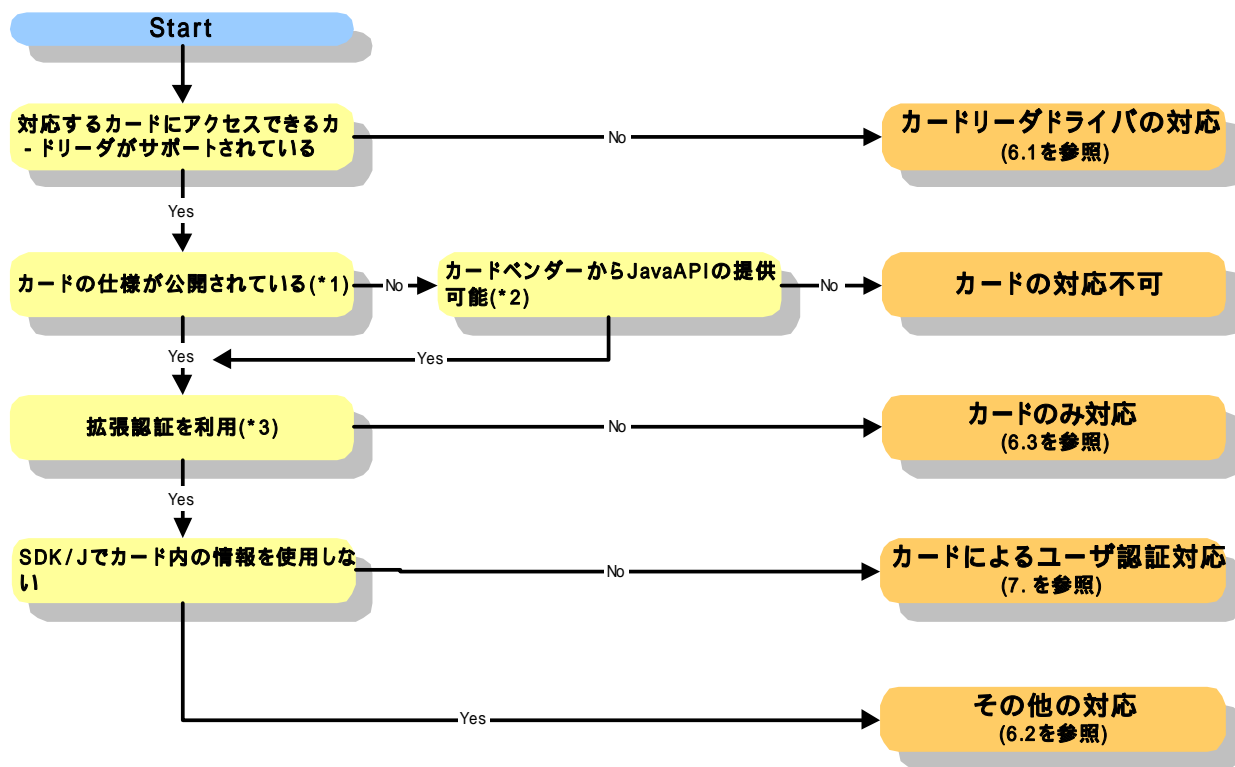
詳細は「Panel Service ユーザーズガイド」、「Panel Service 開発者ガイド」を参照してください。

5.5. Authentication Service

SDK Applicationへ提供する抽象的なサービスで、認証機能を隠蔽してSDK Applicationに提供することを目的としています。Card Access、Network Authentication、Panel Serviceを自由に組み合わせてSDK Applicationに認証機能を提供することが可能です。特に隠蔽する必要がなければ、当サービスを実装する必要はありません。

6. カードを利用した認証について

カードを利用した認証を行う場合、以下のフローを参考にしてください。



(*1) カードの情報を取得するにはカードの仕様、及び取得するデータのフォーマットが必要です。

(*2) カードベンダーからカードのデータをアクセスするインターフェースがJavaのAPIで公開が可能な場合、SDK/Jで対応することができます。

(*3) 本体機能の拡張認証を表します。拡張機能とはシステム本体側でカードを利用した認証を行うことを表します

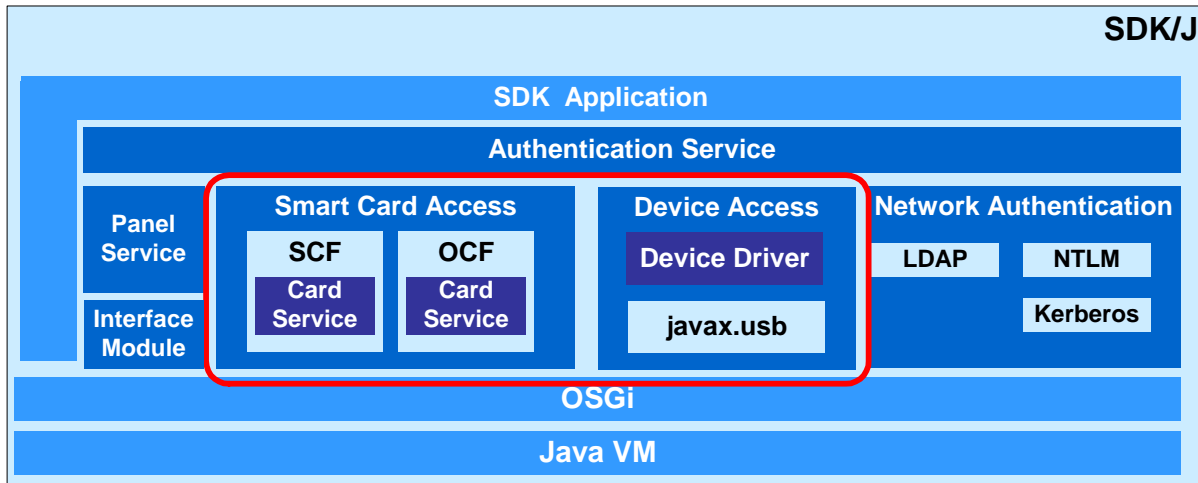
6.1. カードリーダードライバの対応

詳細は、「8. サポートしているカードリーダーについて」を参照してください。

6.2. その他の対応

詳細はRiDPiにお問い合わせください。

6.3. カードのみ対応



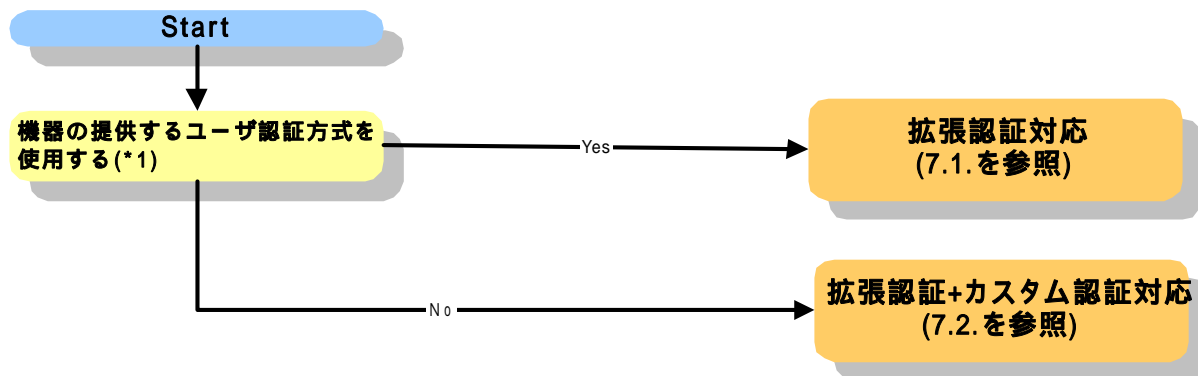
赤枠内のSCF, OCF, javax.usbのいずれか1つのアクセス方法を選定します。

SCF、OCFでは、サンプルとしてJavaCard、CryptoflexのCardServiceを提供しています。

javax.usbを使用したDevice Driverのサンプルとしては、いくつかのUSBカードリーダーのドライバサンプルを提供しています。

7. カードによるユーザ認証対応

カードを利用したユーザ認証を行う場合、「6. カードを利用した認証について」で示したフローに引き続き、以下のフローを参考にしてください。

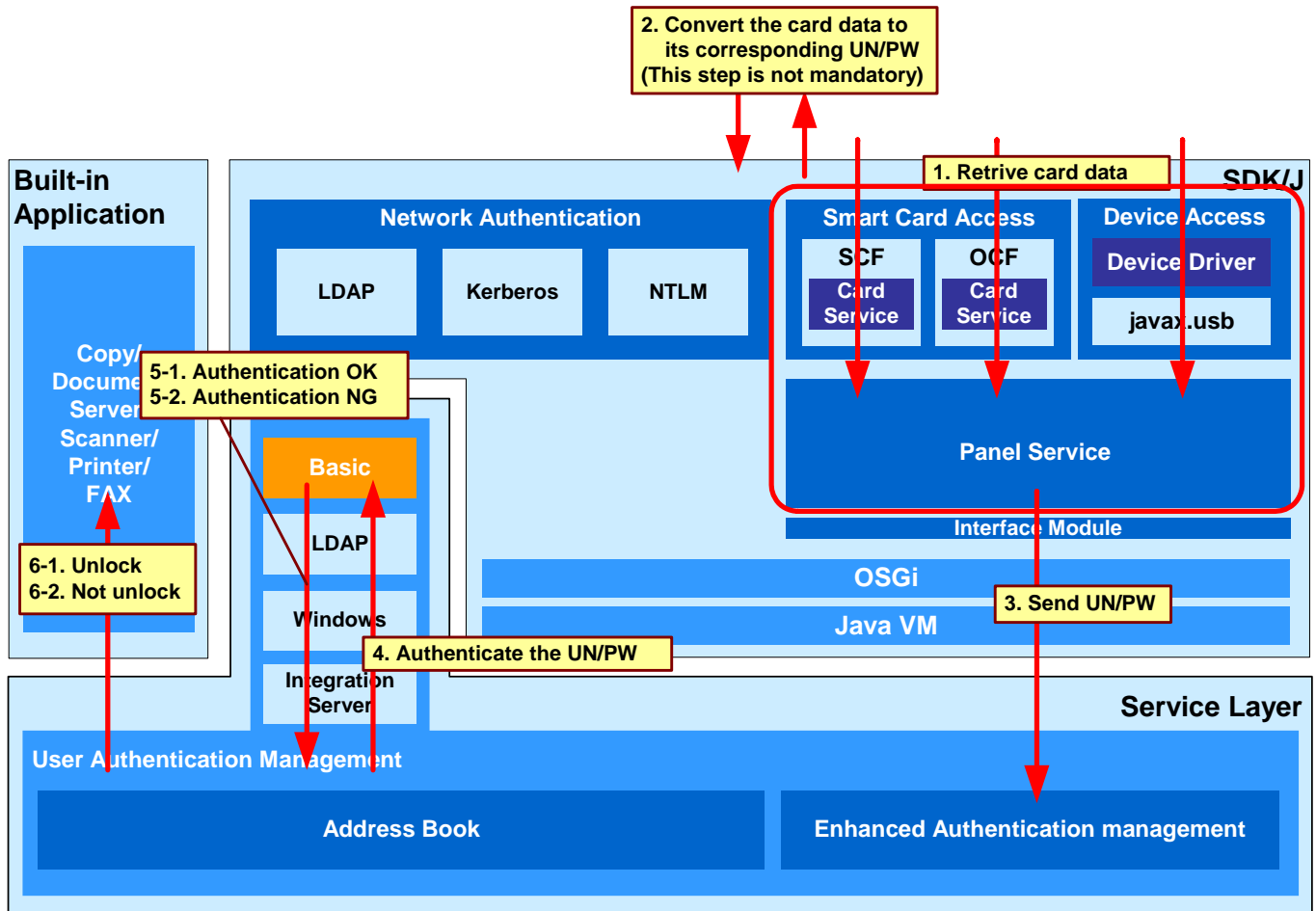


(*1)機器の提供するユーザ認証は、以下のいずれかになります。詳細は、各機器のユーザガイドを参照ください。

- Basic認証
- LDAP認証
- Windows認証
- 統合サーバー認証

これらの認証方式以外のユーザ認証処理を行う場合は、SDK/Jの認証カスタマイズ機能で実装したカスタム認証との連携が必要となります。SDK/Jの認証カスタマイズ機能は機器のユーザ認証をSDK/Jで実装することができる機能です。詳細は、SDK/Jのドキュメントを参照してください。

7.1. 拡張認証対応



拡張認証を使用してユーザ認証にログインユーザ名・ログインパスワードを入力する処理を実装します。

赤枠内は最低限実装する必要があるモジュールを示しています。

なお、このケースでは、機器にPanelService使用のための設定が必要です。

1. Retrieve card data

Smart Card AccessまたはDevice Accessを使用して、カードから情報を取得します。「SmartCard Framework開発者ガイド」、「OpenCard Framework開発者ガイド」、「javax.usb開発者ガイド」を参照ください。

2. Convert the card data to its corresponding UN/PW

カードから取得した情報をそのままユーザ認証のログインユーザ名・ログインパスワードとして使用しない場合、カード情報をログインユーザ名・ログインパスワードに変換します。例えば、LDAPサーバにカードのシリアル番号を送信し、ユーザ名を取得する、などが考えられます。

3. Send UN/PW

PanelService を使用して、ユーザ認証にログインユーザ名・ログインパスワードを送信します。詳細は、「PanelService開発者ガイド」を参照ください。

4. Authenticate the UN/PW

機器に設定された認証方式で、PanelServiceから入力されたログインユーザ名・ログインパスワードの認証が行われます。

5. Authentication OK/NG

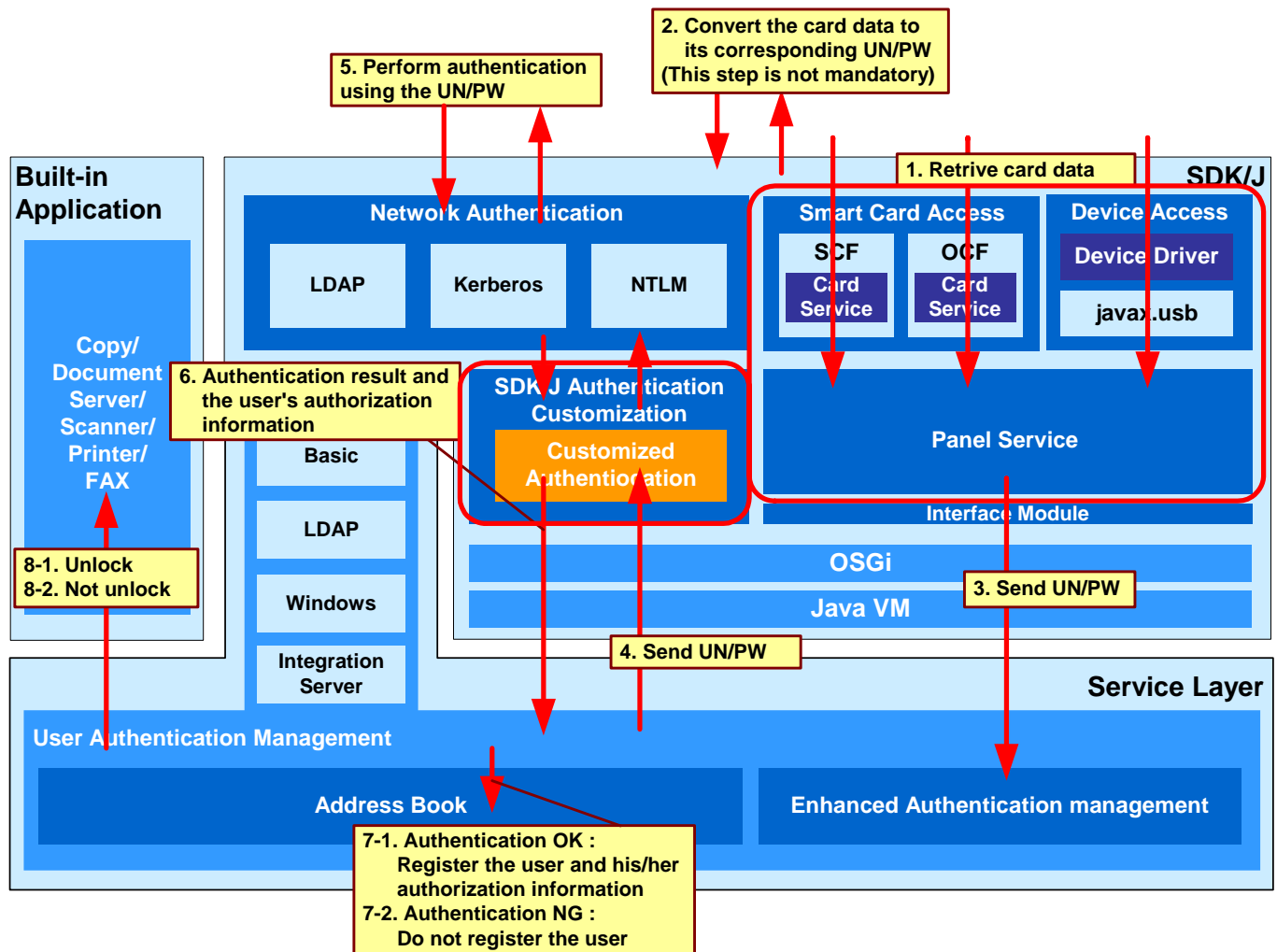
機器のユーザ認証モジュールにおいて、ユーザ認証結果が判断されます。

6. Unlock/not unlock

ユーザ認証がOKの場合、機器の画面ロックが解除されます。ログイン中のユーザは、アドレス帳に登録されている利用権限の範囲内で機器を使用することが出来ます。

そうでない場合、画面ロックは解除されません。

7.2. 拡張認証 + カスタム認証対応



拡張認証を使用してユーザ認証にログインユーザ名・ログインパスワードを入力する処理と、そのログインユーザ名・ログインパスワードを使用してユーザ認証を行う処理を実装します。

赤枠内は最低限実装する必要があるモジュールを示しています。

なお、このケースでは、機器にPanel ServiceおよびSDK/Jカスタム認証を使用するための設定が必要です。

1 ~ 3.

「7.1. 拡張認証対応」と同様となります。

4. Send UN/PW

SDK/Jの認証カスタマイズ機能を使用して実装した認証アプリケーションに、PanelServiceから入力されたログインユーザ名・ログインパスワードが渡されます。

5. Perform authentication using the UN/PW

認証アプリケーション内で、ログインユーザ名・ログインパスワードを使用してユーザ認証を行います。必要に応じて、Network Authenticationなどのライブラリが使用できます。また、認証がOKの場合は、そのユーザがロ

グイン後に使用できる機能の利用権限を設定します。

6. Authentication result and the user's authorization information

認証アプリケーションから認証結果およびユーザの権限情報が返されます。

7. Address book update

ユーザ認証がOKの場合、ユーザ情報および認証アプリケーションが設定したユーザの利用権限をアドレス帳に登録します。

ユーザ認証がNGの場合、アドレス帳への登録は行われません。

8. Unlock/not unlock

ユーザ認証がOKの場合、機器の画面ロックが解除されます。ログイン中のユーザは、上記「7. Address book update」にてアドレス帳に登録した利用権限の範囲内で機器を使用することが出来ます。

そうでない場合、画面ロックは解除されません。

8. サポートしているカードリーダーについて

8.1. PC/SC準拠のスマートカードリーダー

PC/SC daemonではMUSCLE projectにより提供されている以下のライブラリを使用しています。

- pcsc-lite 1.2.9 beta 10
- ccid 1.1.0

AuthenticationPackageで動作確認しているカードリーダーは以下の通りです。

Contact Type

Compliant	Supported Card Readers		For Information
	Manufacturer	Model	
ISO7816	Gemalto	GemPC Twin	http://www.gemalto.com/
		Reflex USB v3	
		GemPC Key (product id 0x3438)	
	Omnikey	CardMan 3121	http://www.omnikey.com/
	SCM	SCR 331	http://www.scmmicro.com/
	Microsystems	SDI 010 (Contact slot only)	
	C3PO	LTC31 (product id 0x0006)	http://www.c3po.es/

使用したいカードリーダーが上記リストにない場合は、RiDPにお問い合わせください。

pcsc-lite 1.2.9 beta10 および ccid 1.1.0 に関しては、以下のURLを参照ください。

<http://pcsc-lite.alioth.debian.org/>

また、ccid 1.1.0 のソースコードは、以下のURLより入手可能です。

<http://anonscm.debian.org/viewvc/pcsc-lite/tags/ccid/rel-1.1.0/>

8.2. その他のカードリーダー

javax.usbを使用してデバイスのドライバを実装することで、サポートが可能です。詳細は「javax.usb開発者ガイド」を参照ください。

AuthenticationPackageでは以下のカードリーダーのサンプルドライバを提供しています。

Type	Compliant	Card Readers		More Information
		Manufacturer	Model	
Contact-less	125kHz Proximity	RFIDeas, Inc.	pcProx USB >RDR-6081AKU >RDR-6281AKU >RDR-6381AKU >RDR-6N81AKU	http://www.rfideas.com/
	13.56MHz	RFIDeas, Inc.	Air ID Enroll USB (Mifare) >RDR-7581AKU	http://www.rfideas.com/
			RFID1356i Enroll USB (iClass, Mifare) >RDR-7081AKU	
		Interflex	IF 72 (Legic)	http://www.interflex.de/
Contact	Magstripe	Tysso	TMSR-33	http://www.tysso.com/

変更履歴

Ver. 1.0_R103	8.サポートしているカードリーダーについて 8.1. PC/SC準拠のスマートカードリーダー ccid 1.1.0 のソースコードのURLリンクを見直し
Ver. 1.0_R102	SDK/J 開発キット R1.02 同梱のドキュメントをベースに作成 “8.サポートしているカードリーダーについて” のリーダー一覧に含まれるURL リンクを見直し