資料1

生体認証活用の実現方式

2021年3月3日

1．用語・略称の定義

項番	用語・略称	内容
1	PIN	・知識認証で使用する数字のみの文字列。暗証番号とも言う。
2	パスワード	・知識認証で使用する数字以外を含む文字列。
3	利用者用PIN	・利用者証明用電子証明書のPIN（4桁の数字）
4	署名用パスワード	・署名用電子証明書のパスワード（6～16桁の英数字）
5	利用者用証明書	・利用者証明用電子証明書
6	利用者用秘密鍵	・利用者証明用の秘密鍵
7	署名用証明書	・署名用電子証明書
8	署名用秘密鍵	・署名用の秘密鍵
9	カード	・マイナンバーカード
10	スマホ	・Androidスマートフォン
11	Secure Lock Screen	・画面ロックを設定して、スマホの電源を入れたり、画面を復帰させる際に、PIN、パターン、パスワードなどによって画面ロックを解除する仕組み。近年多くのスマホでは指紋で画面ロックを解除可能。
12	プライマリ認証	・Secure Lock Screenで利用できる、最も高い認証レベルに位置付けられる認証方法。 ・端末ローカルで認証するPIN/パスワード/パターンのことを言う。
13	セカンダリ認証	・Secure Lock Screenで利用できる、プライマリ認証の次に高い認証レベルに位置付けられる認証方法。 ・生体認証のことを言う。

2．森山委員のご提案（第4回検討会、資料2）を受けて

提案1-1: Android OSが提供するAPIとマイナンバーの機能のスマートフォンへの搭載における生体認証の利活用に向けた実現方法について

Androidスマートフォンに具備されている生体認証の機能は、アプリケーション開発者にBiometricPromptAPIが提供されようになったAndroid9以降は特に以前と比較して成熟している。CDDによって要件が明確になり、性能測定・評価についても定められている。そこで、マイナンバーカードの機能のスマートフォンへの搭載にあたっては、生体認証の性能について強・Strong/Class3を使用するため“BIOMETRIC_STRONG”を指定することを前提に、既に議論して来た「ローカルPIN」（利用者用PIN）による認証に加えて、生体認証（BiometricPromptAPI）の結果を使えるようにしてはいかがでしょうか？

提案1-2:生体認証の利活用に際し、ローカルPIN導入の課題と使い勝手の改善に資する画面ロック解除の利活用について

マイナンバーカードの機能のスマートフォンへの搭載にあたっては、マイナンバーカードに設定する署名用パスワード、利用者用PINに加えて、GP-SEに「ローカルPIN」（利用者用PIN）を設定する必要があると認識している。この「ローカルPIN」（利用者用PIN）を利用者に別途覚えていただくことについて、使い勝手の観点から懸念が指摘されている。この解決のため、スマートフォンにおける生体認証が「セキュアな画面ロック解除（Secure Lock Screen ）」におけるセカンダリー認証の位置づけであることを勘案し、プライマリー認証である画面ロック解除のために設定するPIN/パスワード/パターンも利活用できるようにしてはいかがでしょうか？

※上記について本資料で示す「1．用語・略称の定義」に基づき一部修正しています。

・利用者用PINによる認証と生体認証（BiometricPromptAPI）が併用可能な方式とする。
・生体認証に加えて、プライマリ認証であるPIN/パスワード/パターンを活用していく。

3．生体認証活用の実現方式

生体認証活用の実現方式における主要ポイントを以下に示す。

（1）外部認証（External Authenticate）の導入 【参考1】
・生体認証の成功をトリガとして外部認証を実行する。
・従来、利用者用PINの認証を電子証明書の読出し、署名計算のアクセス権としてきたが、利用者用PINの認証に加えて外部認証を電子証明書の読出し、署名計算のアクセス権とすることで、利用者用PINの認証と外部認証が併用できるよう設計する。

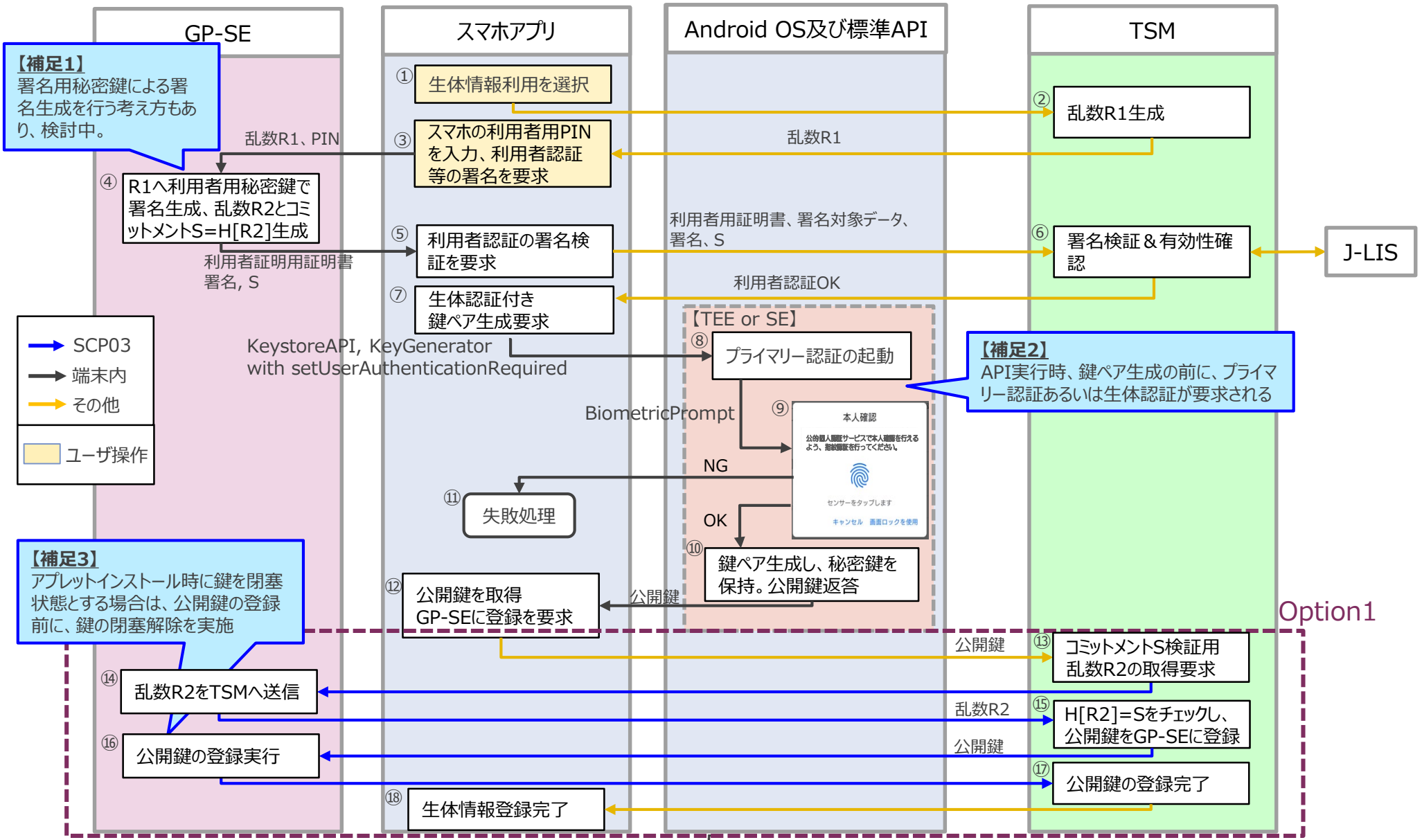
（2）生体認証に連動させた暗号オブジェクト利用
・AndroidのKeystore APIにより外部認証に必要な鍵ペア生成及び暗号化処理を行う。
・Keystore APIの活用方法として、setUserAuthenticationRequired（true）を設定する。これにより、生体認証が鍵ペア生成及び暗号化処理の実行条件となり、OSレベルで生体認証が成功しないと鍵ペア生成及び暗号化処理が実施できないメカニズムとすることができる。【参考2】【参考3】
・また、setUserAuthenticationRequired（true）の設定によって、生体認証だけでなくプライマリ認証であるPIN/パスワード/パターンも許容することになる。

詳細な処理フローを次頁以降に示す。
〇生体認証＋外部認証（アクティベート時）の詳細フロー
・Option1：外部認証用の公開鍵をTSMから書込む方式
・Option2：外部認証用の公開鍵をスマホアプリから直接書込む方式
〇生体認証＋外部認証（認証時）の詳細フロー

【現在検討中の課題】
・Option1、Option2をGP-SEへのデータ登録に関するポリシー、実装効率の観点で比較検討中。

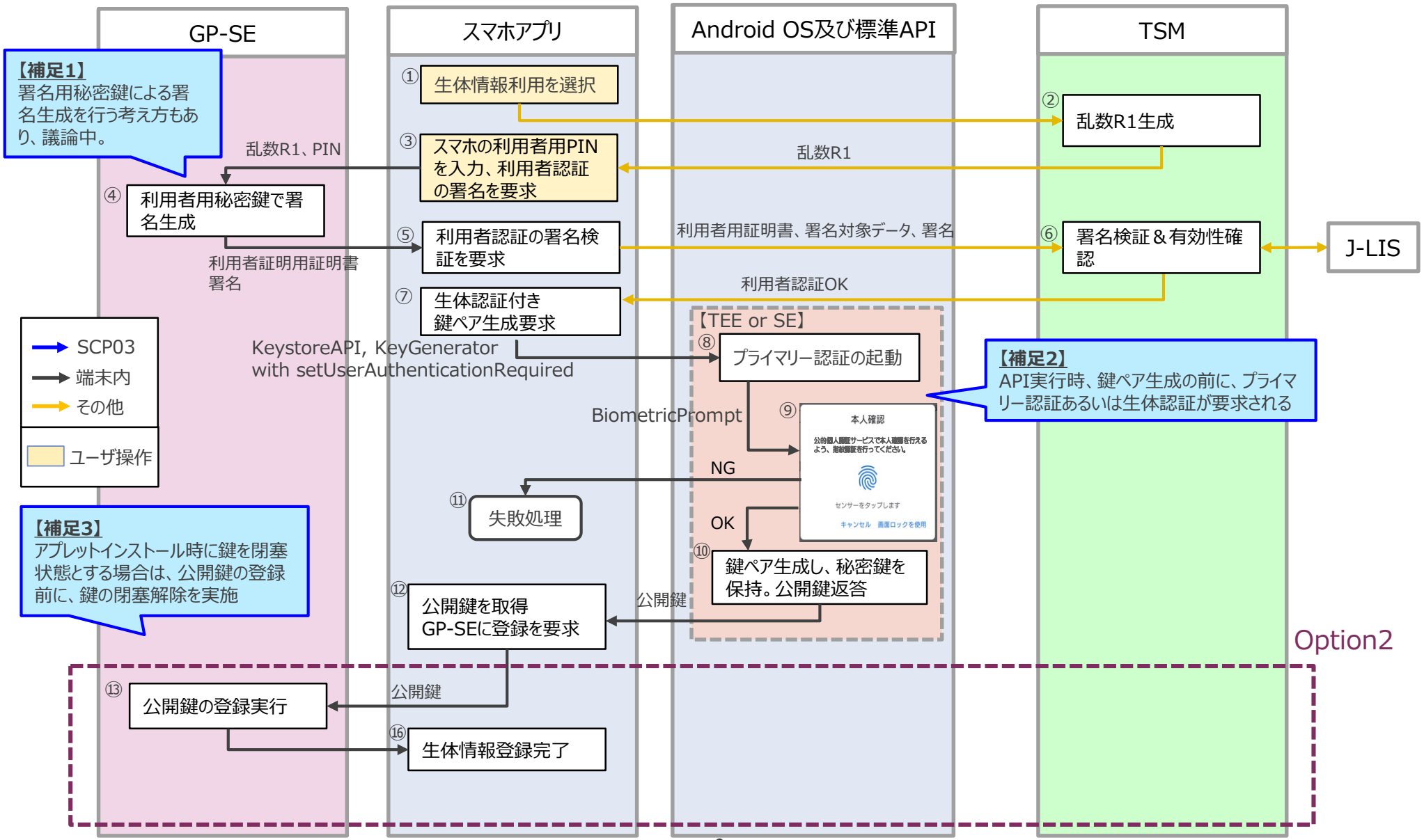
4. 生体認証＋外部認証（アクティベート時）の詳細フロー　Option1

・生体認証の利用を開始するためのフローを以下に示す。



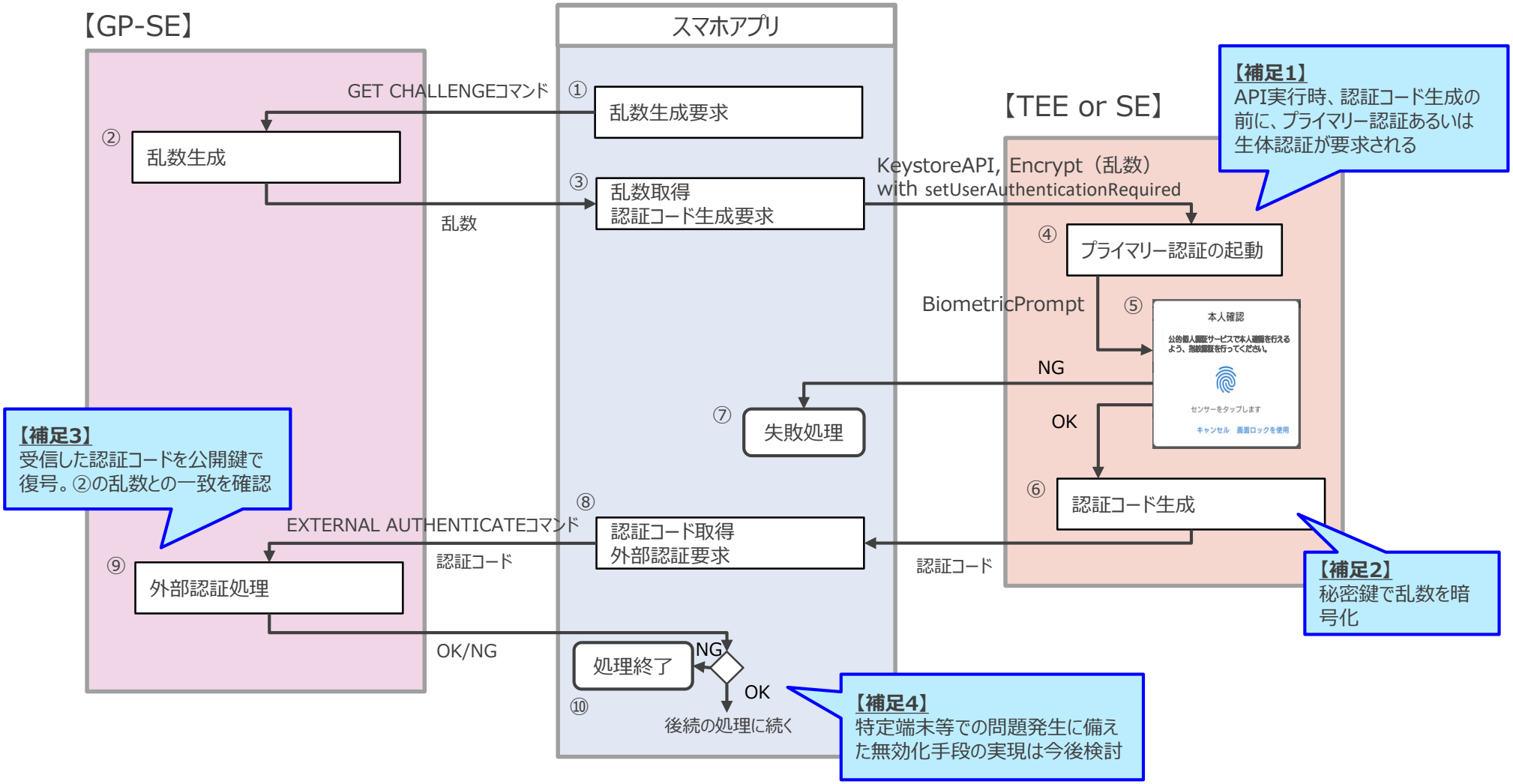
5. 生体認証＋外部認証（アクティベート時）の詳細フロー　Option2

・生体認証の利用を開始するためのフローを以下に示す。



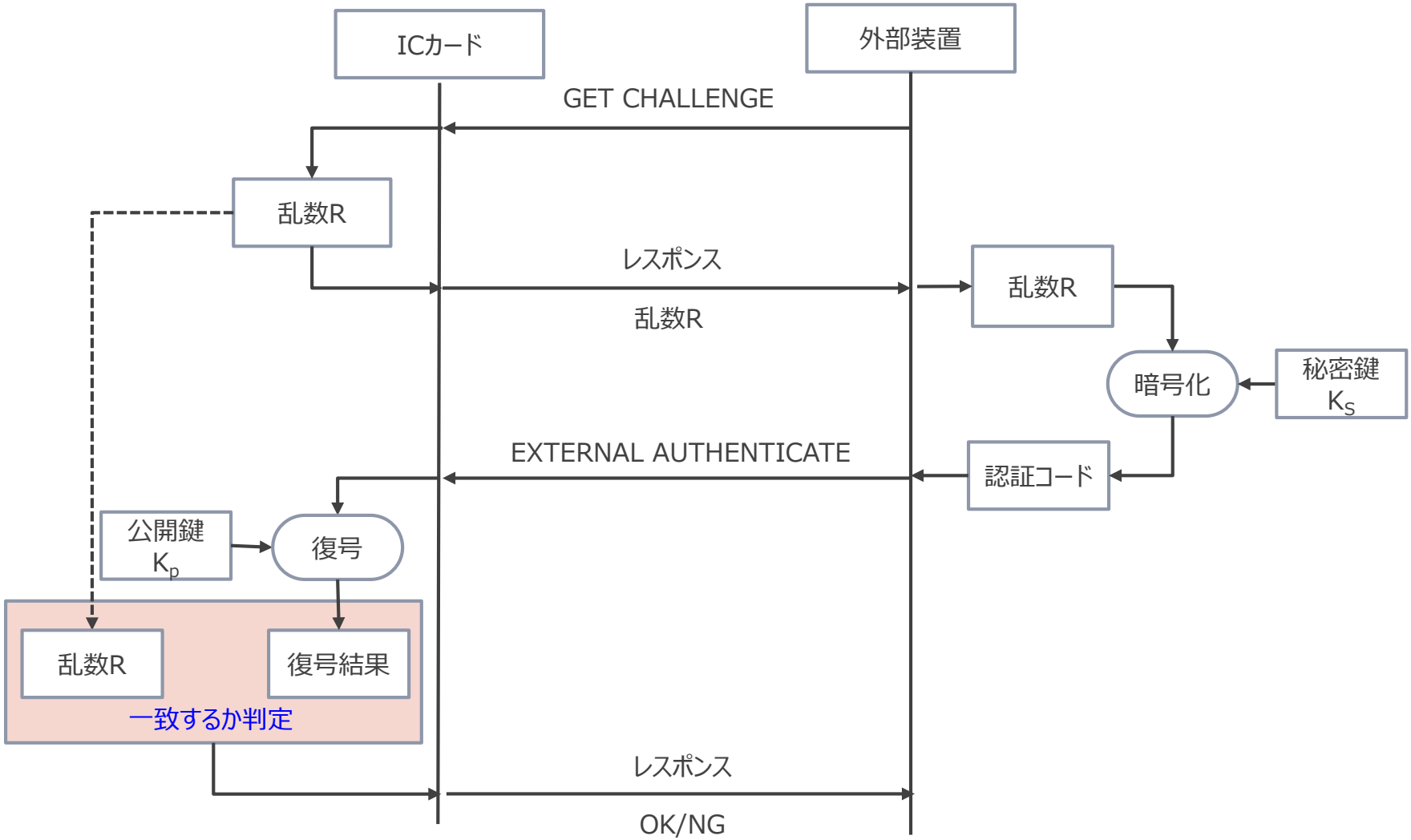
6．生体認証＋外部認証（認証時）の詳細フロー

・認証実行時のフローの主要部分を以下に示す。
・生体認証が成功すると、TEE（or SE）とGP-SEの間で外部認証を実施。GP-SE内には外部認証の認証結果が保持される（外部認証の認証結果が後続で実施される電子証明書の読出し、署名計算のアクセス権となる）。



【参考1】外部認証の仕組み

・外部認証とは、ICカードから見て外部装置が正当な装置（アクセスを許可した装置）であることを確認する手段のことを言う。
・外部装置は秘密鍵K_Sを保持し、ICカードは公開鍵K_pを保持するものとする。



【参考2】暗号オブジェクトで生体認証プロンプトを使用する方法と理由①

https://medium.com/androiddevelopers/using-biometricprompt-with-cryptoobject-how-and-why-aace500ccdb7

キーストアシステムとAndroid上の生体認証システムの両方が、特に材料と機密性の高い操作を安全な空間(TEE / SE)に保つため、独自のセキュリティ対策を提供します。しかし、アプリに関連付けられているSecretKeyをロック解除するために生体認証が必要な場合、データの安全性はさらに高まります。これは、トランザクション全体が安全な領域(TEE/SE)で行われるためです。それでも、生体認証はデータを暗号化するプロセスの一部に過ぎないことに注意することが重要です。単にユーザーが存在することを確立するだけです。

生体認証システムとキーストアシステムが連携してユーザーのデータを保護する方法は次のとおりです。

1. 開発者は、 setUserAuthenticationRequired(true)を設定して、シークレットキーにアクセスするために生体認証を要求するように要求します。
2. アプリがSecretKeyに関連付けられているデータを要求すると、ユーザーは有効な生体認証資格情報を入力するように求められます。
3. 生体認証センサーは TEE と安全に通信するので、フレームワークもサードパーティ製アプリもトランザクションに対して確実に行なえないです。したがって、ユーザーが指紋センサーをタップすると、材料はTEEによって直接読み取られます。
4. 生体認証資格情報が登録されている資格情報と一致する場合、TEE の生体認証コンポーネントはハードウェア認証トークン (HAT) を提供します。HAT には HMAC が含まれており、メッセージの整合性と信頼性の検証に使用できます。
5. TEE/SE およびキーマスターの生体認証コンポーネントは、また、TEE/SE 内で、秘密鍵を共有します。したがって、フレームワークがこの HAT をキーストア システムに転送すると、Keymaster は HAT の信頼性と整合性を検証し、適切なキーのロックを解除できます。
6. 生体認証フレームワークは、アプリのonAuthenticated()コールバックを呼び出します。

※自動翻訳にて翻訳したものであること、ご配慮ください。

【参考3】暗号オブジェクトで生体認証プロンプトを使用する方法と理由②

https://medium.com/androiddevelopers/using-biometricprompt-with-cryptoobject-how-and-why-aace500ccdb7

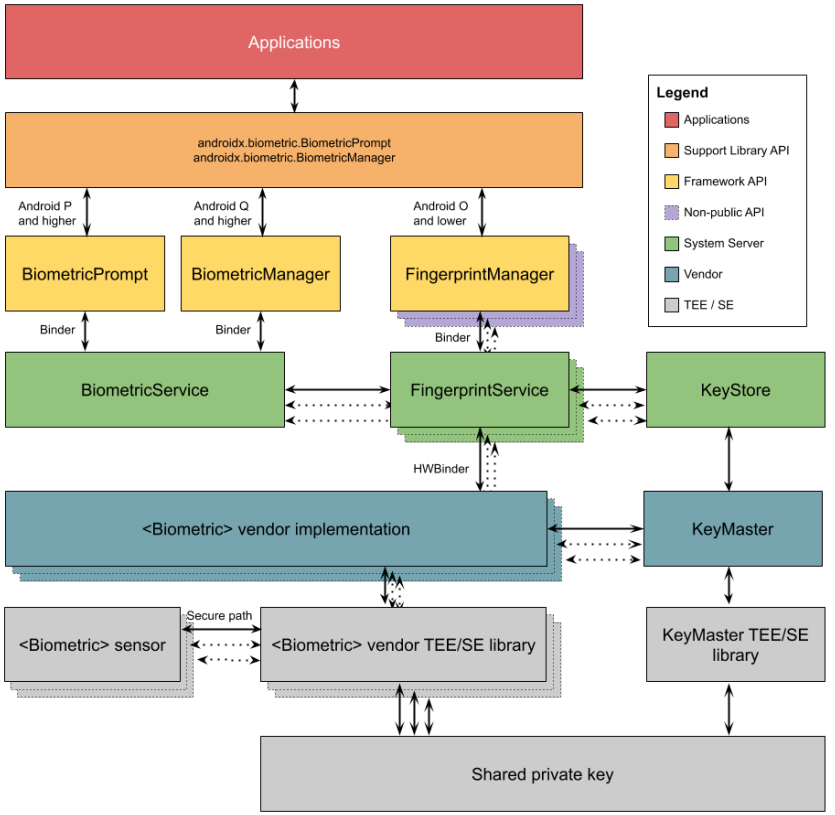
システムは生体認証資格情報を既存のテンプレートと照合しようとしているため、新しい生体認証資格情報が登録されている場合、デフォルトでは生体認証に関連付けられているすべての既存のキーが無効になります。

そうすれば、敵対者は指紋や顔を登録するだけでは、それを使用して個人データにアクセスすることはできません。秘密鍵は単に動作を停止し、それに依存するデータは本質的に失われます。

したがって、アプリが、銀行アプリなどの価値の高いトランザクションを処理する場合は、ユーザーが新しい生体認証資格情報を追加するタイミングを示すコールバックを監視します。

そのコールバックで、ユーザーに対して、アプリでの生体認証資格情報の再登録を許可する前に、意図的かどうかをユーザーに通知し、そのユーザーに確認します。

※自動翻訳にて翻訳したものであること、ご配慮ください。



【参考4】利用者用PINと生体認証の併用の基本的な考え方

利用者用PINと生体認証の併用のために、従来の利用者用PINの認証によるフローに対して以下を改良する。

・生体認証の成功に連動させて外部認証（External Authenticate）を実施する。【補足1】
生体認証の成功によりGP-SEの認証結果の状態を変えるために外部認証を活用する。

・署名生成処理の実行条件を「PIN認証OKあるいは外部認証OK」とし、利用者用PINの認証、外部認証のいずれかが成功していれば署名生成処理を実行可能とする。【補足2】