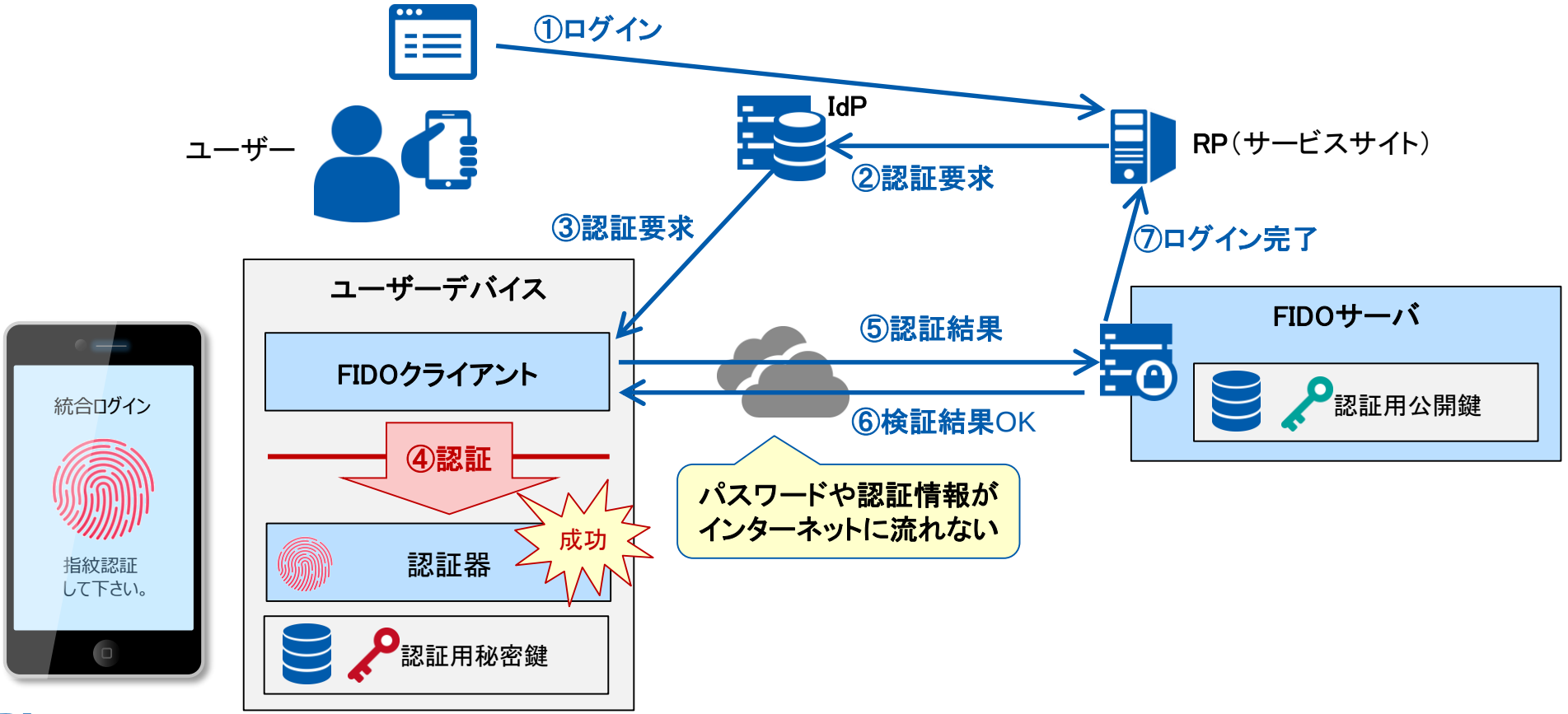
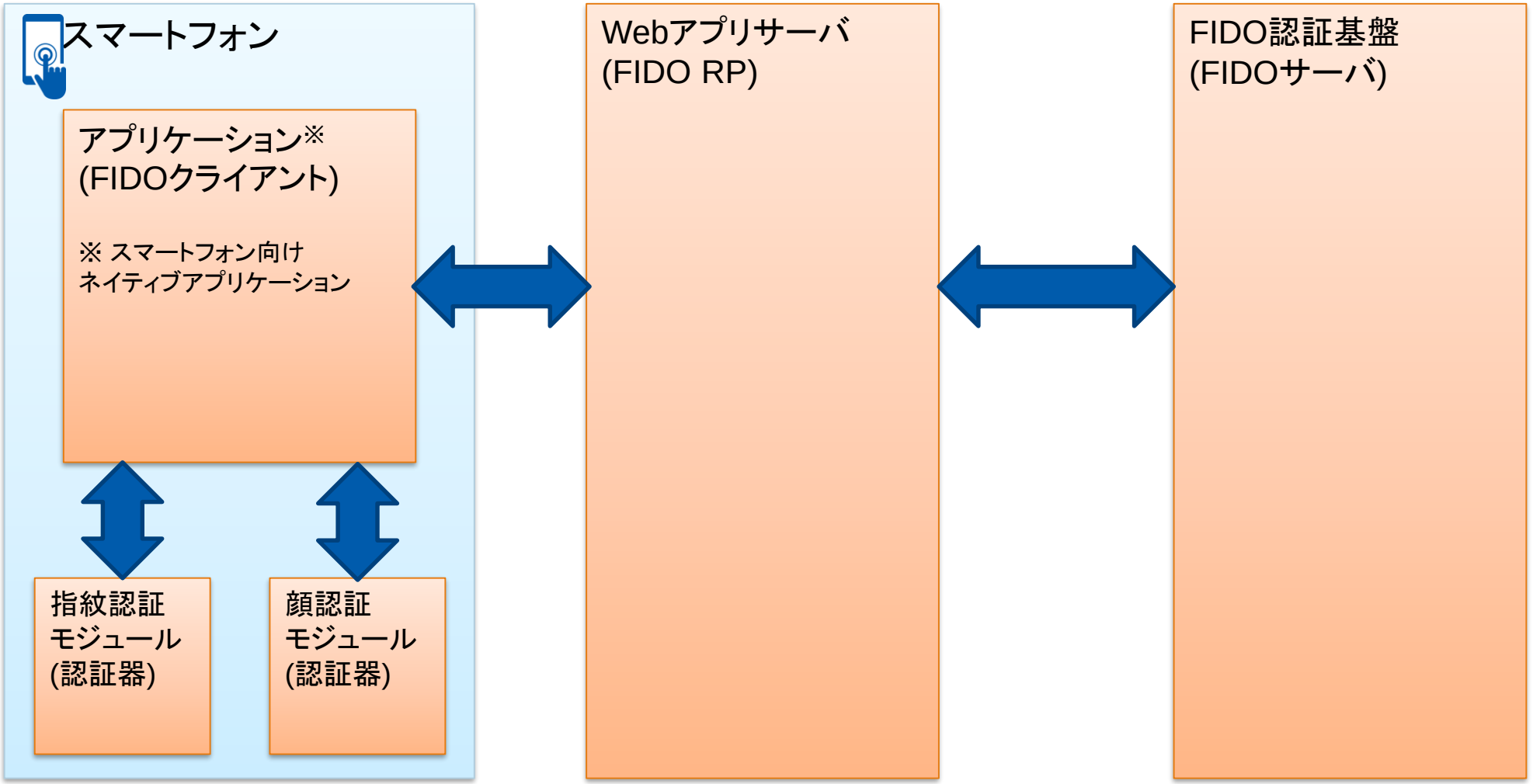
次世代認証技術「FIDO」

- FIDO認証は、公開鍵暗号方式を用いた認証方式の一種である。認証に必要な秘密情報は認証を行う端末側のみに保存され、ネットワーク上での伝送やサーバー側での保存の必要がないことを特徴とする。
- Webブラウザの2段階認証を想定したU2F、モバイル端末での内蔵認証器利用を想定したUAFが規定されている。



FIDO構成要素の例（FIDO UAFの場合）

- FIDOクライアント、FIDOサーバから構成される。ケースによって、Webアプリケーションサーバが中継する。



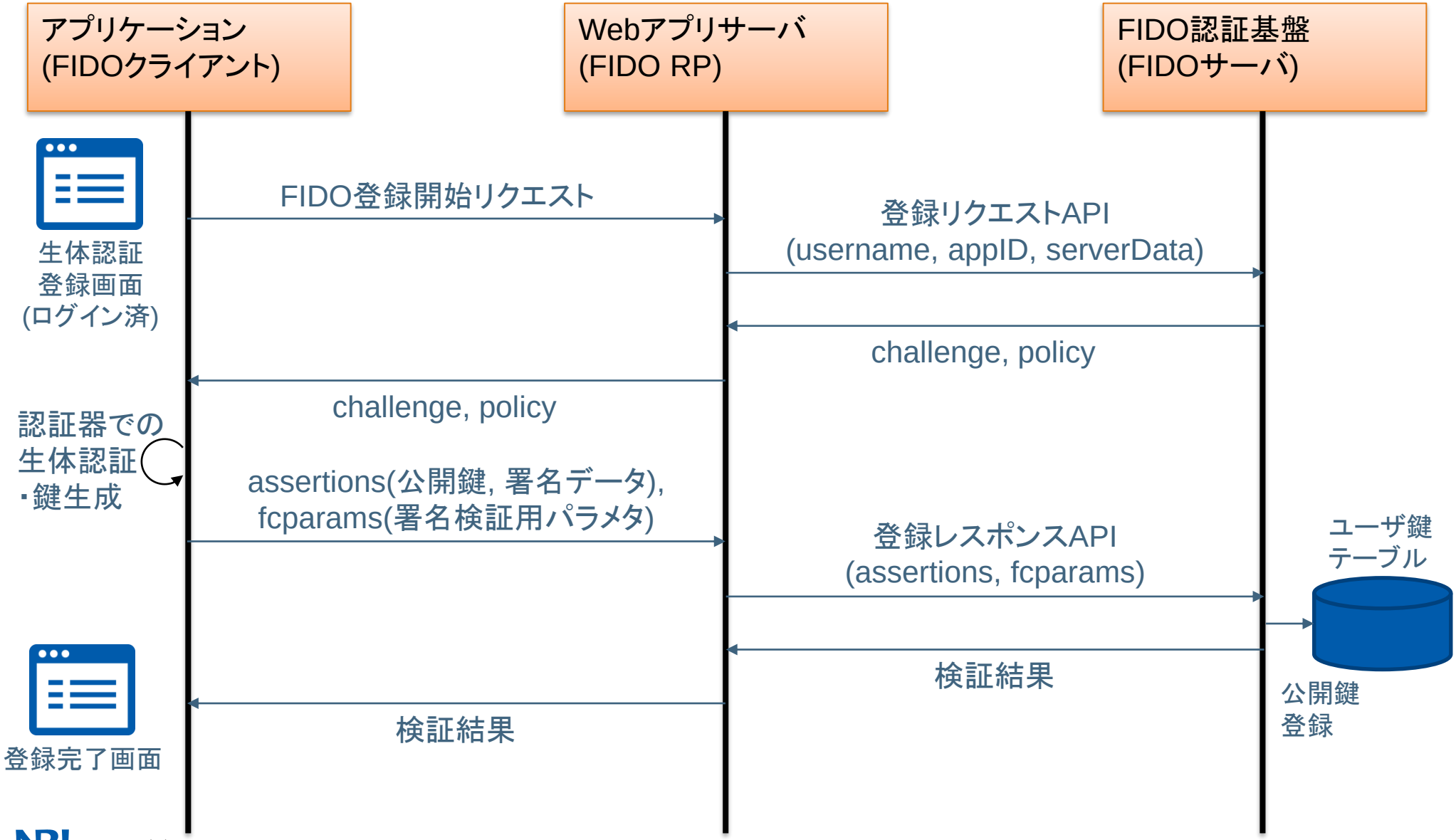
FIDOにおけるユースケース

- 登録
  - FIDO認証を行う前に1度だけ実施する。
  - {FIDOクライアント(アプリ)、ユーザ、認証器}のペアに対して秘密鍵＆公開鍵を作成し、FIDOサーバに公開鍵を登録する。
  - Challenge-Response形式のやり取りを実施する。

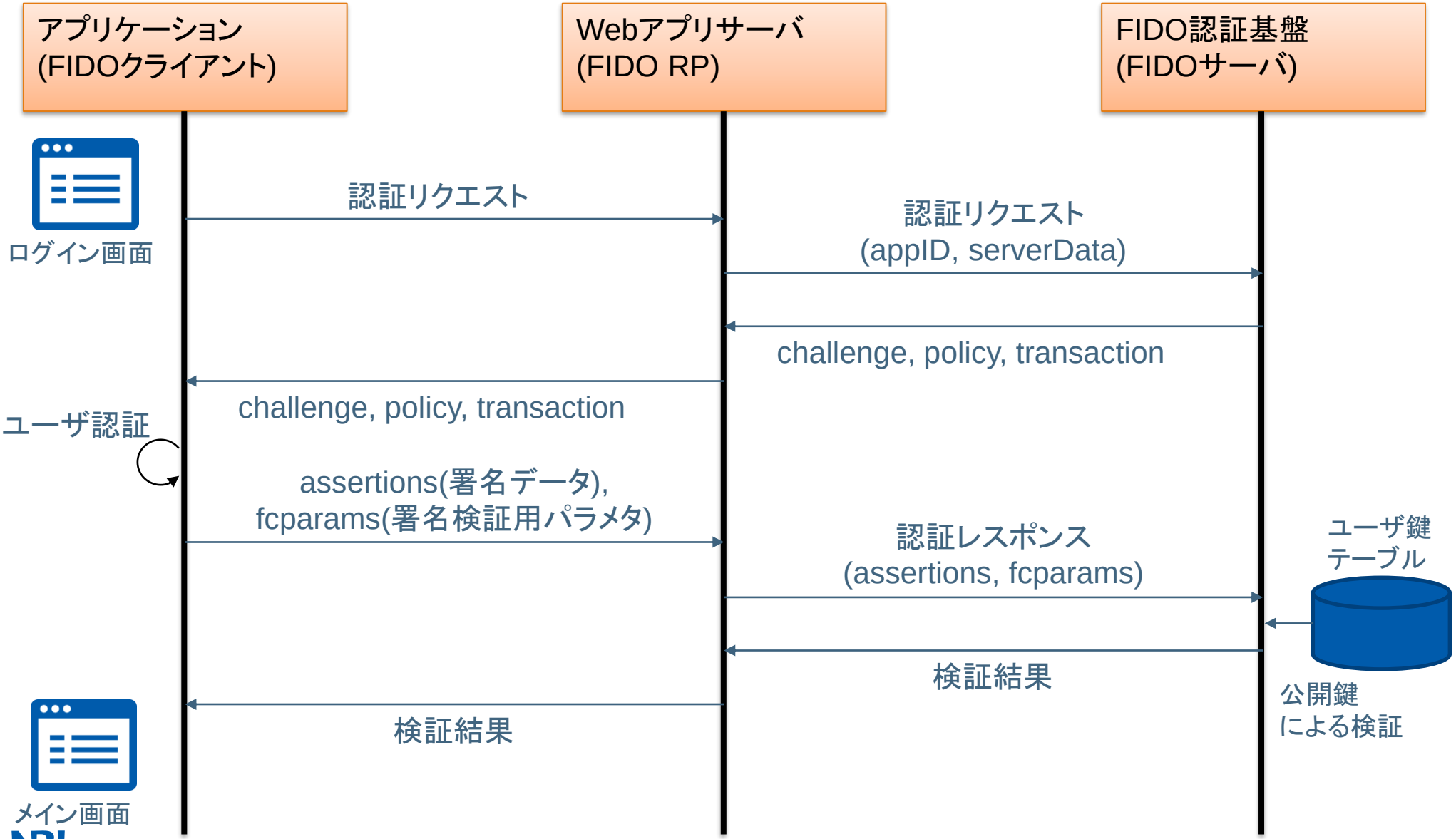
- 認証
  - ユーザが認証器を用いて認証を実施すると、FIDOクライアントが認証結果を秘密鍵で署名しFIDOサーバに渡す。FIDOサーバはその内容を検証する。
  - Challenge-Response形式のやり取りを実施する。

- 登録解除
  - FIDO認証を行わなくなった場合(ユーザID削除時など)に実施する。
  - FIDOサーバに登録されている公開鍵情報を削除する。

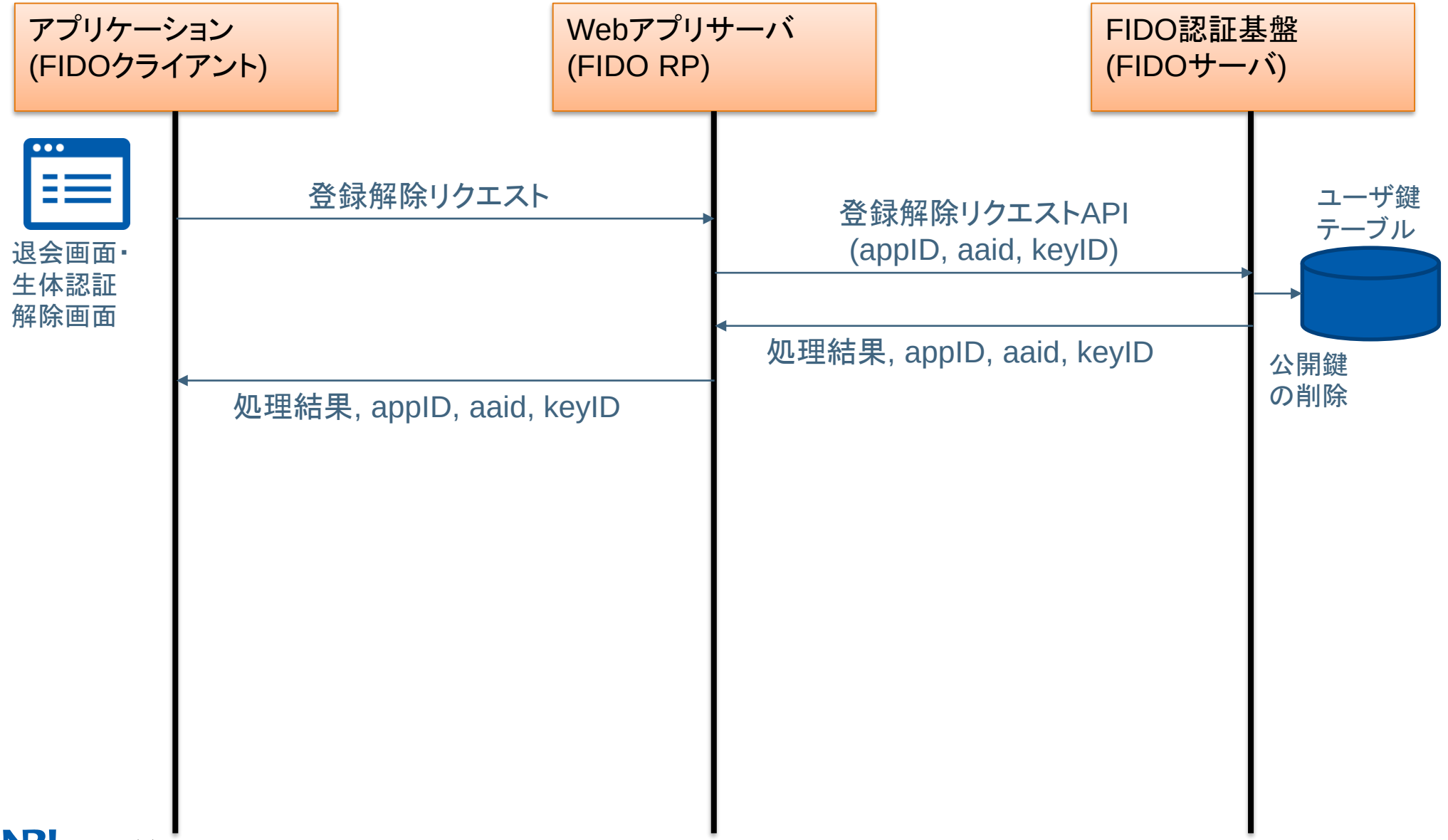
処理シーケンス例（登録）



処理シーケンス例（認証）



処理シーケンス例（登録解除）



FIDO2.0概要

概要

- より広範なプラットフォームでFIDO認証機能を提供することを目的として、FIDO U2F および UAF を拡張した認証仕様群。
- 大きな仕様として、Web Authentication APIとCTAPが存在。

Web Authentication API

- WebサイトがWebブラウザのJavascriptを介して認証器の情報にアクセスできるようにするインターフェースを定義。
- 2018年4月、W3Cにおける勧告候補の仕様となった。

CTAP(Client To Authenticator Protocol)

- プラットフォーム(OS)やWebブラウザと、FIDO Authenticator(認証器)間の通信プロトコルを定義。

FIDO2.0で可能になること

- Webブラウザを利用したパスワードレス認証
  - 以下のいずれかの方法での認証が可能になる。
    - 1要素認証（USBキーなど）による認証
    - 多要素認証
  - 従来のFIDO U2F仕様は、パスワード認証＋追加認証の構成が前提となっているが、その制約がなくなる。

- 無線通信によるAuthenticator利用
  - CTAP2.0の実装により、従来のU2F対応デバイスに加え、無線通信を介した認証デバイス利用が可能となる。
    →スマートフォン、スマートウオッチなどを利用した認証が見込まれる。


NRI
未来創発
Dream up the future.