

Modern Authentication

FIDO2 Web Authentication (WebAuthn) を学ぶ

栗原 淳

兵庫県立大学 大学院応用情報科学研究科
株式会社ゼタント

May 6, 2020

はじめに

はじめに

この講義では、

- パスワード認証に代わるモダンな認証方式「FIDO」の概要
- FIDO の認証を Web ブラウザ経由で利用する「FIDO2 WebAuthn」の利用

のさわりを学ぶ。

この講義の対象と事前準備

対象:

- 暗号・セキュリティ技術に興味がある初学者
- Web に新しい認証技術を導入したい Web 系のエンジニア

※但し、ある程度の公開鍵暗号・電子署名の知識を前提とする¹

必須ではないが触って楽しむのには必要な事前準備:

- Bash/Zsh, Git が使えるようになっていること
- Node.js, npm, yarn が使えるようになっていること
- Google Chrome 系ブラウザ and/or Firefox が利用可能のこと

¹どういうものか、というのを知つていれば十分。「JavaScript を使って学ぶ End-to-End セキュリティ」の資料を読んでいることを推奨
(https://github.com/junkurihara/class-e2e_security_js)。

パスワード認証から FIDO へ

認証とは

認証

「何らかの手段」で対象の正当性を確認すること。

- メッセージの正当性を確認 ⇒ メッセージ認証
- サービス利用ユーザの正当性を確認 ⇒ ユーザ認証
- etc.

※このスライドで単純に「認証」と呼んだときは、認証対象を「正規ユーザ本人」としたユーザ認証・本人認証を指すこととする。

本人認証の3つの要素

本人認証において、正当性確認のため検証されるものは大きく3要素に分類。

■ 知識

⇒ 本人しか知らない知識を持っていればOK (ex. パスワード)

■ 所有物

⇒ 本人しか持っていない物を提示できればOK (ex. HWキー)

■ 生体

⇒ 本人の体の一部を提示できればOK (ex. 指紋)



本人しか知らない



本人しか持っていない
(複製できない)



本人の体の一部

オンラインサービスでのパスワード認証

- サービスの利用者の識別子 (ID) と対応するパスワードをサービス事業者に登録、サービス利用時に利用者が自分の ID とパスワードを入力する。
- パスワードは個人の記憶にのみ存在するため、**パスワードを知っている人はそのサービスに登録してある本人と同一人物と考えることができる。**

おそらく、誰にとっても最も馴染み深い認証方式！

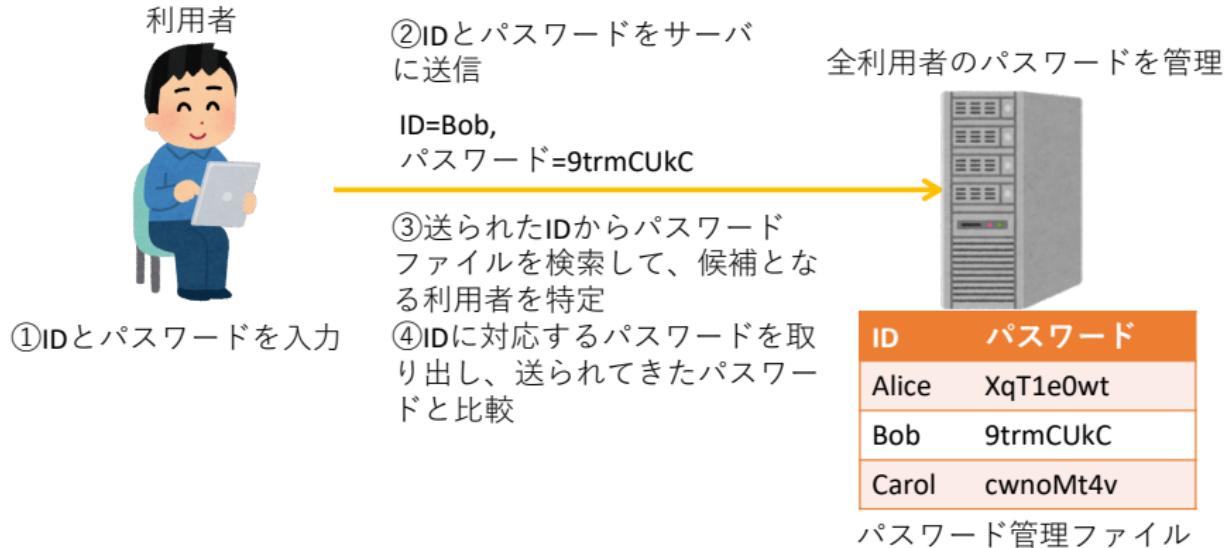


Figure: オンラインでの単純なパスワード認証

オンラインでのパスワード認証の問題

英数字・記号を組み合わせたパスワード:

- 攻撃者にとって比較的予測しやすい²
- 「強い」 パスワードを使わせるにはユーザ教育が必要³
- 覚えられない
- etc...



予測できず、誰が使っても強力で、確実に認証できる方法が必要
⇒ ハードウェアセキュリティキーを使った認証が人気に
⇒ FIDO はそのような手法の標準化された方式

²しかもオンラインだと予測→認証トライを繰り返せる

³教育なしだと覚え易く「弱い」ものを利用しがち

FIDO (Fast IDentity Online)

業界団体 FIDO Alliance⁴ の策定する、ハードウェアセキュリティキー+生体認証⁵と公開鍵暗号方式をベースとしたオンラインでの本人認証技術。

現在は FIDO2 (v2.0) が最新の規格。以降、FIDO2 の内容について触れていく。

厳密には、FIDO2 はパスワードレス認証をサポートしつつも、パスワード+デバイス・生体認証の多要素での認証もサポートする。

⁴<https://fidoalliance.org>

⁵すなわち、「所有物」と「生体」の二要素を同時に使った認証が可能。

FIDO 認証概略

FIDO 認証の特徴:

- 公開鍵暗号を利用した、オンラインでの認証方式の提供
 - 認証器によるローカルでの本人認証
 - 認証器内部に閉じた署名生成
- ⇒ 秘密鍵・パスワード等の秘密情報は外部に出ない

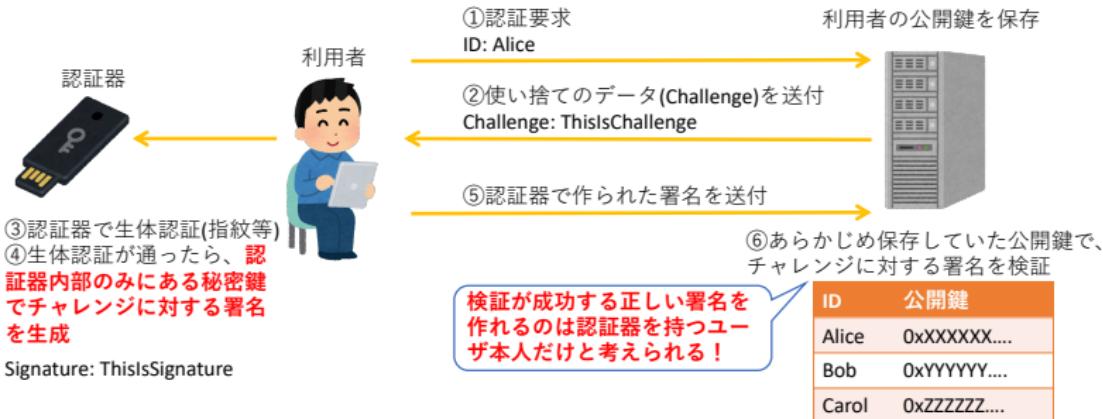
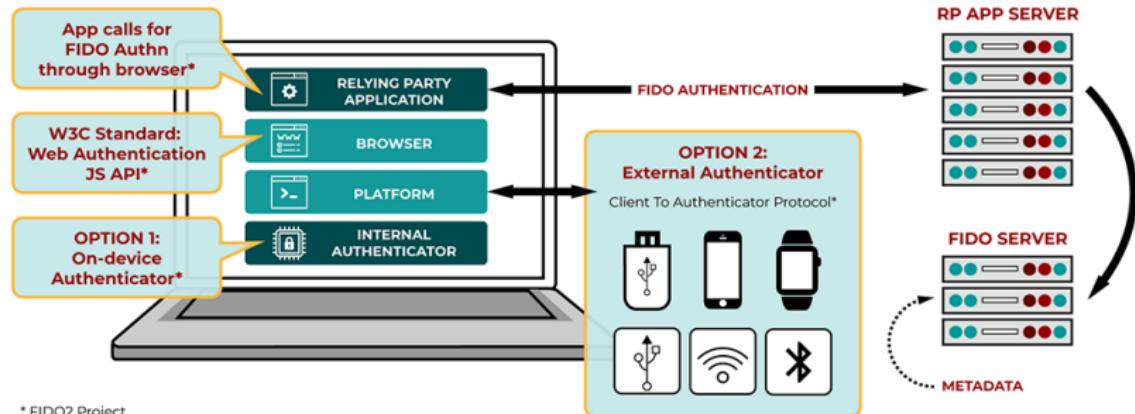


Figure: FIDO 認証概略

FIDO2 の要素

FIDO2 は、WebAuthn (Web Authentication)⁶と、CTAP
(Client-to-Authenticator Protocol)⁷の 2つの要素で構成される。



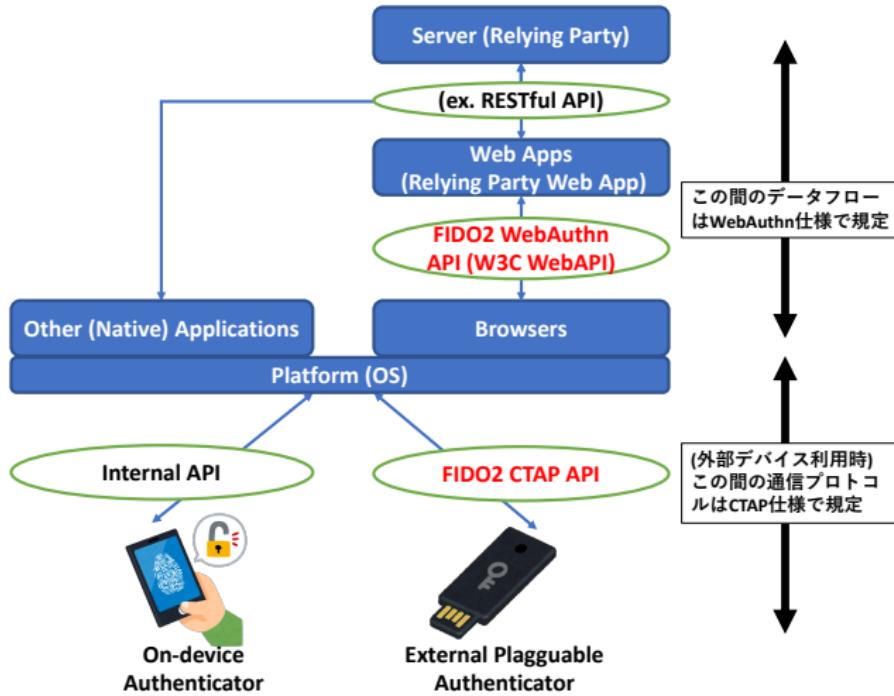
* FIDO2 Project

Figure: ©FIDO Alliance, from <https://fidoalliance.org/specifications/>

⁶Spec: <https://www.w3.org/TR/webauthn-1/>

⁷Spec: <https://fidoalliance.org/specs/fido2/fido-client-to-authenticator-protocol-v2.1-rd-20191217.html>

- **WebAuthn**: 内部/外部認証器を Call する WebAPI と、WebApp・サーバ間のデータフローを規定。
- **CTAP**: 外部認証器を Call する API と、クライアント/プラットフォームと認証器の通信プロトコルを規定。



FIDO2 CTAP⁸

USB/BLE/NFC 等で接続された HW セキュリティキーなどの外部認証器と、クライアントアプリ（ブラウザ等）およびプラットフォーム（OS）との間の通信プロトコルを規定。以下の要素で構成。

- USB/BLE/NFC など物理層の種別に応じた、通信確立のためのプロトコル
- 認証器での処理を Call する API
 - 外部認証器の情報取得
 - PIN によるローカルでのユーザ認証⁹
 - 認証器組込の秘密鍵での、ユーザ秘密鍵・証明書生成
 - ユーザ秘密鍵による署名の生成、など

ブラウザ・OS(のドライバ)は上記を実装した上で、より上位の WebAuthn のプロトコルをサポート。

⁸ <https://fidoalliance.org/specs/fido-v2.0-ps-20190130/fido-client-to-authenticator-protocol-v2.0-ps-20190130.html>
⁹ 指紋認証やジェスチャーなどは認証器のみで完結するので API は用意されない。署名生成などのときに認証器内での認証を要求するフラグを立てる。

FIDO2 WebAuthn¹⁰

Web ブラウザをプラットフォームとし、内部/外部認証器によって生成される署名を用いた、オンラインサーバでのユーザ認証のプロトコルを規定。より具体的には、以下を規定する。

- 認証器でのユーザの公開鍵証明書の生成、サーバへの登録プロトコル
- 認証器での署名生成、サーバでの認証プロトコル
- 認証器とやりとりするためブラウザが具備すべき Web API¹¹。
大雑把に以下の 2 種類。
 - ユーザの公開鍵証明書の生成 (Credential Creation)
 - ユーザ秘密鍵による署名の生成 (Assertion Generation)

認証器とのやり取りはブラウザ/プラットフォームがサポート。
⇒ 基本的に Web App の観点からは、WebAuthn のみを意識する。

¹⁰ <https://www.w3.org/TR/webauthn-1/>

¹¹ JavaScript で Call される API。ブラウザの内部でさらに認証器の API (CTAP や内部 API) を Call する。

補足: FIDO1

FIDO1 (v1.x) は、以下の 2 つの要素で構成されている。

- UAF (Universal Authentication Framework): 生体認証機能を持つ FIDO 対応端末 (スマートフォン等) でパスワードレス認証を行う機構。USB 接続などの外部 HW セキュリティキーは利用できない。
- U2F (Universal 2nd Factor)¹²: ID・パスワード認証に加えた 2 要素認証を行うのに、外部 HW セキュリティキーを利用可能とする機構。

FIDO2 は、UAF と U2F を統合し、さらに外部 HW キーを用いてもパスワードレス認証可能な、より利便性の高い規格と見做せる。

¹²U2F は FIDO2 規格では CTAP1 と改称。FIDO2 で追加された仕様は CTAP2 と呼ばれる。

FIDO2 対応の認証器

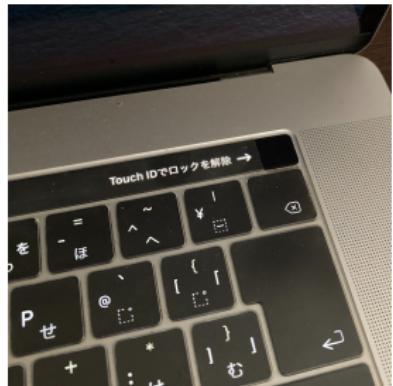
USB/NFC/BLE 等対応の外部認証器 (External Authenticator)、端末付属の認証器 (On-device/Internal Authenticator) 共々、様々な対応デバイスがリリースされつつある。



Security Key by Yubico
FIDO2 専用¹³



YubiKey 5Ci
FIDO2+OpenPGP+etc...



MacbookPro TouchID
FIDO2 認証可能¹⁴

¹³ FIDO2 CTAP1=FIDO1 U2F には対応。

¹⁴ ブラウザ等が TouchID API を Call できれば FIDO2 の On-device Authenticator として動作。Chrome 等は対応済。

FIDO2 標準化状況

FIDO は業界団体の策定した規格ではあるが、

- **FIDO2 CTAP**: ITU-T で勧告として国際標準化¹⁵
- **FIDO2 WebAuthn**: W3C で勧告として国際標準化¹⁶

と、認証器とプラットフォーム/ブラウザ間の通信プロトコル、
サーバ・ブラウザ間の認証プロトコルの両者共に国際標準として
策定済。

¹⁵<https://fidoalliance.org/>

fido-alliance-specifications-now-adopted-as-itu-international-standards/

¹⁶<https://www.w3.org/2019/03/pressrelease-webauthn-rec.html.ja>

この後、FIDO2 WebAuthn の内容に実際に触れ、最新の認証技術について理解を深めてみよう。¹⁷

¹⁷ 今回は Web 技術から学ぶセキュリティに注力するため、ローレイヤの FIDO2 CTAP については別の機会で。

実験環境の準備

準備

説明を聞きつつ手を動かすため、まず環境準備。

今回は以下の 2 つを WebAuthn の API を Call しながら実験してみる。

- 認証器を使って「ユーザ登録」

⇒ 認証器からのメッセージを解してみて実際に証明書および生の公開鍵を取り出してみる。

- 認証器を使って「ユーザ認証」

⇒ 署名を解してみて、登録時に取り出した公開鍵で署名が通ることを確認してみる。

⇒ この 2 つが FIDO2 WebAuthn のパスワードレス認証の基礎。

環境

以下の環境が前提:

- Node.js LTS (≥ 12) がインストール済で yarn が使える¹⁸
- ブラウザとして、Google Chrome (系ブラウザ)、もしくは Firefox がインストール済み
- Visual Studio Code や WebStorm などの統合開発環境がセットアップ済みだとなお良い

¹⁸インストールコマンド: `npm i -g yarn`

JavaScript プロジェクトの準備

1 プロジェクトの GitHub リポジトリを Clone

```
$ git clone https://github.com/junkurihara/xxxxxxxxxxxxxxxxxxxx  
$ cd sample
```

2 依存パッケージのインストール

```
$ yarn install
```

3 ライブラリのビルド

```
$ yarn build
```

認証器の準備

実験の前に認証器をセットアップしておく。例えば「Security Key by Yubico」の場合は、「YubiKey Manager」をインストールし、PINを設定。¹⁹

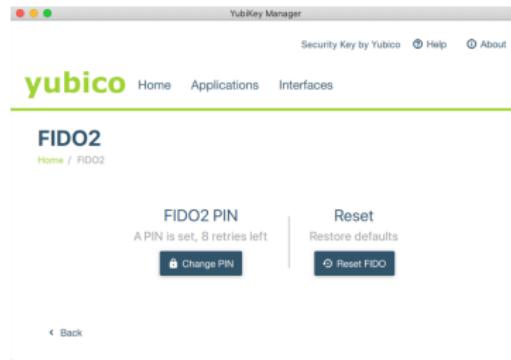


Figure: YubiKey Manager (Mac)

¹⁹ 「PIN+認証器へのタッチ」が生体認証という扱い。PIN 設定はなくても動作するが、タッチだけで生体認証したことになってしまう。PIN ではなく指紋認証を使うような認証器では、指紋登録が前もって必要。

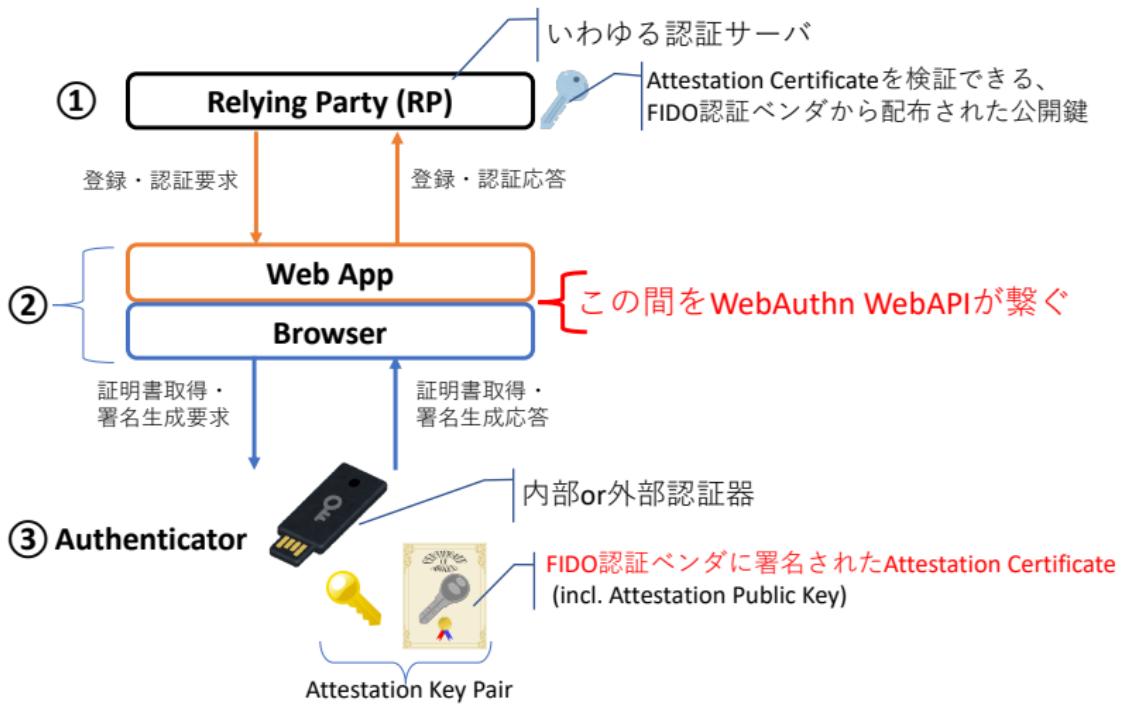
FIDO2 WebAuthn

FIDO2 WebAuthn 事始め

FIDO2 WebAuthn のフローの参加エンティティ

WebAuthn の動作フローでは、以下の 3 つの (抽象化された) 参加エンティティが存在。

- ① **Relying Party (RP)**: サービス提供者の認証サーバ
- ② ブラウザ+RP の **WebApp**: ユーザおよび認証器とやり取り
- ③ **Authenticator**: 内部/外部認証器。以下をセキュアに保持。
 - **Attestation Key Pair**: 公開鍵・秘密鍵ペア
 - **Attestation Certificate**: 上記の公開鍵に対し、FIDO2 で承認された製造元が署名した証明書



WebAPI として用意される WebAuthn API は、ブラウザ経由で WebApp が認証器とやりとりする役割を担う。

FIDO2 WebAuthn の 2 つのフロー

FIDO2 WebAuthn は、2つの動作フローを規定する。

- **ユーザ登録フロー**: 認証器を使って、Relying Party にユーザの ID や認証情報=公開鍵²⁰を登録する処理
- **ユーザ認証フロー**: 認証器を使って、Relying Party に事前に認証情報を登録したユーザ自身であることを証明する処理。

以降、この2つのフローの中身を見ていくが、その前に FIDO2 WebAuthn において **登録・認証の安全性を担保する Attestation** という概念について解説しよう。

²⁰Credential Public Key/Certificate のこと

FIDO2 における Attestation

FIDO2 では、「Attestation」という重要な概念が存在する。

FIDO2 における Attestation

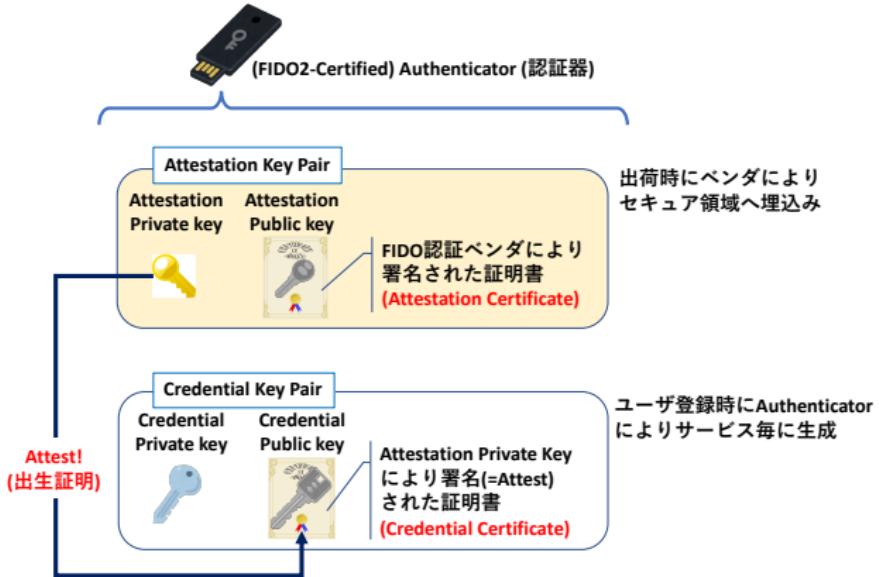
主として、「新しく生成・登録するユーザの公開鍵が、正しく FIDO2 認定を受けている認証器で生成された公開鍵であることを保証する機関」という意味。すなわち、**出生証明**。

Relying Party は、出生証明を確認してユーザを登録。
⇒ 偽造認証器を挿されたユーザの登録を弾ける。
⇒ 認証器に基づく FIDO2 認証の安全性は維持。



※認証器で生成するユーザの鍵ペアを **Credential Key Pair**、Attest されたその公開鍵証明書を **Credential Certificate** と呼ぶ。

Attestation の流れ。Attestation は 2 段階の証明で成立:



ユーザ登録時にユーザ公開鍵 (Credential Public Key) を出生証明して登録
⇒ Credential Certificate を Attestation Certificate で検証
⇒ Attestation Certificate を FIDO 認証ベンダの公開鍵²¹で検証

²¹ルート証明書

補足: Attestation の種類

- **Basic:** ベンダが認証器モデルごとに特有の Attestation Key Pair を埋込む。同じモデルの認証器では同じ鍵ペアでも良い。
- **Self:** Attestation Private Key = Credential Private Key で、Credential Certificate が自己証明書になる。
- **AttCA²²:** Attestation Certificate を動的に生成する手法。外部に信頼できる第三者の認証局を設け、認証器が Attestation (Identity) Key Pair を生成して、認証局へその公開鍵への署名を依頼。
- **ECDAA²³:** 楕円曲線上の匿名認証 (Direct Anonymous Attestation; DAA) を利用して、認証器の情報を与えることなく出生証明を実現。
- **None:** Attestation なし。

この資料では **Basic** 前提。

Basic でも HW 構造的に秘密鍵は認証器から取出せない。AttCA では、認証器の TPM に埋め込まれた鍵を、証明書生成ではなく認証局との暗号通信用に用いる。

²² Attestation Certificate Authority

²³ Elliptic Curve based Direct Anonymous Attestation; アルゴリズム仕様は現状ドラフト。

この後やってみること

この後は、

- ユーザ登録フロー
- ユーザ認証フロー

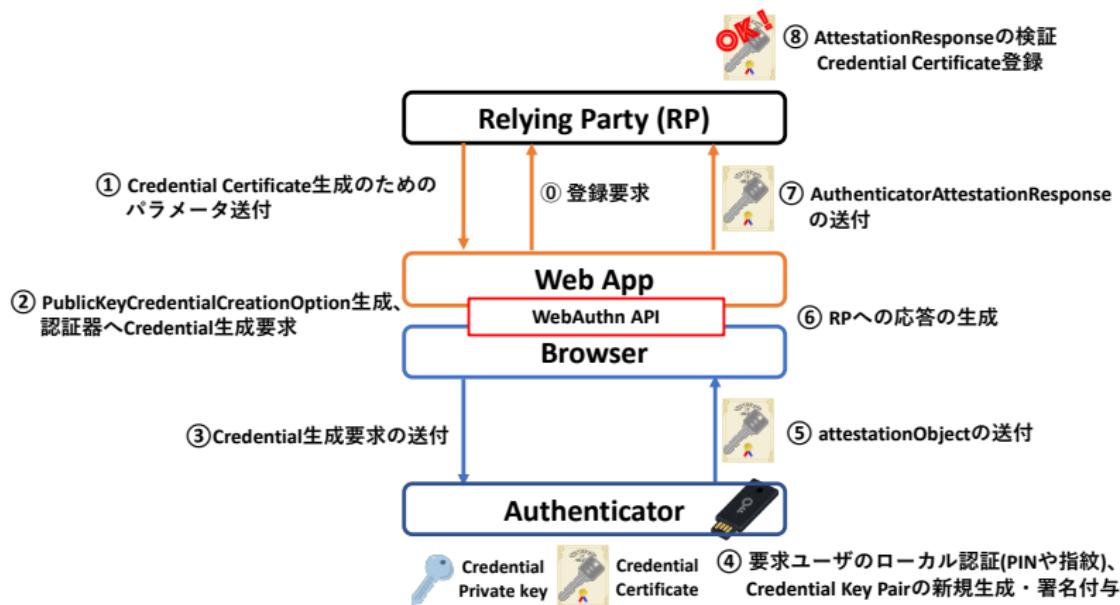
の両者において、localhostでRPを模擬²⁴しつつ、認証器・ブラウザ間でやりとりされるデータと、認証器内部での処理をコードを見ながら確認・解説していく。

²⁴ ブラウザ・RPとのやりとりは標準がないことと、処理フロー・データフローを理解することに重点をおくため。しかし Python Flask 等で REST API でやりとりするサーバは簡単に実装可能。

FIDO2 WebAuthn ユーザ登録フロー

WebAuthn ユーザ登録フロー

以下のような流れで WebAuthn の認証のための登録を行う。

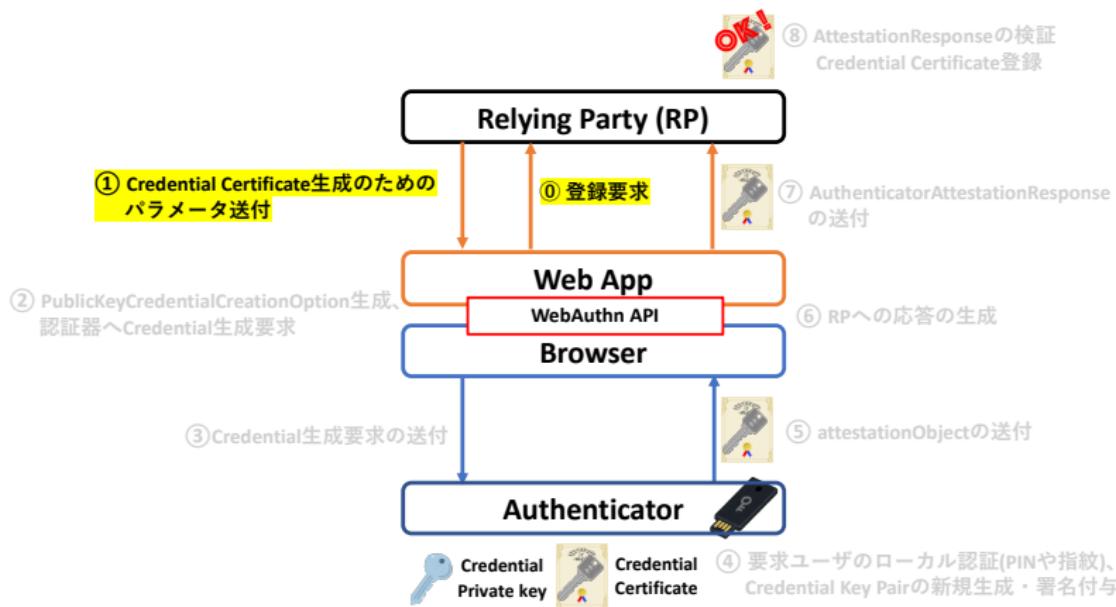


単純に言うと、認証器で Credential Certificate を生成、その出生証明を RP で確認・登録という処理。

このユーザ登録の各ステップを、実際のデータを確認しながら追っていく。

WebAuthn ユーザ登録: RPへユーザ登録要求

①, ② ユーザ登録のため Credential 生成パラメタを RP から取得。



WebApp と RP 間の要求・応答フォーマットは規定されていない。
⇒ RP 側の (REST) API は実装者に任せられている。

WebApp が RP から取得するパラメタは以下の通り。²⁵

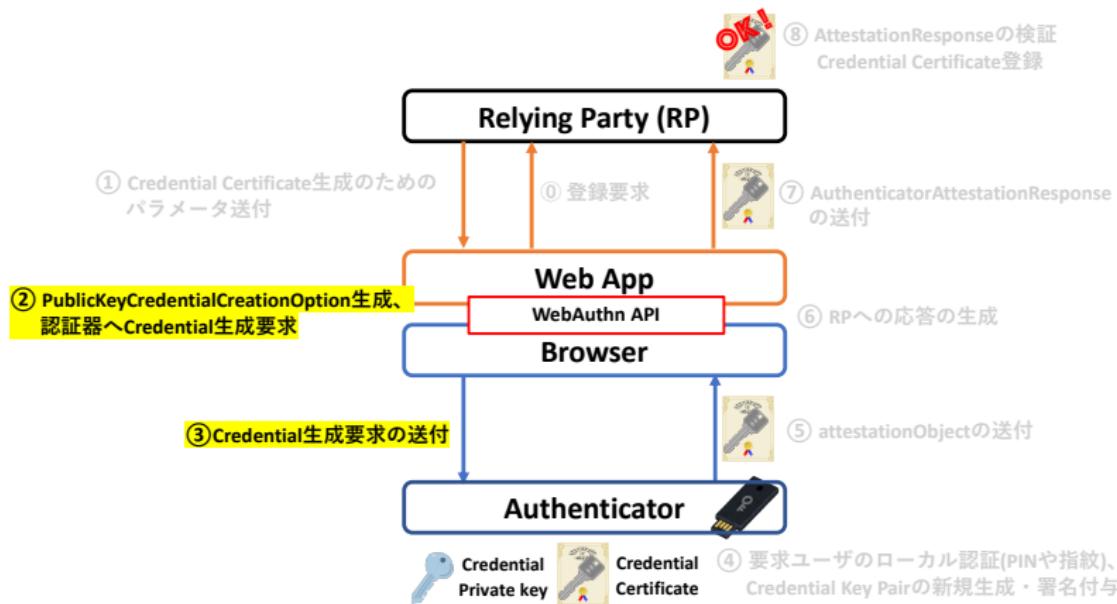
- **Challenge:** 暗号学的にランダムな使い捨ての binary string (最低 16bytes, 通常 32bytes 程度)
- **User Info:** ユーザ情報。ID、メールアドレス、名前。
- **Relying Party Info:** RP(すなわちサービス) の名前、FQDN、アイコンのアドレス。

ブラウザは、これらを PublicKeyCredentialCreationOptions Object にし、WebAuthn API 経由で認証器へ Credential 生成を要求。

²⁵ UserInfo, RP Info は WebApp すなわちユーザが自分で定めることも (一応) できる。

WebAuthn ユーザ登録: 認証器へ Credential 生成要求

②, ③ ブラウザの API を Call して認証器へ Credential 生成を要求。



PublicKeyCredentialCreationOptions Object をブラウザの `window.navigator.credentials.create()` へ入力。

実際に JavaScript のコードを見ていく。

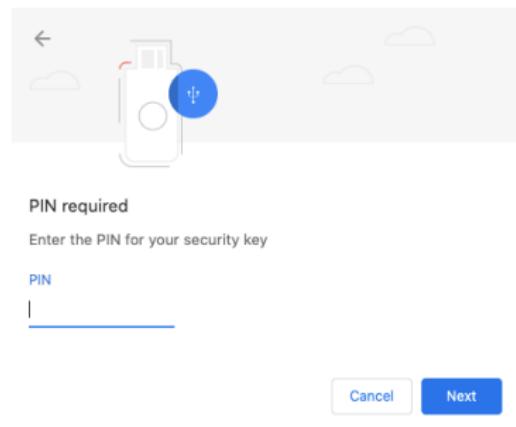
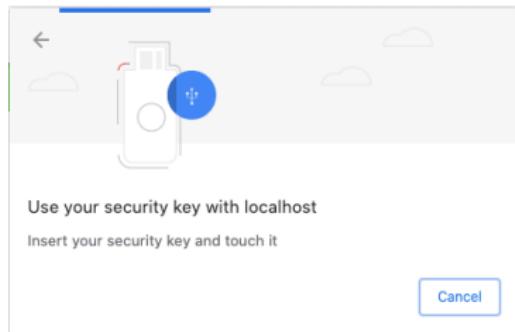
PublicKeyCredentialCreationOptions の構造 (./test/credential-params.ts)

```
const createCredentialDefaultArgs: CredentialCreationOptions = {
    publicKey: {
        // Challenge 本当はサーバーで生成した暗号学的に安全な乱数をセット (16bytes 以上)
        challenge: new Uint8Array([0x8C, 0x0A, 0x26, 0xFF, 0x22, ...]).buffer,
    },
    // Relying Party Info (a.k.a. - Service)
    rp: {
        id: 'localhost', // テストコードはローカルで走るため
        name: 'Example RP'
    },
    // User Info
    user: {
        id: new Uint8Array(16),
        name: 'john.p.smith@example.com',
        displayName: 'John P. Smith',
    },
    // 利用したい Public Key Credential Params のリスト (認証器は先頭から試行):
    pubKeyCredParams: [
        {
            type: 'public-key', // As of March 2019, only 'public-key' is accepted.
            alg: -7 // Signature Algorithm (ECDSA with SHA-256)
        },
        // Attestation Type (optional, default は 'none' (RP による attestation 検証なし))
        attestation: 'direct', // 'direct' は認証器の生成した Attestation を直接 RP に送るタイプ
        // Time Out (optional, in msec)
        timeout: 60000, // 認証器からの応答をブラウザはどれくらい待つか。
    }
};
```

PublicKeyCredentialCreationOptions Object を使ってブラウザの WebAuthn API を以下のように Call すると、**認証器の挿入・接続要求、PIN 入力要求がブラウザ通知される。**

```
window.navigator.credentials.create() の Call (./test/test.spec.ts)
```

```
const cred: Credential|null  
= await window.navigator.credentials.create(createCredentialDefaultArgs);
```



この流れは、Shell からサンプルコードのディレクトリで以下を実行すると確認できる。

ユーザ登録→ユーザ認証の一連のテストコードを実行

```
$ yarn test
```

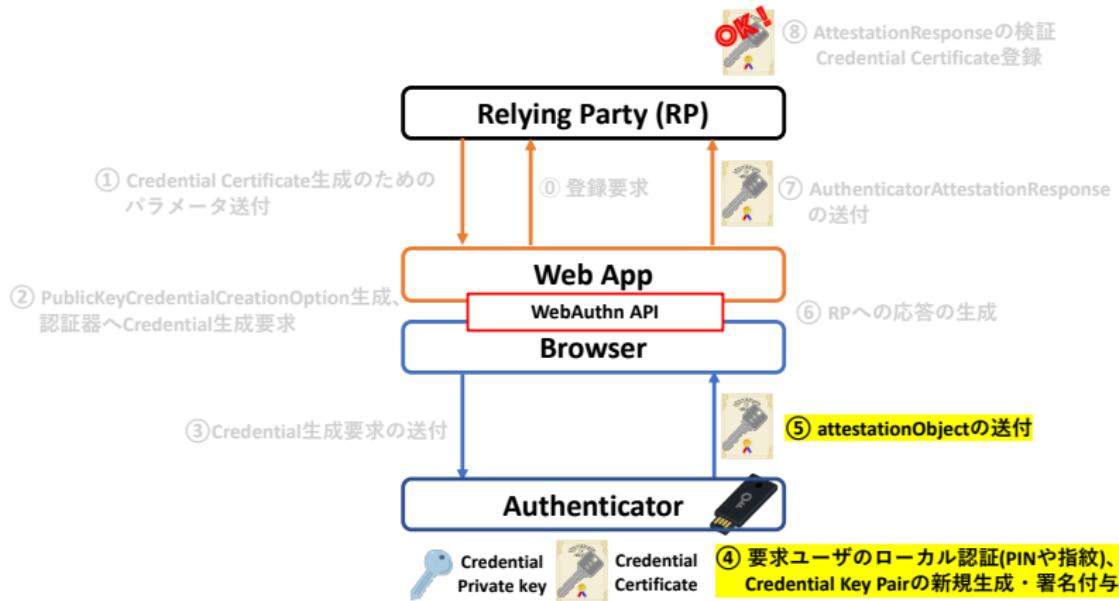
ブラウザにダイアログが出たところで認証²⁶を行えば、認証器内部で Credential が生成&出生証明される。

それでは、次の Credential 生成ステップと、生成した Credential の中身を覗いてみよう。

²⁶Security Key by Yubico の場合は PIN 入力+タッチ

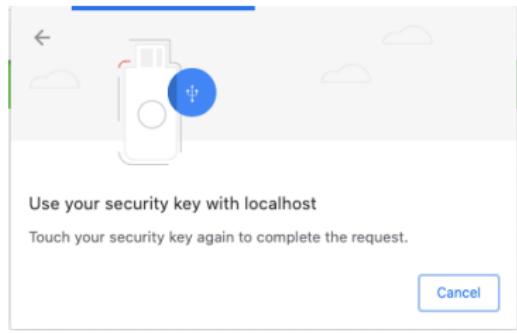
WebAuthn ユーザ登録: Credential 生成・取り出し

④, ⑤ 認証器で Credential 新規生成、Credential Certificate を取得。

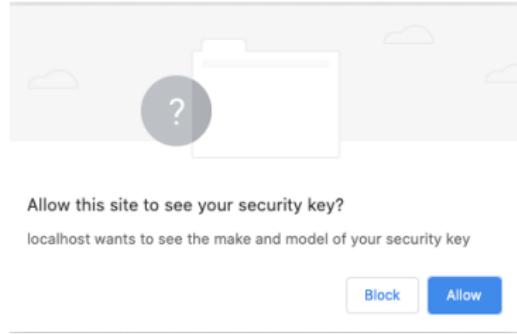


前ステップの `create()` の返り値として、Attestation Certificate や Credential Public Key (`attestationObject`) を格納した `PublicKeyCredential Object` をブラウザが取得。

前ステップの後、認証器ローカルでの生体認証²⁷、および FIDO2 WebAuthn の利用確認が求められる。



認証要求

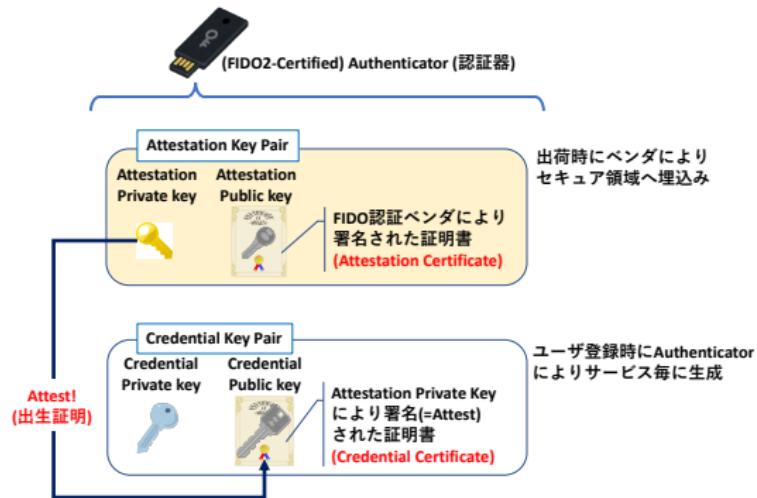


FIDO2 利用意思の確認

²⁷ Security Key by Yubico の場合、PIN 入力の後にタッチすること。

認証と利用意思確認が完了すると、認証器内部で以下の処理を実行。

- 1 ローカルでの生体認証結果の確認
- 2 `create()` で入力されたパラメタに応じて、ユーザの新しい鍵ペア ‘Credential Key Pair’ を生成
- 3 認証器内部の Attestation Private Key で Credential Key Pair に署名、 Credential Certificate を生成
- 4 Credential Certificate を出力²⁸



²⁸ Attestation Type: direct の場合は Attestation Certificate も出力

`create()` の返り値 `PublicKeyCredential Object` は単純に以下の 4 つの要素で構成されている。

PublicKeyCredential の構造 (\$ yarn test の途中出力)

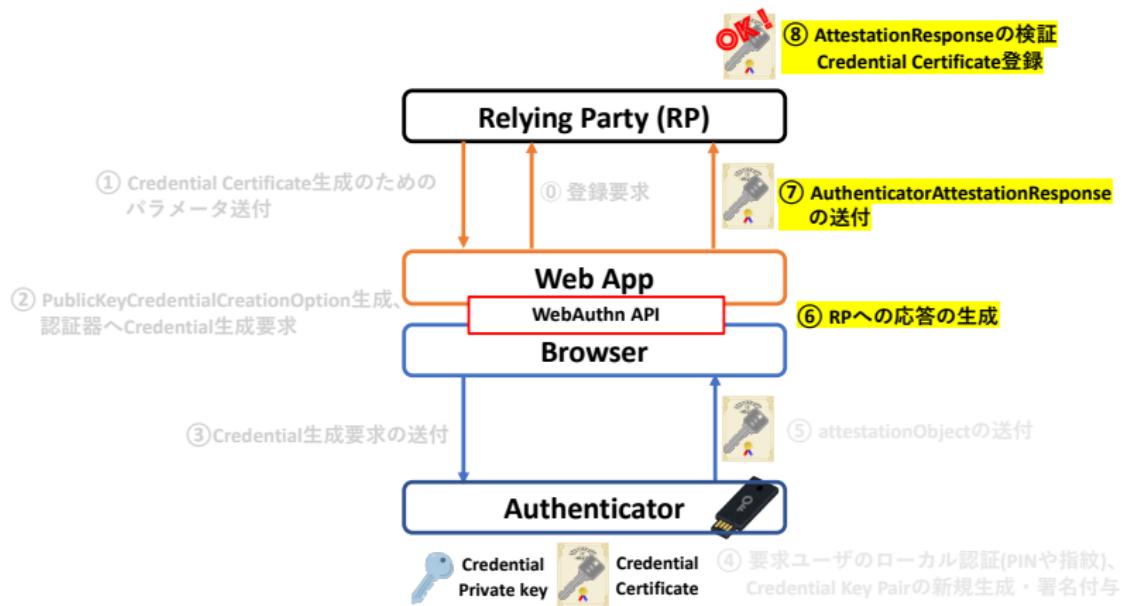
```
'----- [Response from Authenticator: PublicKeyCredential] -----'  
'> Credential ID: HfM8J_xY7mn7bfiHxF7f7MLxf...' ← 生成した公開鍵の ID  
'> Credential Raw ID: [object ArrayBuffer]' ← 生成した公開鍵の ID のバイナリ版  
'> Credential Type: public-key' ← 公開鍵証明書なので'public-key'  
'> AuthenticatorAttestationResponse.clientDataJSON: [object ArrayBuffer]' ← RP の Challenge に対する応答 (バイナリ)  
'> AuthenticatorAttestationResponse.attestationObject: [object ArrayBuffer]' ← ここが Credential Certificate  

```

このうち、「`clientDataJSON`」と「`attestationObject`」からなる `AuthenticatorAttestationResponse` を RP に送って検証・登録する。次のステップでその検証について解説する。

WebAuthn ユーザ登録: Attestation の検証

⑥, ⑦, ⑧ ブラウザが AuthenticatorAttestationResponse を RP に送って、そこで Attestation の検証とユーザ登録を実行。



基本的にこれは RP の行うバックエンドの処理なことに注意。

“TBD あとでちゃんとく”

ClientDataJSON と attestationObject の意味と構造。

- client data json: challenge への応答、その検証
- attestationObject:
 - fmt: format = 基本は packed
 - attStmt: attestationCertificate と、それによる検証が可能な Signature
 - authData: credentialPublicKey やそのメタ情報。attestation private key による署名対象

attestationObject の内容の検証結果 (\$ yarn test の途中出力)

```
LOG: '----- [Verification result on PublicKeyCredential.AuthenticatorAttestationResponse] -----'
LOG: '> Verification result: true' // Credential Public Key の Attestation の署名検証成功

LOG: '> Credential Public Key: // 新しく作った Credential Public Key (毎回変化)
-----BEGIN PUBLIC KEY-----
MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEt11IqJnVr2Wi4nIip57LPhoAejRG
TH86zg3S7CUySFibLqVOQrbQ00ADz9IpYHoKzQCbbHcl3o8Zj7WgHUy1yQ==
-----END PUBLIC KEY-----'

LOG: '> Attestation Certificate: // 上の公開鍵についてた署名を検証した公開鍵証明書 (固定)
-----BEGIN CERTIFICATE-----
MIICvDCCAaSgAwIBAgIEBMX/+DANBgkqhkiG9w0BAQsFADuMSwwKgYDVQQDEyNZ
dWJpY28gVTJGIFJvb3QgQ0EgU2VyaWFsIDQ1NzIwMDYzMTAgFw0xNDA4MDEwMDAw
MDBaGA8yMDUwMDkwNDAwMDAwMFowbTELMAkGA1UEBhMCU0UxEjAQBgNVBAoMCVl1
YmljbyBBQjEiMCAGA1UECwwZQXV0aGVudGljYXRvcibBdhRlc3RhdGlvbjEmMCQG
A1UEAwdWXViawNvIFUyRiBFBSBTZXjPwYwgODAwODQ3MzIwWTATBgcqhkJOPQIB
BggqhkJOPQMBBwNCAAQc2Np2EaP17x+IXpULp12A4zSFU5FYS9R/W3GcUyNcJCHk
45m9tXNngkGQk1dmYUk8kUwuZyTfk5T8+n3qixgEo2wajAiBgrBgeEAYLEcGIE
FTEuMy42LjEuNC4xLjQxDgyLjEuMTATBgsrBgeEAYL1HAIBAQQEawIFIDAhBgsr
BgeEAYL1HAEBBAQSBBd4oBHjApNFYAGFxEfntx9MAwGA1UdEwEB/wQCMAAwDQYJ
KoZIhvcaNAQELBQAQDggEBAHcYT091LRoF8wpThdwthvj6wGNxcLAiYqUZXPX+0Db+
AGVODSkVvEVSmj+JXmrBzNQel3FW4AupOgbgrJmmcWWEBZyXSpRQtYcl2LTNU0+I
z9WbyHNN1wQJ9ybFwj608xBuoNRC0rG8wgYbMC4usyRadt3dYOVdQi0cfaksVB2V
NKnw+tQUWKoZsPhtuzFx8NlazLQBep1W2T0FCNFEg7x/1+ZcfNhT13azAbaurJ
2J0/ff6H0PXJP6h+Obne4xfz0+8ujftWDUSh9oaiVRYf+tgam/tzOKyEU38V2liV
11zMyHKWrXiK0AfYDgb58ky2HSrn/AgE5MW/oXg/CXc=
-----END CERTIFICATE-----'
```

FIDO2 WebAuthn ユーザ認証フロー

WebAuthn ユーザ認証フロー

WebAPI の観点では、認証器においてユーザ秘密鍵で署名生成。

まとめ

