還在用過時的 OTP 保護帳號？
來看看 FIDO U2F 吧！

Jong-Shian Wu
吳忠憲

我是誰

- 吳忠憲 Jong-Shian Wu
- 台灣大學快速密碼學實驗室
- 密碼學、資訊安全、程式語言、軟體工程

我們平時是如何登入帳號的呢？

(考慮 Web 的例子)

Alice 的電腦

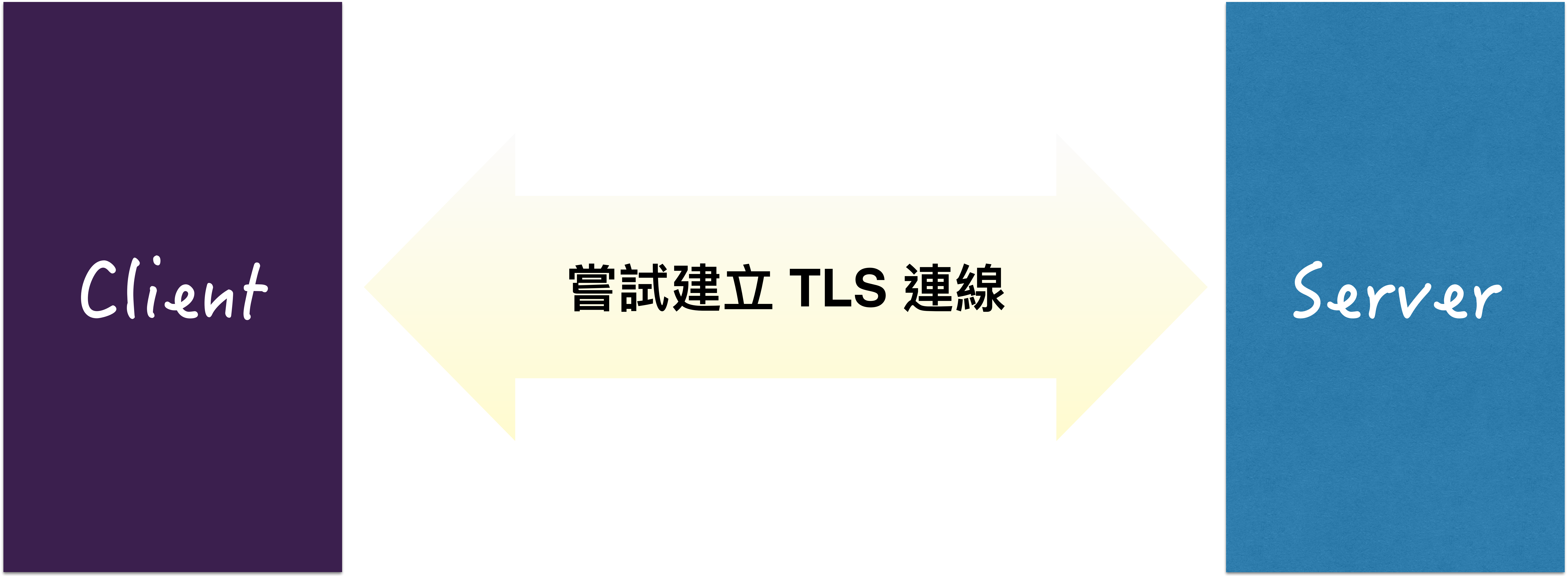
`https://bob.com`

Client

Server

Alice 的電腦

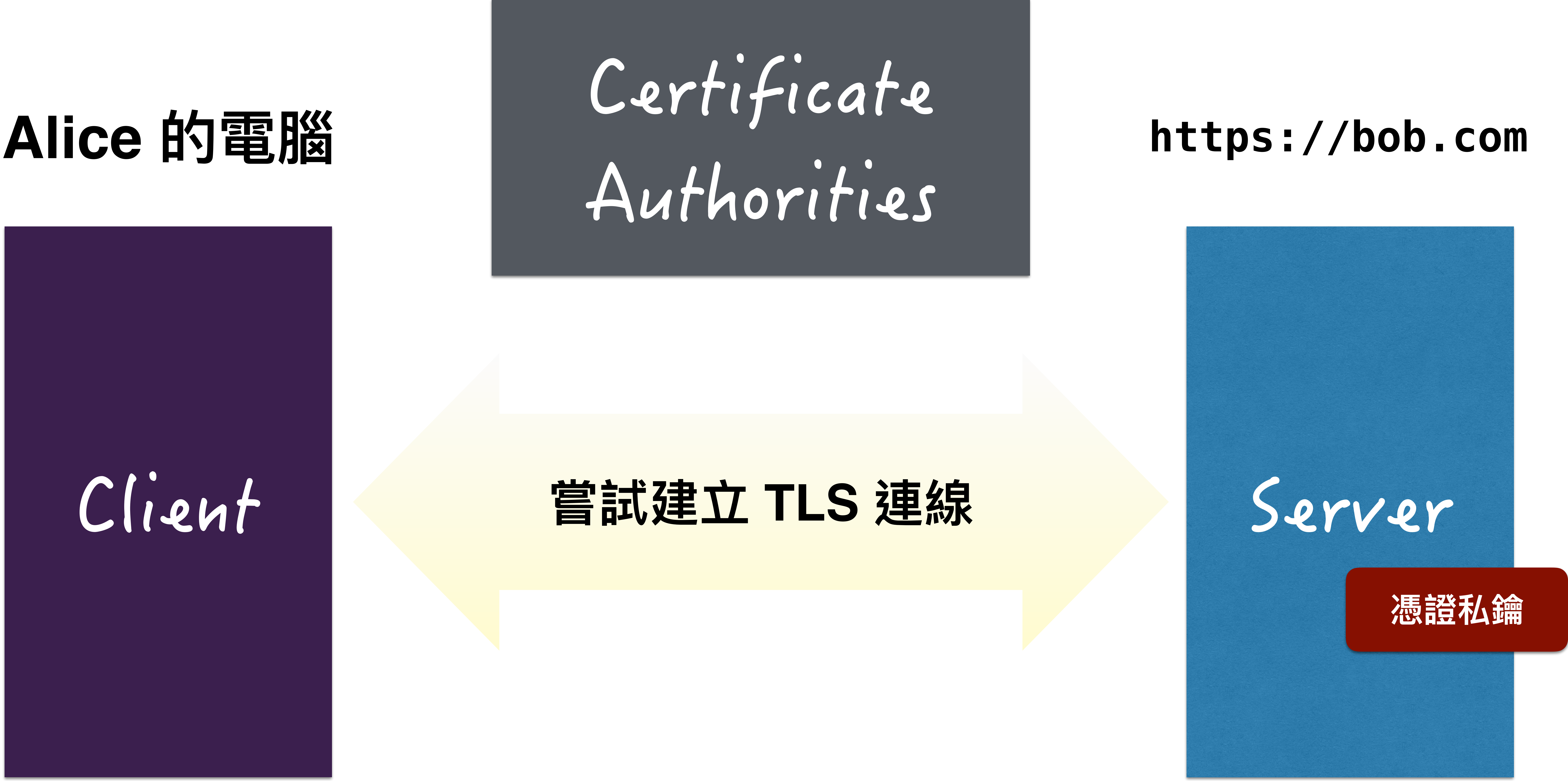
`https://bob.com`



Client

嘗試建立 TLS 連線

Server



Alice 的電腦

Certificate
Authorities

https://bob.com

Client

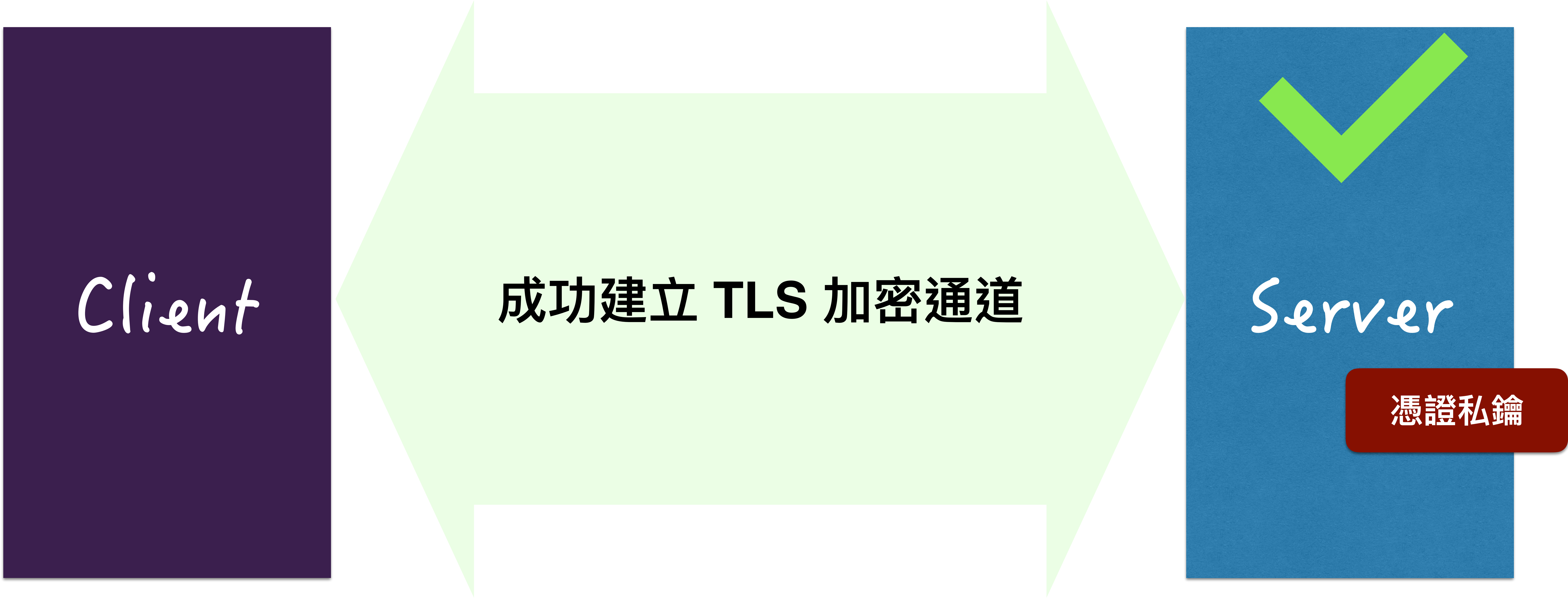
嘗試建立 TLS 連線

Server

憑證私鑰

Alice 的電腦

https://bob.com



Client

成功建立 TLS 加密通道

Server ✓

憑證私鑰

Alice 的電腦

https://bob.com

Client

密碼 (明文)

Username & Password

Server

✓

憑證私鑰

密碼 (打亂後)

(做 salted hash 檢查)

Alice 的電腦

`https://bob.com`

Client

密碼 (明文)

Cookie

Username & Password

Login Token (Cookie)

✓

Server

憑證私鑰

密碼 (打亂後)

Cookie

Alice 的電腦

https://bob.com

Client

密碼 (明文)

Cookie

用 HTTPS 搭配 Cookie
建立的 Login Session

Server

憑證私鑰

密碼 (打亂後)

Cookie

「密碼」的問題？

1. 被重複使用
2. 不重複且夠亂的密碼容易忘記、輸入不便
3. 密碼明文會暴露於許多地方
4. 一不小心，就可能被「釣走」

gandi.net
no bullshit™
Service status
Shopping cart
Webmail
English
Domain names
Hosting
SSL
Corporate
Why Gandi?
Discussion
Help
Log in
Home
Register
New TLDs
Transfer
Renew
Restore
Whois
Reseller
Selection
Identification
Contacts
Services and DNS zone files
Contracts
Payment
Follow up
Go
Add
Hide suggestions
?

Whenever possible, Gandi automatically applies a discount of 15% off the standard price per year for registrations of 3 years or more.

Sunrise? Landrush? GoLive? Click here to learn more about the **700 new generic TLDs** being released.

drop6ox.com

drop6ox.com is available

1 year - NT$425

Here are some results in other extensions that might interest you.

drop6ox ×

Shopping Cart

Your shopping cart is **empty**

Results :

20 per page

Sort by:

一次性密碼 (OTP) 兩步驟驗證

1. 每 30 秒自動刷新的「一次性」密碼
2. 軟體或硬體實作
3. 密碼與 OTP 同時被偷走的難度較高

OTP 兩步驟驗證的問題？

1. 再次增加麻煩
2. 對稱式架構，秘密金鑰會出現於兩端，須妥善保存
3. OTP 也可以被「釣走」，和密碼一樣

非對稱式（公鑰）認證架構

持有 Alice 私鑰

持有 Alice 公鑰

Alice

Bob

Challenge:
請對以下資料做數位簽章

`0Azi/Pk+dPLeERyvl4UoDU8TV1nD/kciGl9esK1ryPE=`

非對稱式（公鑰）認證架構

持有 Alice 私鑰

持有 Alice 公鑰

Response:
這是我所產生的數位簽章，請檢查

`lDVkxzgHW2qlcWT9R9NNT9QLvCw7LivuobeoEdcQl4I=`

最常見的有 RSA 與 ECDSA

1. RSA 支援較廣泛
2. ECDSA 速度較快、消耗更少儲存空間

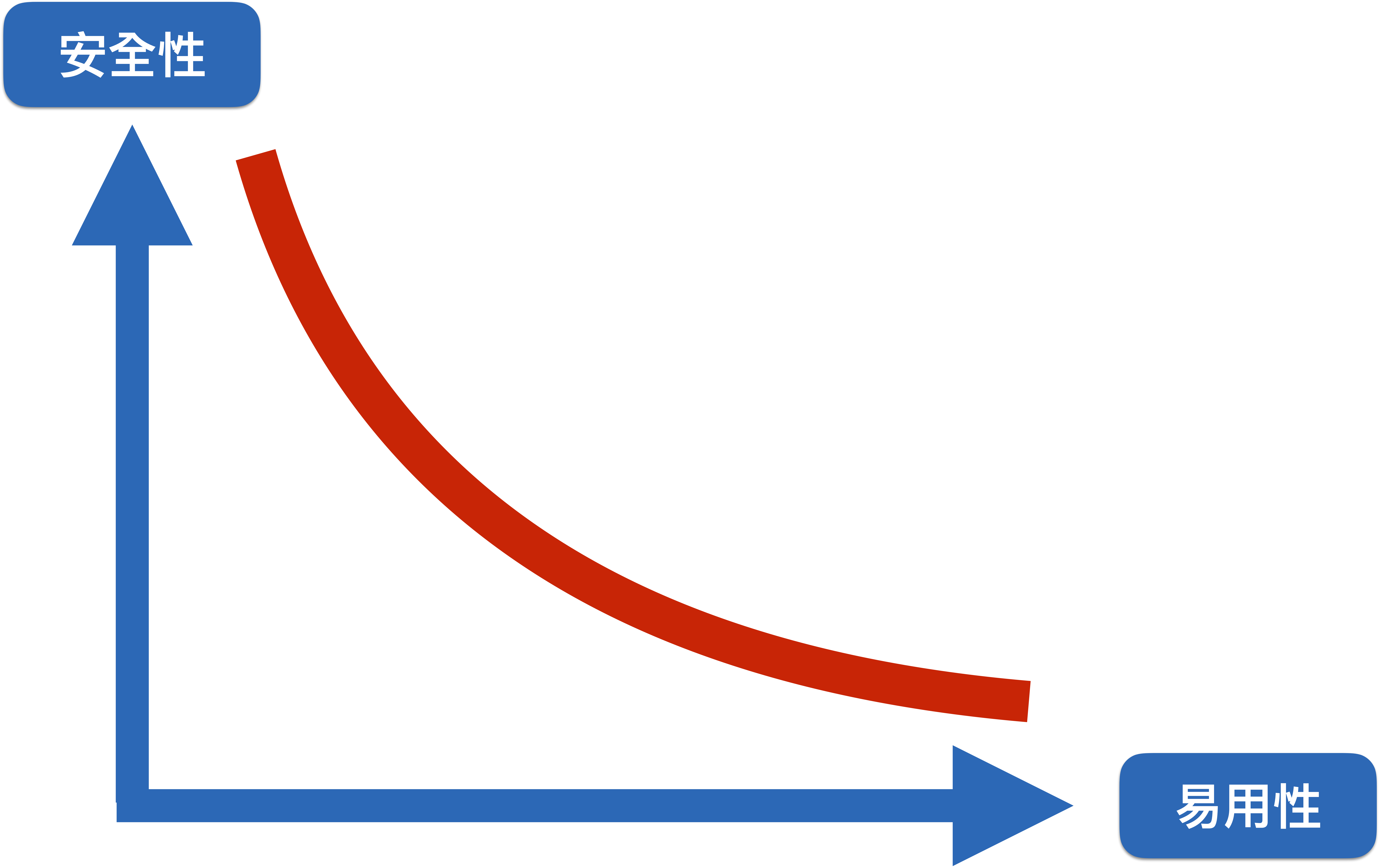
同等級 RSA 與 ECDSA 金鑰長度比較

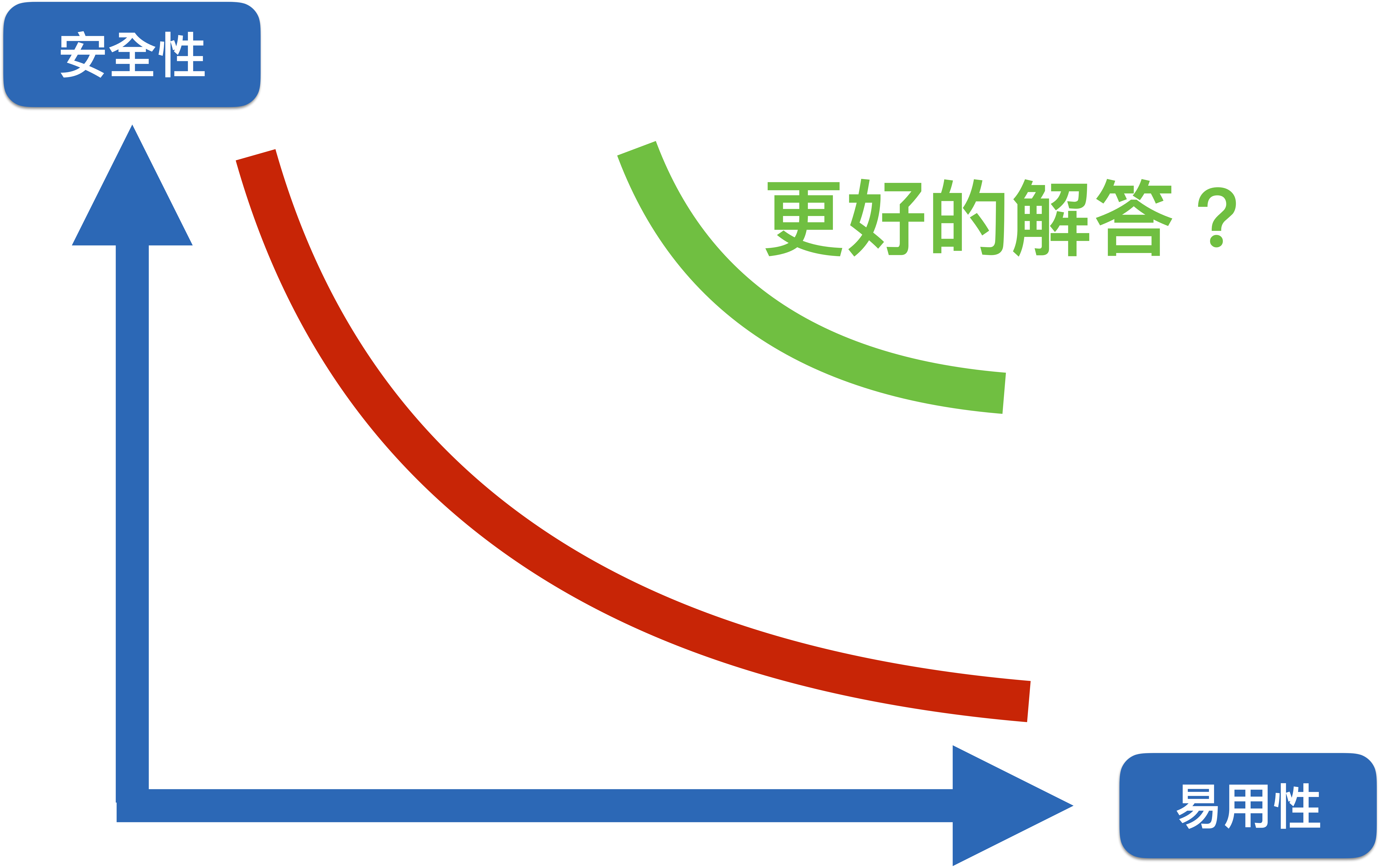
AES	RSA	ECDSA
128	3072	256
192	7680	384
256	15360	512

非對稱式（公鑰）認證架構

- 只有「公鑰」、「簽名」會離開客戶端
- 最重要的「私鑰」、「簽章計算」都在本地端進行

- 例一： TLS 的 client-side certificate
- 例二： SSH 的 PubkeyAuthentication 登入
- 許多非常不 user-friendly 的例子


安全性
易用性


安全性
更好的解答？
易用性

於是 FIDO 聯盟出現了

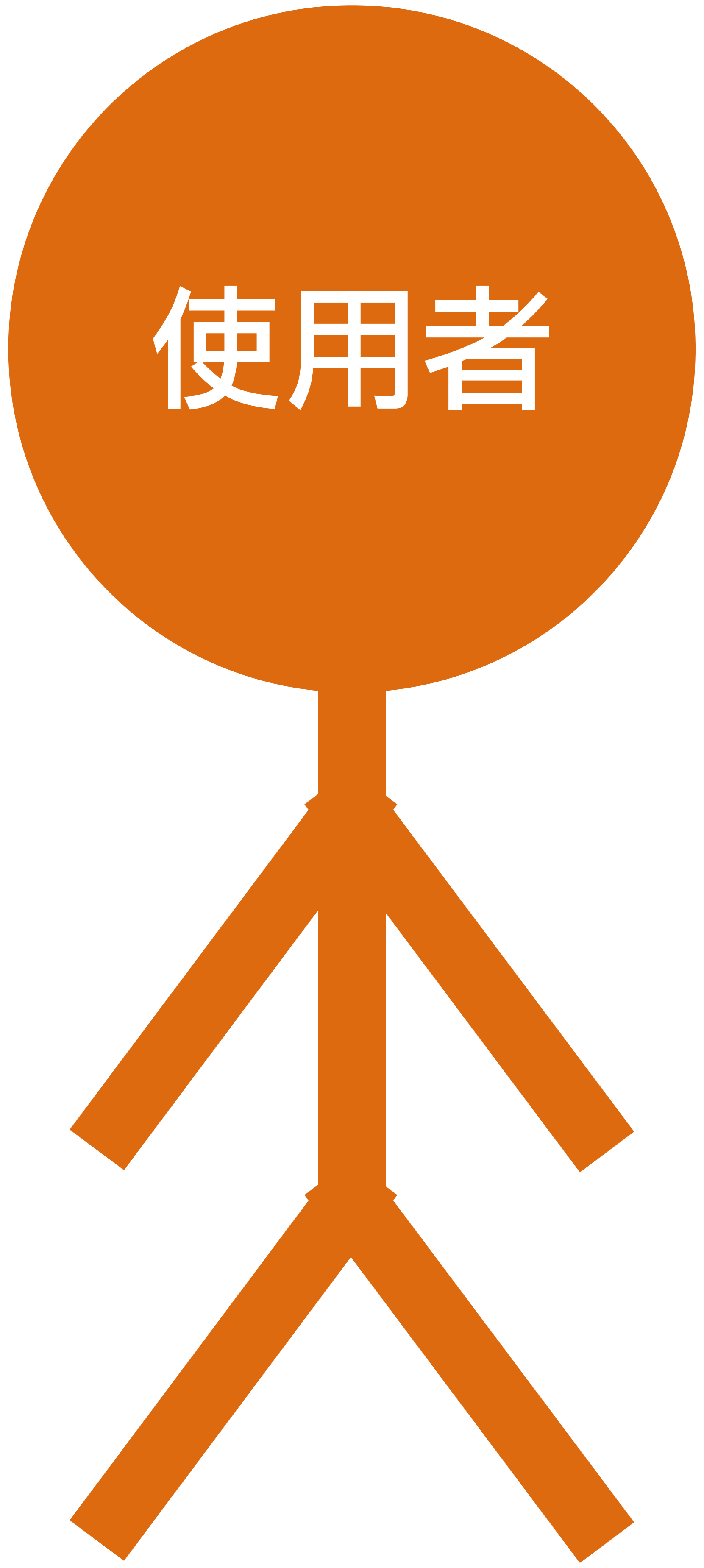
`fidoalliance.org`

FIDO 聯盟

- 提出跨平台、通用的、高安全強度的身份認證協議
- 更安全、更便利
- 標準化： U2F / UAF / FIDO 2.0

UAF 提供「免密碼」使用者體驗

UAF 將身份認證拆成兩段



終端設備

手機、平板、筆電
或獨立的硬體設備

遠端服務

某個服務的
遠端伺服器

UAF 將身份認證拆成兩段

使用者

密碼 / 指紋 /
聲紋 / ....

終端設備

手機、平板、筆電
或獨立的硬體設備

遠端服務

某個服務的
遠端伺服器

UAF 將身份認證拆成兩段

使用者

密碼 / 指紋 /
聲紋 / ....

終端設備

手機、平板、筆電
或獨立的硬體設備

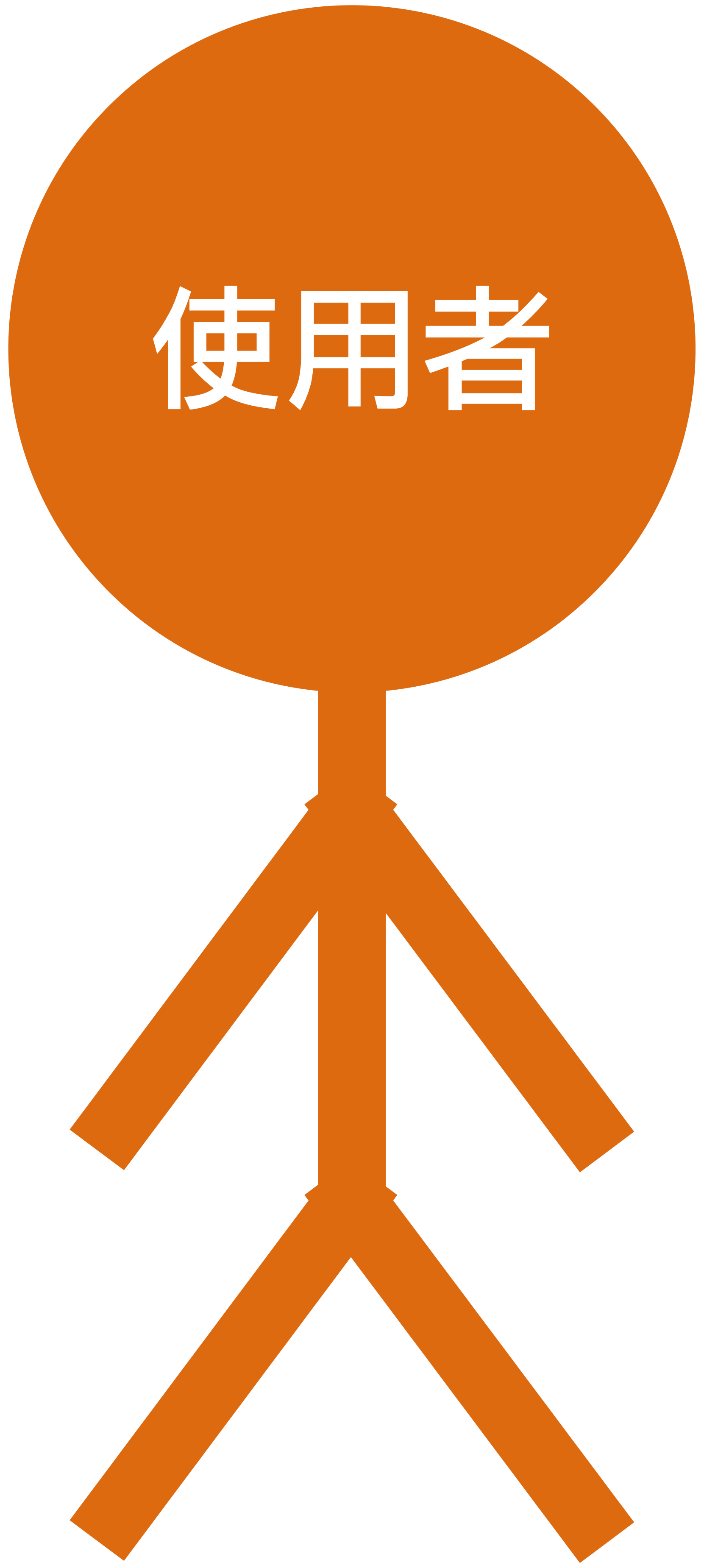
公鑰數位簽章

遠端服務

某個服務的
遠端伺服器

U2F 提供比 OTP 更強的替代品

傳統 OTP 兩步驟身份驗證



終端設備

手機、平板、筆電

OTP 產生器

軟體、硬體

遠端服務

某個服務的
遠端伺服器

傳統 OTP 兩步驟身份驗證

使用者

密碼

終端設備

手機、平板、筆電

密碼

OTP 產生器

軟體、硬體

遠端服務

某個服務的
遠端伺服器

傳統 OTP 兩步驟身份驗證

使用者

密碼

終端設備

手機、平板、筆電

密碼

OTP 產生器

軟體、硬體

一次性密碼

遠端服務

某個服務的
遠端伺服器

U2F 提供第二步身份驗證

使用者

終端設備

手機、平板、筆電

U2F 鑰匙

USB/NFC/BLE

遠端服務

某個服務的
遠端伺服器

U2F 提供第二步身份驗證

使用者

密碼

終端設備

手機、平板、筆電

密碼

遠端服務

某個服務的
遠端伺服器

U2F 鑰匙

USB/NFC/BLE

U2F 提供第二步身份驗證

使用者

密碼

終端設備

手機、平板、筆電

密碼

U2F 鑰匙

USB/NFC/BLE

公鑰數位簽章

遠端服務

某個服務的
遠端伺服器

目前已經部署 U2F 的知名網站

快速概覽 U2F 運作機制

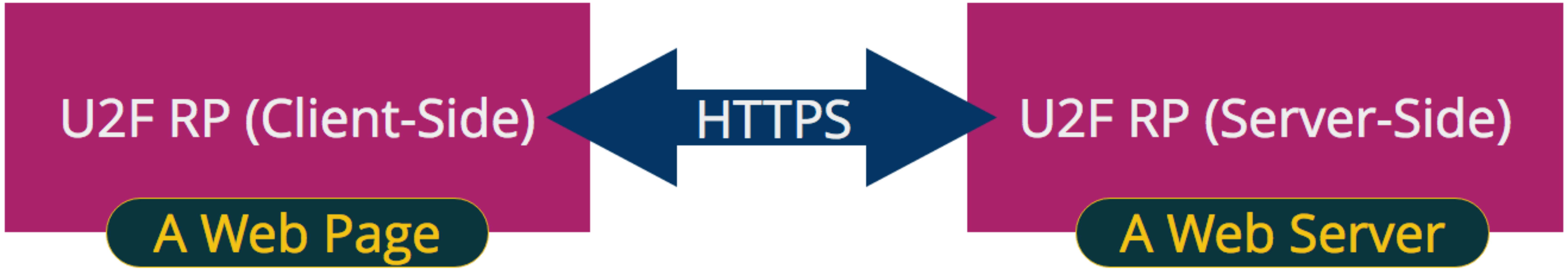
有三個角色

- U2F Relying Party (有 client 端和 server 端)
- U2F Client (瀏覽器原生實作或擴展)
- U2F Authenticator (如 USB 版的 Yubico Security Key)

有兩個操作流程

1. Registration
   使用者想要註冊一個新的 U2F security key

2. Authentication
   要求使用者使用註冊過的 U2F security key 證明身份



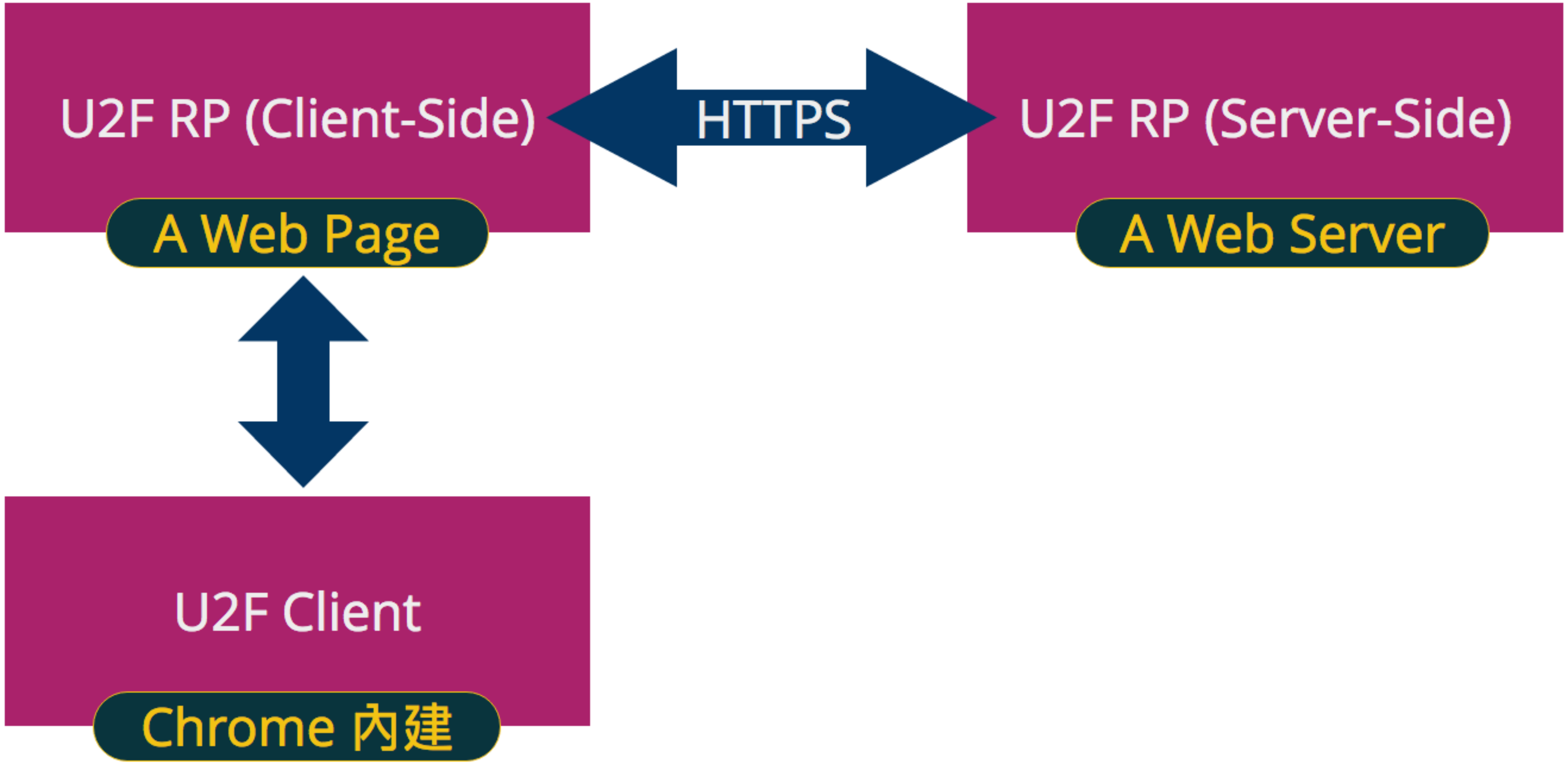
U2F RP (Client-Side)

A Web Page

HTTPS

U2F RP (Server-Side)

A Web Server



U2F RP (Client-Side)

A Web Page

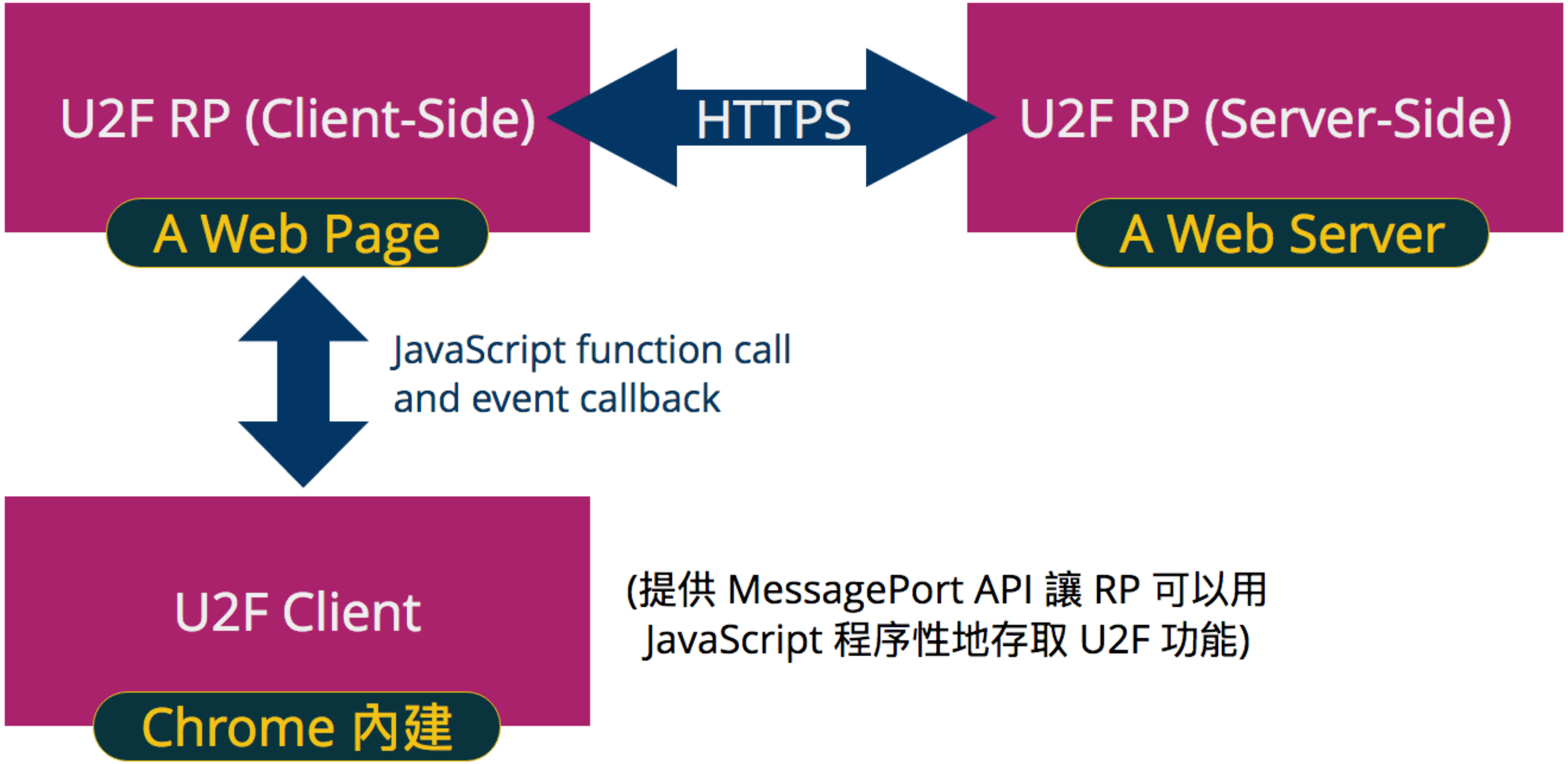
HTTPS

U2F RP (Server-Side)

A Web Server

U2F Client

Chrome 內建



U2F RP (Client-Side)

A Web Page

HTTPS

U2F RP (Server-Side)

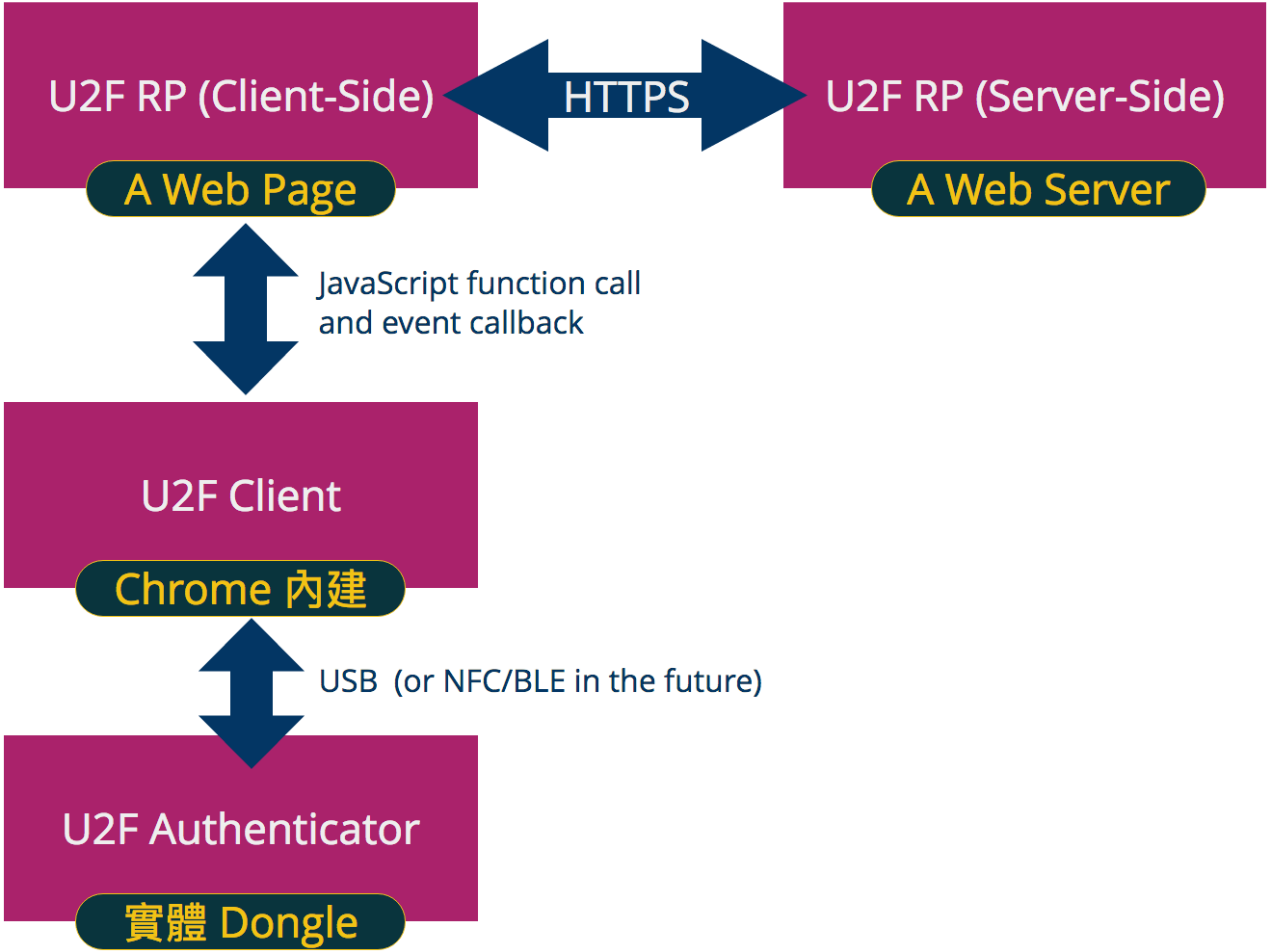
A Web Server

JavaScript function call
and event callback

U2F Client

Chrome 內建

(提供 MessagePort API 讓 RP 可以用
JavaScript 程序性地存取 U2F 功能)



U2F RP (Client-Side)

A Web Page

HTTPS

U2F RP (Server-Side)

A Web Server

JavaScript function call
and event callback

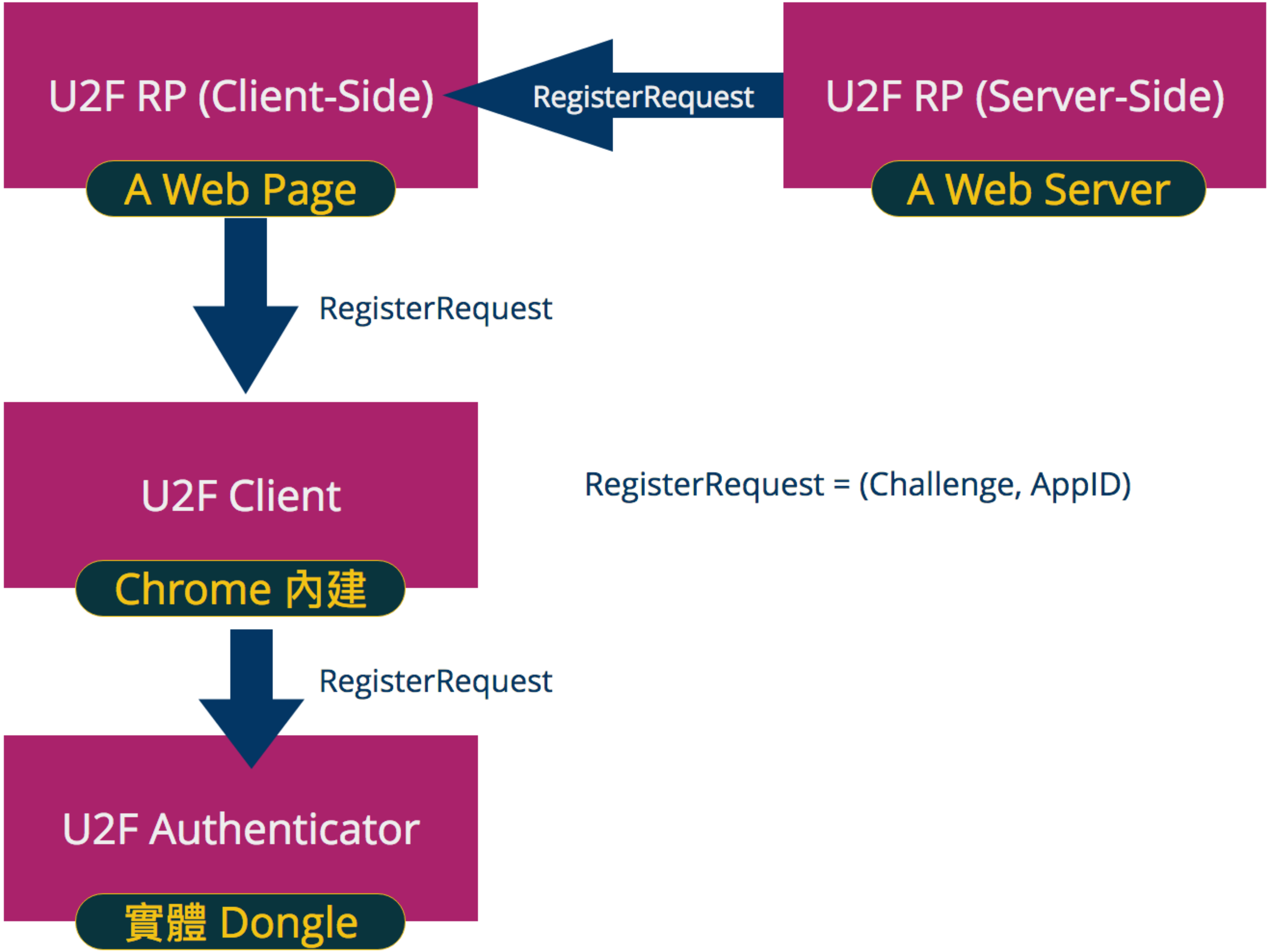
U2F Client

Chrome 內建

USB (or NFC/BLE in the future)

U2F Authenticator

實體 Dongle



U2F RP (Client-Side)

A Web Page

RegisterRequest

U2F RP (Server-Side)

A Web Server

RegisterRequest

U2F Client

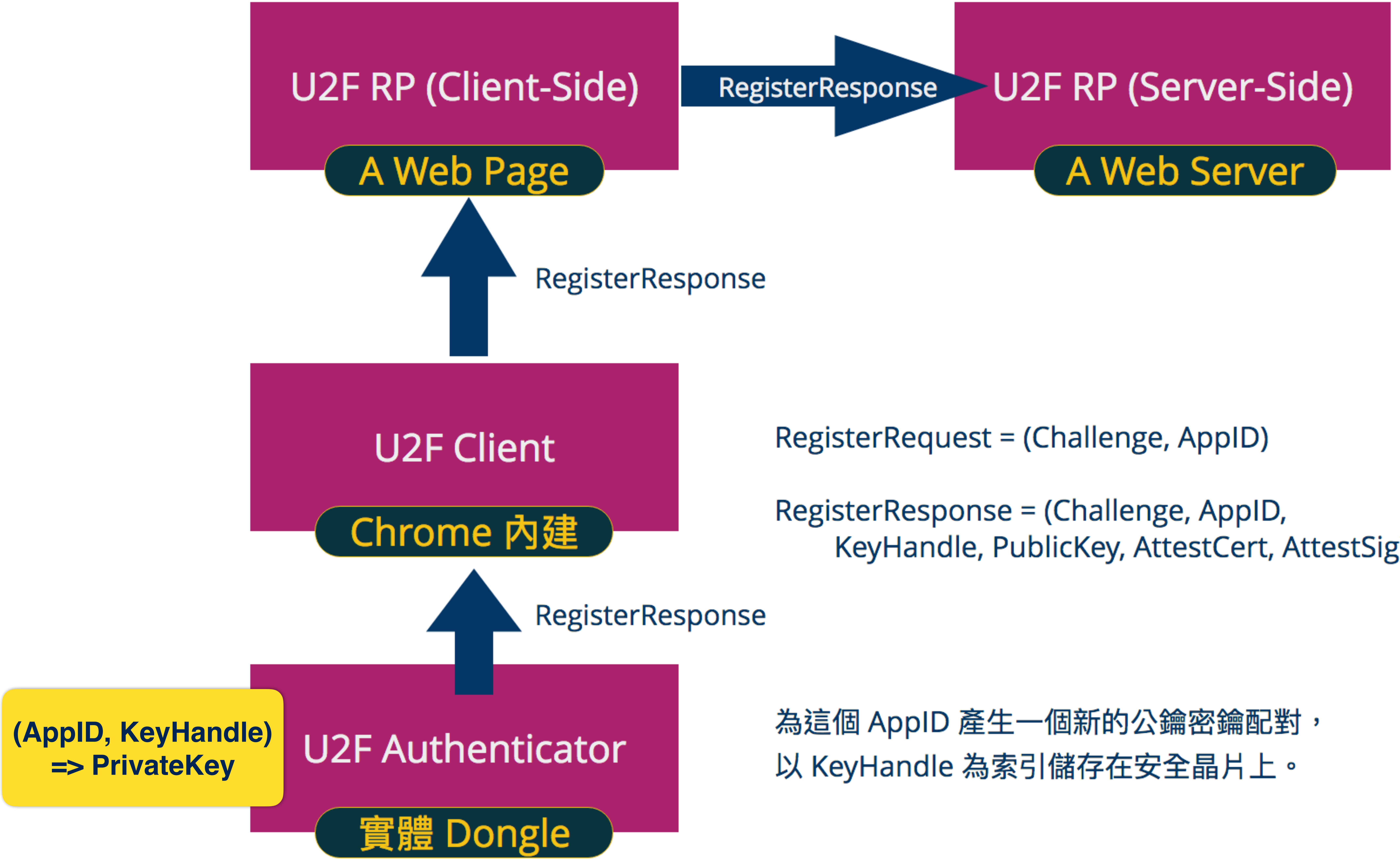
Chrome 內建

RegisterRequest

U2F Authenticator

實體 Dongle

RegisterRequest = (Challenge, AppID)



U2F RP (Client-Side)

A Web Page

RegisterResponse

U2F RP (Server-Side)

A Web Server

RegisterResponse

U2F Client

Chrome 內建

RegisterResponse

(AppID, KeyHandle)
=> PrivateKey

U2F Authenticator

實體 Dongle

RegisterRequest = (Challenge, AppID)

RegisterResponse = (Challenge, AppID,
KeyHandle, PublicKey, AttestCert, AttestSig)

為這個 AppID 產生一個新的公鑰密鑰配對，
以 KeyHandle 為索引儲存在安全晶片上。

(KeyHandle, PublicKey)

U2F RP (Client-Side)

A Web Page

RegisterResponse

U2F RP (Server-Side)

A Web Server

RegisterResponse

U2F Client

Chrome 內建

RegisterResponse

U2F Authenticator

實體 Dongle

(AppID, KeyHandle)
=> PrivateKey

RegisterRequest = (Challenge, AppID)

RegisterResponse = (Challenge, AppID,
KeyHandle, PublicKey, AttestCert, AttestSig)

為這個 AppID 產生一個新的公鑰密鑰配對，
以 KeyHandle 為索引儲存在安全晶片上。

(KeyHandle, PublicKey)

U2F RP (Server-Side)

A Web Server

SignRequest

U2F RP (Client-Side)

A Web Page

SignRequest

U2F Client

Chrome 內建

SignRequest

U2F Authenticator

實體 Dongle

(AppID, KeyHandle)
=> PrivateKey

SignRequest = (Challenge, AppID, KeyHandle)

(KeyHandle, PublicKey)

U2F RP (Client-Side)

A Web Page

SignResponse

U2F RP (Server-Side)

A Web Server

SignResponse

U2F Client

Chrome 內建

SignResponse

(AppID, KeyHandle)
=> PrivateKey

U2F Authenticator

實體 Dongle

SignRequest = (Challenge, AppID, KeyHandle)

SignResponse = (Challenge, AppID, KeyHandle
AuthCounter, AuthSig)

使用 KeyHandle 對應到的密鑰做數位簽章。
AuthCounter 是隨著操作而不斷遞增的計數器。

U2F 的安全性

- **Web 流量強制使用 HTTPS**

U2F 的安全性

- **Web 流量強制使用 HTTPS**
- **防釣魚：U2F 訊息和瀏覽器所看到的 web origin 綁定**

U2F 的安全性

- **Web 流量強制使用 HTTPS**
- **防釣魚：U2F 訊息和瀏覽器所看到的 web origin 綁定**
- **其實 authenticator 根本不知道你登入了哪個網站**

U2F 的安全性

- **Web 流量強制使用 HTTPS**
- **防釣魚：U2F 訊息和瀏覽器所看到的 web origin 綁定**
- **其實 authenticator 根本不知道你登入了哪個網站**
- **完全沒有 trusted 3rd party 介入，無 OAuth 那種隱私疑慮**

U2F 的安全性

- **Web 流量強制使用 HTTPS**
- **防釣魚：U2F 訊息和瀏覽器所看到的 web origin 綁定**
- **其實 authenticator 根本不知道你登入了哪個網站**
- **完全沒有 trusted 3rd party 介入，無 OAuth 那種隱私疑慮**
- **伺服器不擔心「公鑰」資料被看到，只要確保不被竄改**

U2F 的安全性

- **Web 流量強制使用 HTTPS**
- **防釣魚：U2F 訊息和瀏覽器所看到的 web origin 綁定**
- **其實 authenticator 根本不知道你登入了哪個網站**
- **完全沒有 trusted 3rd party 介入，無 OAuth 那種隱私疑慮**
- **伺服器不擔心「公鑰」資料被看到，只要確保不被竄改**
- **使用者可以用特製的硬體保護 ECDSA 私密金鑰**

U2F 函式庫實作

花一些時間在讀書…

https://fidoalliance.org/specs/fido-u2f-v1.0-ps-20141009/

怎麼學新東西最快？

- 讀標準文件
- 買別人做好的產品來試試看（硬體）
- 找 GitHub 上有開源的函式庫來看看

怎麼學新東西最快？

- 讀標準文件
- 買別人做好的產品來試試看（硬體）
- 找 GitHub 上有開源的函式庫來看看

Yubico 已經開源過類似的專案

- https://github.com/Yubico/python-u2flib-server
- 不喜歡他包裝的介面
- 不喜歡它依賴的一些外部套件
- 程式碼行數尚未破萬...

怎麼學新東西最快？

- 讀標準文件
- 買別人做好的產品來試試看（硬體）
- 找 GitHub 上有開源的函式庫來看看
- 何不自幹一個函式庫試試看？！

需要什麼

- 大數運算
- 橢圓曲線密碼學
- ASN.1 與 X.509 的資料結構處理
- U2F 標準實作

第一版的效能

```
+------------------------------------------------------+
| On my laptop            U2F operation     ECDSA      |
+------------------------------------------------------+
| lightu2f (original)     100.0 ms         99.9 ms     |
+------------------------------------------------------+
```

第一版的效能

```
+-----------------------------------------------------+
| On my laptop            U2F operation     ECDSA     |
+-----------------------------------------------------+
| lightu2f (original)     100.0 ms         99.9 ms    |
| OpenSSL (0.9.8zh)           N/A           1.0 ms    |
+-----------------------------------------------------+
```

第一版的效能

```
+-----------------------------------------------------+
| On my laptop            U2F operation     ECDSA     |
+-----------------------------------------------------+
| lightu2f (original)    100.0 ms         99.9 ms    |
| OpenSSL (0.9.8zh)          N/A           1.0 ms    |
| OpenSSL (1.0.2h)           N/A           0.1 ms    |
+-----------------------------------------------------+
```

橢圓曲線核心運算優化

- 蒙哥馬利階梯
- 尋找 U2F 指定曲線 (P-256) 目前最快的階梯演算法

  (Memory-Constrained Implementations of Elliptic Curve Cryptography in Co-Z Coordinate Representation)
- 重構、實作新的演算法

4. Rule to add two points with different x-coordinates: Let $(x_1, y_1) \in E(\mathbb{F}_p)$ and $(x_2, y_2) \in E(\mathbb{F}_p)$ be two points such that $x_1 \neq x_2$. Then $(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$, where:

$$x_3 \equiv \lambda^2 - x_1 - x_2 \pmod{p}, \; y_3 \equiv \lambda(x_1 - x_3) - y_1 \pmod{p}, \text{ and } \lambda \equiv \frac{y_2 - y_1}{x_2 - x_1} \pmod{p}.$$

5. Rule to add a point to itself (double a point): Let $(x_1, y_1) \in E(\mathbb{F}_p)$ be a point with $y_1 \neq 0$. Then $(x_1, y_1) + (x_1, y_1) = (x_3, y_3)$, where:

$$x_3 \equiv \lambda^2 - 2x_1 \pmod{p}, \; y_3 \equiv \lambda(x_1 - x_3) - y_1 \pmod{p}, \text{ and } \lambda \equiv \frac{3x_1^2 + a}{2y_1} \pmod{p}.$$

Algorithm 6 Out-of-place differential addition-and-doubling in projective co-Z coordinate system using $10\mathsf{M} + 5\mathsf{S} + 13\mathsf{add}$ and 10 registers.

```
Require: $X_1$, $X_2$, $T_D = x_D Z$, $T_a = aZ^2$, $T_b = 4bZ^3$
Ensure: $X_1$, $X_2$, $T_D$, $T_a$, $T_b$
    1. $R_2 \leftarrow X_1 - X_2$
    2. $R_1 \leftarrow {R_2}^2$
    3. $R_2 \leftarrow {X_2}^2$
    4. $R_3 \leftarrow R_2 - T_a$
    5. $R_4 \leftarrow R_3^2$
    6. $R_5 \leftarrow X_2 + X_2$
    7. $R_3 \leftarrow R_5 \times T_b$
    8. $R_4 \leftarrow R_4 - R_3$
    9. $R_5 \leftarrow R_5 + R_5$
    10. $R_2 \leftarrow R_2 + T_a$
    11. $R_3 \leftarrow R_5 \times R_2$
    12. $R_3 \leftarrow R_3 + T_b$
    13. $R_5 \leftarrow X_1 + X_2$
    14. $R_2 \leftarrow R_2 + T_a$
    15. $R_2 \leftarrow R_2 - R_1$
    16. $X_2 \leftarrow {X_1}^2$
    17. $R_2 \leftarrow R_2 + X_2$
    18. $X_2 \leftarrow R_5 \times R_2$
    19. $X_2 \leftarrow X_2 + T_b$
    20. $X_1 \leftarrow R_3 \times X_2$
    21. $X_2' \leftarrow R_1 \times R_4$
    22. $R_2 \leftarrow R_1 \times R_3$
    23. $R_3 \leftarrow R_2 \times T_b$
    24. $R_4 \leftarrow {R_2}^2$
    25. $R_1 \leftarrow T_D \times R_2$
    26. $R_2 \leftarrow T_a \times R_4$
    27. $T_b \leftarrow R_3 \times R_4$
    28. $X_1 \leftarrow X_1 - R_1$
    29. $T_D \leftarrow R_1$
    30. $T_a \leftarrow R_2$
return $(X_1, X_2, T_D, T_a, T_b)$
```

第二版的效能

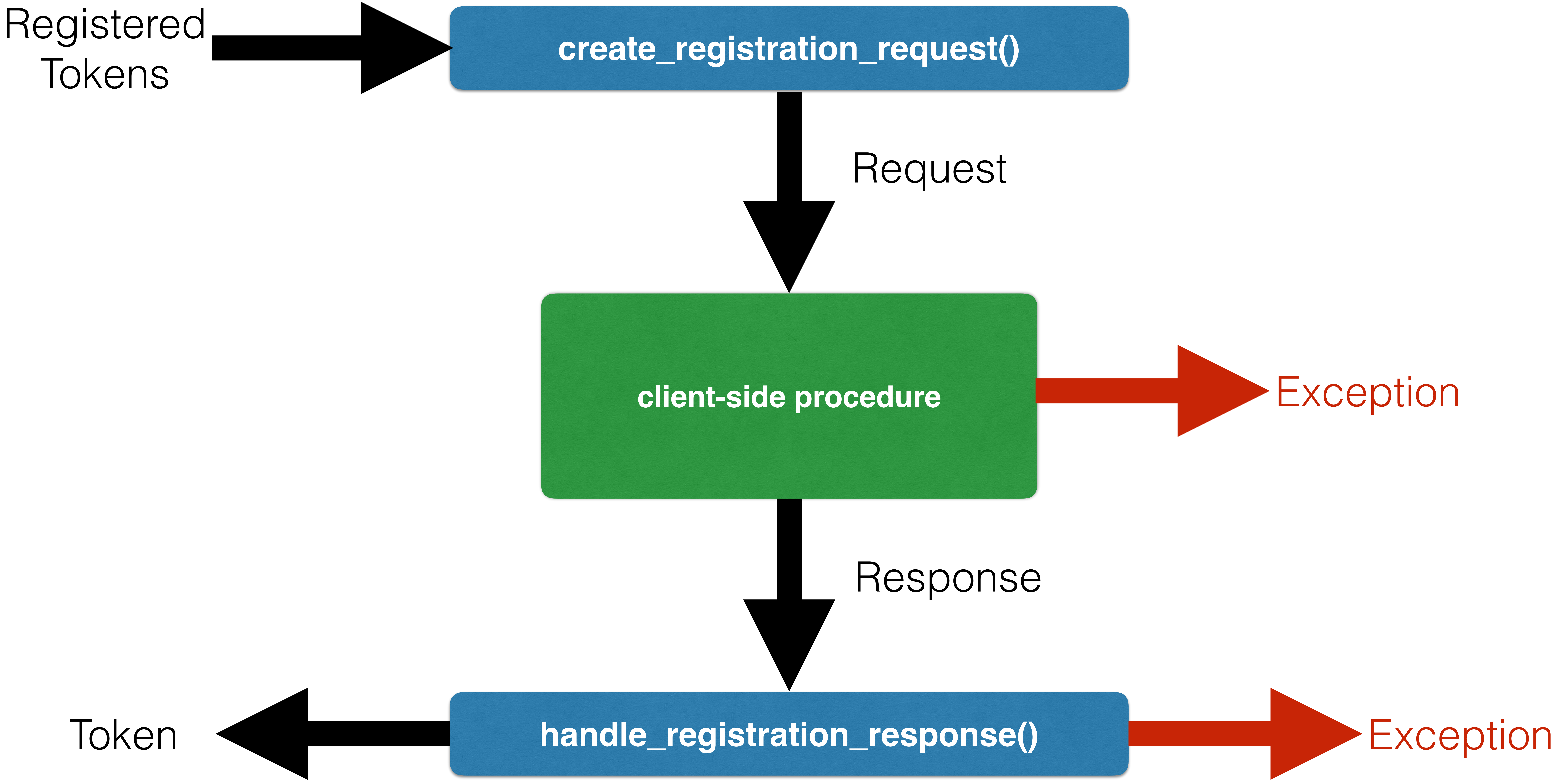
```
+-----------------------------------------------------+
| On my laptop            U2F operation     ECDSA     |
+-----------------------------------------------------+
| lightu2f (original)     100.0 ms         99.9 ms    |
| OpenSSL (0.9.8zh)           N/A           1.0 ms    |
| OpenSSL (1.0.2h)            N/A           0.1 ms    |
| lightu2f                 10.0 ms          9.7 ms    |
+-----------------------------------------------------+
```

第二版的效能

```
+-----------------------------------------------------+
| On my laptop            U2F operation     ECDSA     |
+-----------------------------------------------------+
| lightu2f (original)     100.0 ms         99.9 ms    |
| OpenSSL (0.9.8zh)           N/A           1.0 ms    |
| OpenSSL (1.0.2h)            N/A           0.1 ms    |
| lightu2f                 10.0 ms          9.7 ms    |
| python-u2flib-server     70.0 ms          0.3 ms    |
+-----------------------------------------------------+
```

`concise/lightu2f.py`

- 單一檔案套件 (不到 800 行)
- 還需要繼續重構
- 文件待補
- https://github.com/concise/lightu2f.py



Registered Tokens

create_registration_request()

Request

client-side procedure

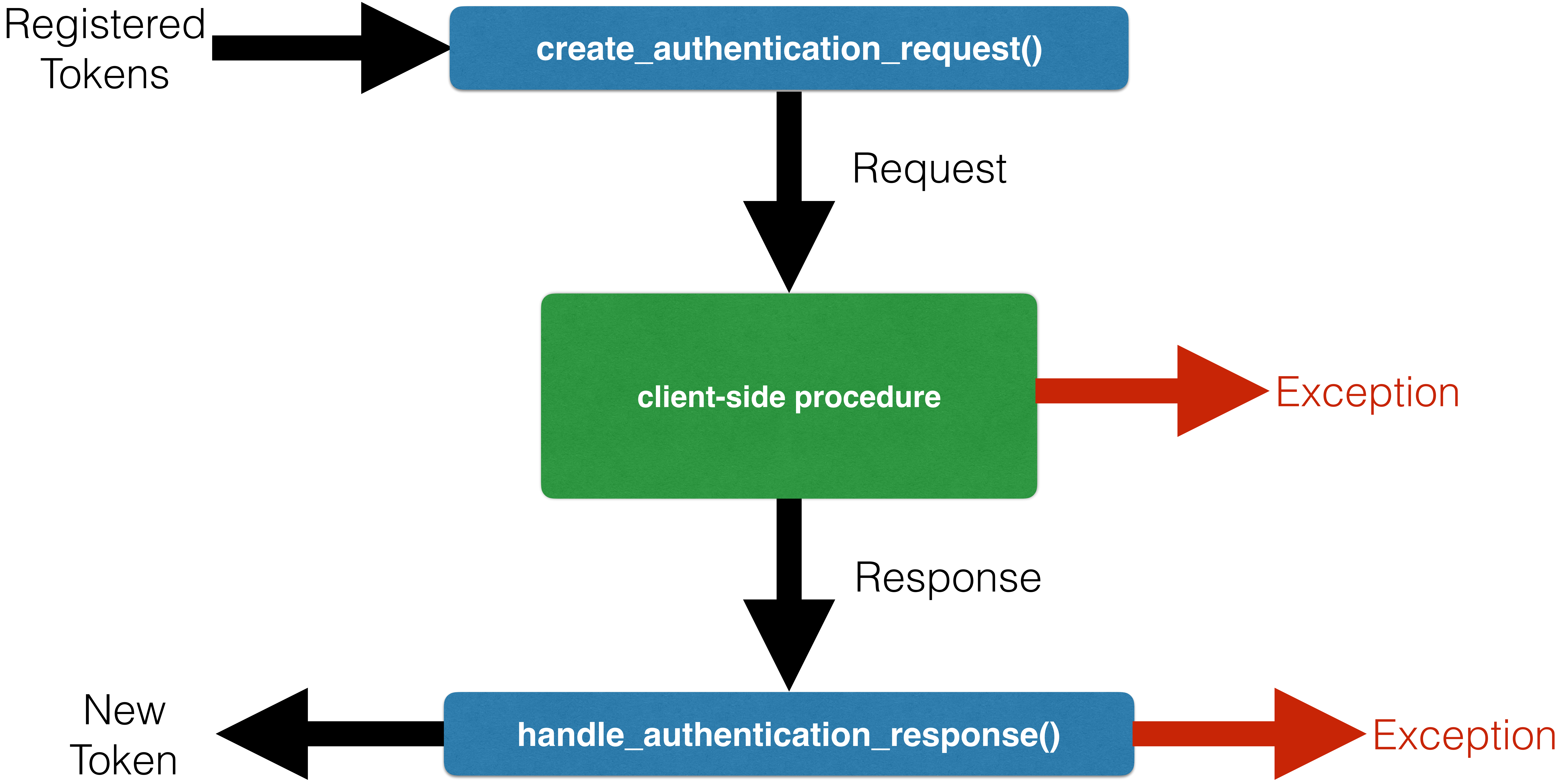
Exception

Response

Token

handle_registration_response()

Exception



Registered Tokens

create_authentication_request()

Request

client-side procedure

Exception

Response

New Token

handle_authentication_response()

Exception