W3C TPAC 2023 : 톺아보기

Secure Login on Foldable Web

Passkey, and Device Posture API

SAMSUNG Internet

Gooroomee W3C

임동우 (삼성전자 MX사업부)

Samsung Internet 브라우저 PM

W3C 표준화 삼성전자 대표 (AC Rep.)

Chromium / WebKit 오픈소스 Committer

Contents

Gooroomee W3C

1

Samsung Internet Browser

SAMSUNG Internet

SAMSUNG

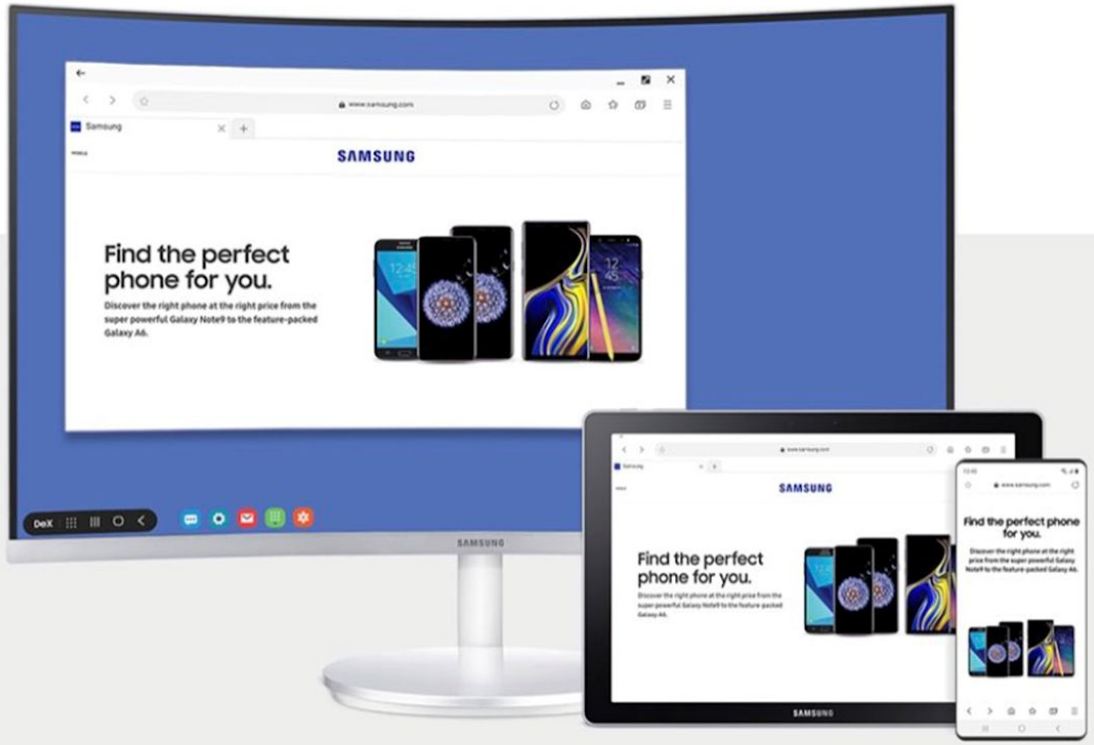
1st party browser of Samsung

2nd Most used browser in Android platform

3 platforms are supported : Android OS, Tizen OS, Wear OS

4 times Engine rebaseline per year, based on chromium

SAMSUNG Internet



Galaxy Experience

- Multi Device Experience
- S Pen
- Foldable Web

Privacy

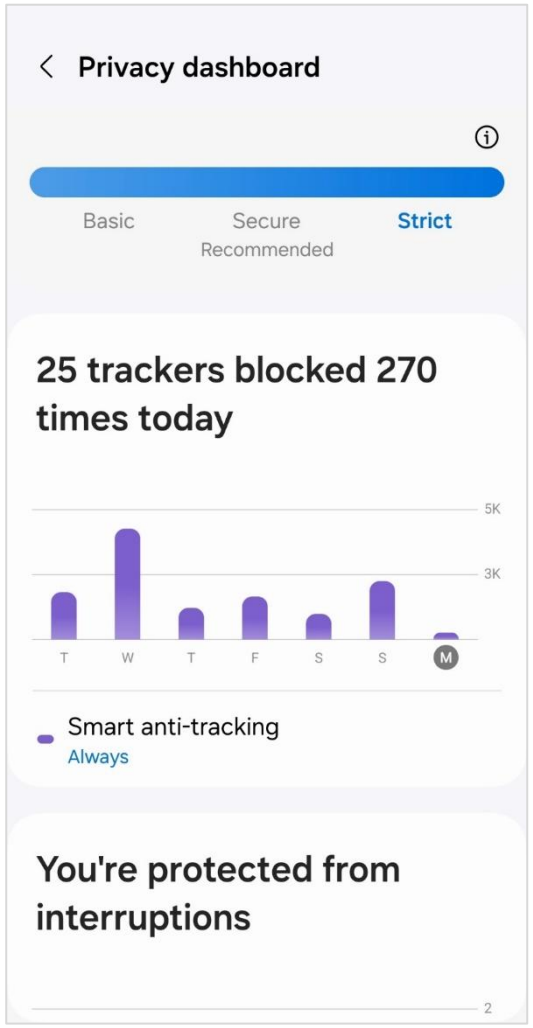
- Smart Anti-Tracking
- Privacy Dashboard
- Web Authentication

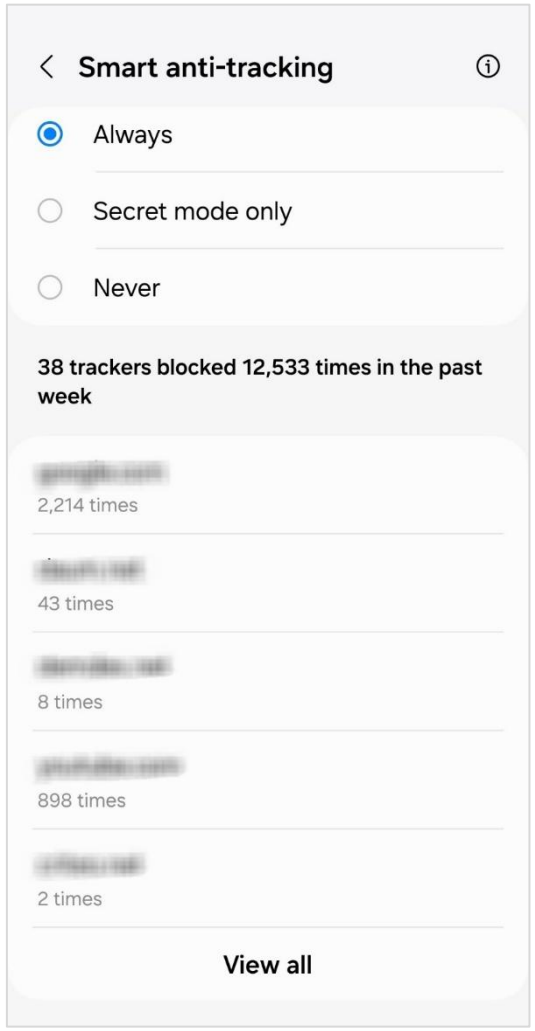
Usability

- Video Assistant
- Content Blocking
- Customize Menu

Privacy Dashboard

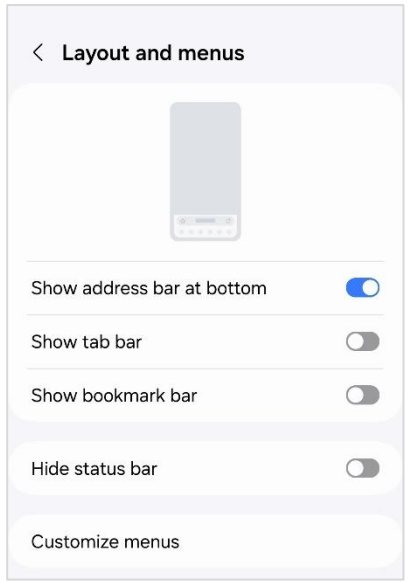
- Smart Anti-Tracking
- Tracker Block/Detect records
  - Daily summary of blocking
  - Detected tracker list

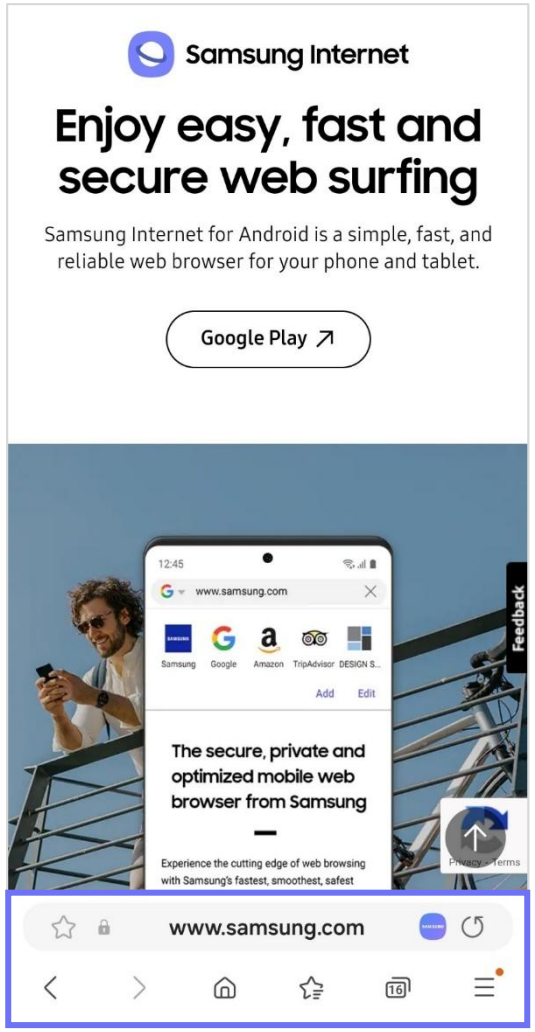


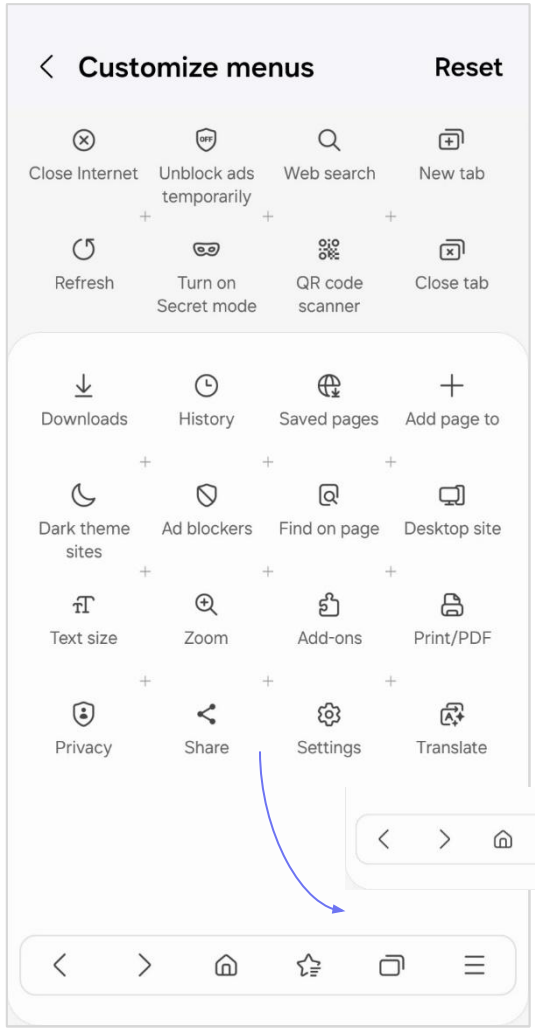


Customization

- App layout settings
- Customizable Toolbar items







2

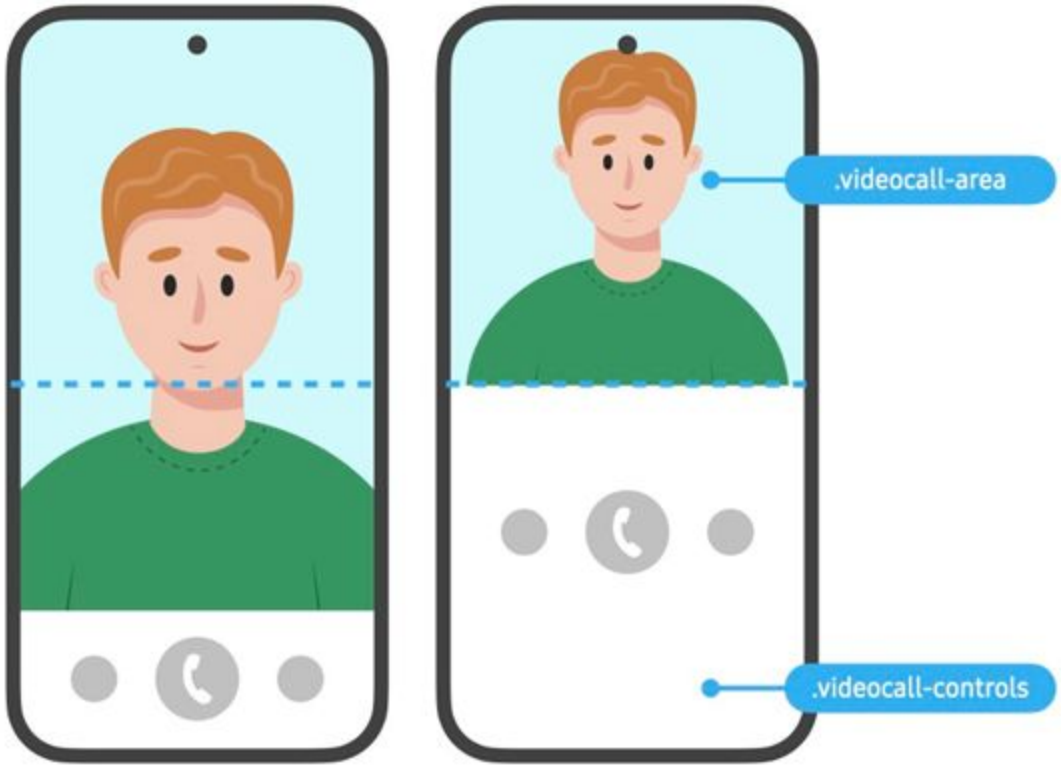
Device Posture API

02 / Device Posture API

Galaxy Z Fold 5 / Flip 5

What is benefit of Foldable devices? FLEX MODE

Content as seen on a flat screen for reference



~~Posture: Flat~~
~~Angle: 180°~~

Continuous

~~Posture: Laptop~~
~~Angle: 90°~~

Folded

~~Book, Tent, Tablet~~

Device Posture API

Device Posture API

W3C®

02 / Device Posture API

DevicePosture types

Continuous

"Flat" or "Tablet"

Folded

"Book" or "Laptop"

~~Folded-over~~

~~"Tent" position~~

02 / Device Posture API

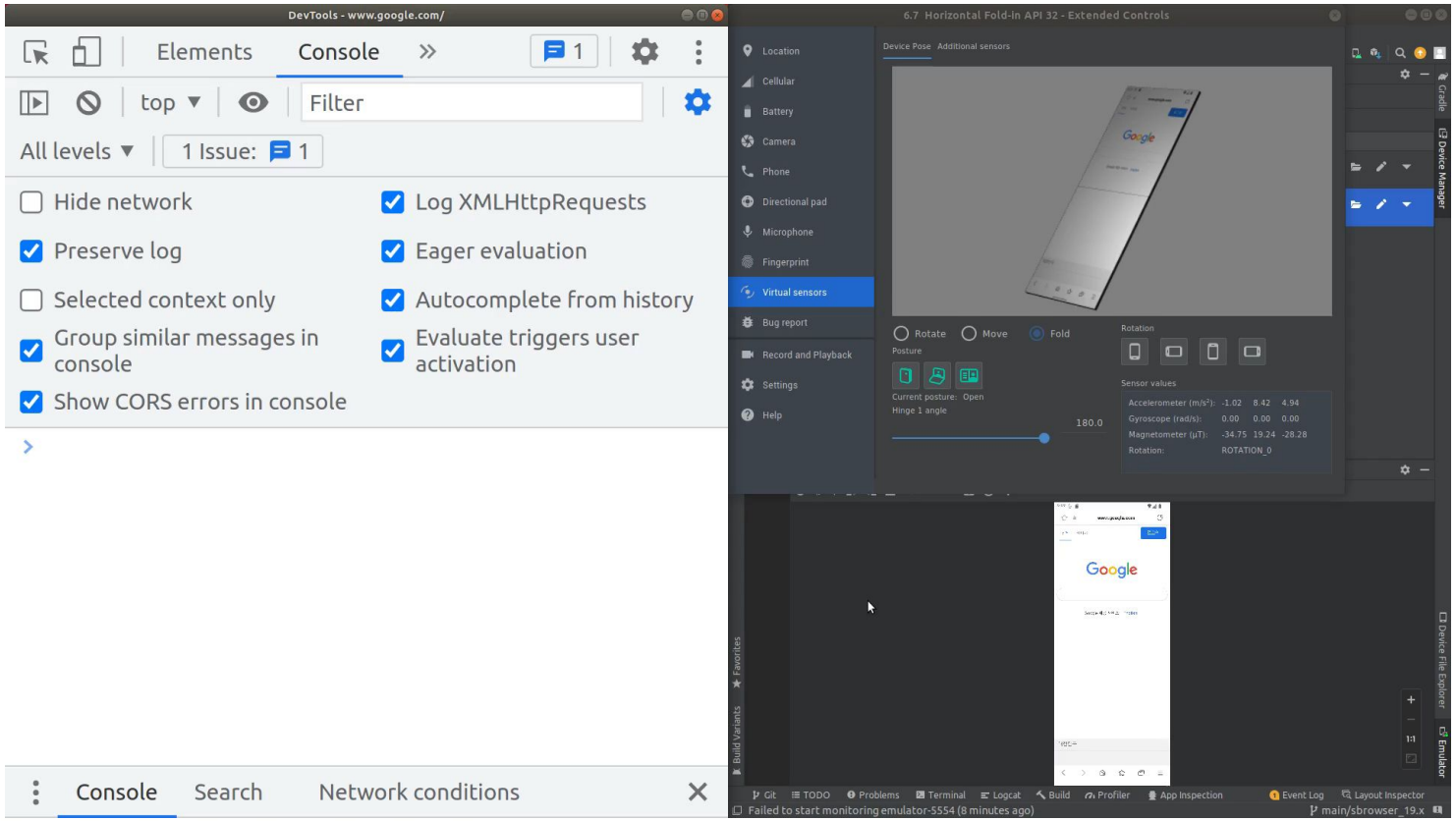
TPAC 2023, Devices and Sensors Working Group

- 현재 버전의 spec 에 이견 없음
- TAG (Technical Architecture Group) 리뷰 완료
- Wide Review 시작하기로 의결
  - Wide/Horizontal Review : Accessibility, Privacy, Security, Internationalization

※ *Working Draft ☐ Candidate Recommendation ☐ Proposed Recommendation ☐ W3C Recommendation*

02 / Device Posture API

DevicePosture onchange attribute



DevicePosture onchange attribute

```
navigator.devicePosture.addEventListener("change
",
        () => { console.log(`Current Posture is:
        ${navigator.devicePosture.type}`);
})
```

DevicePosture media feature

```
@media (device-posture: folded) {
    body {
      display: flex;
      flex-flow: column nowrap;
    }

    .videocall-area, .videocall-controls  {
      flex: 1 1 env(fold-bottom);
    }
  }
```

Foldable Web Experience on Whereby

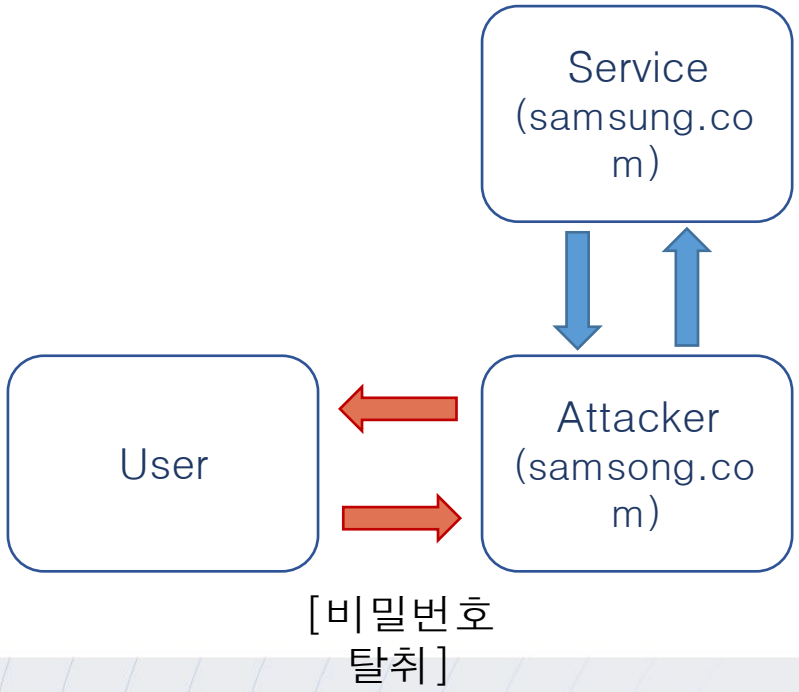
SAMSUNG × Whereby

3

Passkey

비밀번호 : 불편하고, 보안에 취약

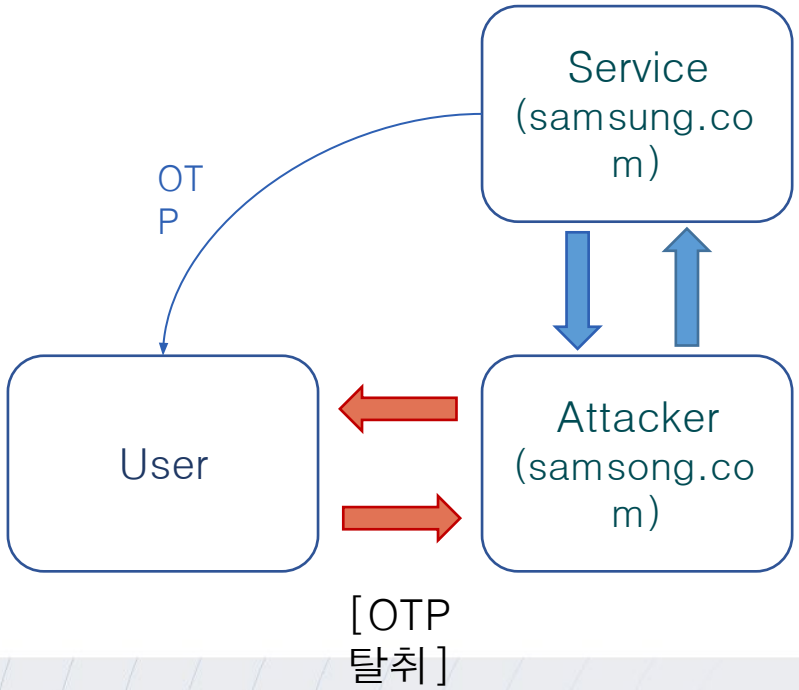
– 여러 웹사이트에 동일한 비밀번호 사용하는 사용자 존재함



탈취한 ID / 비밀번호를 여러 사이트에서 사용 가능

2nd Factor 인증 (OTP) : 여전히 보안 이슈 존재

- Man-in-the-middle 공격에 여전히 취약함

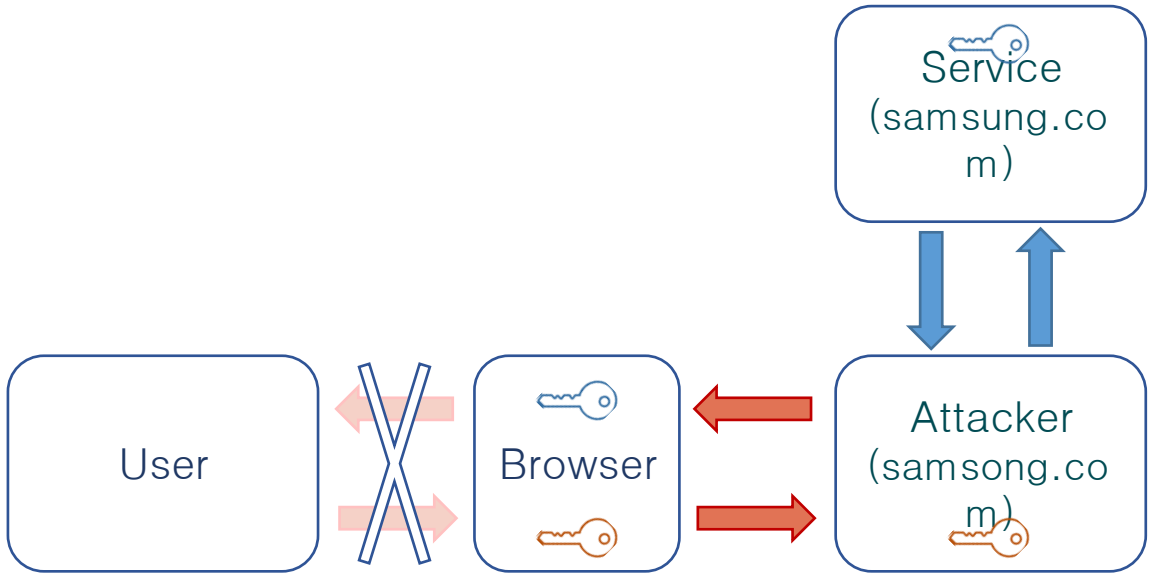


동일한 방식으로 OTP 탈취 및 사용 (일회성)

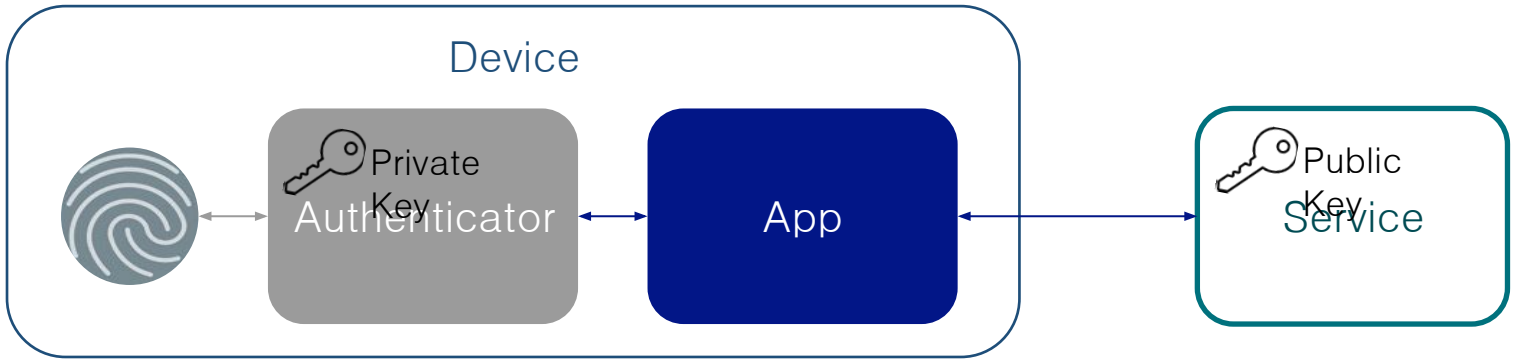
Key pair 방식의 인증

- User Agent (브라우저)가 현재 로딩되어 있는 페이지 도메인을 확인

  * Key pair 생성 후 Public key를 전달한 도메인을 확인 후 Private key 사용



FIDO UAF/U2F : **생체 인증**을 활용한 강력한 **본인 인증** 표준 (FIDO Alliance)



FIDO UAF/U2F 등록 프로세스

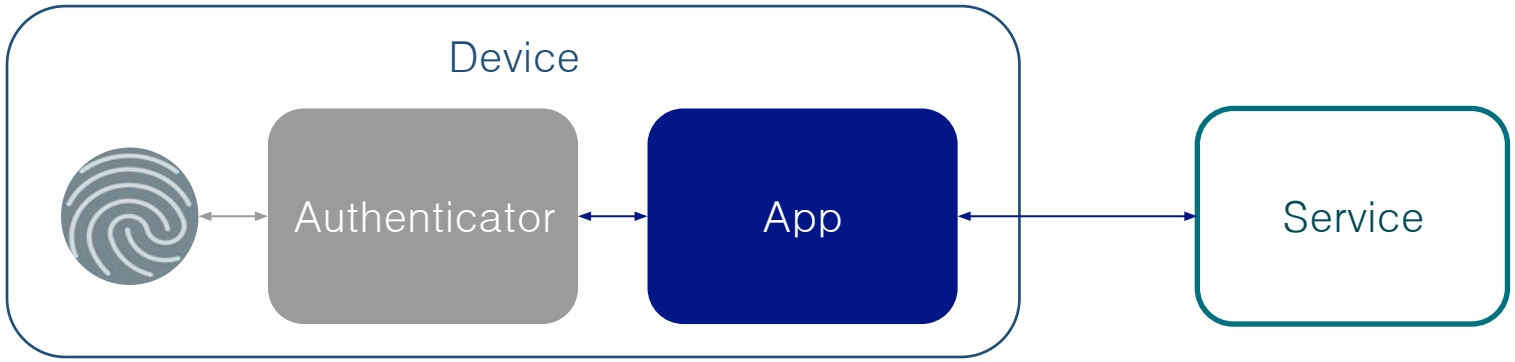
- Save User Info, Domain,
- Create Credential, Key-pair
- Save Private key

User Info	Kim Samsung
Domain	samsung.com
Credential	0x9ske876…
Private key	0x5krn863…

User Info, Challenge →

Credential, Public Key, Encrypted Challenge by Private key →

User Info	Kim Samsung
Credential	0x9ske876…
Public key	0x2kmb407…



FIDO UAF/U2F 인증 프로세스

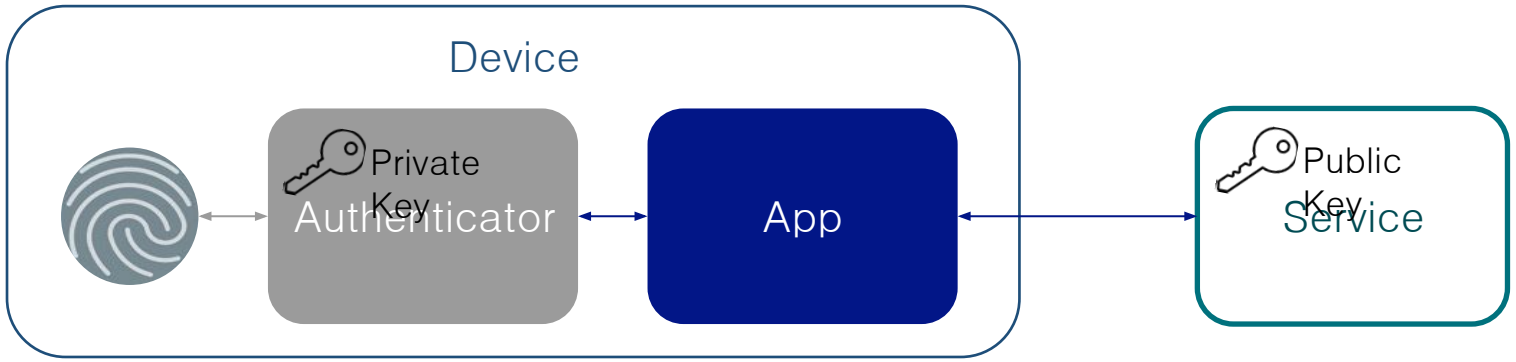
- Check User Info, Domain

User Info	Kim Samsung
Domain	samsung.com
Credential	0x9ske876…
Private key	0x5krn863…

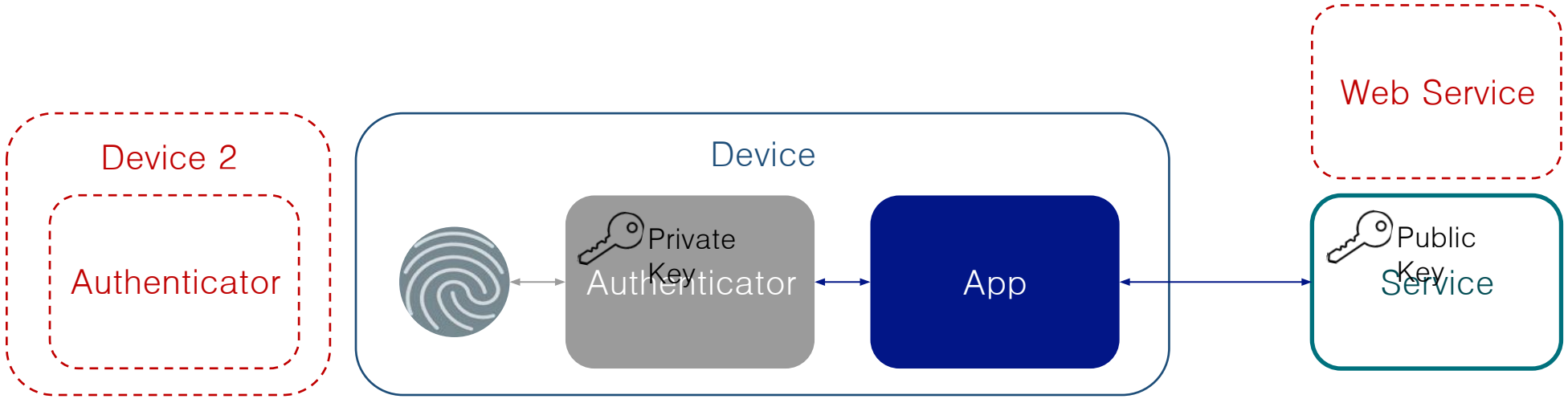
User Info, Challenge →

Credential, Encrypted Challenge by Private key ←

User Info	Kim Samsung
Credential	0x9ske876…
Public key	0x2kmb407…



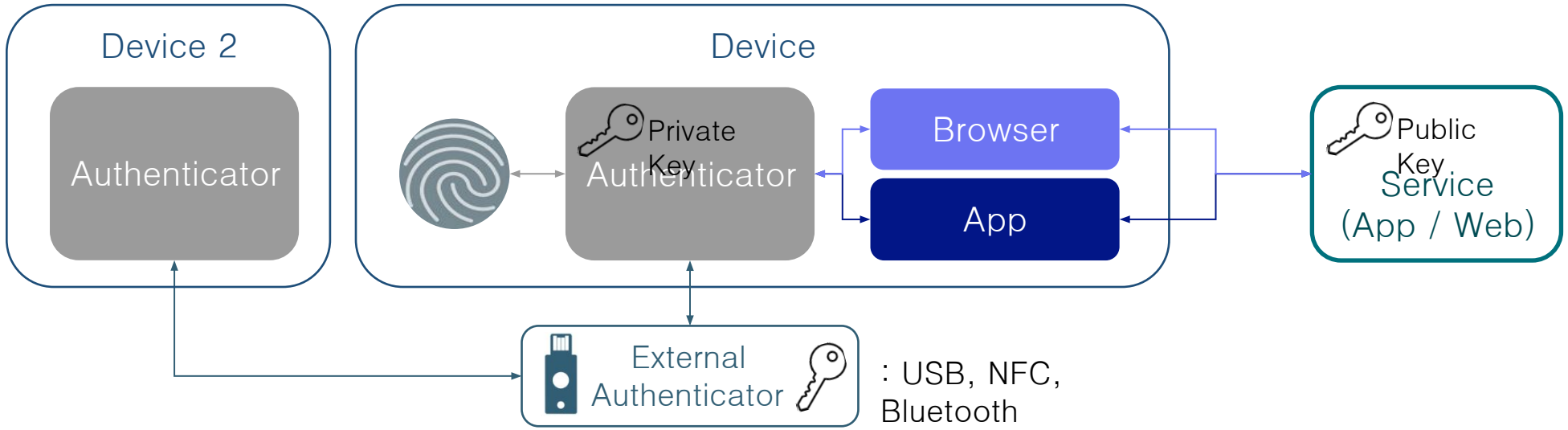
FIDO UAF/U2F 의 제약사항



03 / Passkey

FIDO2 : FIDO UAF/U2F

+ **CTAP** (Remote Authenticator) + **Web API** (Web Authentication API)



Web Authentication 등록 프로세스

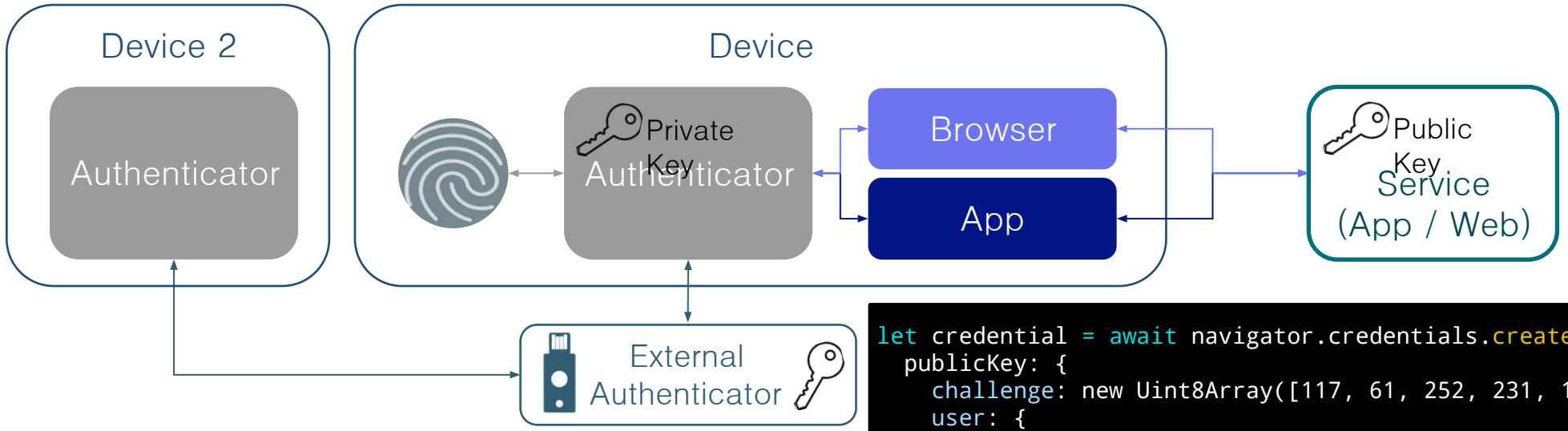
- Save User Info, Domain,
- Create Credential, Key-pair
- Save Private key

User Info	Kim Samsung
Domain	samsung.com
Credential	0x9ske876…
Private key	0x5krn863…

User Info, Challenge →

← Credential, Public Key, Encrypted Challenge by Private key

User Info	Kim Samsung
Credential	0x9ske876…
Public key	0x2kmb407…




```
let credential = await navigator.credentials.create({
  publicKey: {
    challenge: new Uint8Array([117, 61, 252, 231, 191, 241, ...]),
    user: {
      id: new Uint8Array([79, 252, 83, 72, 214, 7, 89, 26]),
      displayName: “Kim Samsung"
    },
    pubKeyCredParams: [ {type: "public-key", alg: -7} ]
  }
});
```

Web Authentication 인증 프로세스

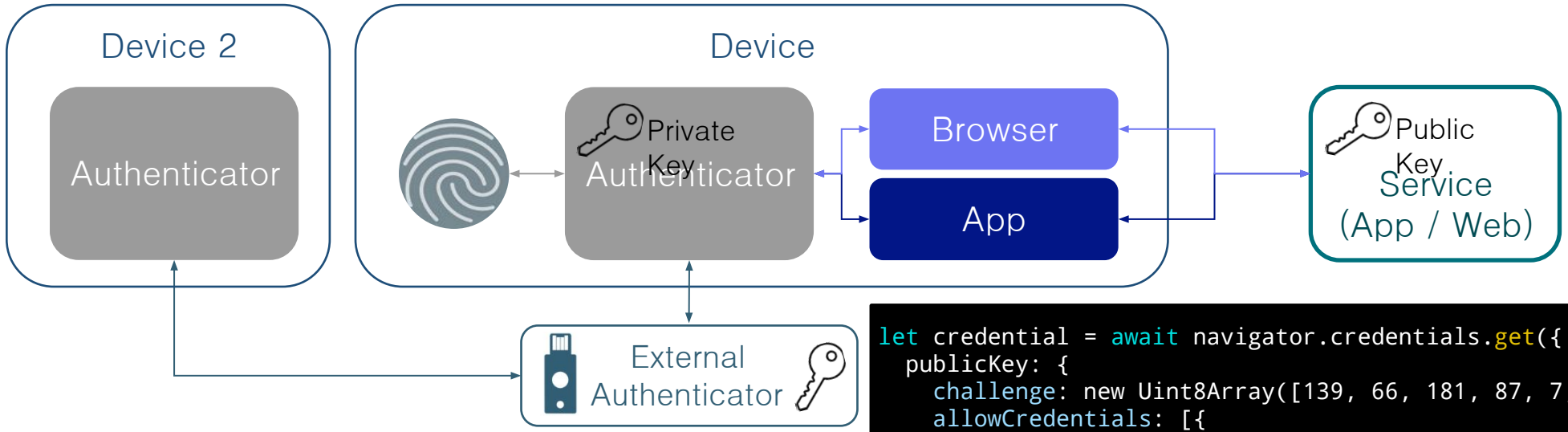
- Check User Info, Domain

User Info	Kim Samsung
Domain	samsung.com
Credential	0x9ske876…
Private key	0x5krn863…

User Info, Challenge →

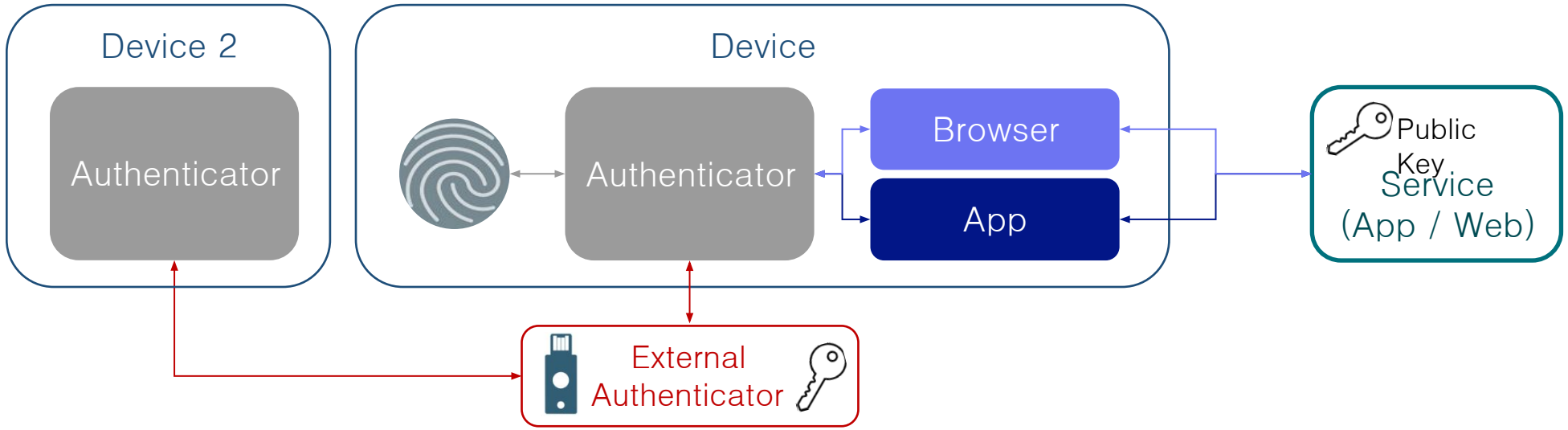
Credential, Encrypted Challenge by Private key →

User Info	Kim Samsung
Credential	0x9ske876…
Public key	0x2kmb407…

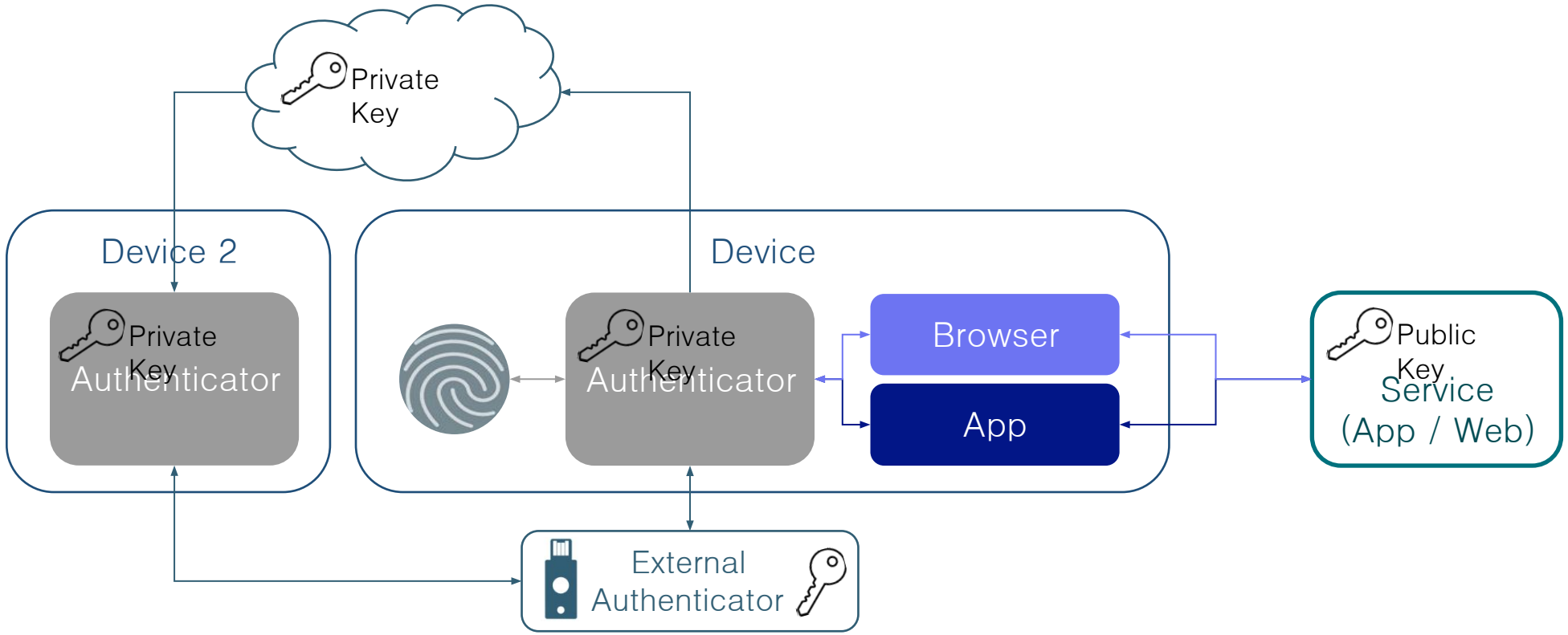



```
let credential = await navigator.credentials.get({
  publicKey: {
    challenge: new Uint8Array([139, 66, 181, 87, 7, 203, ...]),
    allowCredentials: [{
      type: "public-key",
      id: new Uint8Array([64, 66, 25, 78, 168, 226, 174, ...])
    }],
    userVerification: "required",
  }
});
```

FIDO2 의 제약사항


Device 2
Authenticator
Device
Authenticator
Browser
App
Public Key
Service
(App / Web)
External
Authenticator

Passkey : FIDO2 + **Private Key sync** (Web Authentication API Level 3)



03 / Passkey

Passkey 지원 현황

- Google, Microsoft, Apple 의 Passkey 지원 동의
  * 2022년 5월, FIDO Alliance에서 공식 발표

- Google account 로그인 시 Passkey를 primary option으로 적용
  * 2023년 10월, Google blog : “Passwordless by default: Make the switch to passkeys”

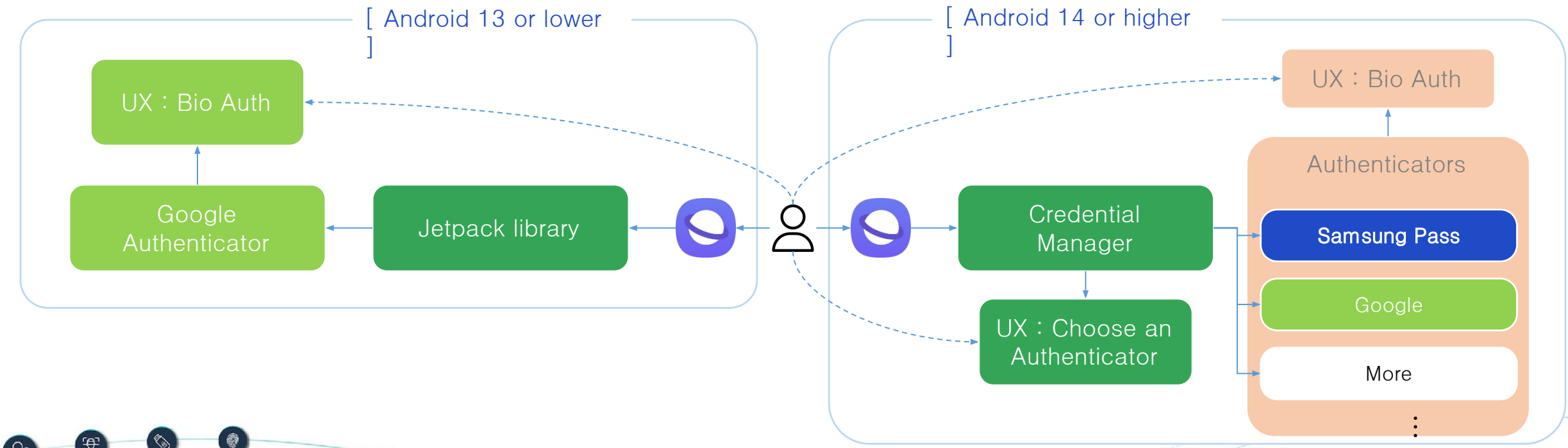
Samsung의 Passkey 지원 현황

- Samsung Internet
  - * v17.0 부터 Web Authentication API 지원 시작 (22년 5월)
  - * v23.0 부터 Passkey 지원 시작 (23년 10월)

- Samsung Pass : Android U (One UI 6.0) 부터 Passkey provider 로서 동작
  - * Key pair 생성, Private key 관리 및 동기화, 사용자 인증, Challenge 서명 등

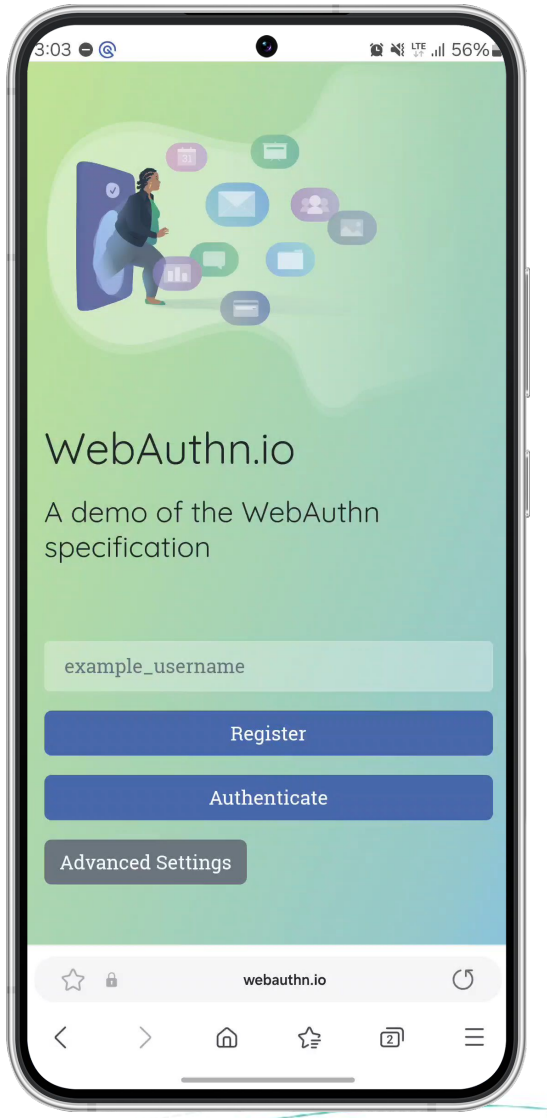
How Samsung Internet supports Passkeys

- **Manage Passkeys through Credential Manager** (Android 14 or higher)
  - Credential Manager: An Android Framework Library for Multi-Authenticator
    ※ On Android 13 or lower, support Google Authenticator by Jetpack library
  - Users can choose an Authenticator that they prefer



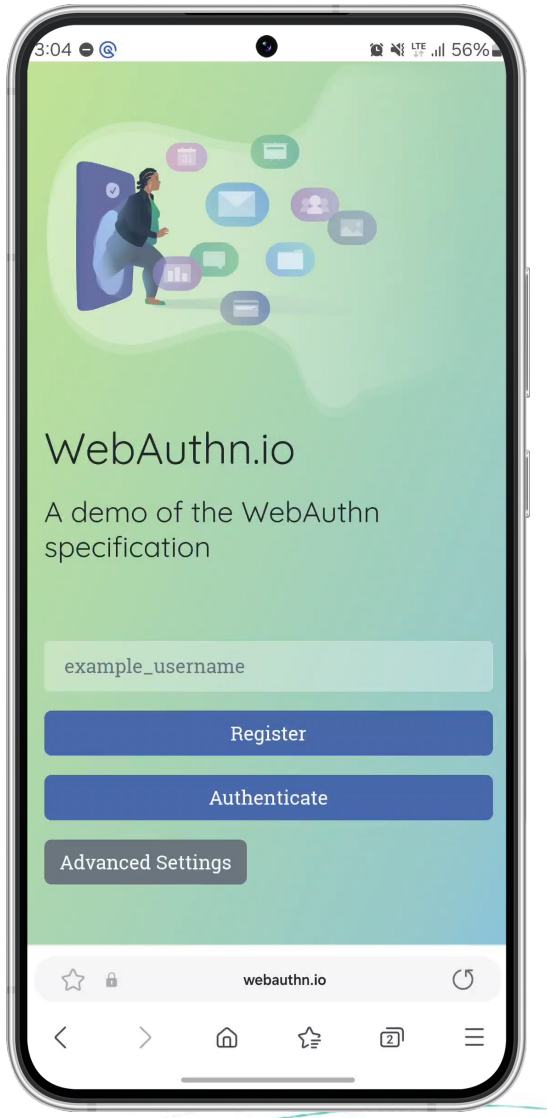
Passkey User flow on Samsung Internet

- **Registration**
  - Enter ID for sign up
  - Choose authenticator to create Passkey
  - Verify with fingerprint
  - Registration done



Passkey User flow on Samsung Internet

- **Sign in**
  - Touch sign in button
  - Choose a Passkey from authenticator list
  - Verify with fingerprint
  - Sign in done



감사합니다