

WebAuthn Reference Implementation

FIDO2: What, Why, How

Julian Stampfli

February 6, 2019

Project source

`https://github.com/Tartori/web-authn-demo`

Table of Contents

Introduction

WebAuthn - Registration

WebAuthn - Authentication

WebAuthn - Authenticator Data

Summary/Conclusion

Demo

Table of Contents

Introduction

WebAuthn - Registration

WebAuthn - Authentication

WebAuthn - Authenticator Data

Summary/Conclusion

Demo

Drawbacks

- Hard to remember good passwords
- Weak passwords are chosen
- Passwords are reused

Passwords

Drawbacks

- Hard to remember good passwords
- Weak passwords are chosen
- Passwords are reused

Benefits

- EASY!!
- ...

Passwords

Drawbacks

- Hard to remember good passwords
- Weak passwords are chosen
- Passwords are reused

Benefits

- EASY!!
- ...
- People are used to them

- Standard for Passwordless Authentication
- Easy to use(?)

- Standard for Passwordless Authentication
- Easy to use(?)
- Authenticator (Token) instead of password

FIDO2 vs Passwords

Passwords

- Have it remembered
- Enter it
- Hope it is protected

FIDO2 vs Passwords

Passwords

- Have it remembered
- Enter it
- Hope it is protected

FIDO2

- Bring your Authenticator
- Plug it in
- Press a button
- Like an OTP

OTP

- Generated with shared secret
- Kind of like a password
- Secure against Replay attacks
- Weak against MitM
- Weak against verifier compromise

FIDO2 vs OTP

OTP

- Generated with shared secret
- Kind of like a password
- Secure against Replay attacks
- Weak against MitM
- Weak against verifier compromise

FIDO2

- Generated with public key crypto
- Save(ish) against MitM
- Save against verifier compromise
- Save against remote attacks

FIDO2 vs FIDO U2F

- FIDO U2F predecessor of FIDO2
- FIDO2 used for passwordless and second factor
- FIDO2 keeps the keys on Authenticator
- Interoperable

How does FIDO2 work

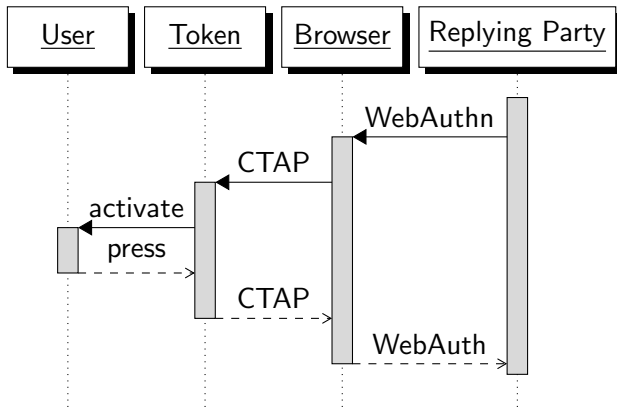


Table of Contents

Introduction

WebAuthn - Registration

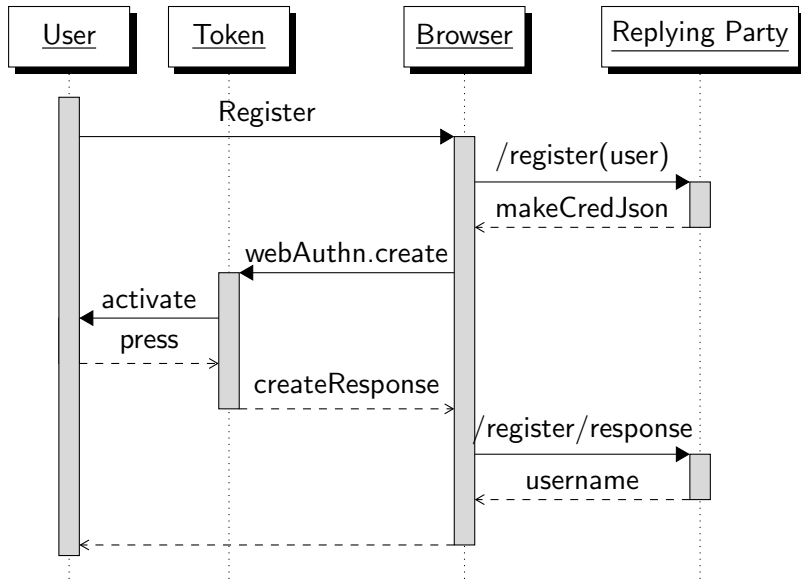
WebAuthn - Authentication

WebAuthn - Authenticator Data

Summary/Conclusion

Demo

Registration



Create Registration JSON I

```
1      {
2        "public-key": {
3          "challenge": "UvwcjUM5UOASx2AK9...",
4          "fidoResponse": "direct",
5          "rp": {
6            "name": "BFH",
7            "id": "dev.webauthn.demo"
8          },
9          "user": {
10           "id": "lPVdjYV97NDuLLMg...",
11           "name": "test",
12           "displayName": "test"
13         },
```

Create Registration JSON II

```
1      "pubKeyCredParams": [  
2          {  
3              "type": "public-key",  
4              "alg": -7  
5          }  
6      ],  
7      "attestation": "direct",  
8      "timeout": 60000,  
9  }  
10 }
```

Registration Response

```
1      {
2        "rawId": "qKk7sFYyBRex6K6twW5...",
3        "response": {
4          "attestationObject": "o2NmbXRm...",
5          "clientDataJSON": "eyJjaGF..."
6        },
7        "getClientExtensionResults": {},
8        "id": "qKk7sFYyBRex6K6twW5...",
9        "type": "public-key"
10     }
```

Registration Response

- 19 Steps have to be completed
- 1-7 parse and validate clientDataJSON
- 8-13 parse and validate attestationObject
- 14 verify signature
- 15,16 verify trustworthiness
- 17,18 verify and update user data
- 19 - fail if any step failed

Client Data Parsed

```
1  {  
2    "challenge": "UvwcjUM5UOASx2AK9...",  
3    "new_keys_may_be_added_here": "do not  
      compare clientDataJSON ",  
4    "origin": "https://dev.webauthn.demo:8  
      888",  
5    "type": "webauthn.create"  
6  }
```

Attestation Data Parsed

```
1      {
2          "fmt": "packed",
3          "attStmt": {
4              "alg": -7,
5              "sig": "MEQCIBRsm+gm5tY75S/uEk...",
6              "x5c": [
7                  "MIICvDCCAaSgAwIBAgIEA63wEjA..."
8              ]
9          },
10         "authData": "kn8Lq9EV0MBhHa/k+ZE..."
11     }
```

Table of Contents

Introduction

WebAuthn - Registration

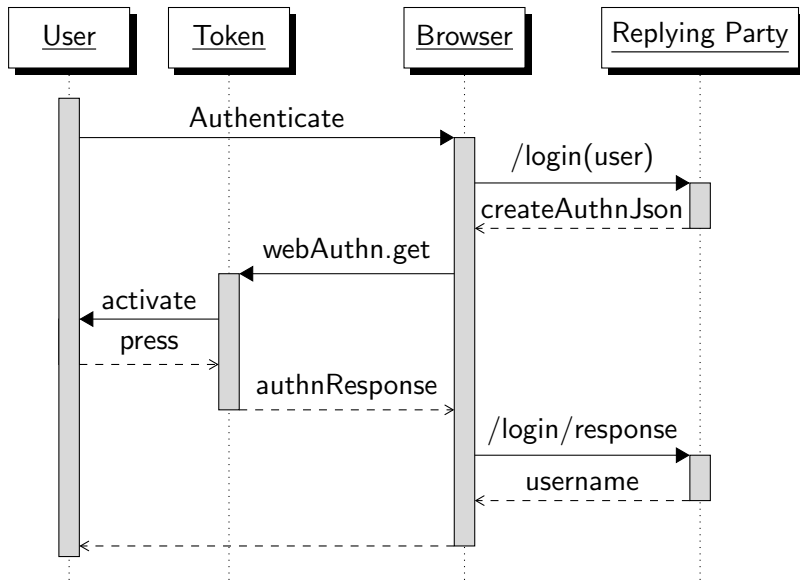
WebAuthn - Authentication

WebAuthn - Authenticator Data

Summary/Conclusion

Demo

Authentication



Create Authentication JSON

```
1      {
2        "public-key": {
3          "challenge": "rfmx563tPscMU...",
4          "rpId": "dev.webauthn.demo",
5          "allowCredentials": [
6            {
7              "type": "public-key",
8              "id": "NWlv8Cd3lXkE8r4_..."
9            }
10          ],
11          "timeout": 60000,
12        }
13      }
```

Authentication Response

```
1      {  
2          "rawId": "NWiv8Cd3lXkE8r4_Ondf6f...",  
3          "response": {  
4              "authenticatorData": "kn8Lq9EV",  
5              "signature": "MEUCIAhdPPqzV69p...",  
6              "userHandle": "",  
7              "clientDataJSON": "eyJjaGFsbGV..."  
8          },  
9          "getClientExtensionResults": {},  
10         "id": "NWiv8Cd3lXkE8r4_Ondf6fPDe...",  
11         "type": "public-key"  
12     }
```

Authentication Response Steps

- 18 Steps have to be completed
- 1-3 validate user and authenticator
- 4 parse several fields
- 5-10,15 parse and validate clientDataJSON
- 11-14 parse and validate authenticatorData
- 16,17 verify signature and sign count
- 18 - fail if any step failed

Client Data Parsed

```
1  {  
2    "challenge": "pT5Z7r07quoidUbLxB...",  
3    "origin": "https://dev.webauthn.demo:8  
4      888",  
5    "type": "webauthn.get"  
6  }
```

Table of Contents

Introduction

WebAuthn - Registration

WebAuthn - Authentication

WebAuthn - Authenticator Data

Summary/Conclusion

Demo

Authenticator Data

- RP ID hash
- Flags
- Sign Count
- Attested Credential Data (Registration)
- Extensions (Optional)

Table of Contents

Introduction

WebAuthn - Registration

WebAuthn - Authentication

WebAuthn - Authenticator Data

Summary/Conclusion

Demo

Summary

- Passwordless
- Registration and authentication very similar
- Rather complex
- Need for libraries

Conclusion

Summary

- Passwordless
- Registration and authentication very similar
- Rather complex
- Need for libraries

Conclusion

- Wide adoption?
- Used in eID?
- Used internally?
- Complexity?
- User verification?

Further Research

- FIDO2 over NFC
- Other authenticators
- Managing authenticators

Table of Contents

Introduction

WebAuthn - Registration

WebAuthn - Authentication

WebAuthn - Authenticator Data

Summary/Conclusion

Demo

`https://dev.webauthn.demo:8888`

Questions

`https://github.com/Tartori/web-authn-demo`