

High Level WebAuthn Registration flow

- WebAuthn registration process overview
 - Pre-requisites
 - Purpose of this section
- WebAuthn registration using Microsoft Windows
 - Client configuration for Microsoft Windows
 - Registration for User-Verified flow on Windows
 - Registration selections for User-Verified flow on Windows
 - Registration process and UX design for User-Verified flow on Windows
 - Registration for the Server-Verified flow on Windows
 - Registration selections for the Server-Verified flow on Windows
 - Registration flow and UX design for the Server-Verified flow on Windows
 - Registration for Usernameless flow on Windows
 - Registration selections for Usernameless flow on Windows
 - Registration process and UX design for Usernameless flow on Windows
- WebAuthn registration using Apple MacOS
 - Client configuration for Apple MacOS
 - Registration for the User-Verified flow on MacOS
 - Registration selections for the User-Verified flow on MacOS
 - Registration process and UX design for the User-Verified flow on MacOS
 - Registration for the Server-Verified flow on MacOS
 - Registration selections for the Server-Verified flow on MacOS
 - Registration process and UX design for the Server-Verified flow on MacOS
 - Registration for Usernameless flow on MacOS
 - Registration selections for Usernameless flow on MacOS
 - Registration process and UX design for Usernameless flow on MacOS
- WebAuthn registration using the Apple iOS Safari browser
 - Client configuration for Apple iOS with Safari
 - Registration for the User-Verified flow on Apple iOS with Safari
 - Registration selections for the User-Verified flow on Apple iOS with Safari
 - Registration process and UX design for the User-Verified flow on Apple iOS with Safari
 - Registration for the Server-Verified flow on Apple iOS with Safari
 - Registration selections for the Server-Verified flow on Apple iOS with Safari
 - Registration process and UX design for Server-Verified flow on Apple iOS with Safari
 - Registration for the Usernameless flow on Apple iOS with Safari
 - Registration selections for the Usernameless flow on Apple iOS with Safari
 - Registration process and UX design for the Usernameless flow on Apple iOS with Safari

WebAuthn registration process overview

Pre-requisites

The WebAuthn registration process described in this section is first and foremost based on the registration specification in the W3C WebAuthn standard. The WebAuthn registration process is equivalent to the WebAuthn Make Credentials procedure. All WebAuthn registration parameters, JSON objects, and generic WebAuthn flows are based on the W3C WebAuthn standard.

In addition to the W3C WebAuthn standard, the specific registration flow described in this section adheres to the New Account Creation section of the Identifier First Flow document. The Identifier First Flow description explains the creation of an account as well as the WebAuthn registration process.

Furthermore, the Custom Registration Flow in the High Level Architecture document describes the technical environment in more depth. This document describes the AWS architecture, Lambda components and the SQL database that need to be deployed for hosting a WebAuthn Relying Party for the WebAuthn Starter Kit.

It is recommended to study the documents mentioned above as a pre-requisite before continuing reading this section.

Finally, the WebAuthn Starter Kit must have been deployed at AWS as described in the tutorial Automated WebAuthnKit deployment at AWS. The URL that is deployed for the WebAuthn Starter Kit React web app at the AWS frontend is considered as the WebAuthnKit URL throughout the remainder of this document.

Purpose of this section

Now, this section describes how to perform the WebAuthn registration process by using Microsoft Windows, an Apple iOS smartphone with the Safari browser, and an Apple iOS smartphone with an app that implements WebAuthn.

As described in the Identifier First Flow page, there are a number of routes the registration flow can take, depending of what clients, parameters and selections that are used during the registration process. For each section, the client's configuration is described, as well as the registration scenario.

WebAuthn registration using Microsoft Windows

Client configuration for Microsoft Windows

The client configuration used in this section is the following:

- Operating system: Microsoft Windows 10 Pro (edition 2004)
- Web browser: Google Chrome (version 84.0.4147.105)
- FIDO2 implementation: Microsoft's [Web Authentication API](#), which is a Win32 API that exposes the [W3C WebAuthn](#) functions to Windows 10 applications (including Google Chrome), and Microsoft's CTAP2 stack

Registration for User-Verified flow on Windows

Registration selections for User-Verified flow on Windows

The FIDO authenticator used in this section is the following:

- A YubiKey 5 NFC (version 5.2.6) is used as FIDO authenticator. The FIDO2 application on the YubiKey is **activated**. The YubiKey 5 has not been registered with this service, so there are no FIDO2 credentials or PIN-codes set.

The registration route described in this section is derived from the following parameters and selections according to the Identifier First Flow page:

- The WebAuthn MakeCredentials parameter UserVerification is set to 'Preferred', which resolves to the CTAP2 parameter UV=1 for a FIDO2 enabled YubiKey used with Google Chrome on Windows 10. This behaviour is equivalent to setting the WebAuthn MakeCredentials parameter UserVerification to 'Required'.
- A Server-Verified PIN is not set for this account as part of the registration process (since the CTAP2 parameter UV=1 is set).

Registration process and UX design for User-Verified flow on Windows

The selections for the registration process result in the registration flow and UX described in this section.

Step 1.1: The YubiKey 5 with the FIDO2 application is selected as authenticator. (In other words, a platform authenticator is not used.)

Step 1.2: The user visits the WebAuthnKit URL. The site redirects the user to the Login page. Since a new user account shall be created, the user enters a new username.

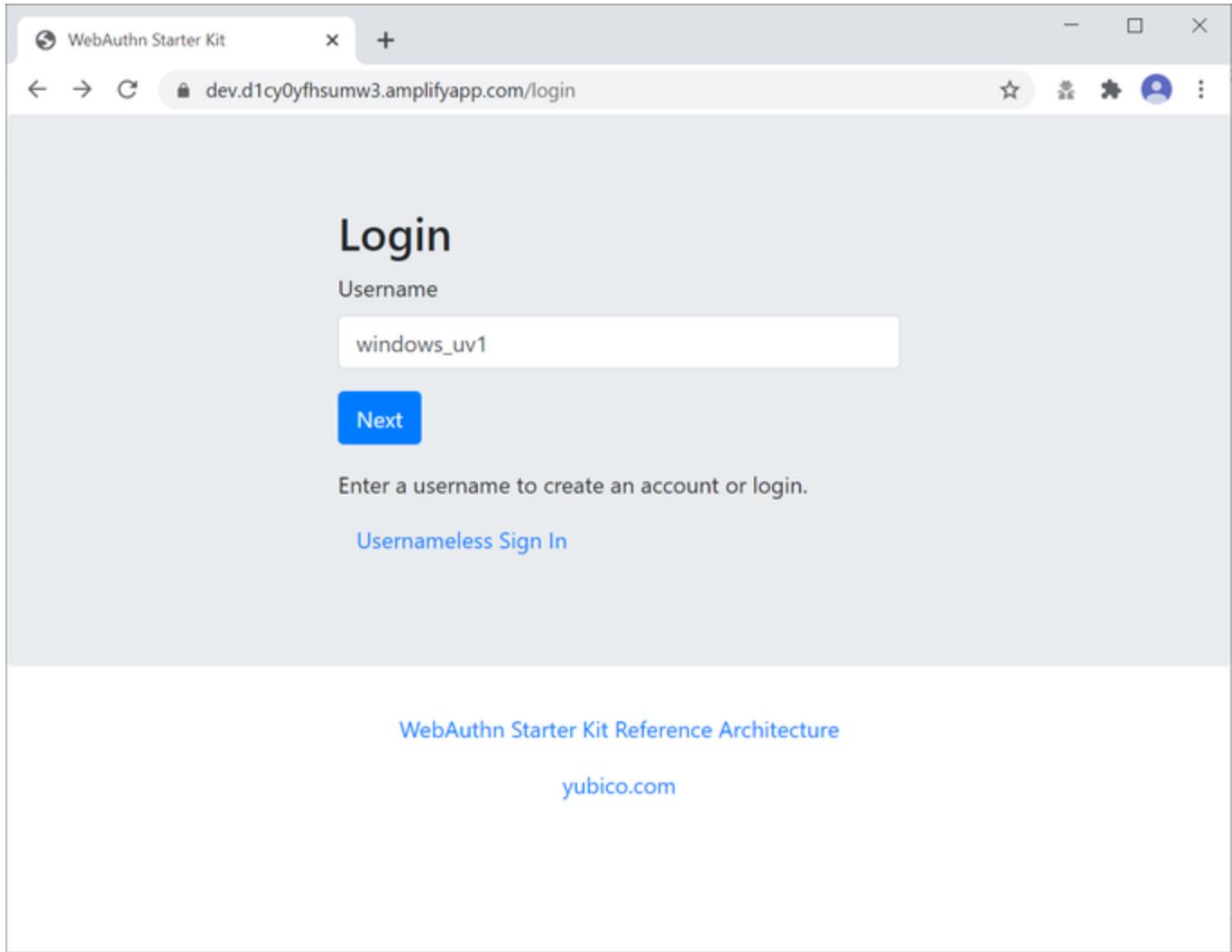


Figure 1 - Login page on Windows for WebAuthn registration

Step 1.3: The user presses “Next” in the window above, and a new account is created for the user.

Step 1.4: Next, the registration page is shown below. The WebAuthn parameter UserVerification is set to 'Preferred' (CTAP2 UV=1) for this registration process. The user inserts the YubiKey 5 into the computer and presses the button “Register Security Key”.

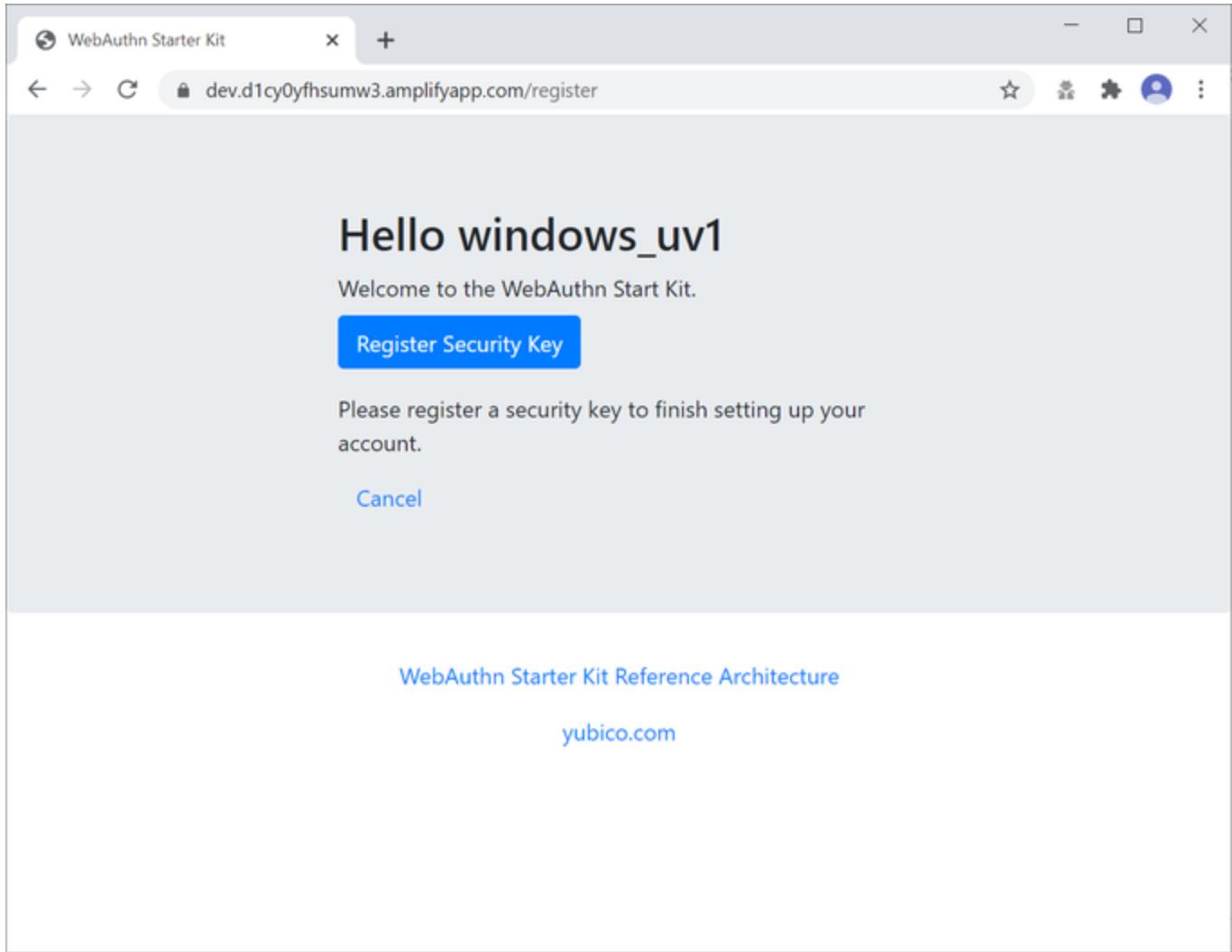


Figure 2 - Registration page for security key

Step 1.5: Windows displays a security dialog box, in which the user enters a new PIN-code for the YubiKey. (If a YubiKey is used with PIN-code already set for the FIDO application, there will be a dialog box with a field for the user to enter the PIN-code.)

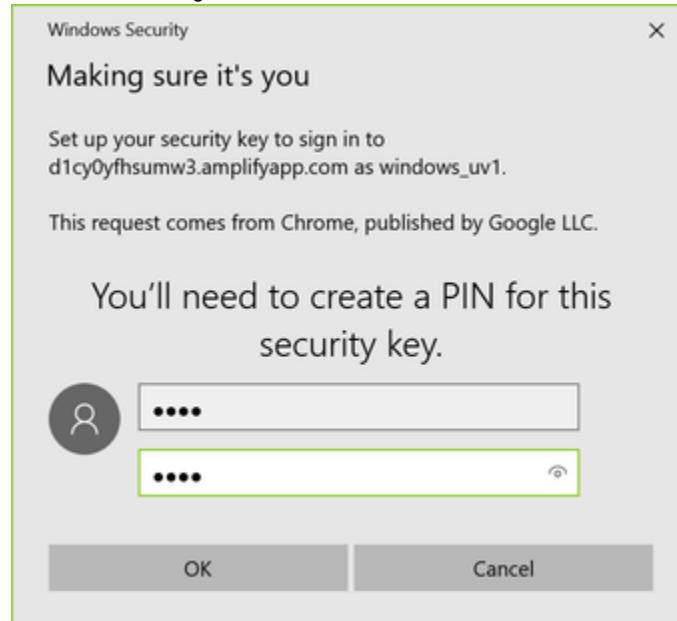


Figure 3 - Create PIN for the YubiKey's FIDO2 application

Step 1.6: Windows displays a security dialog box with instructions for the user to touch the security key. The user touches the sensor on the YubiKey.

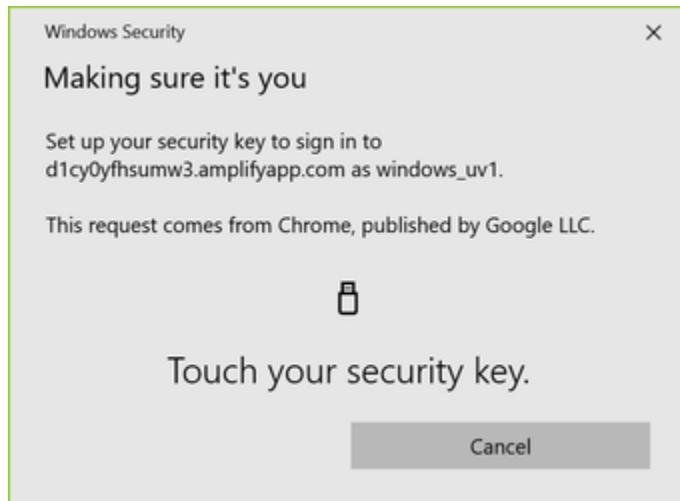


Figure 4 - Touch the YubiKey for FIDO2 registration

Step 1.7: Windows displays a security dialog box with a request to use the security key for this site. The user approves this by pressing the "Allow" button.

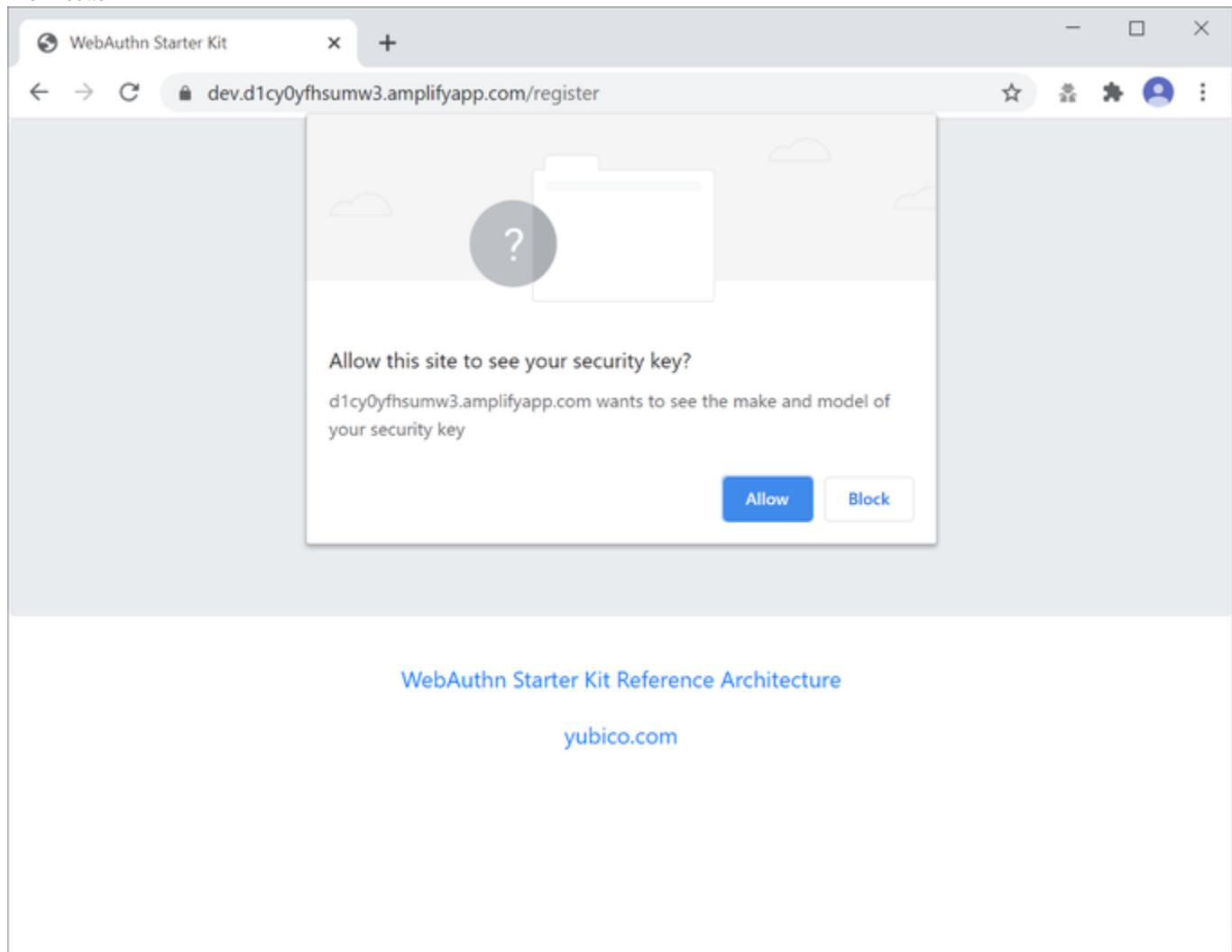


Figure 5 - Allow the YubiKey to be used for this site

Step 1.8: This completes the registration process. The user's account is created and an OpenID Connect token is returned to the browser.

Registration for the Server-Verified flow on Windows

Registration selections for the Server-Verified flow on Windows

The FIDO authenticator used in this section is the following:

- A YubiKey 5 NFC or YubiKey 4 is used as FIDO authenticator. The FIDO2 application on the YubiKey 5 is **deactivated**. The YubiKey has not been registered with this service, so there are no FIDO2 credentials or PIN-codes set.

The registration route described in this section is derived from the following parameters and selections according to the Identifier First Flow page:

- The WebAuthn MakeCredentials parameter UserVerification is set to 'Preferred', which resolves to the CTAP2 parameter UV=0 for a FIDO2 disabled YubiKey used with Google Chrome on Windows 10. The backward compatible FIDO U2F flow of WebAuthn is therefore used. This behaviour is equivalent to setting the WebAuthn MakeCredentials parameter UserVerification to 'Discouraged'.
- A Server-Verified PIN is set for this account as part of the registration process (since the CTAP2 parameter UV=0 is set).

Registration flow and UX design for the Server-Verified flow on Windows

The registration process for the Server-Verified flow is identical to the User-Verified registration process with one notable exception:

The FIDO authenticator will not require a PIN-code (as shown in figure 1.3); the FIDO authenticator will only require the user to touch the FIDO authenticator. Instead, a the user must set a Server-Verified PIN when creating the account. The Server-Verified PIN is used as first factor authentication to protect the account.

An example of how to set a Server-Verified PIN is shown in the screenshot below.

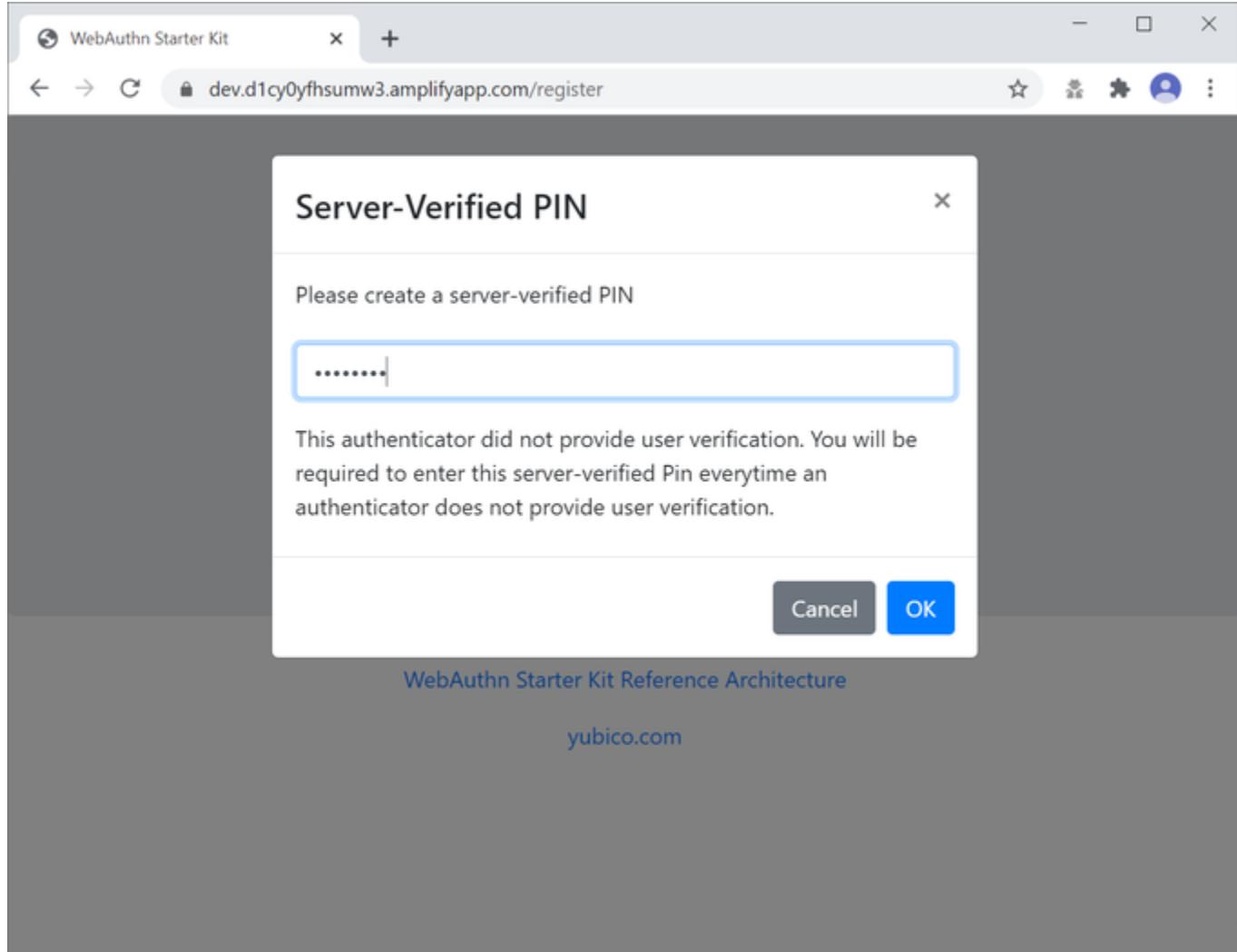


Figure 6 - The user sets a Server-Verified PIN

Registration for Usernameless flow on Windows

Registration selections for Usernameless flow on Windows

The FIDO2 authenticator used in this section is the following:

- A YubiKey 5 NFC (version 5.2.6) is used as FIDO2 authenticator. The YubiKey 5 is configured with FIDO2 credentials and a PIN-code according to section High Level WebAuthn Registration flow.

The registration route described in this section is derived from the following parameters and selections according to the Identifier First Flow page:

- The WebAuthn MakeCredentials parameter UserVerification is set to 'Preferred', which resolves to the CTAP2 parameter UV=1 for a FIDO2 enabled YubiKey used with Google Chrome on Windows 10. This behaviour is equivalent to setting the WebAuthn MakeCredentials parameter UserVerification to 'Required'.
- The WebAuthn MakeCredentials parameter authenticatorSelection.requireResidentKey is set to 'True'.
- A Server-Verified PIN is not set for this account as part of the registration process (since the CTAP2 parameter UV=1 is set).

Registration process and UX design for Usernameless flow on Windows

The WebAuthn Usernameless registration process requires that the user already has enrolled for FIDO credentials to a FIDO authenticator, and that the user has authenticated to the WebAuthn Starter Kit website.

Step 2.1: The user uses the FIDO authenticator to log on to the WebAuthn Starter Kit website as shown in the picture below.

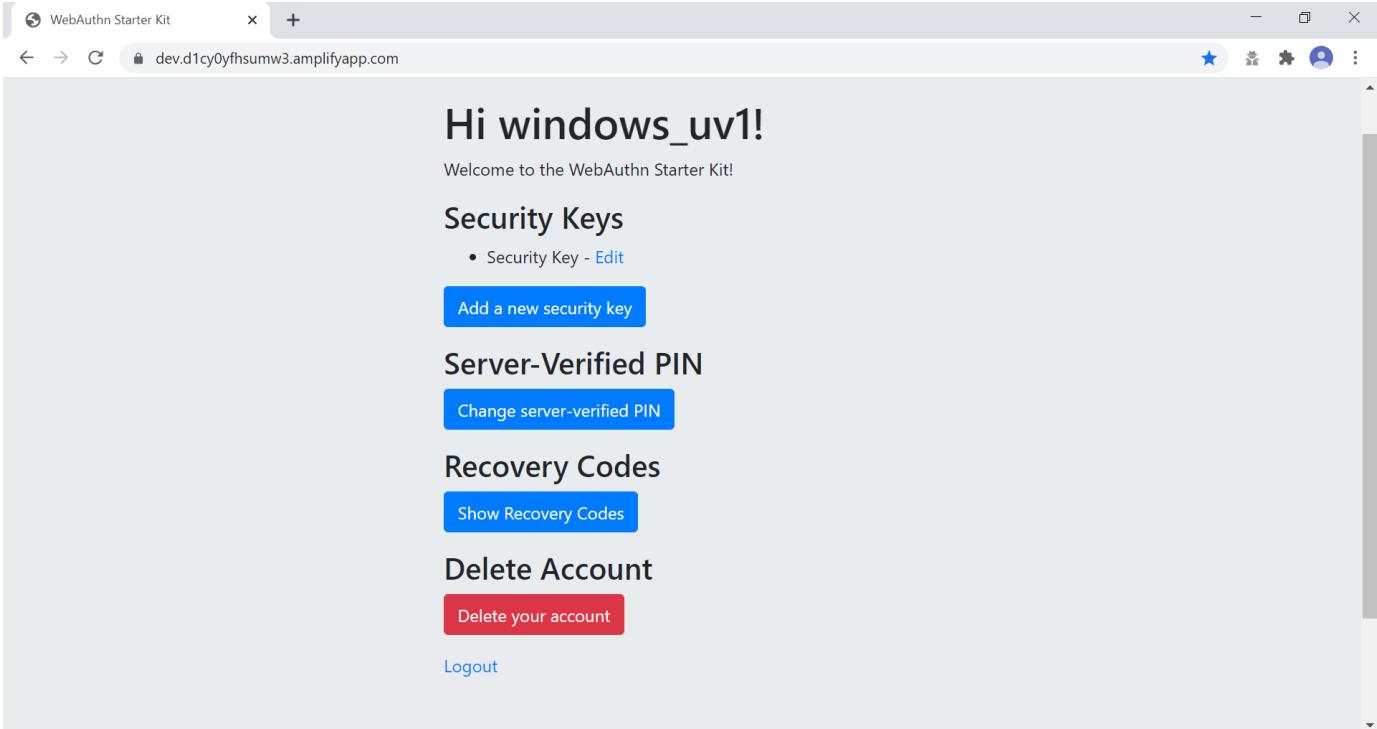


Figure 7 - WebAuthn Starter Kit administration website

Step 2.2: The user presses the button "Add a new security key". In the GUI that appears, the user enters a nickname for the usernameless FIDO authenticator, and marks the checkbox to "Enable usernameless login with this key". The user presses the button "Register security key" to complete the operation.

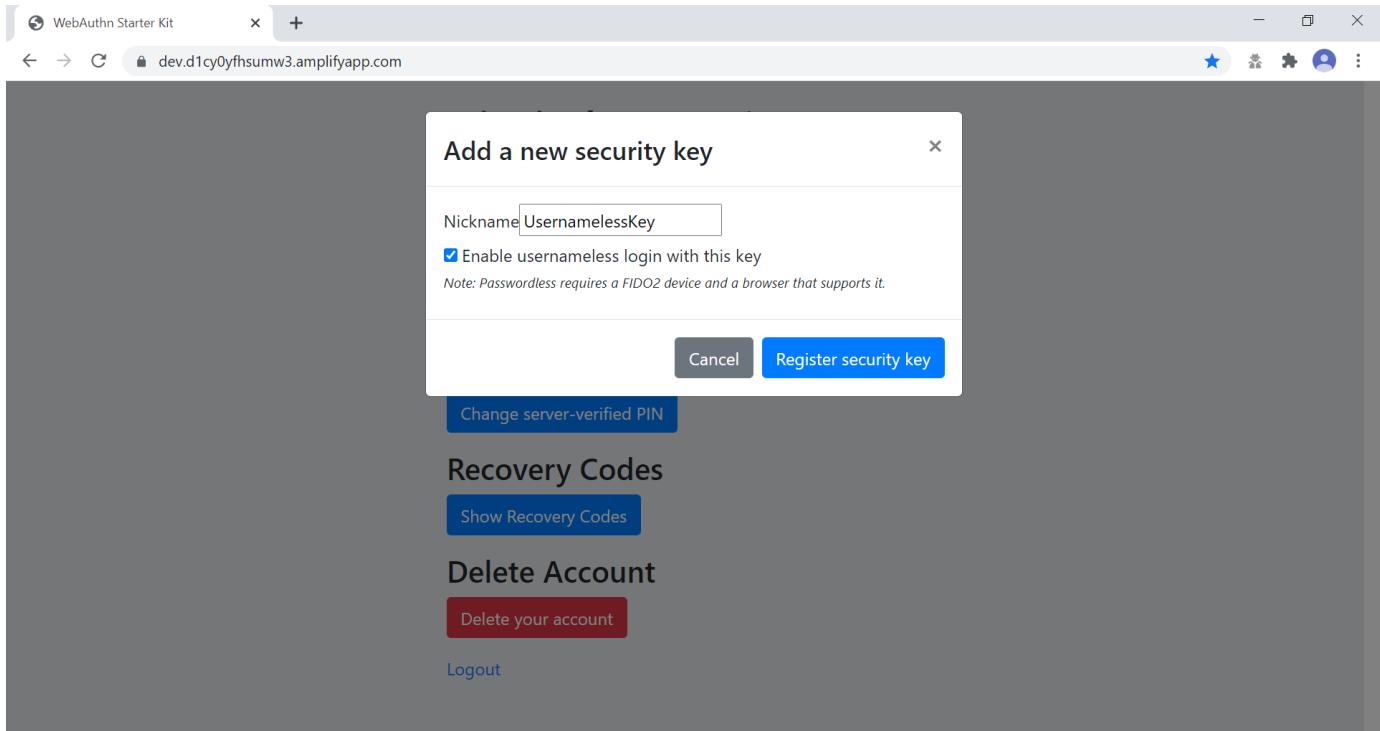


Figure 8 - Entering the nickname of a new security key

The user adds the security key according to the instructions in the section Adding a FIDO authenticator for Windows. When this process is completed, the new YubiKey is added to the user's account, which is shown in the picture below.

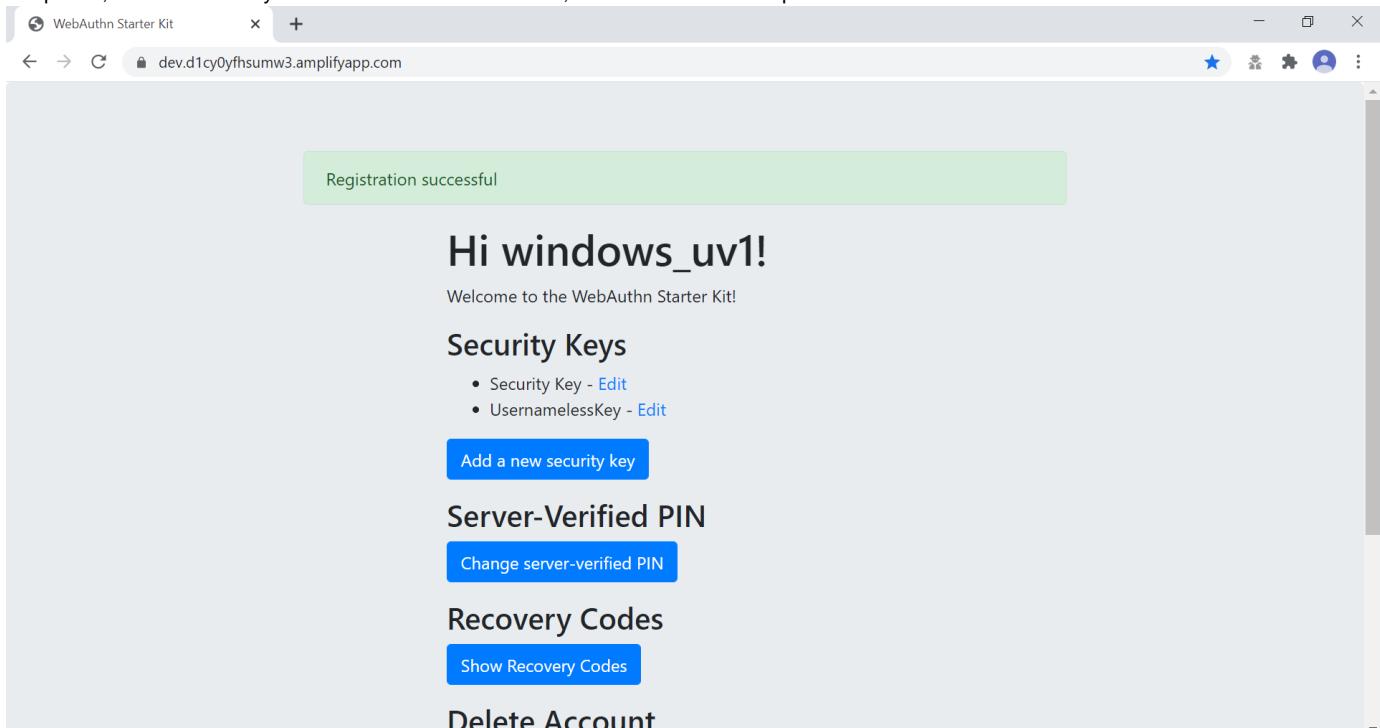


Figure 9 - An additional YubiKey is added to the user's account

At this stage, the security key with resident credentials for can be used for Usernameless authentication in to the same account.

If the user needs to re-use the same security key for the Usernameless flow, it is necessary to first delete the originally registered security key. Then only one security key is registered for the Usernameless flow.

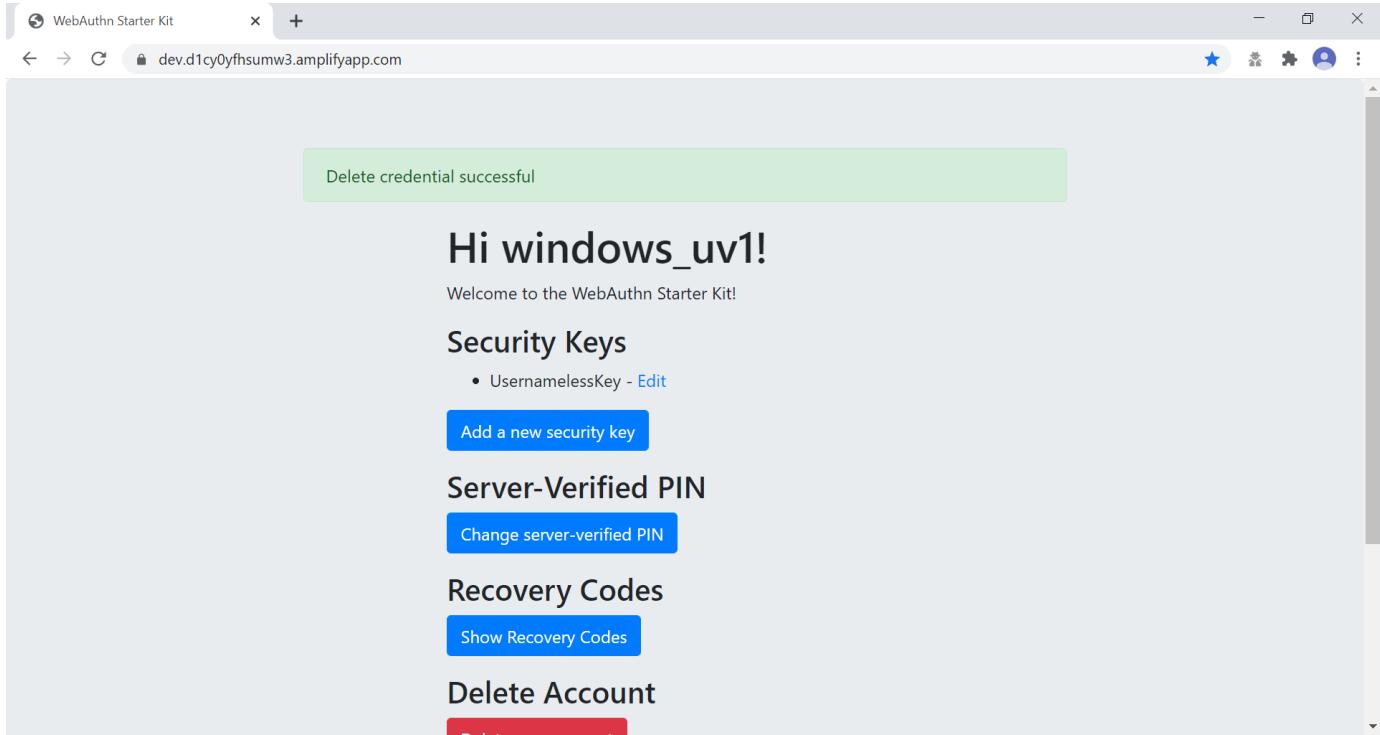


Figure 10 - Only one security key is configured for the Usernameless flow

WebAuthn registration using Apple MacOS

Client configuration for Apple MacOS

The client configuration used in this section is the following:

- Operating system: Apple MacOS Catalina 10.15.6
- Web browser: Google Chrome (version 84.0.4147.125)
- FIDO2 implementation: Google Chrome's Web Authentication API, which is an API that exposes the [W3C WebAuthn](#) functions to MacOS applications (including Google Chrome), and Google's CTAP2 stack

Registration for the User-Verified flow on MacOS

Registration selections for the User-Verified flow on MacOS

The FIDO authenticator used in this section is the following:

- A YubiKey 5 NFC (version 5.1.2) is used as FIDO authenticator. The FIDO2 application on the YubiKey is **activated**. The YubiKey 5 has a PIN-code set, but there are no FIDO2 credentials enrolled.

The registration route described in this section is derived from the following parameters and selections according to the Identifier First Flow page:

- The WebAuthn MakeCredentials parameter UserVerification is set to 'Preferred', which resolves to the CTAP2 parameter UV=1 for a FIDO2 enabled YubiKey with PIN used with Google Chrome on MacOS. This behaviour is equivalent to setting the WebAuthn MakeCredentials parameter UserVerification to 'Required'.
- A Server-Verified PIN is not set for this account as part of the registration process (since the CTAP2 parameter UV=1 is set).

Registration process and UX design for the User-Verified flow on MacOS

The selections for the registration process result in the registration flow and UX described in this section.

Step 3.1: The YubiKey 5 with the FIDO2 application is selected as authenticator. (In other words, a platform authenticator is not used.)

Step 3.2: The user visits the WebAuthnKit URL. The site redirects the user to the Login page. Since a new user account shall be created, the user enters a new username.

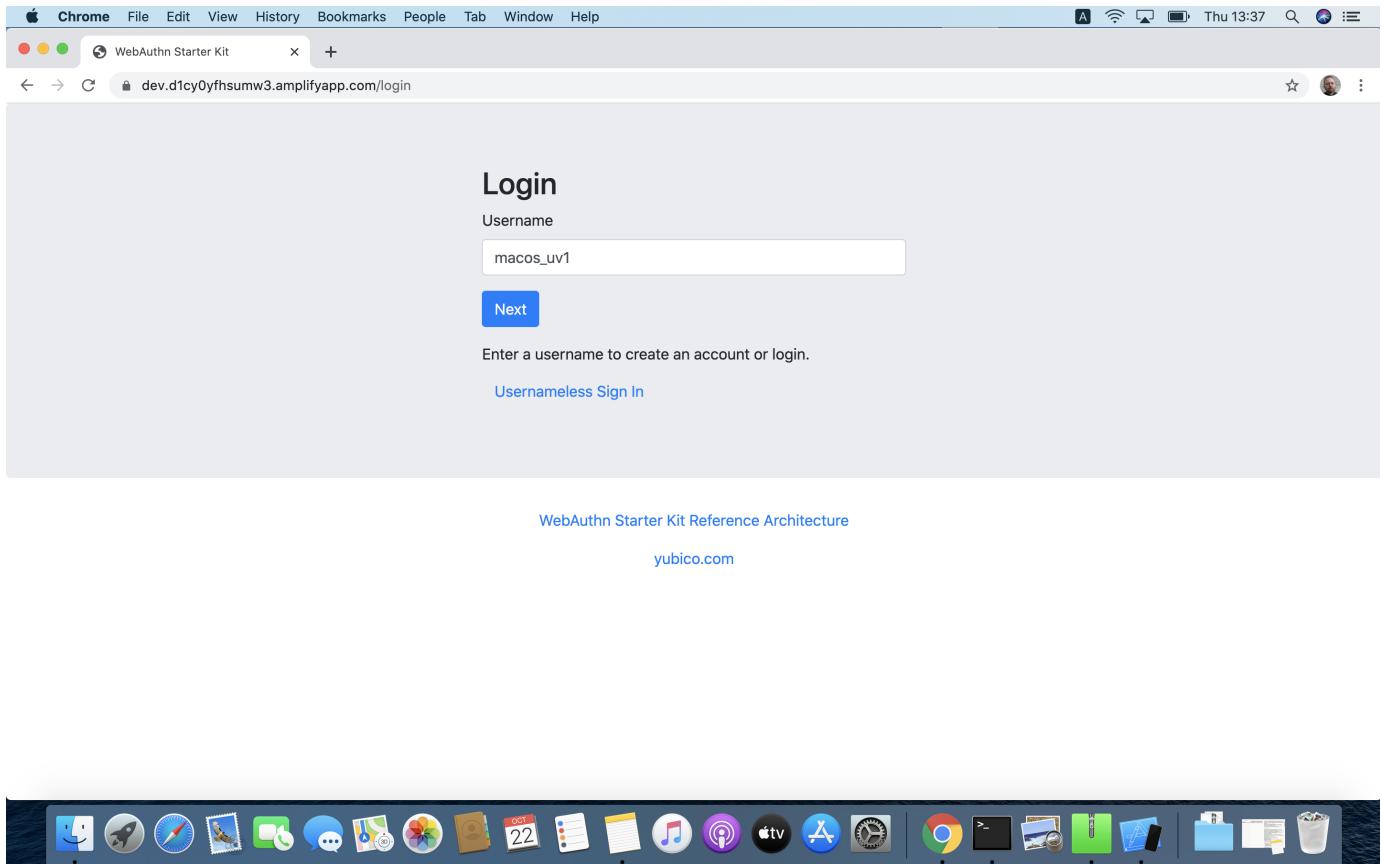
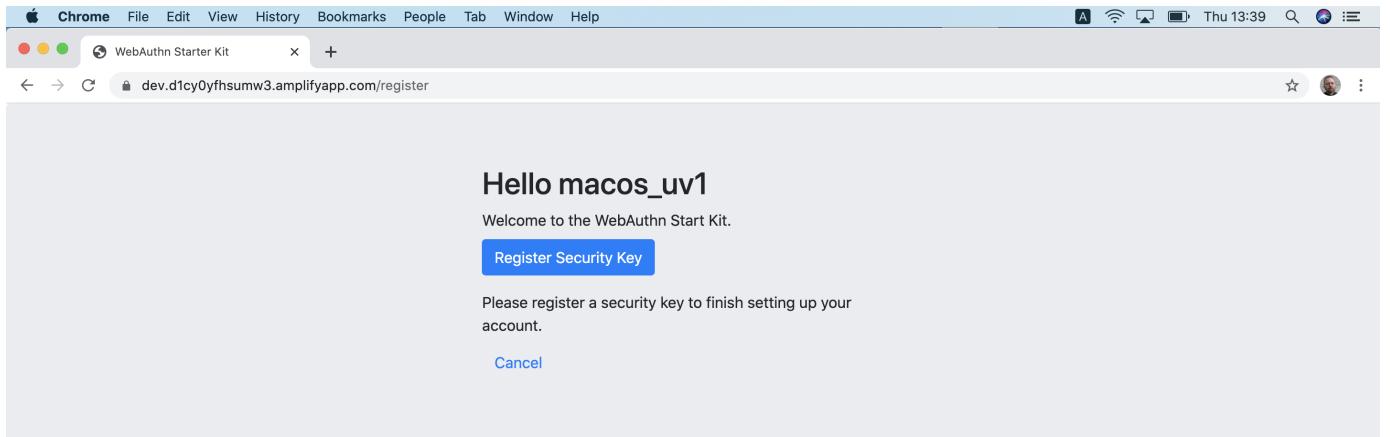


Figure 11 - Login page on MacOS for WebAuthn registration

Step 3.3: The user presses “Next” in the window above, and a new account is created for the user.

Step 3.4: Next, the registration page is shown below. The WebAuthn parameter UserVerification is set to 'Preferred' (CTAP2 UV=1) for this registration process. The user inserts the YubiKey 5 into the computer and presses the button “Register Security Key”.



WebAuthn Starter Kit Reference Architecture

yubico.com



Figure 12 - Registration page for security key

Step 3.5: Google Chrome displays a security dialog box, in which the user can select the authentication mechanism. The user selects “USB security key”.

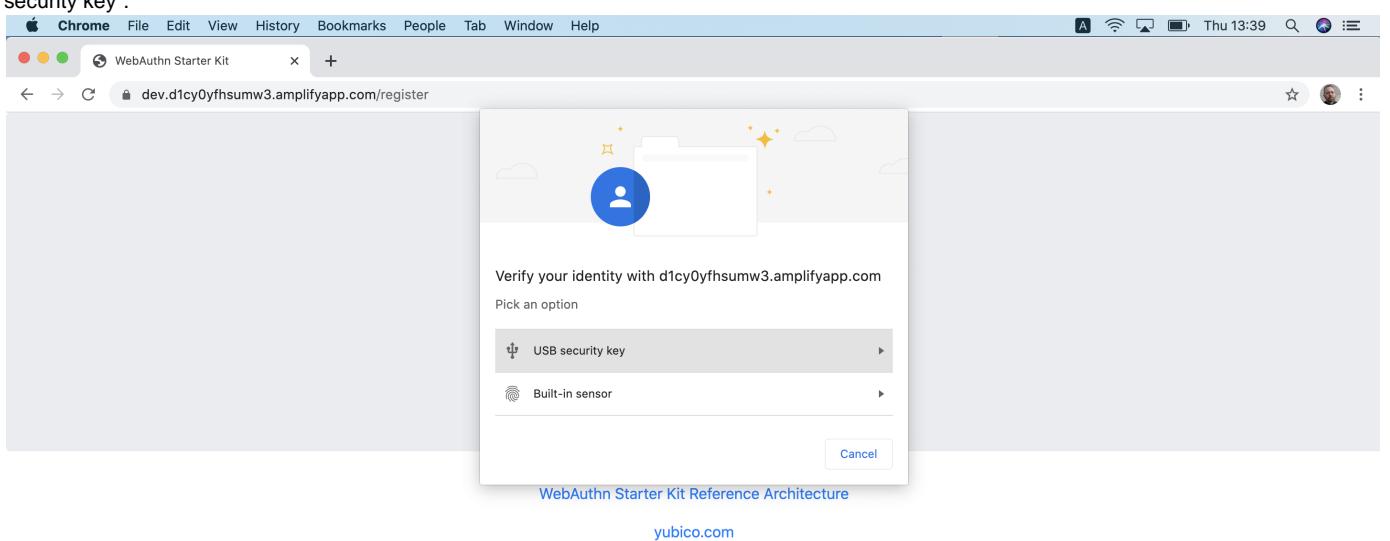


Figure 13 - Select authentication mechanism

Step 3.6: Google Chrome displays a security dialog box, which requests the user to insert the security key and touch it. The user inserts the YubiKey and presses the sensor.

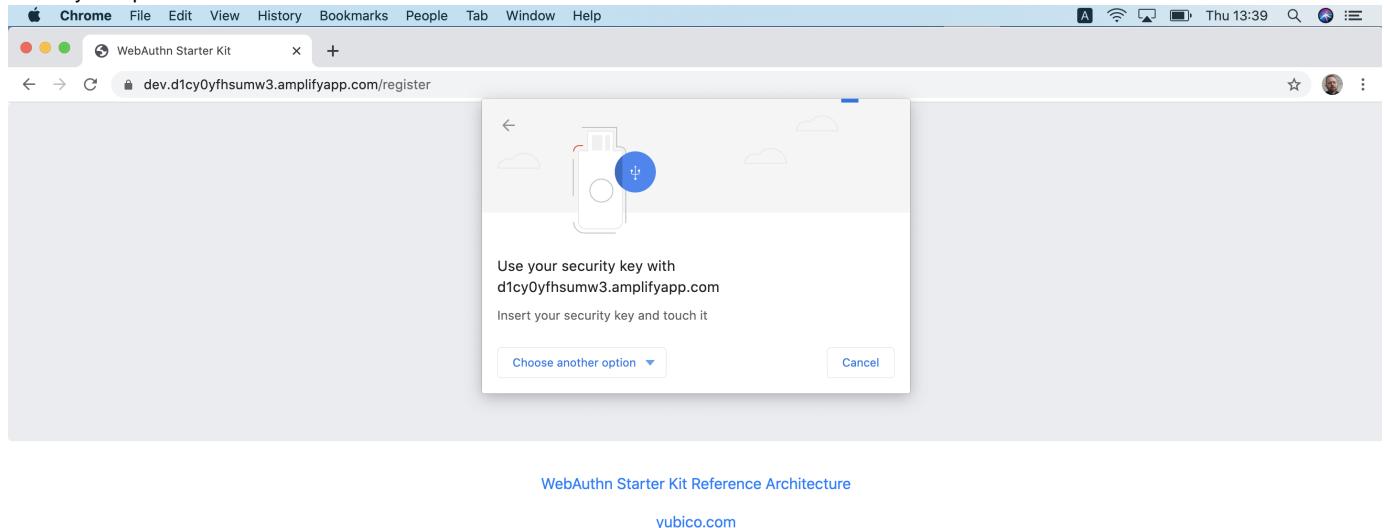


Figure 14 - Insert the FIDO authenticator and touch it

Step 3.7: Google Chrome displays a security dialog box, in which the user enters the PIN-code for the YubiKey.

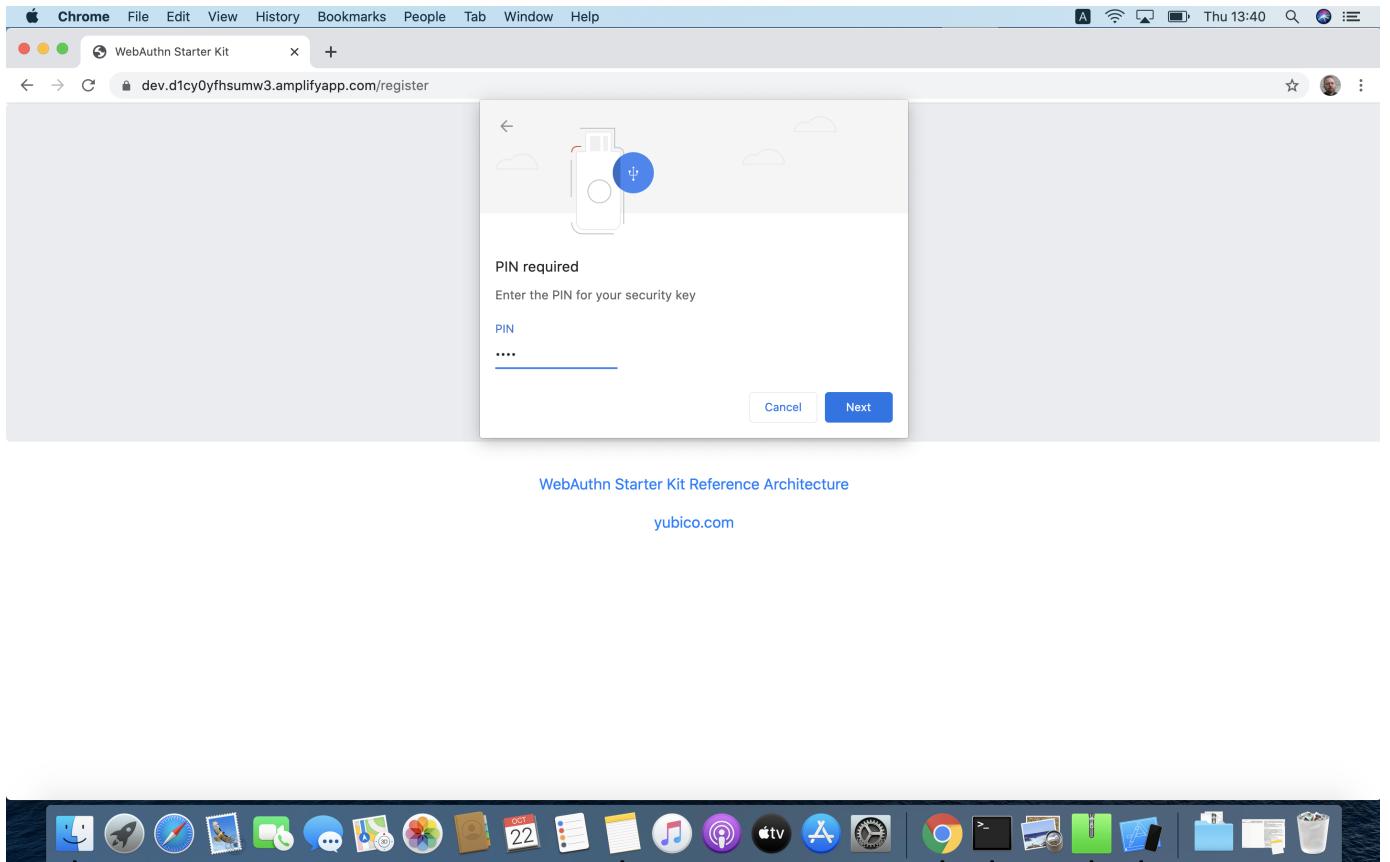


Figure 15 - Enter the PIN for the FIDO authenticator

Step 3.8: Google Chrome displays a security dialog box, which requests the user to touch the security key one more time. The user inserts the YubiKey and presses the sensor again.

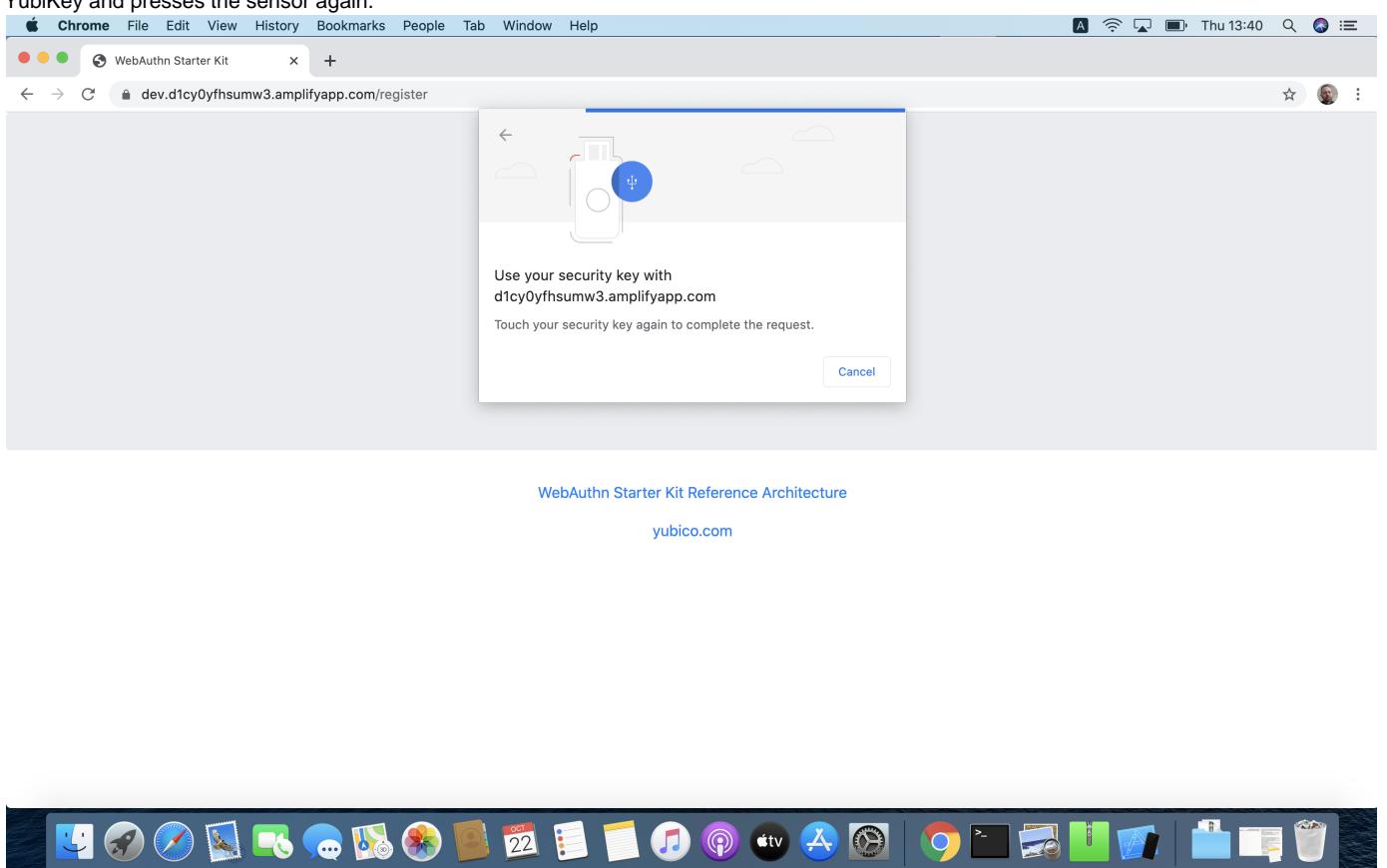


Figure 16 - Touch the FIDO authenticator one more time

Step 3.9 This completes the registration process. The user's account is created and an OpenID Connect token is returned to the browser.

Registration for the Server-Verified flow on MacOS

Registration selections for the Server-Verified flow on MacOS

The FIDO authenticator used in this section is the following:

- A YubiKey 4 or YubiKey 5 NFC is used as FIDO authenticator. The FIDO2 application on the YubiKey 5 is **deactivated**, which triggers the the Server-Verified behaviour on MacOS. Also a YubiKey with the FIDO2 application activated, but with no PIN-code set, will trigger the the Server-Verified flow on MacOS (which is a significant difference from Windows that will prompt the user for setting a PIN and activate the User-Verified process).

The registration route described in this section is derived from the following parameters and selections according to the Identifier First Flow page:

- The WebAuthn MakeCredentials parameter UserVerification is set to 'Preferred', which resolves to the CTAP2 parameter UV=0 for a FIDO2 disabled YubiKey used with Google Chrome on MacOS. The backward compatible FIDO U2F flow of WebAuthn is therefore used. This behaviour is equivalent to setting the WebAuthn MakeCredentials parameter UserVerification to 'Discouraged'.
- A Server-Verified PIN is set for this account as part of the registration process (since the CTAP2 parameter UV=0 is set).

Registration process and UX design for the Server-Verified flow on MacOS

The registration process for the Server-Verified flow is identical to the User-Verified registration process with one notable exception:

The FIDO authenticator will not require a PIN-code (as shown in figure 11); the FIDO authenticator will only require the user to touch the FIDO authenticator. Instead, a the user must set a Server-Verified PIN when creating the account. The Server-Verified PIN is used as first factor authentication to protect the account.

An example of how to set a Server-Verified PIN is shown in the screenshot below.

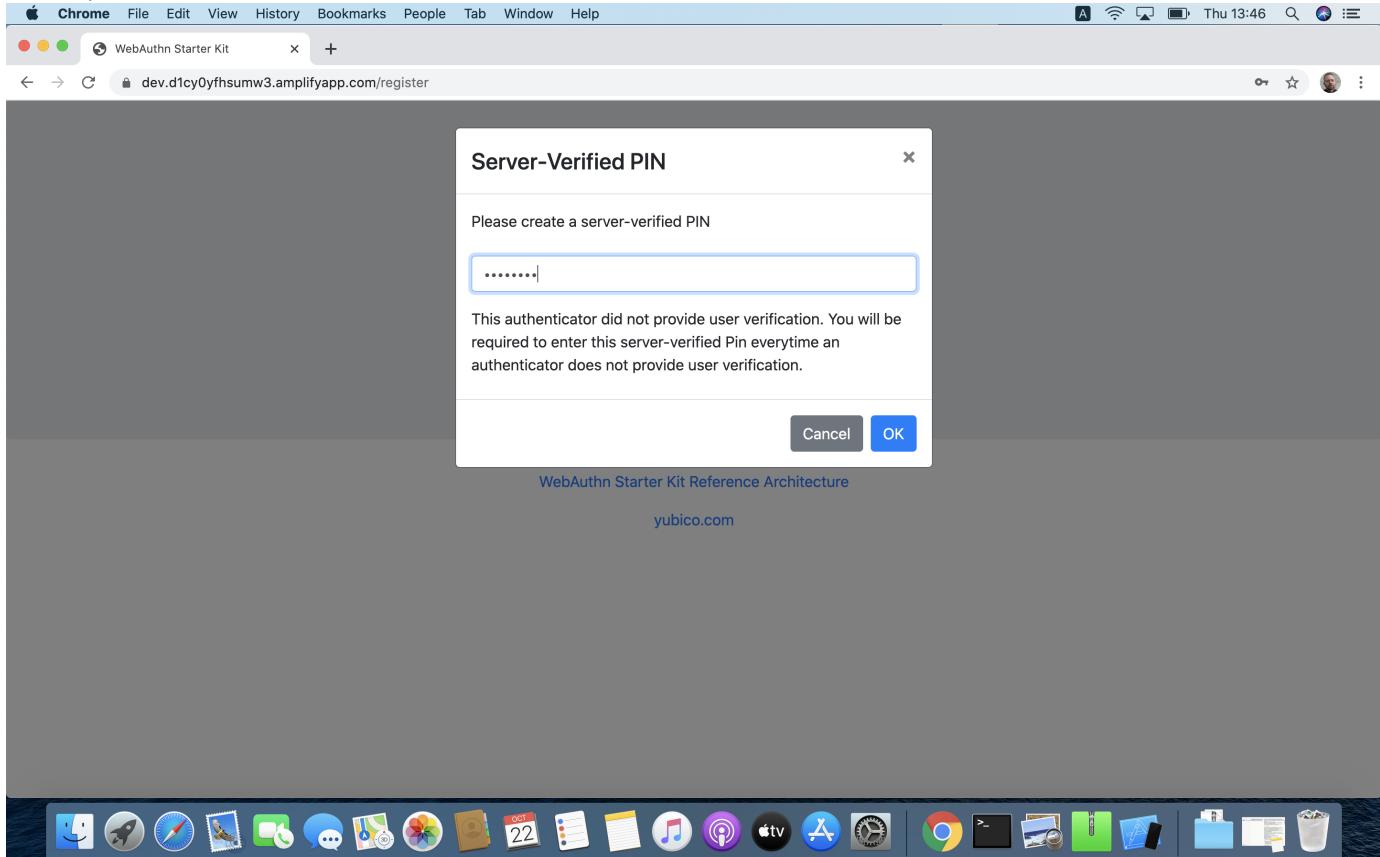


Figure 17 - The user sets a Server-Verified PIN

Registration for Usernameless flow on MacOS

Registration selections for Usernameless flow on MacOS

The FIDO2 authenticator used in this section is the following:

- A YubiKey 5 NFC (version 5.2.6) is used as FIDO2 authenticator. The YubiKey 5 is configured with FIDO2 credentials and a PIN-code according to section High Level WebAuthn Registration flow.

The registration route described in this section is derived from the following parameters and selections according to the Identifier First Flow page:

- The WebAuthn MakeCredentials parameter UserVerification is set to 'Preferred', which resolves to the CTAP2 parameter UV=1 for a FIDO2 enabled YubiKey used with Google Chrome on MacOS. This behaviour is equivalent to setting the WebAuthn MakeCredentials parameter UserVerification to 'Required'.
- The WebAuthn MakeCredentials parameter authenticatorSelection.requireResidentKey is set to 'True'.
- A Server-Verified PIN is not set for this account as part of the registration process (since the CTAP2 parameter UV=1 is set).

Registration process and UX design for Usernameless flow on MacOS

The WebAuthn Usernameless registration process requires that the user already has enrolled for FIDO credentials to a FIDO authenticator, and that the user has authenticated to the WebAuthn Starter Kit website.

Step 4.1: The user uses the FIDO authenticator to log on to the WebAuthn Starter Kit website as shown in the picture below.

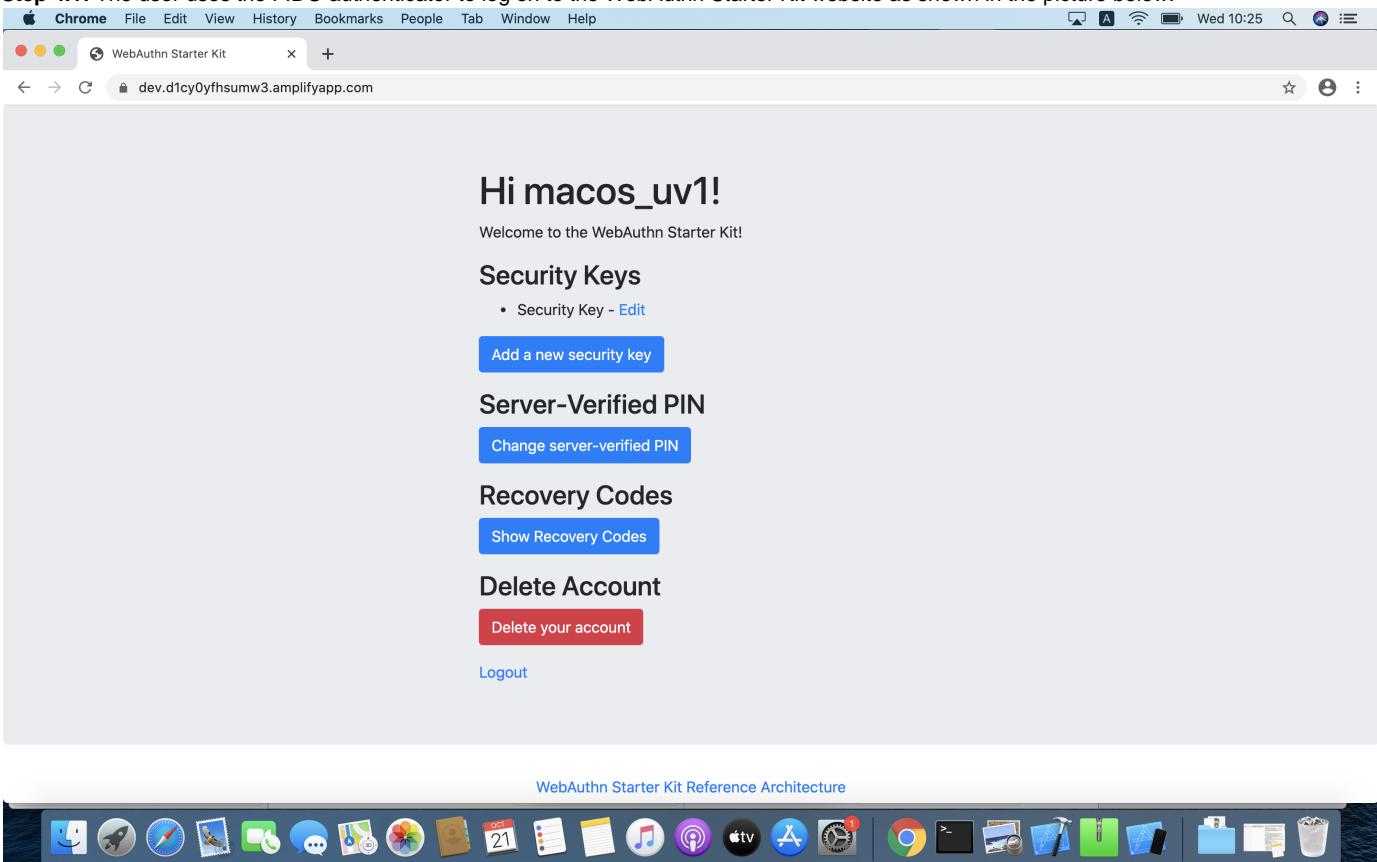


Figure 18 - WebAuthn Starter Kit administration website

Step 4.2: The user presses the button "Add a new security key". In the GUI that appears, the user enters a nickname for the usernameless FIDO authenticator, and marks the checkbox to "Enable usernameless login with this key". The user presses the button "Register security key" to complete the operation.

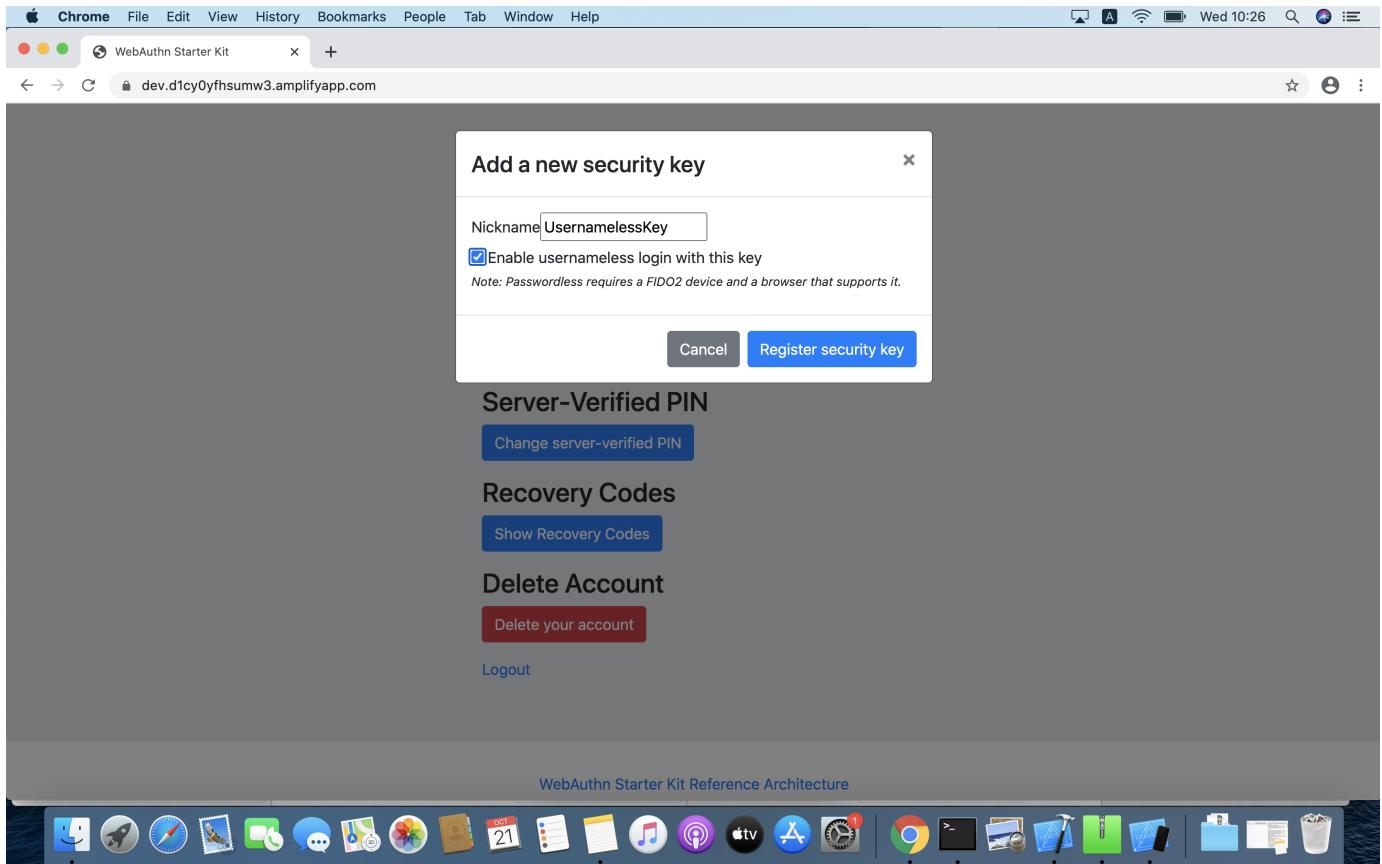


Figure 19 - Entering the nickname of a new security key

The user adds the security key according to the instructions in the section Adding a FIDO authenticator for MacOS. When this process is completed, the new YubiKey is added to the user's account, which is shown in the picture below.

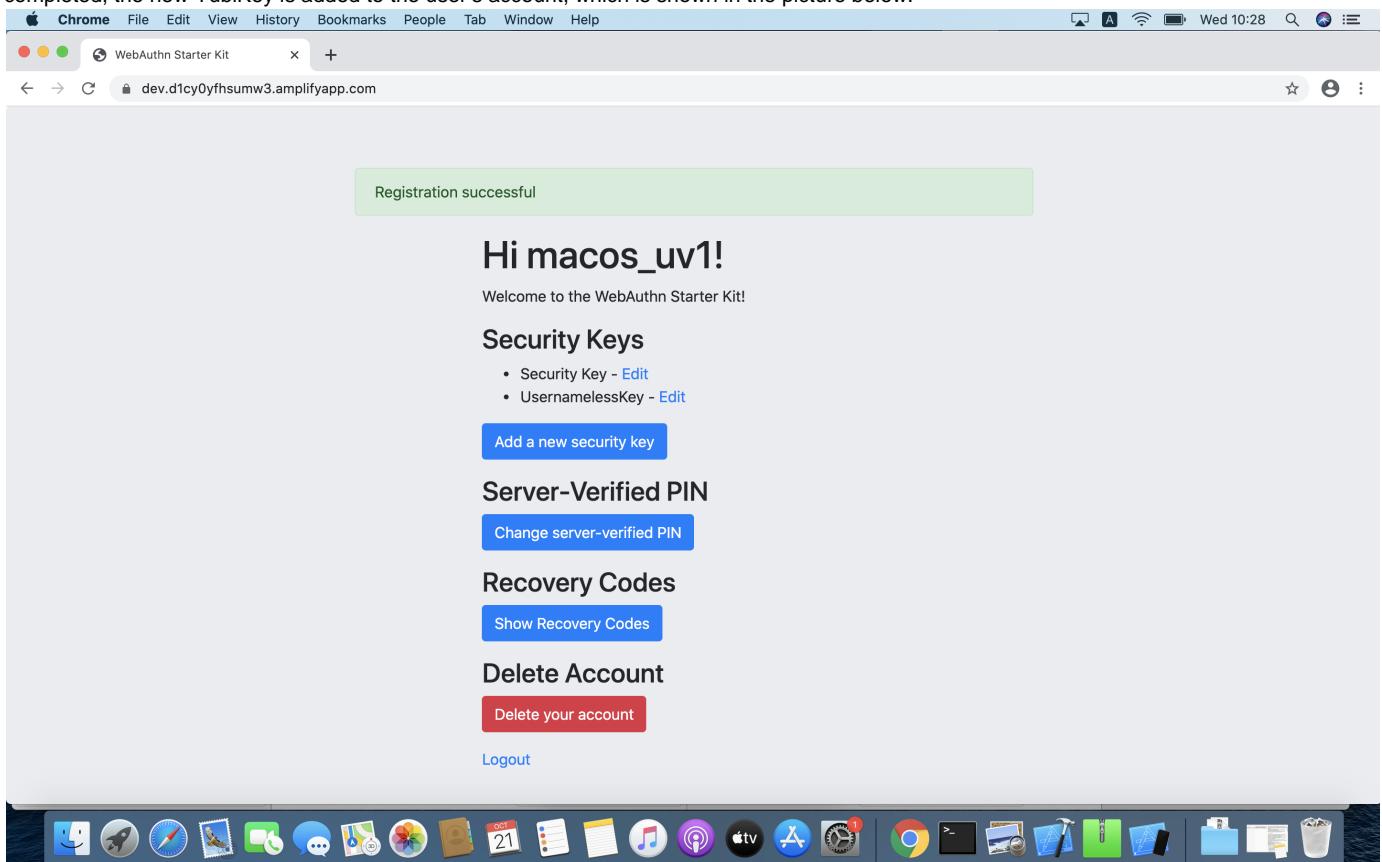


Figure 20 - An additional YubiKey is added to the user's account

At this stage, the security key with resident credentials for can be used for Usernameless authentication in to the same account.

If the user needs to re-use the same security key for the Usernameless flow, it is necessary to first delete the originally registered security key. Then only one security key is registered for the Usernameless flow.

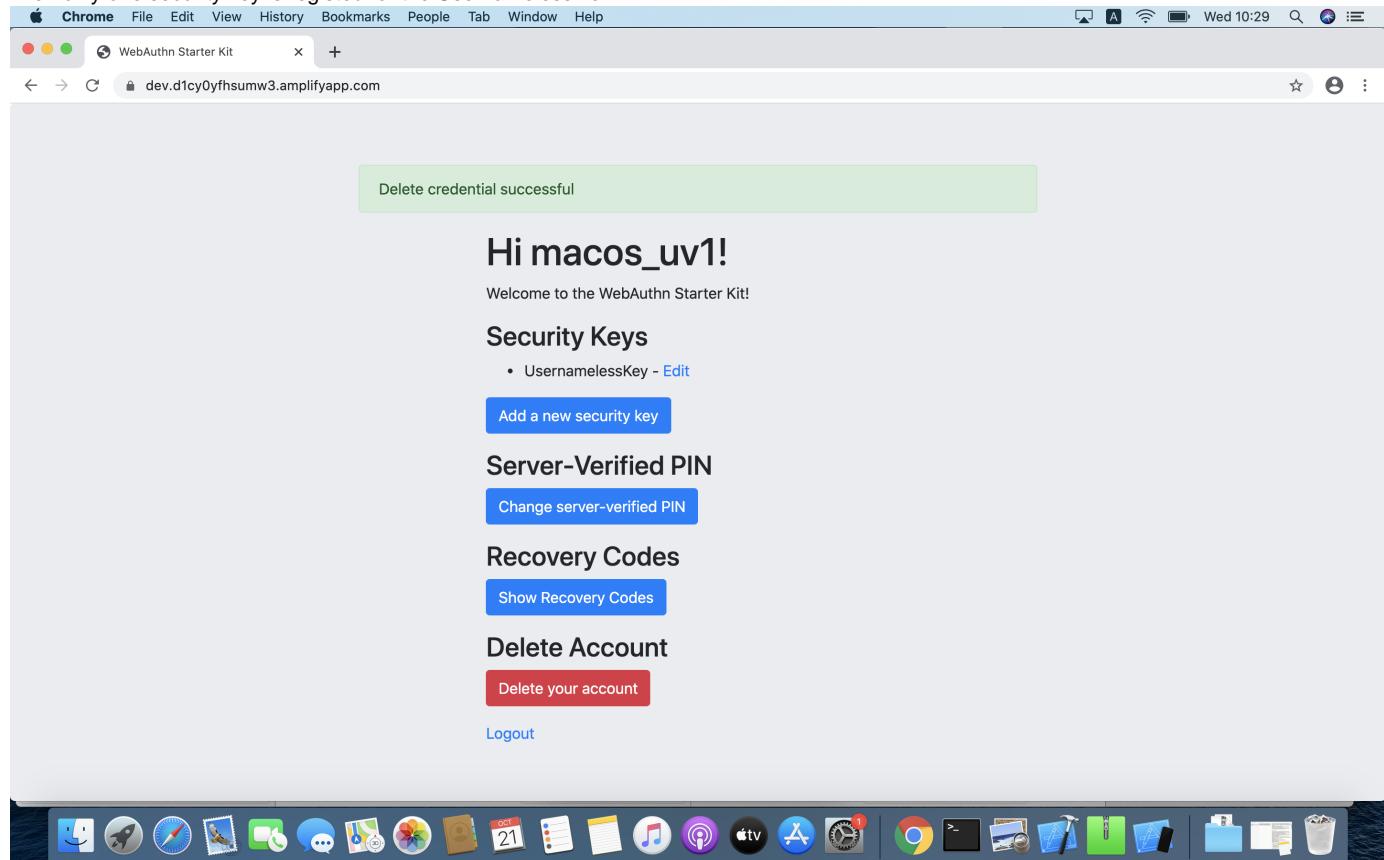


Figure 21 - Only one security key is configured for the Usernameless flow

WebAuthn registration using the Apple iOS Safari browser

Client configuration for Apple iOS with Safari

The client configuration used in this section is the following:

- Operating system: Apple iPhone iOS 14 developer beta 6
- Web browser: Apple iPhone Safari 14 developer beta 6
- FIDO2 implementation: Apple iPhone iOS 14 developer beta 6, which is an API that exposes the [W3C WebAuthn](#) functions to iOS applications (including Safari)

Registration for the User-Verified flow on Apple iOS with Safari

Registration selections for the User-Verified flow on Apple iOS with Safari

The FIDO authenticators used in this section is the following:

- A YubiKey 5Ci (version 5.2.7) is used as FIDO authenticator, which is plugged into the iPhone's lightning port. The FIDO2 application on the YubiKey is **activated**. The YubiKey 5Ci has a PIN-code set, but there are no FIDO2 credentials enrolled.
- A YubiKey 5 NFC (version 5.2.6) is also used as FIDO authenticator, which is tapped to the iPhone's NFC receiver. The FIDO2 application on the YubiKey is **activated**. The YubiKey 5 has a PIN-code set, but there are no FIDO2 credentials enrolled. The Yubico OTP application over NFC is deactivated, to avoid the NFC tag pop-up window.

The WebAuthn registration results are identical when using both YubiKeys.

The registration route described in this section is derived from the following parameters and selections according to the Identifier First Flow page:

- The WebAuthn MakeCredentials parameter UserVerification is set to 'Preferred', which resolves to the CTAP2 parameter UV=1 for a FIDO2 enabled YubiKey with PIN used with Safari on Apple iOS. This behaviour is equivalent to setting the WebAuthn MakeCredentials parameter UserVerification to 'Required'.
- A Server-Verified PIN is not set for this account as part of the registration process (since the CTAP2 parameter UV=1 is set).

Registration process and UX design for the User-Verified flow on Apple iOS with Safari

The selections for the registration process result in the registration flow and UX described in this section.

Step 5.1: The YubiKey with the FIDO2 application is selected as authenticator. (In other words, a platform authenticator is not used.)

Step 5.2: The user visits the WebAuthnKit URL. The site redirects the user to the Login page. Since a new user account shall be created, the user enters a new username.

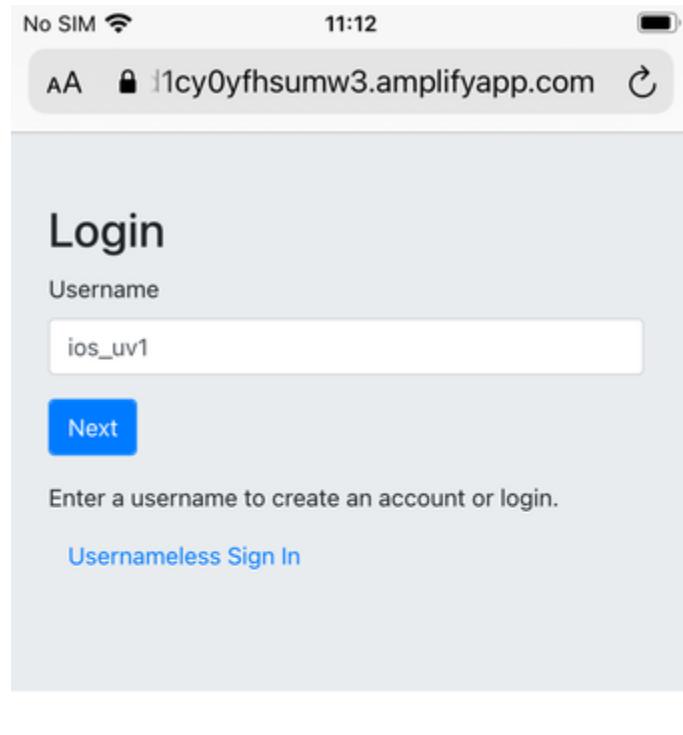
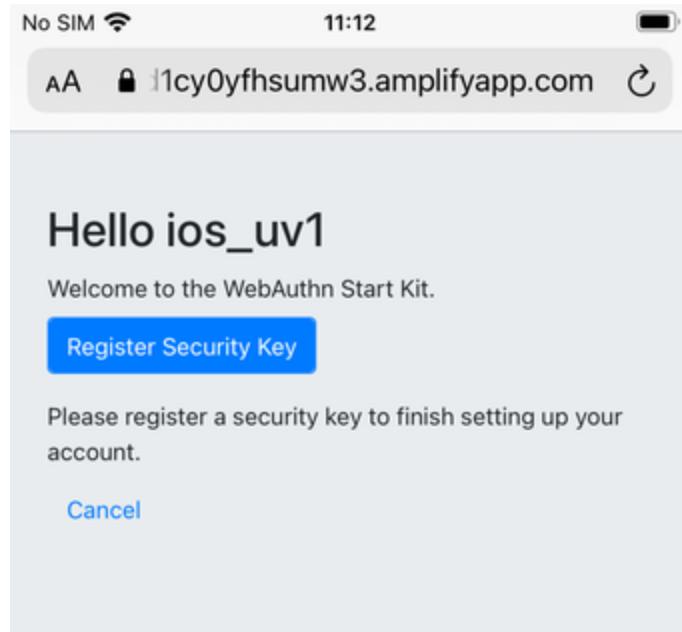


Figure 22 - Login page on MacOS for WebAuthn registration

Step 5.3: The user presses "Next" in the window above, and a new account is created for the user.

Step 5.4: Next, the registration page is shown below. The WebAuthn parameter UserVerification is set to 'Preferred' (CTAP2 UV=1) for this registration process. The user inserts the YubiKey 5Ci into the iPhone or taps the YubiKey 5 NFC and presses the button "Register Security Key".



[WebAuthn Starter Kit Reference Architecture](#)

[yubico.com](#)



Figure 23 - Registration page for security key

Step 5.5: Safari displays a security dialog box, which requests the user to insert the security key and touch it. The user inserts the YubiKey 5Ci and presses the sensor or taps the YubiKey 5 NFC.

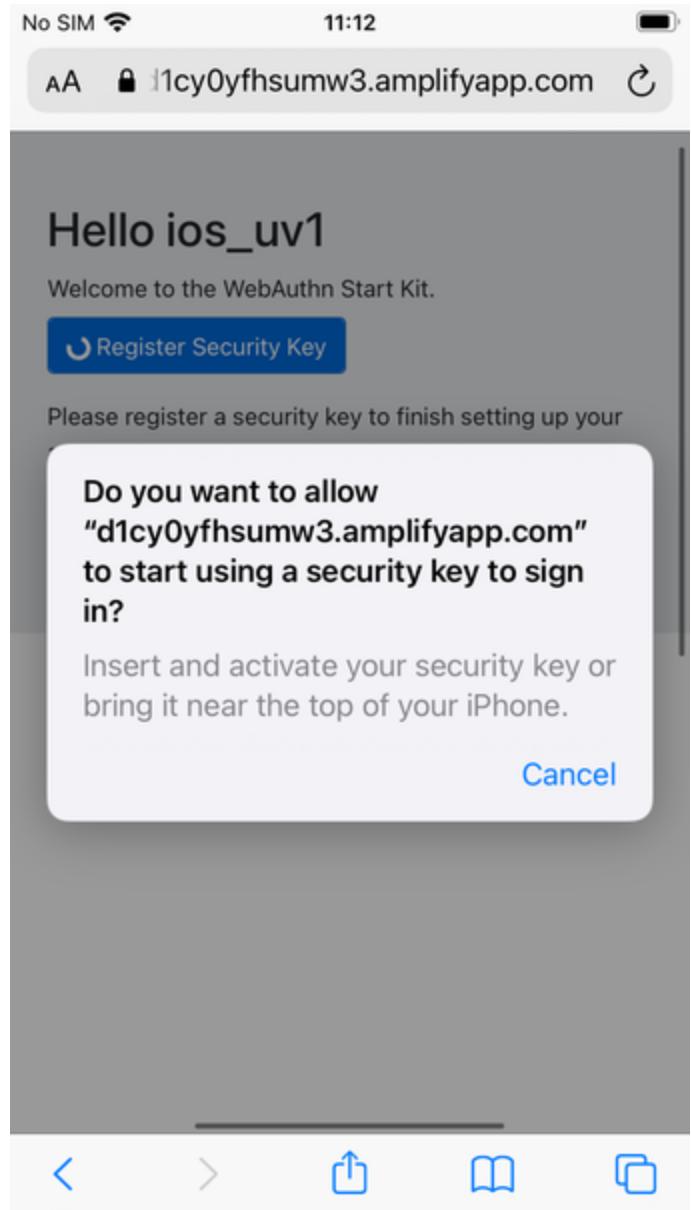


Figure 24 - Insert the FIDO authenticator and touch it

Step 5.6: Safari displays a security dialog box, in which the user enters the PIN-code for the YubiKey.

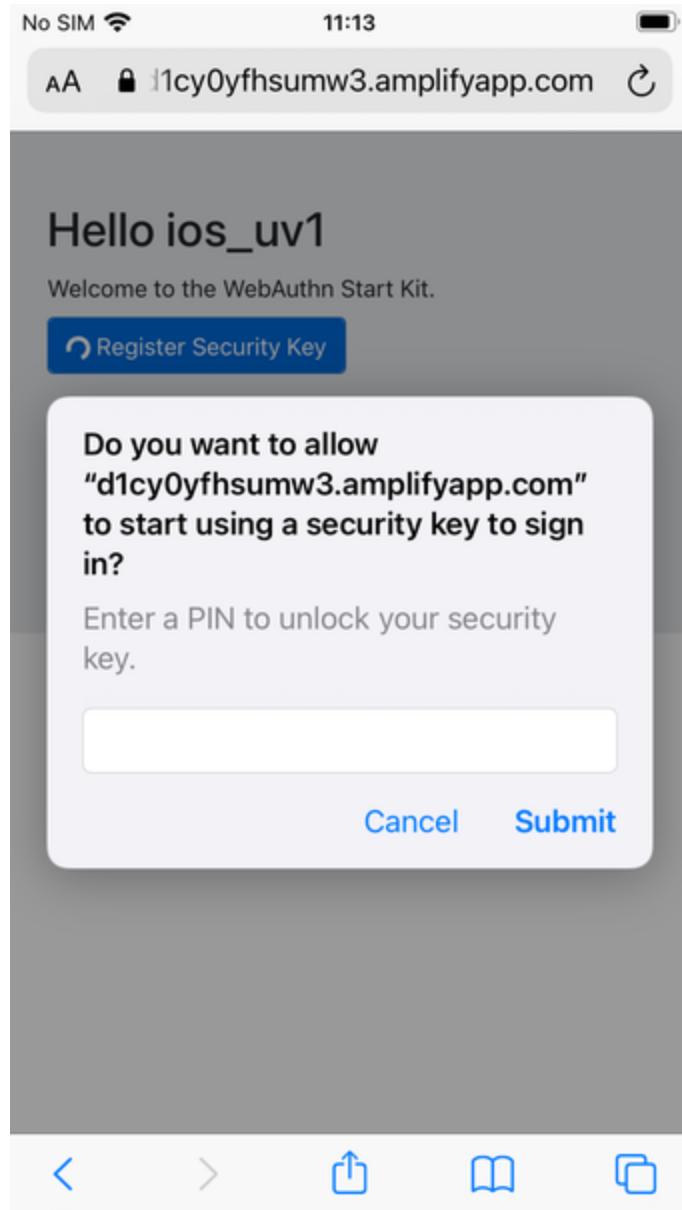


Figure 25 - Enter the PIN for the FIDO authenticator

Step 5.7: Safari displays a security dialog box, which requests the user to touch the security key one more time. The user inserts the YubiKey and presses the sensor again.

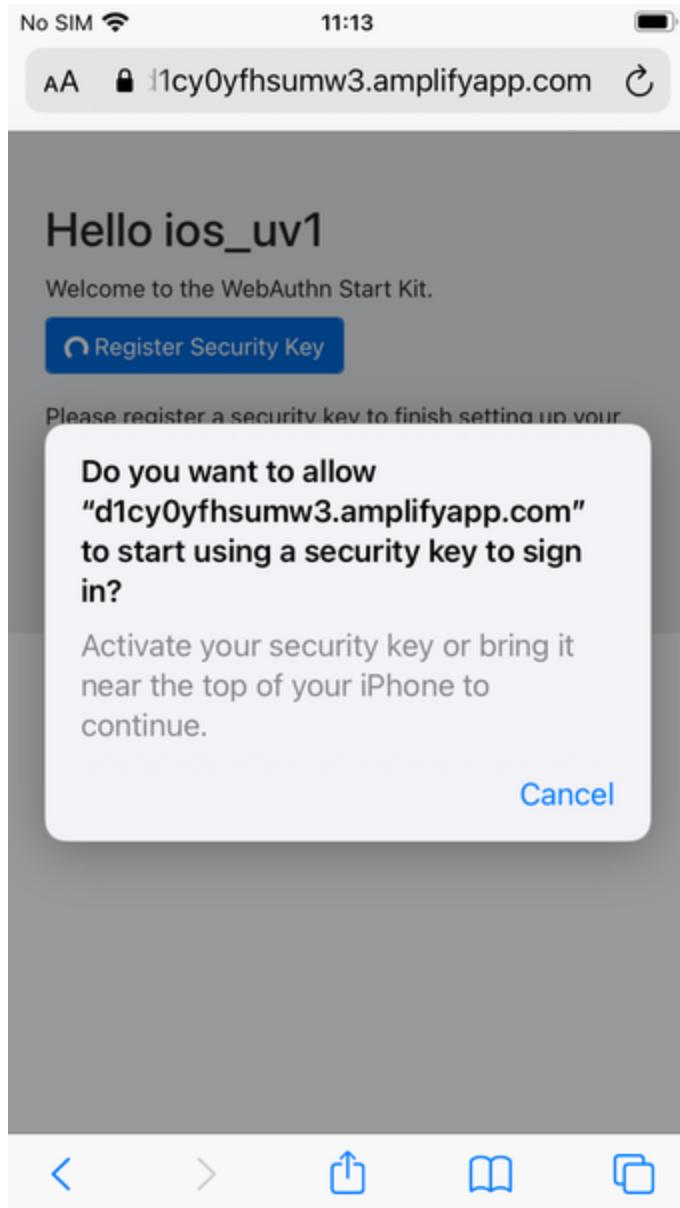


Figure 26 - Touch the FIDO authenticator one more time

Step 5.8: The account is created and an OpenID Connect token is returned to the browser.

Registration for the Server-Verified flow on Apple iOS with Safari

Registration selections for the Server-Verified flow on Apple iOS with Safari

The FIDO authenticators used in this section are the following:

- A YubiKey 5Ci is used as FIDO authenticator, which is plugged into the iPhone's lightning port. The FIDO2 application on the YubiKey is **deactivated**, which triggers the the Server-Verified behaviour on Apple iOS. Also a YubiKey with the FIDO2 application activated, but with no PIN-code set, will trigger the the Server-Verified flow on Apple iOS (which is a significant difference from Windows that will prompt the user for setting a PIN and activate the User-Verified process).
- A YubiKey 5 NFC (version 5.2.6) is also used as FIDO authenticator, which is tapped to the iPhone's NFC receiver. The FIDO2 application on the YubiKey 5 is **deactivated**, which triggers the Server-Verified behaviour on Apple iOS. Also a YubiKey with the FIDO2 application activated, but with no PIN-code set, will trigger the Server-Verified flow on Apple iOS (which is a significant difference from Windows that will prompt the user for setting a PIN and activate the the User-Verified flow). The Yubico OTP application over NFC is deactivated, to avoid the NFC tag pop-up window.

The registration route described in this section is derived from the following parameters and selections according to the Identifier First Flow page:

- The WebAuthn MakeCredentials parameter UserVerification is set to 'Preferred', which resolves to the CTAP2 parameter UV=0 for a FIDO2 disabled YubiKey used with Safari on Apple iOS. The backward compatible FIDO U2F flow of WebAuthn is therefore used. This behaviour is equivalent to setting the WebAuthn MakeCredentials parameter UserVerification to 'Discouraged'.
- A Server-Verified PIN is set for this account as part of the registration process (since the CTAP2 parameter UV=0 is set).

Registration process and UX design for Server-Verified flow on Apple iOS with Safari

The registration process for the Server-Verified flow is identical to the User-Verified registration process with one notable exception:

The FIDO authenticator will not require a PIN-code (as shown in figure 19); the FIDO authenticator will only require the user to touch the FIDO authenticator. Instead, the user must set a Server-Verified PIN when creating the account. The Server-Verified PIN is used as first factor authentication to protect the account.

An example of how to set a Server-Verified PIN is shown in the screenshot below.

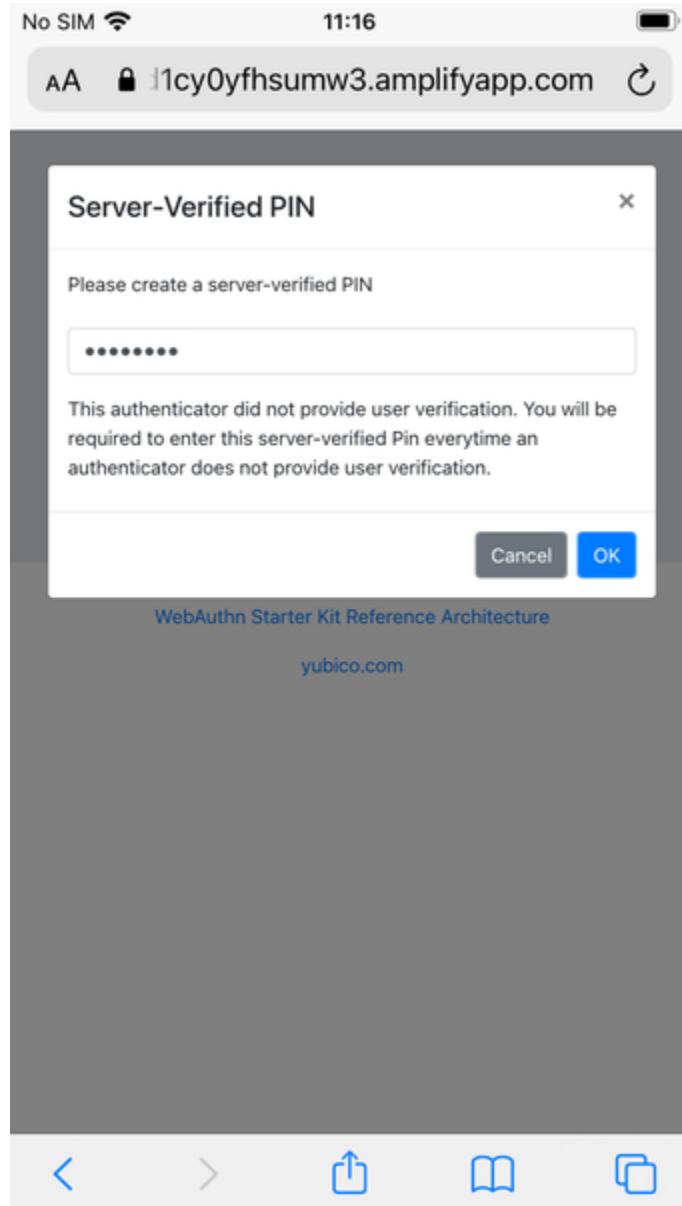


Figure 27 - The user sets a Server-Verified PIN

Registration for the Usernameless flow on Apple iOS with Safari

Registration selections for the Usernameless flow on Apple iOS with Safari

The FIDO authenticators used in this section is the following:

- A YubiKey 5Ci (version 5.2.7) is used as FIDO authenticator, which is plugged into the iPhone's lightning port. The FIDO2 application on the YubiKey is **activated**. The YubiKey 5Ci has a PIN-code set, but there are no FIDO2 credentials enrolled.
- A YubiKey 5 NFC (version 5.2.6) is also used as FIDO authenticator, which is tapped to the iPhone's NFC receiver. The FIDO2 application on the YubiKey is **activated**. The YubiKey 5 has a PIN-code set, but there are no FIDO2 credentials enrolled. The Yubico OTP application over NFC is deactivated, to avoid the NFC tag pop-up window.

The WebAuthn registration results are identical when using both YubiKeys.

The registration route described in this section is derived from the following parameters and selections according to the Identifier First Flow page:

- The WebAuthn MakeCredentials parameter UserVerification is set to 'Preferred', which resolves to the CTAP2 parameter UV=1 for a FIDO2 enabled YubiKey with PIN used with Safari on Apple iOS. This behaviour is equivalent to setting the WebAuthn MakeCredentials parameter UserVerification to 'Required'.
- The WebAuthn MakeCredentials parameter authenticatorSelection.requireResidentKey is set to 'True'.
- A Server-Verified PIN is not set for this account as part of the registration process (since the CTAP2 parameter UV=1 is set).

Registration process and UX design for the Usernameless flow on Apple iOS with Safari

The WebAuthn Usernameless registration process requires that the user already has enrolled for FIDO credentials to a FIDO authenticator, and that the user has authenticated to the WebAuthn Starter Kit website.

Step 6.1: The user uses the original FIDO authenticator to log on to the WebAuthn Starter Kit website as shown in the picture below.

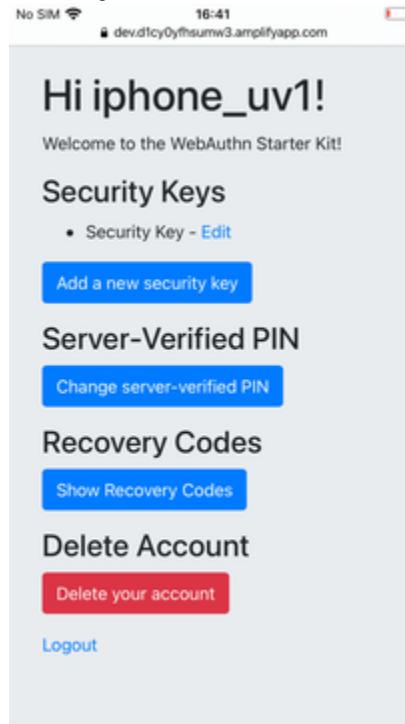
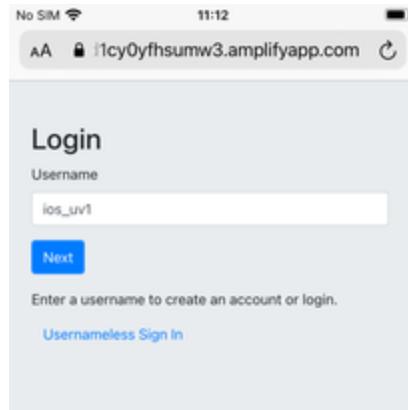


Figure 28 - WebAuthn Starter Kit administration website

Step 6.2: The user presses the button "Add a new security key". In the GUI that appears, the user enters a nickname for the usernameless FIDO authenticator, and marks the checkbox to "Enable usernameless login with this key". The user presses the button "Register security key" to complete the operation.



WebAuthn Starter Kit Reference Architecture

yubico.com



Figure 29 - Entering the nickname of a new security key

The user adds the security key according to the instructions in the section Adding a FIDO authenticator for Apple iOS Safari. When this process is completed, the new YubiKey is added to the user's account, which is shown in the picture below.

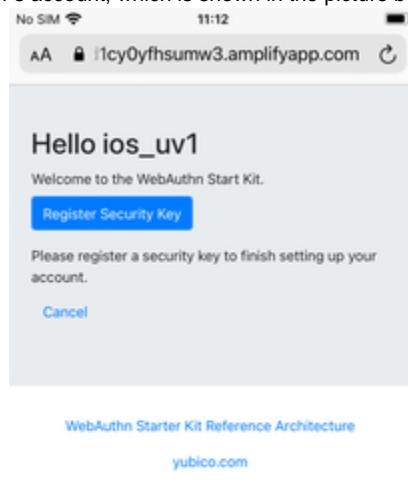


Figure 30 - An additional YubiKey is added to the user's account

At this stage, the security key with resident credentials for can be used for Usernameless authentication in to the same account.

If the user needs to re-use the same security key for the Usernameless flow, it is necessary to first delete the originally registered security key. Then only one security key is registered for the Usernameless flow.

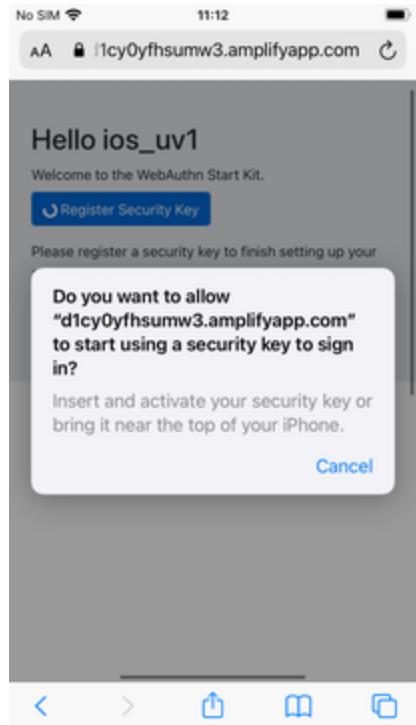


Figure 31 - Only one security key is configured for the Usernameless flow