Cirrent

Wi-Fi Onboarding Technologies for Connected Products

Introduction

Wi-Fi onboarding is the first thing most people do with connected products. First impressions are important, so the leading product companies are very thoughtful about how to create a great out-of-box experience and simplify the Wi-Fi onboarding of connected products.

Unfortunately the process is not always easy. 39% of negative reviews of connected products are related to initial setup and connectivity. Improving this process is critical to the success of the industry, and to the success of each individual product.

This guide characterizes the different Wi-Fi onboarding solutions available to developers of connected products, and compares the different approaches to make actionable recommendations.

Objectives & Considerations

The Wi-Fi onboarding process emcompasses two major functions:

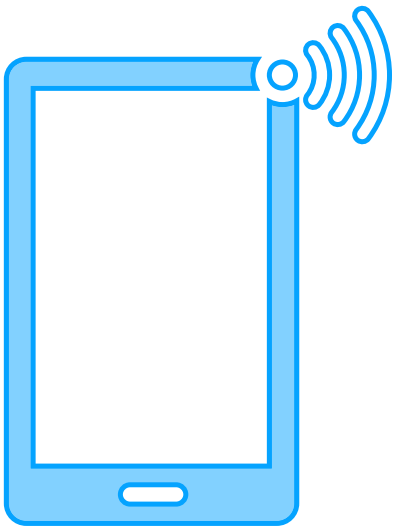
- Device-User Binding (DUB): this is the process of associating a specific device (typically represented by the device id or serial number) with a specific user (typically represented by the user's login).
- Secure Credential Distribution (SCD): this is the process of sending the Wi-Fi network credentials to the device.

This should be done with these considerations in mind:

- Ease of use. It is critically important for products to be as easy to use as possible. A good onboarding solution looks like magic to the end user - it just works!
- Scope of applicability. There are a wide variety of different onboarding devices -- iPhones, Android phones of different makes and models and firmware versions, and in some cases even desktops and laptops. Onboarding solutions must cover all possible cases to ensure the maximum target market.
- Hardware cost. Hardware is hard. Onboarding solutions should not drive hardware requirements if at all possible, to reduce the friction for development of new solutions and to minimize overall manufacturing costs.
- Development time. The consumer market moves quickly, so onboarding solutions should be easy to implement.
- Supportability. Onboarding solutions should tie in with support systems to provide a rich data stream to diagnose and debug issues -- both for users in the field and for continuous product improvement.
- Lifecycle support. Onboarding is not done just once: it is also done when the internet service provider ships a new router, the owner moves to another house, or the product is sold to another user.

Solution Comparison

There are many Wi-Fi onboarding solutions currently in use and soon to be available including: Soft Access Point, Bluetooth Low Energy (BLE), ZipKey, Amazon Wi-Fi Simple Setup, Wi-Fi Easy Connect and Homekit Wireless Accessory Configuration (WAC). Each of these is described below.



Soft Access Point

Description

SoftAP is an abbreviation for software enabled access point, also known as a virtual router. Manufacturers often use SoftAP to let users configure their Wi-Fi network names and passwords into headless products. The product uses its Wi-Fi radio to create a temporary access point for the sole purpose of getting the network name and password for the user's private network from the app on a smartphone.

Most products today use the SoftAP process to get connected. However, this process has a high failure rate: about 20% of people get hopelessly stuck and are unable to get their product connected to their home Wi-Fi network.

Hardware Requirements

SoftAP can be done with any reasonably modern Wi-Fi chip. It requires no additional hardware.

Onboarding Device Applicability

SoftAP can work with both Android and iOS, but cannot be done reliably with a web browser (because many desktop computers still use ethernet). Both Android and iOS have their own difficulties with SoftAP:

- iOS: in iOS the app can now control the Wi-Fi subsystem to join a pre-defined SSID. For products where the SSID is standardized, this removes the requirement for the user to select the Wi-Fi network to join. However, even in this case the SoftAP onboarding process is unreliable and error prone. For products where the SSID is not well defined (for example where the SSID is unique per device) the user is required to select the specific Wi-Fi network, which is difficult and confusing for many customers.

- Android: On Android, it's even worse. While the app can control the Wi-Fi subsystem to get the phone on the product's SoftAP network, the fragmentation of hardware and software in the Android ecosystem makes results unpredictable. Some phones will immediately fall off the SoftAP network because there is no internet connectivity. Others will stay on for a while, then fall off midway through the process. Others will stay on the SoftAP network even after the onboarding is complete, or will reconnect to the SoftAP network, leaving the phone disconnected from the internet. This makes developing an app complex at best, and at worst makes it impossible to provide a good user experience.

- Browser: SoftAP cannot be done reliably on a computer browser because the instructions for different operating systems are different, and the machines may be connected over ethernet rather than Wi-Fi.

Advantages

The advantage of SoftAP is that it is within the control of the product company, works with standard hardware, and works with all Wi-Fi routers. Its universality has made Soft AP the go-to solution for most products in the past.

Recommendations

SoftAP has complexity related to iOS (difficult process for the user) and Android (unpredictable problems with various phone and software versions) as described above. In addition, Soft AP is difficult for users to figure out, and it is difficult to engineer a reliable Soft AP solution.

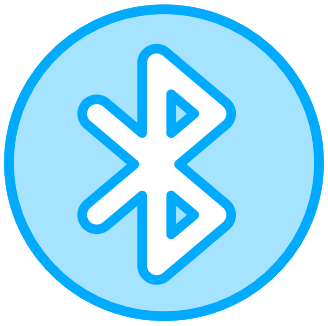
Because the phone and the device are disconnected from the internet during the process, if anything goes wrong, things fall apart. If the user successfully gets the private network name and password sent to the product, then the product and app disconnect from each other while the product tries to connect to the private network.

If all goes well, they'll both reconnect to the internet, but if the password is wrong or the product can't join, the app and product can no longer communicate, and the user gets lost in the process.

In addition, the user is required to enter the Wi-Fi password in the app when using the Soft AP process.

Disadvantages

The SoftAP process results in a poor out-of-box experience, so while many companies feel like they have no choice, it should be avoided where possible. For those cases where there is no choice, it's advisable to use software in the connected product and mobile app that has been proven across a variety of phones and routers. Where possible, use other solutions instead of or to augment Soft AP.



Bluetooth Low Energy

Description

Bluetooth Low Energy (BLE) can be used to create a local wireless link between a smartphone and a device to exchange the Wi-Fi credentials.

Hardware Requirements

To use BLE for Wi-Fi onboarding, the device must include a BLE chipset, associated hardware, and antenna. As Wi-Fi and BLE combo chips have become more common and cost competitive, BLE has become more common in Wi-Fi connected products. In many cases the BLE is used exclusively for Wi-Fi onboarding.

Onboarding Device Applicability

Most modern smartphones have BLE capability built in, and can take advantage of the BLE to facilitate Wi-Fi onboarding. However many desktop computers do not have BLE technology (or don't have an easy way for consumers to manage the BLE connection), so browser onboarding is not well supported.

- iOS: BLE in iOS is fairly predictable and dependable
- Android: BLE in Android is not reliable, and varies between different hardware and software versions. Flakiness of the BLE connection can cause support issues if this is the primary onboarding mechanism.
- Browser: BLE is typically not accessible through a browser so it is not possible to use a browser for Wi-fi onboarding with BLE

Advantages

There are two big advantage of BLE over SoftAP:

1. The user doesn't have to go into settings on iOS. In both iOS and Android the BLE connection can be controlled directly through the app with no user intervention, so it can be a simple user experience.

2. The phone and device stay connected throughout the process, and the phone can stay connected to the internet. If there is a problem, it is much easier to recover because the app remains online. It is more straightforward to engineer a reliable process with BLE than with Soft AP.

Disadvantages

The BLE onboarding solution cannot be done with a browser, Android implementations may be flakey, and the user is required to enter the password for the Wi-Fi network.

Recommendations

If a Bluetooth chip is available in the product for other purposes (like music streaming) then this should be used for Wi-Fi onboarding instead of Soft AP.

Amazon Wi-Fi Simple Setup

Description

Amazon announced Wi-Fi Simple Setup in late 2018 as part of their Frustration-Free Setup program. Customers will be able to connect supported smart devices to their Wi-Fi network in a few steps.

Hardware Requirements

Wi-Fi Simple Setup can be done with any reasonably modern Wi-Fi chip. It requires no additional hardware.

Onboarding Device Applicability

Amazon Wi-Fi Simple Setup will be available to product manufacturers making connected products.

For end users to get the benefit of Wi-Fi Simple Setup, they must purchase that product through Amazon.com and have an existing, connected 2nd generation or newer Echo device in the home. They must also choose to allow Amazon to save their credentials.

Advantages

If the end user has an existing Amazon Echo in the home, the user experience to onboard a Wi-Fi Simple Setup-enabled device is simple and delightful. If the user purchased the Wi-Fi Simple Setup Device from Amazon.com using the Amazon account and the user has stored the Wi-Fi credentials in the Amazon Wi-Fi locker, then the device can automatically connect to Wi-Fi.

Disadvantages

For consumers to take full advantage of Wi-Fi Simple Setup, they must purchase the connected products from Amazon.com. Products purchased from other retailers will not realize the benefits of this solution.

Product manufacturers will potentially need to create separate SKUs for their products enabled with Wi-Fi Simple Setup.

Another disadvantage is that the end user must already have a 2nd generation or later Amazon Echo device connected in their home. In 2019, there are estimated to be around 40 million homes with an Echo. Amazon continues to gain market share in the smart speaker space but its competitors like Google and Apple are catching up.

As of early 2019, Amazon Wi-Fi Simple Setup is not launched.

Recommendations

If the majority of your products are sold through Amazon.com in territories with high adoption of Amazon Echos, this may be a good solution.

Wi-Fi Easy Connect™

Description

In 2018 the Wi-Fi Alliance introduced Wi-Fi Easy Connect -- a totally new mechanism for connected products to Wi-Fi. The idea behind Wi-Fi Easy Connect is that the user will use a smartphone or tablet to scan a special DPP (Device Provisioning Protocol) quick response code (QR code) on the connected product, and the phone will then send a "connector" to the product that will allow it to connect to the Wi-Fi network. The connector can be either a WPA2 connector (SSID and password), or a WPA3 connecter (a certificate that allows the device to connect to the router). Wi-Fi Easy Connect requires either the smartphone OS or a device in the home to support DPP.

Hardware Requirements

Wi-Fi Easy Connect can be done with any modern Wi-Fi chip that supports Wi-Fi Easy Connect. It requires no additional hardware.

Onboarding Device Applicability

In order to use Wi-Fi Easy Connect, both the mobile phone OS and the connected product must support Wi-Fi Easy Connect. The Wi-Fi Easy Connect-enabled product should be able to display a QR code or have a QR code printed on its packaging or as an insert. In addition, devices will need to support the Device Provisioning Protocol (DPP). Wi-Fi Easy Connect defaults to QR code bootstrapping but BLE and NFC are also supported.

As of early 2019, neither iOS nor Android support DPP. Without this support, product companies will not put DPP QR codes on their products. The path towards adoption of Wi-Fi Easy Connect for connected products is unclear.

Advantages

Wi-Fi Easy Connect envisions a simple process for end users: point the camera at the QR code and the Wi-Fi onboarding happens quickly. Wi-Fi Easy Connect also provides a clear path towards provisioning devices on WPA3 networks, which provide higher security.

Disadvantages

It will take time for home routers to support WPA3 and Easy Connect, and as of now iOS and Android don't have the technology built in yet. Until iOS, Android, or other devices in the home support Wi-Fi Easy Connect it is not a viable option for connected products.

Recommendations

We encourage product companies to keep an eye on Wi-Fi Easy Connect, and consider adopting once iOS, Android, or other devices in the home support Wi-Fi Easy connect.

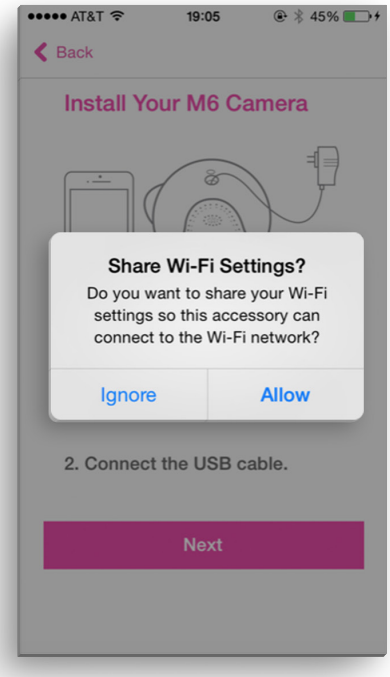
Homekit Wireless Accessory Configuration (WAC)

Description

Apple's Homekit supports a feature called Wireless Accessory Configuration (WAC), which takes the Wi-Fi network credentials from the phone and shares them directly with the device. The iOS app brings up a system dialog box to get the user's confirmation to allow the Wi-Fi network password to be sent to the device.

Hardware Requirements

WAC is only available for products that have been through Apple's MFI program. This is now available in software, and no longer requires a specific Apple MFI chip. However, the product must undergo extensive costs for testing, certification, and approval from Apple.



Onboarding Device Applicability

WAC works only for iOS.

Advantages

WAC provides a nice user experience: it avoids the convoluted SoftAP process on iOS and eliminates the need for the user to type in the Wi-Fi network password.

Disadvantages

While there have been significant reliability issues reported with WAC, it is expected to improve over time. The main disadvantages are the Apple requirements (rigorous branding, testing, and usage guidelines from Apple), and the limited applicability (iOS only).

Recommendations

Products that have BLE should use WAC where possible.

ZipKey

Description

ZipKey is a technology supported by the leading internet service providers to simplify the onboarding of Wi-Fi devices. ZipKey hotspots -- ISP-controlled guest networks that are isolated from the user's private network and allow ZipKey products to connect to the cloud -- make Wi-Fi onboarding a cloud-facilitated process rather than a local process, improving the reliability and eliminating the need for the user to manually enter the Wi-Fi password.

Hardware Requirements

ZipKey is compatible with standard Wi-Fi chips, so no hardware change is necessary.

Onboarding Device Applicability

ZipKey works with all connected products that have an app (iOS and Android), products with a display (like TVs) and network operator CPE.

Advantages

ZipKey provides a great end-user experience, is proven, reliable, and secure, and integrates automatically with ISP network management apps. The user doesn't have to enter the Wi-Fi password, and the process is reliable because the product and app stay connected to the cloud through the entire onboarding process.

ZipKey also provides benefits in the ongoing lifecycle of the product, including reprovisioning, moving between networks, and automatic update of Wi-Fi credentials when they change.

Disadvantages

Not all customers get the password-free onboarding -- only those with a Wi-Fi router from a ZipKey ISP (which includes Comcast and other operators in the US, Europe, and around the world). Today over 127 million homes have ZipKey capability. This continues to grow globally.

Recommendations

ZipKey provides the best possible user experience with the lowest possible cost throughout a the product lifecycle.

Cirrent offers Wi-Fi Provisioning that includes ZipKey Wi-Fi Onboarding, as well as the other Wi-Fi onboarding technologies. With one integration, product companies have all Wi-Fi onboarding methods available.

Other Alternatives

In the past companies have come up with a wide variety of approaches to solving the Wi-Fi onboarding problem, but each had critical flaws that prevented the widespread use of the approach. Each one may be used in some limited cases, but these solutions are not recommended.

- Remote control. Some products with screens (TVs, streaming video products, and digital picture frames) use remote controls to have the user type in the Wi-Fi password. This process can be reliable because the communication channel with the consumer is always available, but typing complex passwords by remote control is cumbersome for users. A remote control can be a good backup for ZipKey for products with screens, but ZipKey should be used where possible to simplify the process for users.

- WPS. Wireless Protected Setup (WPS) uses a button on the router and a button on the product to allow the user to exchange Wi-Fi credentials with no separate user interface. In theory, this should work well, but in practice it not only has major security flaws but also is unreliable for customers. Many home Wi-Fi routers have WPS buttons that are disabled by default from their internet service providers, and this causes tremendous user frustration because users have no visibility into whether WPS is working or not. Without an effective user interface, we expect WPS has caused more frustrated customers than any of the other Wi-Fi onboarding technologies. We strongly discourage the use of WPS for both security and ease-of-use reasons.

- Audio cable. Some products use an audio cable between a smartphone and the device to provision the Wi-Fi credentials. The product used a modulated sound to send the encoded Wi-Fi information down to the device, and the device used a modulated signal to send information back to the app. This process has proven unreliable, the audio cable added cost, and it is inconvenient for people to have to keep an audio cable around for provisioning and reprovisioning. This solution is not recommended.

- Sound. Very low cost products (like the Amazon Dash Button) have used sound to send the Wi-Fi credential information to the device from the smartphone. The device has a mechanism to go into joining mode, where the microphone listens for the app to send the modulated Wi-Fi information. This process is also unreliable and should not be used.

- QR Code with a camera. Some Wi-Fi cameras can be provisioned using a QR code on the smartphone screen. This process works OK, but is sometimes difficult for users because they cannot see what the camera sees, so it is difficult for the user to position the phone accurately enough for the camera to reliably read the QR code. Also because the camera cannot communicate back to the user or the phone app, it can leave the user confused about how to proceed if it is not working. This process is difficult for users to understand and should not be used.

- QR Code with a display. Products with a display or mechanism to display QR code from the product can take advantage of QR code onboarding. Recent updates to smartphone cameras allow users to scan QR codes directly from their existing camera app.

Conclusions

There are many Wi-Fi onboarding solutions available on the market, each with its pros and cons. Wi-Fi onboarding will continue to evolve. And with more options comes more choices that product manufacturers will need to make and more work that they'll need to do to implement the technologies into their products.

Product teams and engineers are already spending a large amount of their time figuring out connectivity. And once it is figured out, they need to keep up with the changes.

Cirrent offers a Wi-Fi Provisioning solution that can include all Wi-Fi onboarding technologies or a subset of the product company's choosing. With Cirrent, product manufacturers can integrate a Wi-Fi provisioning solution once and future-proof their products, allowing them to focus on the product itself.

ONBOARDING SOLUTION	HARDWARE REQUIREMENTS	ADVANTAGES	DISADVANTAGES
SoftAP	Wi-Fi Chip	Works with existing hardware	Complex for iOS users. 40-60% failure rate. Unreliable on Android Unreliable process unless it goes perfectly. User has to enter Wi-Fi password manually
BLE	Bluetooth Low Energy chip and associated components	Eliminates some difficult aspects of SoftAP Product and phone stay connected to the internet	Hardware cost Unreliable on Android User has to enter Wi-Fi password manually
Amazon Wi-Fi Simple Setup	Wi-Fi Chip	Works with existing hardware	User must own a connected 2nd gen or later Amazon Echo device User must have stored credentials in the Amazon Wi-Fi locker Products must be sold via Amazon.com

ONBOARDING SOLUTION	HARDWARE REQUIREMENTS	ADVANTAGES	DISADVANTAGES
Wi-Fi Easy Connect	Wi-Fi Chip	Works with existing hardware	LAN only- no cloud capabilities Unclear how broadly adopted this method will be
ZipKey	Wi-Fi Chip	Works with existing hardware Low cost Product and phone stay connected to the internet Automatically handles reprovisioning on network	Best experience not available in all homes yet
Apple HomeKit Wireless Accessory Configuration (WAC)	Apple MFI compatible chips	User doesn't have to enter SSID and password	Does not help Android users Apple branding and testing
Remote control	Screen Remote control	User can get feedback from the device directly No smartphone app required	Remote control is expensive - should be avoided if possible Users have a hard time entering passwords by remote control