Dear Apple,

Windmill uses the `Command Line Tools Package` (https://developer.apple.com/library/archive/technotes/tn2339/_index.html) to provide continuous delivery to iOS Developers, natively on Apple Platforms. Windmill is built with a well defined process in mind on how to deliver quality apps in an effort to improve consistency, a high level of understanding and agreement across teams, businesses and the industry.

Apps have become more complex and demanding. It takes more developers to build and maintain a high quality iPhone app. Outside of Xcode, there is very little support to developers during the development process.

Windmill is a developer tool available only to registered individuals and organisations with the Apple Developer Program. Windmill on the Mac uses an existing installation of command line tools, as managed by Xcode, to build, test, archive, export and create an ad-hoc distribution so that developers can install their app directly on their Apple devices for testing. Windmill on the iPhone is designed for in-house distribution as documented in the "iOS Deployment Reference" (https://help.apple.com/deployment/ios/#/apda0e3426d7).

Windmill makes it easy for developers to distribute their app continuously while still in development, in regular time intervals, on demand or as a reaction.

- As individual contractors, it enables them to show progress to a client offsite and deploy bug fixes, at will, in time critical moments.
- As part of a team, it enables them to have nightly builds to get daily feedback from a product owner.
- As part of an organisation, it enables them to have weekly meetings with the business and marketing team to do a demo, discuss and plan next week's development.

On the same day developers download and install Xcode they start using Windmill; way before they consider the option to distribute via TestFlight which is best suited for planned, methodical and well calculated testing of an app on its way to the App Store.

Developers have increasingly been making use of cloud services to benefit from continuous integration and ad-hoc distribution during the development phase. Typically these are branded as continuous integration or continuous delivery services.

Existing services operate outside of the App Store, asking developers to hand off their Apple Certificates, Private Keys, Provisioning Profiles and their Apple Developer Account credentials in exchange of automatic provisioning of devices and ad-hoc distribution. BuddyBuild too, before it was acquired by Apple, was asking to upload an Apple Certificate and Private Key in order to have ad-hoc distribution.

Developers will happily share some or all of that information by making a choice, some potentially not realising, to accept whatever risk in exchange for the benefits and value they get from continuous delivery services and tools.

Rejecting Windmill on the iPhone takes away ad-hoc distribution and hinders the development of Windmill as a whole by effectively making it impossible to make use of `StoreKit` to accept payments and manage subscriptions to provide a seamless experience.

I understand that it is well within your jurisdiction to outright prevent Windmill or anything like it from being on the App Store. However, my hope is that Apple takes this opportunity to embrace developer tools like Windmill and redefine what is possible on the App Store from this day onward.

Approving Windmill on the App Store is a win-win situation for both Apple and us, developers. It will empower developers to build quality apps by making use of a tool that is built for purpose on the Apple platforms. A tool that offers unparalleled user experience and is built with security and privacy in mind. Ideals that Apple both embodies and is the champion of.

Security considerations and implementation details

Creating an ad-hoc distribution

Windmill uses `xcodebuild` to archive and export an ad-hoc distribution in the way that is documented by Apple.

> *How do I archive and export my app for distribution? -* ***Building from the Command Line with Xcode FAQ, Technical Note TN2339****.* *https://developer.apple.com/library/archive/technotes/tn2339/_index.html#//apple_ref/doc/uid/DTS40014588-CH1-HOW_DO_I_ARCHIVE_AND_EXPORT_MY_APP_FOR_DISTRIBUTION_*

Since Windmill runs on a Mac under the control of a developer, it does not require, expect nor asks for explicit access to their Private Key, Apple Certificate or Apple Credentials.

Distributing an app

Before Windmill first distributes an app, it requires 2 things to happen. The order is not important.

1. A user must have an active subscription.
2. A user must be logged in their Apple Account and have CloudKit enabled.

A user must have an active subscription

* Using `StoreKit` a user purchases an auto-renewable subscription.
* The receipt is sent to Windmill on the Server.
* The receipt is passed to the App Store for validation.
* The receipt is stored on the server and a subscription is created.
* A JWT claim, valid for the duration of the subscription is sent to Windmill on the iPhone as proof.
* The JWT claim is stored in the keychain.

A user must be logged in their iPhone

Once the user's `CKContainer.default().accountStatus` becomes available AND an active subscription exists:

* The user record name and container identifier is sent to Windmill on the Server, authorised by the subscription claim.
* An account is created and an access token is returned.
* Both the account identifier and access token are stored in the keychain.
* The account identifier and subscription claim are stored in the user's private CloudKit database.

Windmill on the Mac, which has registered to receive subscription notifications, is notified that a subscription exists.

* Both the account identifier and subscription claim are sent to Windmill on the Server.
* The recorded receipt is validated with the App Store.
* Given that the subscription is still valid, an access token is created and returned.
* Windmill on the Mac uses that token to distribute the app.
* Once the app has been successfully distributed, Windmill on the Server sends a push notification and a `content-available` to Windmill on the iPhone.
* Windmill on the iPhone retrieves the list of apps that have been distributed.

Installing an app

Windmill on the iPhone uses a public interface provided by iOS to download and install an app.

Using `itms-services://?action=download-manifest&url=` in a secure way was the toughest security challenge that I faced while building Windmill.

As you very well know, the value of the `url` parameter is an https resource URL. This URL cannot have any query parameters, headers and once it has been handoff to iOS, it cannot be intercepted.

Working within the confines of itms-services

The URL is not publicly visible by default, instead Windmill relies on the link detection functionality when the user taps the INSTALL button. All managed by iOS.

The URL is in the form of

https://api.windmill.io/export/manifest/eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJqdGkiOiJmZHU1QUxrNmdGTHVuYk1Ic1pqciIsInN1YiI6IjcyMzYxYzVmLTkxMDMtNDE4Zi1hYjYzLTFjZjEwNWM1MzAwNSIsImV4cCI6MTU1ODgwODg4MywidHlwIjoiZXhwIiwidiI6MX0.9_gFB_YwG7wf_Ze1cYMu6WS6e01MJAoRIRDbo1U9VEA

Where the last path is a JWT claim that is both signed and will expire. It is also scoped to each specific ad-hoc distribution and can be put in a black list to prevent further installations.

At the time that URL is requested, Windmill on the Server will generate a manifest that is unique to that request and under the `software-package` key, contains the URL where the IPA to be installed is available.

That URL to download the IPA from, is also signed but with a different key to the one that signs the claim, used exclusively to provide access to the IPA and aggressively time-limited to 5 minutes which gives a long enough window for iOS to install the app but short enough to be made public.

Why I believe Windmill complies with the App Store Review Guidelines and the Apple Developer Program License Agreement

Apple Developer Program License Agreement - 2.6 - No Other Permitted Uses

EXCEPT AS OTHERWISE SET FORTH IN THIS AGREEMENT, YOU AGREE NOT TO RENT, LEASE, LEND, UPLOAD TO OR HOST ON ANY WEBSITE OR SERVER, SELL, REDISTRIBUTE, OR SUBLICENSE THE APPLE SOFTWARE, APPLE CERTIFICATES, OR ANY SERVICES, IN WHOLE OR IN PART, OR TO ENABLE OTHERS TO DO SO. YOU MAY NOT USE THE APPLE SOFTWARE, APPLE CERTIFICATES, OR ANY SERVICES PROVIDED HEREUNDER FOR ANY PURPOSE NOT EXPRESSLY PERMITTED BY THIS AGREEMENT, INCLUDING ANY APPLICABLE ATTACHMENTS AND SCHEDULES.

I only rely on Apple Software, Apple Certificates and Services to build and distribute Windmill as an individual developer. Windmill as a platform does not rely on any of these to provide its services.

YOU AGREE NOT TO INSTALL, USE OR RUN THE APPLE SDKS ON ANY NON-APPLE-BRANDED COMPUTER, AND NOT TO INSTALL, USE OR RUN IOS, WATCHOS, TVOS, IPADOS, MACOS AND PROVISIONING PROFILES ON OR IN CONNECTION WITH DEVICES OTHER THAN APPLE-BRANDED PRODUCTS, OR TO ENABLE OTHERS TO DO SO.

Windmill only runs on Apple platforms. That is, the Mac and the iPhone. By using Windmill, a developer can sign and distribute an ad-hoc build by making use of their Provisioning Profile, as managed and made available by Xcode command line tools to install their app on devices they have explicitly registered.

YOU MAY NOT AND YOU AGREE NOT TO, OR TO ENABLE OTHERS TO, COPY (EXCEPT AS EXPRESSLY PERMITTED UNDER THIS AGREEMENT), DECOMPILE, REVERSE ENGINEER, DISASSEMBLE, ATTEMPT TO DERIVE THE SOURCE CODE OF, MODIFY, DECRYPT, OR CREATE DERIVATIVE WORKS OF THE APPLE SOFTWARE, APPLE CERTIFICATES OR ANY SERVICES PROVIDED BY THE APPLE SOFTWARE OR OTHERWISE PROVIDED HEREUNDER, OR ANY PART THEREOF (EXCEPT AS AND ONLY TO THE EXTENT ANY FOREGOING RESTRICTION IS PROHIBITED BY APPLICABLE LAW OR TO THE EXTENT AS MAY BE PERMITTED BY LICENSING TERMS GOVERNING USE OF OPEN-SOURCED COMPONENTS OR SAMPLE CODE INCLUDED WITH THE APPLE SOFTWARE).

Windmill, through the use of Xcode command line tools, provides the ability to compile, test, archive, export and distribute an application on behalf of the developer. Windmill relies on iOS to download and install an ad-hoc build.

YOU AGREE NOT TO EXPLOIT ANY APPLE SOFTWARE, APPLE CERTIFICATES, OR SERVICES PROVIDED HEREUNDER IN ANY UNAUTHORIZED WAY WHATSOEVER, INCLUDING BUT NOT LIMITED TO, BY TRESPASS OR BURDENING NETWORK CAPACITY, OR BY HARVESTING OR MISUSING DATA PROVIDED BY SUCH APPLE SOFTWARE, APPLE CERTIFICATES, OR SERVICES. ANY ATTEMPT TO DO SO IS A VIOLATION OF THE RIGHTS OF APPLE AND ITS LICENSORS OF THE APPLE SOFTWARE OR SERVICES.

Windmill does not make use of anything that isn't made public by Apple and/or what is permitted as such.

IF YOU BREACH ANY OF THE FOREGOING RESTRICTIONS, YOU MAY BE SUBJECT TO PROSECUTION AND DAMAGES. ALL LICENSES NOT EXPRESSLY GRANTED IN THIS AGREEMENT ARE RESERVED AND NO OTHER LICENSES, IMMUNITY OR RIGHTS, EXPRESS OR IMPLIED ARE GRANTED BY APPLE, BY IMPLICATION, ESTOPPEL, OR OTHERWISE. THIS AGREEMENT DOES NOT GRANT YOU ANY RIGHTS TO USE ANY TRADEMARKS, LOGOS OR SERVICE MARKS BELONGING TO APPLE, INCLUDING BUT NOT LIMITED TO THE IPHONE OR IPOD WORD MARKS. IF YOU MAKE REFERENCE TO ANY APPLE PRODUCTS OR TECHNOLOGY OR USE APPLE'S TRADEMARKS, YOU AGREE TO COMPLY WITH THE PUBLISHED GUIDELINES AT HTTP://WWW.APPLE.COM/LEGAL/TRADEMARK/GUIDELINESFOR3RDPARTIES.HTML, AS THEY MAY BE MODIFIED BY APPLE FROM TIME TO TIME.

It it not immediately clear if that is indeed applicable and/or what those cases are. I am willing to comply with the published guidelines. I would very much appreciate further information on this.

Guideline 2.5.2 - Performance - Software Requirements

You state that:

YOUR APP ACCESSES AND DISPLAYS THE CONTENTS OF THE OS FILESYSTEM OUTSIDE OF ITS DESIGNATED SANDBOX.

FOR SECURITY PURPOSES, APPS ARE CONTAINED WITHIN A SANDBOX ENVIRONMENT. INTERACTION WITH OTHER APPS, OR THE REST OF THE OS, CAN ONLY BE DONE THROUGH THE USE OF PUBLIC INTERFACES, SUCH AS UIIMAGEPICKERCONTROLLER, AVAILABLE IN THE IOS SDK. DIRECTLY ACCESSING FILES AND FOLDERS OUTSIDE OF YOUR SANDBOX IS NOT PERMITTED EXCEPT THROUGH THESE PUBLIC INTERFACES.

Additionally, the guideline states that:

APPS SHOULD BE SELF-CONTAINED IN THEIR BUNDLES, AND MAY NOT READ OR WRITE DATA OUTSIDE THE DESIGNATED CONTAINER AREA, NOR MAY THEY DOWNLOAD, INSTALL, OR EXECUTE CODE WHICH INTRODUCES OR CHANGES FEATURES OR FUNCTIONALITY OF THE APP, INCLUDING OTHER APPS.

Windmill makes use of a public interface, more specifically **itms-services://?action=download-manifest&url=**, available in iOS that enables the download and install of an ad-hoc distribution.

Windmill does not directly access files and folders outside of its sandbox. It is iOS that downloads and installs the ad-hoc distribution. Windmill merely hands off that responsibility, to draw a comparison to the `UIImagePickerController`.

The ad-hoc distribution is what Apple has provided developers with, at least for the last 5 years that I can recall, in order to test a release build. In this time, developers should be well informed what it is meant to be used for. It is also publicly available within Xcode as well as its command line tools.

> *Important: Only use Ad Hoc distribution to test your Release build if there is a good reason you cannot use TestFlight. -* ***Technical Note TN2431****,* ***App Testing Guide****,* ***Test your Release Build****.* https://developer.apple.com/library/archive/technotes/tn2431/_index.html#//apple_ref/doc/uid/DTS40017497-CH1-APP_TESTING_PROCEDURE-1__TEST_YOUR_RELEASE_BUILD

There is a good reason not to use TestFlight. That is, to test a release build when an app is still under development and not intended for public distribution. Windmill is built precisely for this very purpose. To help developers test the release build of an app during development.

Windmill also makes reasonable assumptions and puts considerable effort to communicate that it is indeed meant to be used by developers during the development of an app and that it works within the predefined set of boundaries as set by Apple.
As an example, within the Windmill iPhone app, at the time of purchase:

> *Whether it is the end of a sprint, demo day or keeping your team in the loop, the latest build is available to install on your registered* devices using Windmill on the iPhone.*
> ** The device needs to be registered in your Apple Developer Account.*"

As well as in the screen where a user can find a list of apps to install that have been distributed by Windmill on the Mac.

> *A build is only allowed to install and run on registered devices that a developer has explicitly registered in their Apple Developer Account.*

In the Windmill on the iPhone Help Book, Under Getting Started -> Register a device

> *It is recommended that the devices you register are personal to you or directly managed by the organisation you are working for.*

It is also communicated on the website through carefully chosen language which not only frames the use of Windmill for development purposes but also by explicitly calling out against security practices that are not used, endorsed or recommended.

> *Windmill leans on Xcode and its command line tools to sign, export and distribute your application without going anywhere near your private key and distribution certificate or asking you to share them. They are yours to keep. They belong in your keychain. - Windmill on the Mac, Security. https://windmill.io/mac/security/*

> *Windmill installs your applications only on devices you have chosen to register under your Apple Account. Your Apple Account Credentials are not for sharing. - Windmill on the Mac, Security. https://windmill.io/mac/security/*

In Windmill on the Mac by providing visibility on what Signing Certificate was used to distribute an app in the Side Panel.

In the Windmill on the Mac Help Book, under Security -> Revoke a Build which states that:

> ** You can explicitly revoke the distribution certificate for an application in which case the build will become invalid.*

Guideline 5.2.5 - Legal - Intellectual Property

You state that:

YOUR APP IS TOO SIMILAR TO TESTFLIGHT, WHICH CREATES A MISLEADING ASSOCIATION WITH APPLE PRODUCTS.
WE ENCOURAGE YOU TO REVIEW YOUR APP CONCEPT AND EVALUATE WHETHER YOU CAN INCORPORATE DIFFERENT CONTENT AND FEATURES TO BRING IT INTO COMPLIANCE WITH THE APP STORE REVIEW GUIDELINES.

Additionally, the guideline states that:

APPLE PRODUCTS: DON'T CREATE AN APP THAT APPEARS CONFUSINGLY SIMILAR TO AN EXISTING APPLE PRODUCT, INTERFACE (E.G. FINDER), APP (SUCH AS THE APP STORE, ITUNES STORE, OR MESSAGES) OR ADVERTISING THEME.

Windmill on the iPhone is different to TestFlight. It is designed to be used by a developer so that a limited number of users can download and install an ad-hoc distribution of their app. Windmill as a platform, is meant to be used in-house during development. At that phase, chances are an app is incomplete, a preview, not ready for a production like environment.

Even though Windmill does not explicitly state that it is not affiliated or endorsed by Apple, it neither makes any claim that it is. Having said that, I will gladly make that explicit if need be.

It is both fair and reasonable for Apple to expect Windmill on the iPhone to "incorporate different content and features". This first version of the iPhone app is intended to provide significant value to developers in the use of Windmill as well as enabling me to start charging for the service.

Windmill on the iPhone is but one piece in the Windmill puzzle and comes hand in hand with Windmill on the Mac.

Final thoughts

Since 2014, when I first thought of Windmill, things haven't changed much as far as I have been observing. Back then, I utilised Jenkins, Command Line Tools (https://qnoid.com/2019/03/13/iOS-automation-the-current-state-of-affairs.html#main) and ingenuity to build a continuous delivery pipeline (https://www.youtube.com/watch?v=1Vbn7vd7EWY). Jenkins, as of WWDC last year, still had 52% of the marketshare (https://www.macstadium.com/ios-devops-survey).

Windmill on the Mac was first released in February 2018 and is now at version 3.x.x bringing a lot of value to iOS developers (https://windmill.io/changelog/). It monitors their codebase to automate building and testing of their iOS app. It integrates seamlessly with Xcode, so that developers can reliably install their app on a device and upload to iTunes Connect to prepare for a public beta using TestFlight or a release through the App Store.

When the iPhone was first announced, it was introduced without the App Store alongside. The only option for developers was to make use of web technologies. Eventually, the App Store was unveiled and it changed the face of the iPhone and what arrived soon after, the iPad.

With iOS 12 and the upcoming iPadOS, Apple yet again redefines what is made possible within iOS. A Files app that "lets you access and manage your files", including support for external drives, "and, yes, even a USB drive." (https://www.apple.com/ipados/ipados-preview/).

When you compare that to the Mac and macOS, it has really been a tale of two cities.

Even with the introduction of the Mac App Store, the Notarisation service, increased security with the introduction of the T2 chip etc. the Mac and the iPhone are governed by two very distinct sets of rules.

By extension what is allowed on their respective App Stores is also very much a reflection of that. Case in point, the App Store on iOS does not even have a dedicated "Developer Tools" section.

Bare Bones' BBEdit and Panic's Transmit that were once prominent Mac apps, didn't have a place on the Mac App Store until they did.

Windmill is the culmination of the experience I have accumulated as a developer over the past 15 or so years. On top of that, it took months of research and development on the Mac, on the server and on the iPhone, paying great attention to the user experience as well as security and privacy that would not and cannot be made possible without deeply integrating with Apple's tools, platforms and services.

Still, that is not enough. It needs Apple's blessing.

To quote Steve,
> *Our motivation is simple – we want to provide the most advanced and innovative platform to our developers, and we want them to stand directly on the shoulders of this platform and create the best apps the world has ever seen. -* ***Steve Jobs, April, 2010. Thoughts on Flash****.* *https://www.apple.com/hotnews/thoughts-on-flash/*

My hope and wish is to also have Windmill on the Mac App Store.

Windmill belongs on the App Store.