



# Windows® Marketplace for Mobile Outline of Anti-Piracy Model

Date: September 2009

## Contents

Introduction.....	2
The Anti-Piracy Model in Windows Marketplace .....	3
Standard Protection Level .....	4
Advanced Protection Level .....	6
How to Enable Your Application by Using the Advanced Anti-Piracy Layer .....	9
Timeline.....	10
Conclusion .....	11

## Introduction

Anti-piracy protections are important for application developers who want to ensure that their investments and intellectual property (IP) are protected from those seeking to obtain illegitimate copies of their software. There are few things more frustrating to developers than to find their latest creation hacked and available for free online.

Microsoft understands the importance of IP and has a long history of developing protection strategies for its own software and services, as well as third-party developers.

Windows® Marketplace for Mobile is no exception. In this increasingly mobile world, the development of mobile applications and services is imperative for many categories and service areas. Protecting this investment is key to ensuring the long term viability of any development venture, large or small.

Microsoft incorporated feedback from its community of developers in designing a Windows Marketplace anti-piracy strategy that offers a standard level of protection, requires minimal additional work for the developers, and provides enormous flexibility to the developer for tackling illegitimate copies of software.

This white paper introduces in some detail the components of the anti-piracy strategy offered by Windows Marketplace and explains how developers can incorporate it into their applications.

## The Anti-Piracy Model in Windows Marketplace

Windows Marketplace offers a layered approach to anti-piracy that lets developers choose the level of protection best suited to their needs. It is important for developers to understand the costs and benefits of each protection level in order to make a suitable decision. Table 1 summarizes the layered approach.

Protection level	Standard	Advanced
Target applications	Majority of applications	Applications that require extra protection
Changes to source code	No changes required	Some changes required
Developer participation	Included	Optional
Protection offered	Delivery of applications to authorized Windows Live ID users only	Additional key-based validation at run-time

**Table 1. Description of protection levels in Windows Marketplace**

There are two levels of protection available on Windows Marketplace:

- A Standard level which applies to every application and offers a basic level of protection.
- An Advanced level which offers a more robust solution of anti-piracy protection, but requires inclusion of some additional code in the application.

## Standard Protection Level

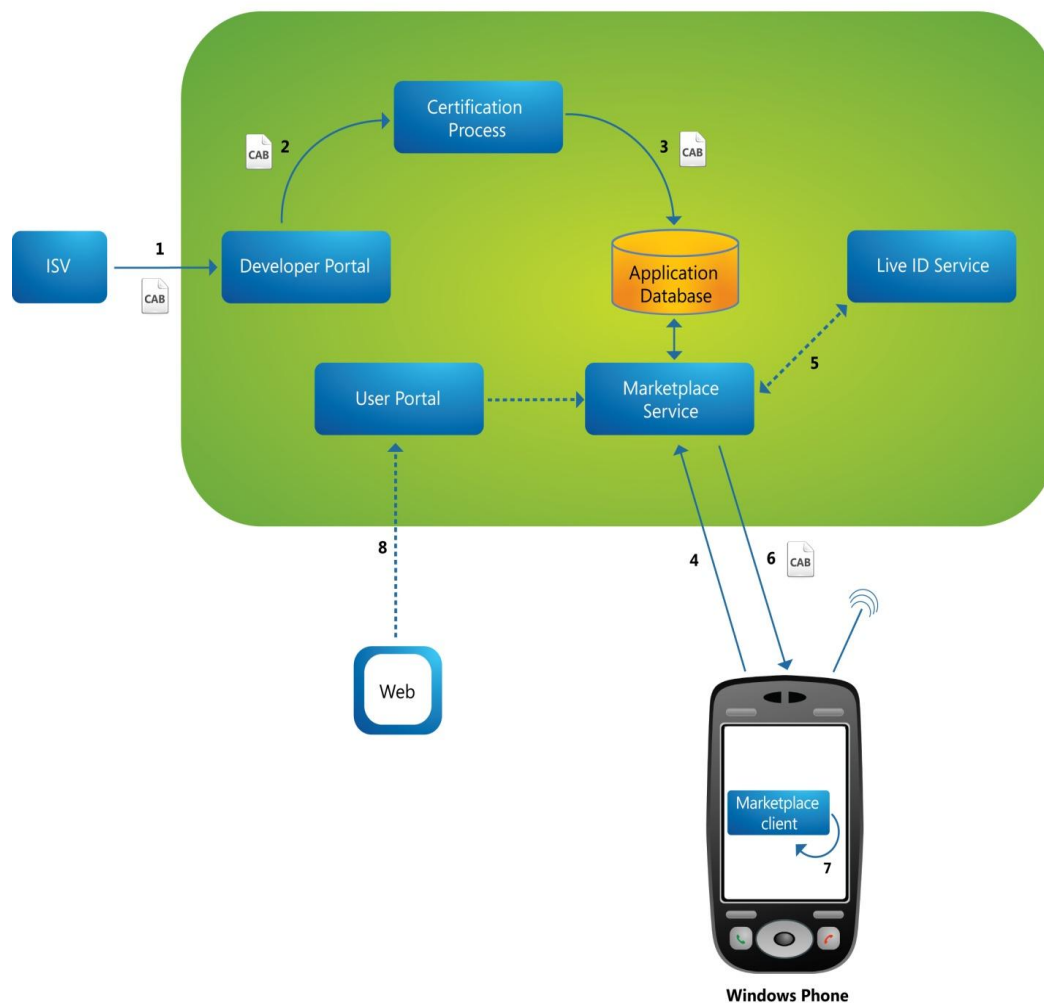
The Standard protection level helps ensure that applications purchased in Windows Marketplace are delivered exclusively to the authorized user based on Windows Live™ ID authorization. No installation (.cab) files remain on the destination phone, which helps prevent the average user from copying the application to an unlicensed phone.

The process by which an application is posted to Windows Marketplace and delivered can be seen in Figure 1. This is detailed as follows:

1. The developer signs in to the Windows Marketplace developer portal (<http://developer.windowsphone.com>) and uploads a .cab file containing the application. The communication is securely established through HTTPS so that no one can intercept the .cab file while in transit.
2. The application goes through the Windows Marketplace certification process to ensure that the application complies with all technical, policy, content, and market validation guidelines.
3. The application .cab file is stored in a secure database hosted by Microsoft, using the same level of security applied to the storage of personal information for hundreds of millions of user accounts for services such as Windows Live™, Bing™, Hotmail™, Xbox Live™, Zune™, and others. Then, the application is ready for purchase and download.
4. A user launches the Windows Marketplace client on a Windows® phone, which establishes a secure communication via HTTPS with the Windows Marketplace service in the Microsoft cloud.
5. The user signs in using a Windows Live ID, which is validated against the Live ID service. All transactions are logged against and can be traced back to this Live ID.
6. The user purchases an application from the catalog and requests the application transfer to the phone. The application .cab file gets transferred through the same HTTPS connection to avoid outside interception during transmission.

7. The application is immediately installed onto the phone and the .cab file is deleted. Therefore, the user cannot access or copy the installation .cab file in any way.
8. If purchase takes place on the Web, there are no files transferred to the PC. The user is instructed to start the Windows Marketplace client on his or her phone, and then follow steps 6 and 7 to download and install the purchased application. The .cab files are never transferred to the phone through the PC, as may be the case for other Web-based application stores.

**Windows Marketplace**



**Figure 1. Visual description of the Standard protection level**

This approach helps ensure that the typical user cannot illegally transfer a copy of the application easily. The vast majority of Windows Marketplace users do not have an interest in illegally sharing applications, and so Microsoft expects the majority of applications on Windows Marketplace to use this level of protection. The resulting level of protection is similar to the one obtained by selling copies of the software via a company Web site, or through a Web-based application store.

Although not a simple task, there are a relatively small number of more advanced hackers with the skill set to potentially copy the application. For developers who want to further enhance the protection of their IP against piracy, an Advanced level of protection is offered.

---

## Advanced Protection Level

The Advanced protection level offers an additional layer of protection, based on the delivery of license keys that validate legitimacy of the bits at run-time. This measure is applied above all the other measures offered by the Standard protection level.

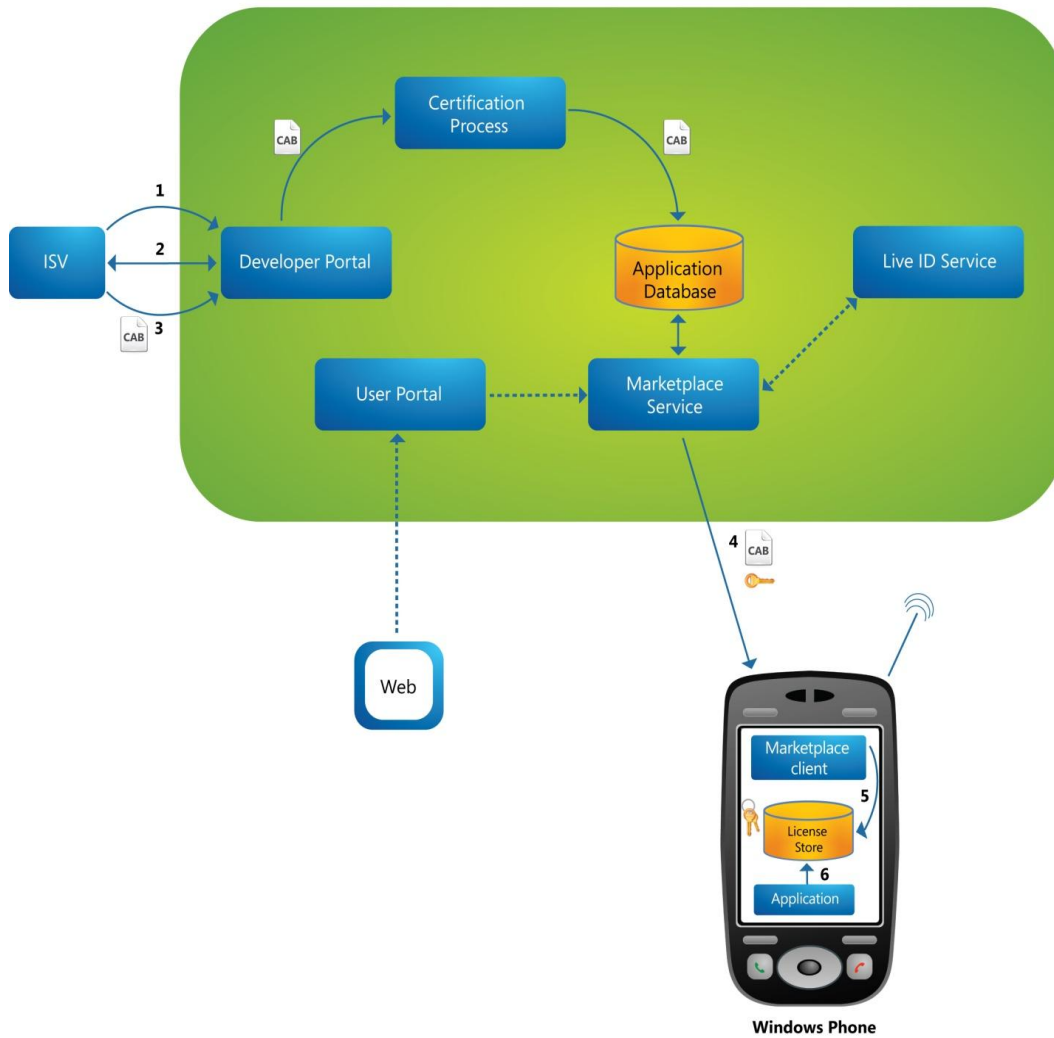
Developers are given a few lines of code to be placed in the application. (The application has to be recompiled before it can be submitted.) This code locally checks for the existence of a device-bound license key provided by the Windows Marketplace service at the time of purchase and detects authorized copies.

The additional steps needed to add the Advanced level of protection correspond to Figure 2. This is detailed as follows:

1. The developer initiates an application submission in the Windows Marketplace developer portal and enters the meta-data associated with the application.
2. The portal provides several lines of code that the developer needs to add directly into the application (in most cases, at the top of the application).

3. The developer recompiles the application containing the validation code, and uploads the resulting .cab file to the developer portal. The application goes through the Windows Marketplace certification process to ensure it complies with all technical, policy, content, and market validation guidelines before it is made available to customers.
4. When a user purchases the application from the Windows Marketplace client, the service sends a license key that is uniquely tied to the application and the device.
5. The application is installed onto the phone and the license key is recorded in a local license store.
6. When the application runs, the validation code provided to the developer verifies available license keys in the license store and validates them against the application and device. The result of this validation indicates whether the application is legitimate or not. If the application does not pass validation when launched, the application does not run.

### Windows Marketplace



**Figure 2. Visual description of the Advanced protection level.**

The developer chooses if and how often the application should be verified (on every run, on first run only, and so on). This approach provides the greatest flexibility to the developer on deciding how to tackle unauthorized copies of the application and how to take appropriate action upon a negative validation result (show an error message, provide a limited version of the application, ask the user to purchase a legitimate copy, and so on).

It is also important to note that the validation takes place locally on the phone without the need for an outside connection to the Windows Marketplace service. This imposes no constraints as to when the validation takes place, and does not require the user to have an open data connection in order to use the application. This is important when users need to run an application outside the cellular data coverage area (for example, playing a game during a flight).

---

## How to Enable Your Application by Using the Advanced Anti-Piracy Layer

As discussed, no action is required to enjoy the benefits of the Standard layer. These instructions describe how to enable your application by using the Advanced anti-piracy layer:

1. Sign in to your account on the Windows Marketplace developer portal (<http://developer.windowsphone.com>), or create an account if you do not have one.
2. Click on "Add Product" then "Add Application" in order to start the application submission process.
3. Click the "Add advanced application protection" button on the page. A pop-up window appears, which displays the validation code that needs to be added to your application.
4. Copy and paste the validation code into your application. You should place the code at the point where you would like to authenticate the application, usually the beginning.
5. Edit the validation code to include the actions you require upon a failed authentication (For example, show an error message, exit the application, and so on).
6. Recompile the application.
7. Upload the newly compiled .cab file, which now includes the anti-piracy code.
8. Click on "Save and Quit."
9. Ensure you have uploaded all the required metadata and click on "Submit for certification."

Once your application is approved and published to the catalog, users can purchase your application and install it on their phones. All license keys are automatically generated by the system and installed onto the licensed phones. If a hacker with advanced capabilities copies your application files onto a new phone, your code detects this and acts accordingly. Also, even if the user manages to copy the license key from the license store onto the new phone, the application does not work since the license key is tied to both the application and the device-unique identifiers where Windows Marketplace has installed the application.

## Timeline

The above anti-piracy strategy is to be rolled out to Windows Marketplace application developers according to the following timeline:

- Windows phone launch—launch of Windows Marketplace service providing Standard protection.
- By the end of 2009—developer portal starts providing protection code to developers.
- By the end of 2009—Windows Marketplace client starts storing and validating license keys.

Table 2 details the timeline for those developers who want to participate in Windows Marketplace for Mobile but are concerned about piracy risks. Applications can be submitted to Windows Marketplace containing the Standard level of protection in October 2009, and after the rollout of the Advanced protection level in December 2009, the free update mechanism can be used to adapt applications to make full use of the Advanced anti-piracy solution.

Phase	10/6/09 ~ 12/09 Standard	12/09 -> Advanced
Description	Anti-piracy documentation released	Full app validation implemented
Action	Submit current applications to Windows Marketplace	Add validation code to apps and submit free update

**Table 2. Timeline for implementing anti-piracy measures.**

## Conclusion

Microsoft’s anti-piracy strategy for Windows Marketplace offers a customized solution for application developers to help protect their creations from unauthorized copying and distribution. The main benefits of this solution are:

- Standard anti-piracy measures are provided for all applications, without requiring any code change, which addresses development needs in the majority of cases.
- Full control is given to the application developer on how to respond to unauthorized copies of their application.
- There is no need to implement costly and complex licensing systems or back-end live services to validate the application copies.
- Full end-to-end solution, integrated with the Windows Marketplace developer portal, is offered.
- Off-line application validation, which does not require a live data connection on the device, is provided.

Windows Marketplace for Mobile provides a tremendous opportunity for application developers to sell their software to millions of Windows phone users around the world. Please follow the guidelines in this white paper to ensure that you understand the benefits and costs associated with the different anti-piracy solutions available to you, and choose the appropriate one based on your needs.

As always, we look forward to your application submissions.

© 2009 Microsoft Corporation. All rights reserved. Microsoft, Windows Mobile, Windows Live, and Windows and other product names are or may be registered trademarks and/or trademarks in the U.S. and/or other countries. The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this document. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this document.

MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

For additional Microsoft Trademark information, please visit:  
<http://www.microsoft.com/about/legal/trademarks/default.aspx>