Introduction to the Windows Biometric Framework (WBF)

Guidelines for IHV, ISVs and OEMs

August 23, 2010

Abstract

This white paper provides information about the Windows Biometric Framework (WBF) for the Windows® 7 operating system. It provides an introduction to WBF, together with guidelines that independent hardware vendors (IHVs), independent software vendors (ISVs,) and original equipment manufacturers (OEMs) should follow when they integrate fingerprint biometric devices with the Windows 7 platform.

WBF is discussed in detail, including the following:

- An overview of WBF and its components.
- An overview of the biometric user experience that WBF provides.
- Guidelines for developing WBF-compatible biometric device drivers and components.
- Guidelines for the distribution of WBF-compatible biometric device drivers and components.

This information applies to the Windows 7 operating system.

References and resources discussed here are listed at the end of this paper.

The current version of this paper is maintained on the Web at:
www.microsoft.com/whdc/device/input/smartcard/WBFIntro.mspx

***Disclaimer**: This document is provided "as-is". Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it.*

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

© 2010 Microsoft Corporation. All rights reserved.

Document History

Date	Change
August 23, 2010	Corrected hyperlinks in "Resources" section.
March 17, 2009	Corrected typo in Figure 1: changed "Foundation" to "Framework".
December 15, 2008	First publication

Contents

Introduction 4

Terminology and Definitions 4

Windows Biometric Framework Overview 5

WBF Core Platform 5

- Windows Biometric Driver Interface (WBDI) 6
- Windows Biometric Service (WBS) 7
- WBF API 9

WBF User Experience 9

- Discovery Points 9
- Application Start Points 10
- Management Capabilities 10
- Supported Scenarios 10

WBF Management 10

- Biometric Device Control Panel 10
- Biometric System Management 11

WBF Driver and Component Distribution 11

Summary 12

© 2010 Microsoft Corporation. All rights reserved.

Resources 12

© 2010 Microsoft Corporation. All rights reserved.

Introduction

Biometrics is an increasingly popular technology that provides convenient access to systems, services, and resources. Biometrics relies on measuring an unchanging physical characteristic of a person to uniquely identify that person. Fingerprints are one of the most frequently used biometric characteristics, with millions of fingerprint biometric devices that are embedded in personal computers and peripherals.

In Windows® 7, the Windows Biometric Framework (WBF) provides support for fingerprint biometric devices through a new set of components. These components improve the quality, reliability, and consistency of the user experience for customers who have fingerprint biometric devices.

This white paper gives a high-level overview of WBF and its components, including the WBF core architecture, user experience and manageability features, and supported distribution mechanisms for the WBF components that third parties develop. This white paper is intended for original equipment manufacturers (OEMs), independent hardware vendors (IHVs), and independent software vendors (ISVs) who want to support fingerprint biometric devices in Windows 7.

Terminology and Definitions

biometric unit (BU)

A common representation of a biometric device that is provided by the Windows Biometric Service (WBS).

BU adapter

A plug-in component of a BU that provides software support for hardware functionality that is not supported by a biometric device.

Biometric Service Provider (BSP)

A kernel-mode service provider that interfaces with WBS.

Fingerprint Management Application (FMA)

A third-party application that extends WBF by providing management capabilities and enables additional scenarios, including enrollment experiences, Web single-sign-on, and management of proprietary attributes of a fingerprint biometric device.

Windows Biometric Driver Interface (WBDI)

An interface that biometric device drivers use to plug into WBF.

Windows Biometric Framework (WBF)

A framework that is introduced in Windows 7 that provides a consistent user experience and management interface for all fingerprint biometric devices.

Windows Biometric Service (WBS)

The service that manages all fingerprint biometric devices through WBDI-compliant device drivers.

© 2010 Microsoft Corporation. All rights reserved.

Windows Biometric Framework Overview

In Windows versions earlier than Windows 7, every fingerprint biometric device vendor was required to provide its own technology stack, including drivers, software development kits (SDKs), and applications. The result was a range of proprietary solutions that lacked a consistent user experience and a common management platform.

The absence of a common programming interface led to incompatibility between application software and fingerprint biometric devices, as well as inconsistency in the quality and reliability of drivers and packages. Also, the differing nature of application stacks and driver models for biometrics devices complicated servicing and maintaining these proprietary solutions.

In Windows 7, the Windows operating system provides native support for fingerprint biometric devices through WBF. This framework provides support for biometric technologies, including the following:

- An improvement in the quality and reliability of fingerprint biometric drivers and management applications.
- A more consistent user experience.
- A common platform and a set of interfaces for software developers.
- Improved manageability and serviceability of fingerprint biometric devices in Windows.

Note Windows 7 and WBF support only fingerprint biometric devices.

The WBF components that deliver these goals include the following:

- Core platform components, including a driver interface definition, pluggable expansion platform, and a client API.
- User experience components that provide a consistent user experience in the Windows operating system. This component includes support for the core scenarios of logon and User Account Control (UAC).
- Management components that let users and administrators configure biometrics and biometrics devices. This component supports biometric configuration either locally on a single computer system or globally for a domain through Group Policy.
- WBF component distribution that lets biometric drivers and components be distributed through online distribution channels.

The rest of this paper provides a brief overview of each WBF component.

WBF Core Platform

The WBF core platform consists of the following components:

- Windows Biometric Driver Interface (WBDI)
- Windows Biometric Service (WBS)
- WBF API

© 2010 Microsoft Corporation. All rights reserved.

Figure 1 shows these components and their relationship to each other.

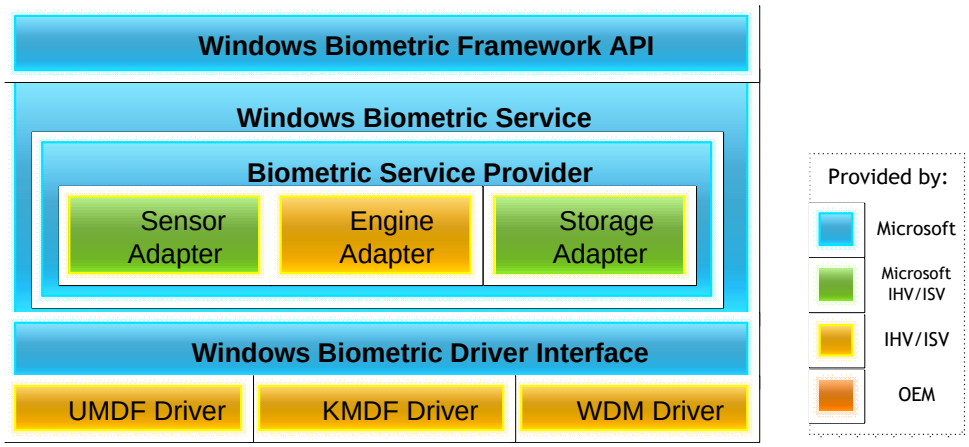

Figure 1. Windows Biometric Framework Core Architecture

Windows Biometric Driver Interface (WBDI)

WBDI provides a common interface that biometric drivers use to expose the device through WBS. WBS exposes all Plug and Play devices that implement WBDI. This lets any user-mode application access biometric device through the WBF API.

WBDI drivers can be implemented by using any driver technology that the Windows operating system supports, including the following:

- User-mode driver framework (UMDF).
- Kernel-mode driver framework (KMDF).
- Windows Driver Model (WDM).

  Note To improve overall driver quality and system stability, we recommend that driver writers use the UMDF driver model whenever possible.

For more information about these driver technologies, see the links in "Resources" at the end of this paper.

WBDI drivers must do the following:

- Support the WBDI driver interface GUID.
- Support all mandatory WBDI I/O controls (IOCTLs), including handling multiple IOCTL requests and supporting IOCTL cancellation.

Driver developers should review the documentation and sample WBDI driver code in the Windows 7 Windows Driver Kit (WDK). Developers should also use the following WDK tools to verify their drivers:

- PREfast for Drivers
- WDF Verifier
- Application Verifier
- WBF tools, including the WBDI driver test harness (WBDIDriverTest.exe)

© 2010 Microsoft Corporation. All rights reserved.

For more information about these tools, see the documentation in the Windows 7 WDK.

Windows Biometric Service (WBS)

WBS is a component that manages fingerprint biometric devices through WBDI drivers that are installed on the system. WBS supports the WBF API, which provides managed access to these devices through client applications.

WBS protects user confidentiality by maintaining a strict separation between client applications and biometric data. Specifically, WBS acts as an I/O proxy between the application and the biometric device, and performs all capture, processing, and storage operations on the device.

The WBS never gives unprivileged client applications direct access to biometric samples or templates. Instead, WBS associates a handle, such as a security identifier (SID) or a GUID, with the biometric data. Applications use this handle to indirectly access the biometric data or template.

Within WBS, fingerprint biometric devices are managed by a component that is named the Biometric Service Provider (BSP). BSP implements all policies or behaviors that are specific to the device's biometric category.

Note In Windows 7, devices that sample fingerprints are the only supported biometric category, and Microsoft supplies the BSP for this type of device.

Another feature of WBS is that it normalizes biometric hardware behavior. Therefore, all fingerprint biometric devices behave more or less the same to client applications, regardless of the device's physical capabilities.

WBS does this by creating a virtual software component, which is known as a biometric unit (BU), for each biometric device. BU is an idealized version of the device that can perform capture, processing, and storage functions.

If the physical device lacks on-board processing or storage capabilities, this functionality is supplied by plug-in components that are called BU adapters. Regardless of the capabilities of the biometric device, its associated BU and BU adapters always provide a common behavioral interface to BSP.

WBS manages all BUs by grouping them together in pools. WBS maintains the following three pools:

- System:
  The system pool contains shareable BUs that provide easy access to Windows-based authentication services. The system pool is used for logon, UAC, and any other client that wants to associate Windows account SIDs with a user's biometric template. Each BSP on the system has exactly one system pool.
- Private:
  The private group contains one or more BUs that is allocated for exclusive use by an application program. The private pool makes it possible to support applications that perform authentication that is not Windows based. There can be as many private pools on the system as there are BUs.

© 2010 Microsoft Corporation. All rights reserved.

- Unassigned:
  The unassigned group contains BUs that do not belong to either the system or private pool. Unlike the other BU pools, the unassigned pool could be empty.

A BU is made up of the following three pluggable BU adapter components:

- Sensor adapter:
  The sensor adapter performs all sample-capture operations.
- Engine adapter:
  The engine adapter performs all processing including data normalization, feature extraction, and biometric template generation. Also, the engine adapter matches biometric data to templates during enrollment, identification, and verification operations.
- Storage adapter:
  The storage adapter stores, manages, and retrieves all templates.

Figure 2 shows the relationship between the BSP, BUs, and the various BU adapters.

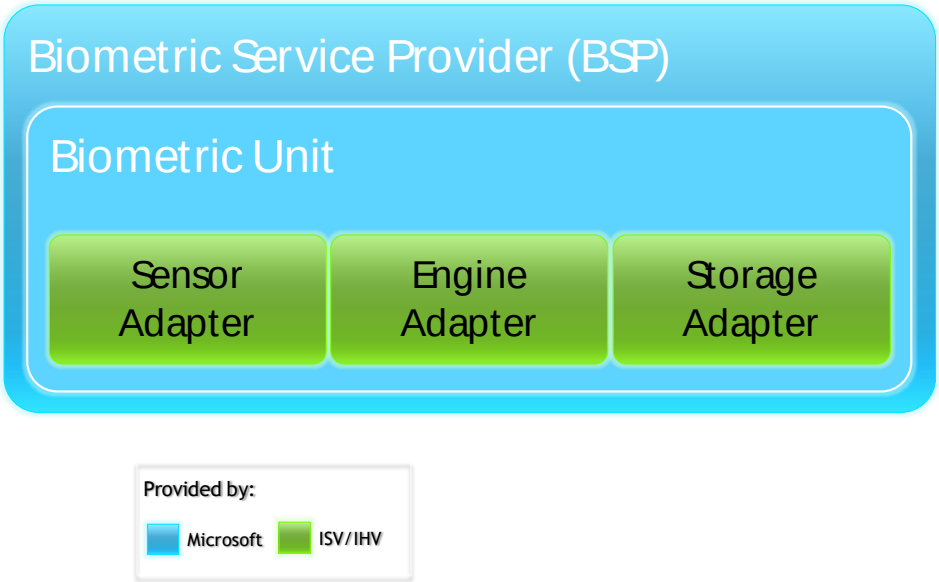

Figure 2. Biometric Service Providers and Biometric Units

In Windows 7, BU adapter components are provided in the following way:

- For fingerprint biometric devices that do not have on-chip storage or matching capabilities, Microsoft provides inbox sensor and storage adapters components. An IHV or ISV must supply the engine adapter component for these devices.
- For fingerprint biometric devices that do support on-chip matching and storage, the IHV or ISV must supply all BU adapter components.

Driver developers who want to write BU adapter components for WBF should see the documentation and sample WBDI driver code in the Windows 7 WDK.

© 2010 Microsoft Corporation. All rights reserved.

WBF API

WBS exposes fingerprint biometric devices through the WBF API. This API lets applications enroll, identify, and verify user identities. In addition, the WBF API provides:

- Query of the biometric device capabilities.
- Biometric device location.
- Session management.
- Event monitors.
- Biometric template storage.

The WBF API also provides an extension API that can be used to access proprietary device-specific capabilities.

Developers who want to write applications that use the WBF API should see the documentation in the Windows 7 SDK.

WBF User Experience

In Windows 7, WBF provides a user experience for fingerprint biometric devices that is consistent with the user experience throughout the Windows operating system itself.

WBF provides a common set of the following:

- Discovery points.
- Application start points.
- Management capabilities.
- Supported end-to-end scenarios.

Discovery Points

Windows 7 provides several ways in which the user can find the biometrics capabilities that are embedded in Windows. These include the following:

- Search:
  The user can search for biometric capabilities by clicking **Start**, and then typing “biometrics”, “fingerprint”, or other related phrases to start the Biometric Devices Control Panel.
- Biometric Devices Control Panel:
  The user can find the Biometric Devices Control Panel under the **Hardware and Sound** category or by selecting the **All** view in Control Panel. For more information about the Biometric Device Control Panel, see Biometric Devices Control Panel.
- Device Manager
  The user can find all WBDI devices in Device Manager under the **Biometrics** device category.

© 2010 Microsoft Corporation. All rights reserved.

Application Start Points

IHVs, ISVs, and OEMs can integrate their own fingerprint management applications (FMAs) with the Biometric Devices Control Panel through the **Manage your fingerprint data** link. When users click this link, the third-party application is started. This link is also available from the User Accounts Control Panel.

This lets third parties provide a customized and branded FMA that is started from a standard point within the Biometric Devices Control Panel. The FMA may be a simple enrollment application or a complex suite of applications and management capabilities.

Windows 7 will not include an inbox FMA or enrollment experience. Only the IHV, ISV, or OEM can provide an enrollment experience with a FMA that uses the WBF API.

Management Capabilities

Through WBF Biometric Devices Control Panel, the user experience for managing fingerprint biometric devices is compatible with managing other devices on the system. In addition, the Biometric Devices Control Panel gives users a way to start proprietary applications for managing device-specific settings.

For more information about the Biometric Devices Control Panel, see Biometric Devices Control Panel.

Supported Scenarios

In Windows 7, two primary end-to-end scenarios are supported:

- Logon:
  Users can log on to a local machine or to a domain by using a fingerprint.
- UAC:
  A user who has administrative credentials can elevate applications through UAC by using a fingerprint.

WBF Management

In Windows 7, the biometric attributes of individual devices or the entire system can be managed through either of the following:

- Biometric Device Control Panel
- Biometrics System Management

Biometric Device Control Panel

The Windows Biometric Device Control Panel gives users basic capabilities for biometrics management on the local system. Specifically, users can:

- Delete personally identifiable information such as fingerprint templates and password data.
- Access Device Manager for troubleshooting fingerprint biometric devices.

© 2010 Microsoft Corporation. All rights reserved.

- Manage biometric settings, including the following:
  - Enable/disable biometrics.
  - Enable/disable local logon.
  - Enable/disable domain logon.

To change biometric settings, the user must have administrative credentials.

Biometric System Management

In addition to the local management of biometrics capabilities through the Biometric Device Control Panel, a user can control the following aspects of biometrics in a domain by using Group Policy:

- Enable/disable biometrics.
- Enable/disable local logon.
- Enable/disable domain logon.
- Set time-out for Fast User Switching (FUS).

  Note FUS works only if an IHV or ISV implements it.

Together with these settings, system administrators can use the following Group Policy capabilities to manage fingerprint biometric devices in their environments:

- Prevent biometric device installation.
- Force the removal of drivers for specific fingerprint biometric devices.
- Disable WBS.

System administrators can also perform specific tasks that are related to biometrics by using logon scripts.

WBF Driver and Component Distribution

In Windows 7, the following distribution channels are available for third-party WBF components, drivers, and FMAs:

- Distribution by OEMs:
  OEMs will be able to include the WBF components, drivers, and FMAs with Windows 7 machines in the factory.
- Windows Update:
  IHVs are strongly encouraged to distribute the WBF components, drivers, and FMAs through Windows Update.
- Windows Solution Center:
  IHVs can distribute the WBF components, drivers, and FMAs through their own Internet sites and have the Windows Solution Center point to these sites.

We recommend that vendors distribute their WBF components, drivers, and FMAs through Windows Update. This improves the serviceability and maintainability of these components in Windows 7.

© 2010 Microsoft Corporation. All rights reserved.

Summary

WBF improves the quality, reliability, and manageability of biometric device drivers and related components.

In addition, WBF provides software developers with a common development platform and set of APIs, and gives users a more consistent biometric experience across the operating system. Although it is still possible to use legacy approaches, WBF is the preferred and supported way to access fingerprint biometric devices in Windows 7.

Resources

Application Verifier

http://msdn.microsoft.com/en-us/library/ff541329(VS.85).aspx

Kernel-Mode Driver Framework

http://msdn.microsoft.com/en-us/library/aa973499.aspx

PRE*f*ast for Drivers

http://msdn.microsoft.com/en-us/library/ff550543(VS.85).aspx

User-Mode Driver Framework

http://msdn.microsoft.com/en-us/library/aa973500.aspx

WDF Verifier Control Application

http://msdn.microsoft.com/en-us/library/ff556129(VS.85).aspx

Windows Driver Kit

http://msdn.microsoft.com/en-us/library/ff557573(VS.85).aspx

Windows Driver Model

http://msdn.microsoft.com/en-us/library/ff565698(VS.85).aspx

Windows Quality Online Services (Winqual)

https://winqual.microsoft.com/

For the latest information about the Microsoft Windows family, see the Windows Web site at http://www.microsoft.com/windows.

August 23, 2010
© 2010 Microsoft Corporation. All rights reserved.