

.NET Bio Solution for Windows 7

Installation and Administrator Guide

All information herein is either public information or is the property of and owned solely by Gemalto NV. and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto's information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

© Copyright 2009-12 Gemalto N.V. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto N.V. and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

GEMALTO, B.P. 100, 13881 GEMENOS CEDEX, FRANCE.

Tel: +33 (0)4.42.36.50.00 Fax: +33 (0)4.42.36.50.90

Printed in France.

Document Reference: D1203575G (formerly DOC118338F)

January 18, 2012

Preface		vi
	Who Should Read This Book	vi
	Conventions	vii
	Contact .NET Bio Support	vii
	Biometric Reader/Sensor Support	vii
Chapter 1	Overview	1
	Why Choose the Gemalto .NET Bio Solution?	1
	Why Biometrics?	1
	Why Biometrics Match-on-Card (MoC)?	2
	Why Gemalto .NET Bio?	2
	Key Features and Benefits	2
	PKI and non-PKI Versions	3
	Changing from One Version to the Other	3
	User Verification Modes	4
	Secure Desktop Scenarios	4
	Biometric Support in the Control Panel	4
	Smart Card Enabled Applications	5
Chapter 2	Installation	6
	System Requirements	6
	Software and Middleware Requirements	6
	Hardware Requirements	6
	Installation	7
	Installation Recommendations	7
	Installing the Fingerprint Sensor	7
	Installing the Smart Card Reader	7
	Installing the Gemalto .NET Biometric Solution	8
	Uninstallation	8
	User Certificate Enrollment	8
Chapter 3	Gemalto .NET Bio Components	9
	On-Card Components	10
	Off-Card Components	10
Chapter 4	Using the Gemalto .NET Bio Solution	13
	Getting Started	14
	User Verification Modes	14
	PKI Version	14
	Non-PKI Version	14
	Biometrics Admin and User Authentication	14
	admin	15
	pin	15
	Changing the Fingerprint Sensor	16
	Enrolling Fingerprints for Biometric Authentication	17
	Tips for Using a Fingerprint Sensor	18

Enrolling Fingerprints	18
Deleting Fingerprints	22
Changing the UVM	24
Logon Scenarios	25
PKI Version	25
Non-PKI Version	30
Changing the PIN	31
Changing Fingerprints	31
Unlocking the PIN	32
Unlocking Fingerprint Authentication	33
Unlocking Fingerprint Authentication via the PIN	33
Locking/Unlocking the System	33
Using Gemalto NET Bio verification in the User Desktop	33
SSL Authentication to Secure Web Sites	35
Encrypting a File or folder using EFS	35
BitLocker To Go	35
Terminology	38
Abbreviations	38

List of Figures

Figure 1 - Gemalto .NET Bio On-Card and Off-Card Components	9
Figure 2 - The Smart Card CP User Interface	11
Figure 3 - The Smart Card Verification CP User Interface	11
Figure 4 - Standard MS Biometrics CP User Interface	11
Figure 5 - FMA GUI	12
Figure 6 - Biometric Admin Authentication Window	15
Figure 7 - Biometric User Authentication Window	15
Figure 8 - Use Biometric Devices with Windows (After Enrollment)	16
Figure 9 - Fingerprint Management Application (After FP Enrollment)	17
Figure 10 - The Settings Window	17
Figure 11 - Use Biometric Devices with Windows (Before Enrollment)	18
Figure 12 - Change Biometric Settings Window	19
Figure 13 - Fingerprint Management Application (Before FP Enrollment)	19
Figure 14 - Manage Fingerprints Window (No FPs Enrolled)	20
Figure 15 - Swipe Prompt	20
Figure 16 - Second Swipe Prompt	21
Figure 17 - Manage Fingerprints Window (One FP Enrolled)	21
Figure 18 - Fingerprint Management Application (After FP Enrollment)	22
Figure 19 - Use Biometric Devices with Windows (After Enrollment)	22
Figure 20 - Manage FP - Delete Fingerprint Prompt	23
Figure 21 - Delete Fingerprint Template Warning	24
Figure 22 - Figure 10: Change User Verification Mode	24
Figure 23 - .NET Bio Smart Card Logon Icon	25
Figure 24 - Credentials Selector	26
Figure 25 - <Ctrl> <Alt> Prompt	26
Figure 26 - Smart Card Logon (PIN Mode)	27
Figure 27 - Smart Card Logon (FP Only)	27
Figure 28 - Unsuccessful Authentication (Red)	28
Figure 29 - Smart Card Logon (PIN or FP Mode)	29
Figure 30 - .NET Bio Smart Card Logon (Non-PKI)	30
Figure 31 - Credentials Selector (Non-PKI Version)	30
Figure 32 - Smart Card Unblock Window	32
Figure 33 - MS Outlook - Sign Email	34
Figure 34 - Unsuccessful SSL Authentication	35
Figure 35 - External Drive Encrypted using BitLocker To Go	37

List of Tables

Table 1 - PKI Vs. Non-PKI	3
---------------------------------	---

Gemalto .NET Bio is an innovative software solution that works with Gemalto .NET smart cards to seamlessly integrate biometrics technology into Windows 7®.

Organizations deploy Gemalto smart cards and tokens among their employees to be used for strong user authentication to their networks as well as for data encryption and digital signature services.

Gemalto .NET smart cards are:

- integrated into the Windows® Smart Card Framework (WSF). This means that they not only work with Windows 7 (and XP and Vista) but any Microsoft and third-party applications that also support WSF architecture;
- compliant with Windows Biometric Framework (WBF), providing a more friendly user experience and interoperability among biometric applications and readers.
- easily supported in Windows 7 and Windows Server 2008 R2. The first time you connect a .NET smart card, Windows Update automatically downloads the required minidrivers. This is known as “plug and play”. This enables the devices to work seamlessly with Microsoft Terminal Services, Active Directory®, Active Directory Federation Services and Windows smart card login.
- the first commercial smart card to implement a streamlined version of the .NET Framework.

Building upon this smart card technology, the Gemalto .NET Bio Solution enables the use of fingerprint match-on-card (MoC) user authentication as an alternative or complement to smart card PIN verification.

With Gemalto .NET Bio, companies can implement a secure two- or three-factor authentication system that is convenient for users, easy to deploy and manage, and fully compatible with the smart card security components in Windows 7. The solution is also compatible with the vast majority of fingerprint sensors available in the market.

Gemalto's .NET Bio Solution is also available for Windows XP and Windows Vista operating systems. This manual explains how to install and use .NET Bio for the Windows 7 version.

Who Should Read This Book

This book is intended for IT administrators who will be deploying the Gemalto .NET Bio Solution across their organization.

It is assumed that the reader of this document has:

- an understanding of the Windows operating systems in general, and ideally someone who has experience with Windows 7.
- An understanding of the Windows Smart Card Framework.
- an understanding of Gemalto .NET smart cards, smart card readers and fingerprint sensors.
- administrative privileges for the PC on which the Gemalto .NET Bio Solution will be used.

Conventions

The following conventions are used in this document:

Numeric values

By default, numeric values are expressed in decimal notation.

- Binary numbers are followed by the 'b' character. For example, the decimal value 13 is expressed in binary as **1101b**.
- Hexadecimal numbers are followed by the 'h' character. For example, the decimal value 13 is expressed in hexadecimal as **0Dh**.

RFU values

The value 00h is assigned to each RFU (Reserved for Future Use) byte.

Contact .NET Bio Support

If you do not find the information you need in this manual, or if you find errors, please report them to Gemalto .NET Bio Support: dotnetbiosupport@gemalto.com

Biometric Reader/Sensor Support

If you experience problems with any fingerprint readers or sensors, make sure that you have loaded the latest drivers from the appropriate web manufacturer's web site.

Note: When downloading Upek or AuthenTec drivers, take care to install the "WinBio" drivers as the sites also have "non WinBio" drivers.

The *.NET Solution for Windows Release Notes* gives a list of the fingerprint readers and sensors supported by Gemalto for the .NET Bio Solution, and a list of the web sites from where you can find the latest drivers.

Overview

Traditionally, smart cards are protected by a PIN intended to verify that the holder of the device is its legitimate owner. Gemalto .NET Bio implements fingerprint verification on the smart card to provide four alternative card holder verification methods:

- PIN only
- Fingerprint only
- PIN or fingerprint
- PIN and fingerprint for the highest level of security.

The following components are required for using the Gemalto .NET Bio Solution:

- smart card reader
- fingerprint sensor for biometric authentication
- Gemalto .NET Bio client software,
- a Gemalto .NET smart card device with the BioManager Assembly loaded on it.

The fingerprint sensor and the smart card reader may be integrated with the client system, or they can be external devices connected via USB.

Why Choose the Gemalto .NET Bio Solution?

The Gemalto .NET Bio Solution integrates the best in authentication technologies - smart cards and fingerprint recognition - to deliver unmatched security and flexibility for Windows 7.

Why Biometrics?

- **Identity:** Biometrics allow user authentication based on a unique physical personal characteristic. From a user's perspective, there is a stronger perception of personal representation compared to user names and passwords or PINs.
- **Security:** Depending on the implementation, biometrics (something you are) can enhance the security of a solution when combined with other authentication factors, such as a smart card or token (something you have) and/or a password or PIN (something you know).
- **Convenience:** Compared to passwords, biometrics cannot be forgotten. Users don't have to keep track of them. They are always available and always with the user.

Why Biometrics Match-on-Card (MoC)?

- **Security:** By design, smart cards are highly secure and tamper-proof. Because of this, storage and verification of biometric credentials on a smart card are safer than on a non-secure device or network. Combining smart cards with biometrics technology produces a highly secure, three-factor authentication solution.
- **Convenience:** Biometrics match-on-card (MoC) technology delivers the ultimate in portability. Users can log on throughout the corporate network using their smart card or token and biometric credentials.
- **Privacy:** The match is performed on the card. Biometric credentials never leave the card, so users can be assured of their privacy.
- **Compliance:** Some countries have security regulations that prevent the storage of biometric information within any database. Biometrics MoC technology ensures compliance by storing information on the card.

Why Gemalto .NET Bio?

Gemalto .NET Bio offers an unmatched level of integration with the Windows 7 operating system, delivering significant benefits for both corporations and end users.

The Gemalto .NET Bio Solution builds on top of the latest release of the Windows Smart Card Framework (WSF) and the Windows Biometrics Framework (WBF). This provides consistency with the Windows 7 environment, while requiring a minimum amount of software to be loaded on the Windows 7 client - less than 4 MB. By complying with the WSF and WBF architectures, the Gemalto .NET Bio Solution supports not only the Windows 7 operating system, but all Microsoft® applications that provide smart card support, as well as third-party applications that support the Windows Smart Card Framework.

Key Features and Benefits

Gemalto .NET Bio replaces passwords with strong two- or three-factor authentication for secure logon, remote access, encryption and digital signature services. It is compatible with approximately 90% of the fingerprint sensors on the market, and supports enrollment of up to 10 fingerprints.

Some of the key benefits include:

- **Portability:** Biometric credentials and digital certificates are stored on the user's smart card; thus, these users can freely and securely roam, log on and use any computer on the corporate network.
- **Convenience:** By replacing a password or PIN with their fingerprint, users no longer need to remember - or type in - long, frequently changing passwords.
- **Security:** For corporations committed to the deployment of a smart card infrastructure, Gemalto .NET Bio enhances security by enabling the use of biometrics as a third factor of authentication. For corporations interested in the deployment of biometric technology for user identification, Gemalto .NET Bio provides secure storage and verification of the biometric credentials inside the .NET smart card.
- **Cost Savings:** The majority of Help Desk calls are related to forgotten passwords or user PINs. Gemalto .NET Bio delivers a secure alternative that greatly reduces the need for password resets, helping to lower Help Desk support costs.
- **Ease of Use:** With a straightforward interface for end users, deployment and management of biometric solutions are streamlined for Windows 7.

PKI and non-PKI Versions

There are two versions of the .NET Bio Solution for Windows 7. The PKI version supports all the features described in this document. The “non-PKI” version provides a limited set of features compared to the full “PKI” version.

Note: Throughout this document, the “non-PKI” version is assumed to use .NET Bio cards that do not have a PKI certificate enrolled.

When you enroll a fingerprint in the Non-PKI version, the computer associates that FP with the user currently logged on. In this way it “knows” which users can logon using Fingerprint authentication.

Smart card logon using fingerprints is done by the card comparing the swiped fingerprint with those stored in the card and the PC checking that the FP is valid for the username (instead of comparing a traditional password with the username).

The FP authentication is managed by the WBF in Windows 7 but the FPs are stored only on the card.

The following table shows the main differences between the two versions:

Table 1 - PKI Vs. Non-PKI

Feature	PKI Version	Non-PKI version
User Verification Modes	4 (see “User Verification Modes”). Possibility to change from one UVM to another.	No possibility to change UVM (UVM1 by default)
Smart Card Logon	Supported	Supported
Computer Unlock	Supported	Supported
Change PIN or FP	Supported	Supported
Unblock PIN or FP	Supported	Unblock PIN supported Unblock FP is not applicable as there is no “tries counter” for FP
Digital signatures	Supported	Not Supported
File encryption with EFS and BitLocker	Supported	Not Supported
Secure web site authentication (SSL)	Supported	Not Supported
VPN authentication with Direct Access	Supported	Not Supported

Changing from One Version to the Other

The version installed by default is the PKI version. To change to the non-PKI version, create a registry file with the following content.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Gemalto\Biometry]
```

```
“PKIDisabled”= dword:00000001
```

Run the .reg file to set the PKIDisabled bit to 1.

Similarly if you want to return to the PKI version, create and run a similar .reg file, but with the content:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Gemalto\Biometry]
```

```
“PKIDisabled”= dword:00000000
```

User Verification Modes

The PKI version of the Gemalto .NET Bio Solution provides a choice of four user verification modes (UVMs), as shown below:

- **PIN only** — This is the default mechanism for user authentication, as defined by the Windows Smart Card Framework
- **Fingerprint only** — Fingerprints are matched against a template previously stored on the smart card. This replaces the use of a smart card PIN. The mechanism is defined by the Windows Biometrics Framework.
- **PIN or fingerprint** — For the ultimate in convenience, users can choose to authenticate with their smart card PIN or fingerprint(s).
- **PIN and fingerprint** — For maximum security, users must present their fingerprint and enter their smart card PIN. Both are matched against values stored in the smart card. This provides highly secure three-factor authentication – the card, the PIN and the fingerprint(s).

Secure Desktop Scenarios

The Gemalto .NET Bio Solution is seamlessly integrated with the Secure Desktop in Windows 7. The Secure Desktop is the user interface that appears whenever the computer is locked (at logon or when the user has locked the desktop) or when the user presses the **Ctrl+Alt+Del** keys. The Secure Desktop works like a secure sandbox - with limited connectivity and access to resources. It is intended to be a safe environment where secure operations are performed, such as management of user credentials.

The Secure Desktop provides biometric support for classic credential management scenarios, such as:

- Smart Card Logon
- Computer Unlock
- Change PIN
- Unblock PIN or Fingerprint

Caution: The unblock PIN and fingerprint scenarios are available only if the unblock card option is enabled as described in “Appendix A - Enabling Unblock Card in Windows 7”.

Biometric Support in the Control Panel

In Windows 7, it is the standard Control Panel that manages biometric support for smart cards. The functions for biometric management can be found in **Control Panel > Hardware and Sound > Biometric Devices**. From here you can:

- Manage fingerprint enrollment
- Change the User Verification Mode (PKI version only)
- Change biometric settings, i.e. the fingerprint sensors connected to the PC.

Smart Card Enabled Applications

In addition to the Secure Desktop usage scenarios, **the PKI version** of Gemalto .NET Bio Solution may be used with other smart card-enabled applications, including:

- Microsoft Office (Word, Excel and PowerPoint) for digital signature of documents
- Microsoft Outlook for digital signatures and encryption of email
- Microsoft Internet Explorer
- Encrypting File System (EFS)
- Other Microsoft applications supporting Windows Smart Card Framework (e.g. Direct Access, BitLocker)
- Third-party applications on Windows 7 supporting Smart Card Framework

Installation

System Requirements

Software and Middleware Requirements

The use of the Gemalto .NET Bio Solution for Windows 7 requires the following:

- Windows 7 (32 and 64-bit platforms) or Windows Server 2008 R2 (64-bit platforms).
- .NET 3.5 framework (this is already integrated in Windows 7 and Windows Server 2008 R2)
- WBF (this is already integrated in Windows 7 and Windows Server 2008 R2)
- .NET biometric middleware — this is installed automatically as part of the Gemalto .NET Biometric Solution. The .NET Biometric Solution is one of the components of Gemalto's .NET solution. For details on how to install it, please consult the section "Installing the .NET Additional Components for Windows 7" in the *.NET Smart Cards in a Windows Environment Administration and User Guide*.
- The Biometric settings must be configured to authorize biometric authentication over a network. This is described in "Enrolling Fingerprints" on page 18.

Note: For information about the Windows Service Packs supported by .NET Bio, please refer to the *.NET Bio Solution for Windows 7 Release Notes*.

Hardware Requirements

The use of the .NET Bio Solution requires the following devices:

- A smart card reader for the Gemalto .NET smart card
- A fingerprint sensor for biometric authentication

Compatible Smart Card Readers

The smart card reader may be integrated with the PC (or laptop) or it can be an external device that is connected via USB. The solution is compatible with any certified Chip Card Interface Device (CCID), USB class or embedded smart card reader.

Compatible Fingerprint Sensors

Both swipe and flatbed fingerprint sensors can be used with the .NET Bio Solution. The fingerprint sensor may be integrated into any laptop, or it can be an external device that is connected via USB. For a list of the fingerprint readers and sensors supported by this version of .NET Bio, please refer to the *Release Notes*.

Note: Gemalto and its partner Precise Biometrics are continuously integrating support for additional fingerprint readers/sensors. Support for new fingerprint readers will be provided through maintenance releases of the Gemalto .NET Bio Solution.

Installation

Installation Recommendations

Do not connect the smart card reader, the fingerprint sensor or insert the smart card before the end of the installation.

Make sure you have the administrative rights to your PC in order to install the prototype. You can log on as the domain administrator or right-click the files to run them as the administrator.

Make sure you perform the installations in the following order:

- 1 The fingerprint sensor
- 2 The smart card reader
- 3 The .NET smart card solution.

Installing the Fingerprint Sensor

First install the biometric driver for your fingerprint sensor. Install the 32-bit or 64-bit version corresponding to the version of Windows 7 installed on the PC.

- If you use a UPEK fingerprint sensor, download the UPEK WBDI driver package at: <http://www.upek.com/support/downloads/drivers/windows7.asp>

This driver is also available in the Microsoft Update catalog at: <http://catalog.update.microsoft.com/v7/site/Search.aspx?q=upek>

- If you use an AuthenTec fingerprint sensor, the driver is downloaded automatically for you from Windows Update. If you think that the driver has not been downloaded for you, then download it from the Windows Update web site at: <http://catalog.update.microsoft.com/v7/site/Search.aspx?q=authentic>

Depending on the package you downloaded, launch and follow the instructions of your installer.

Caution: Take care to install the drivers only. Some sites include logon tools with drivers. Another logon tool in parallel with Gemalto's .NET solution could lead to unpredictable results (for example .NET Bio may be configured for PIN only but the other login tool may allow fingerprints).

Installing the Smart Card Reader

Gemalto recommends that you use the Gemalto GemPC Twin smart card reader as it does not have any particular installation requirements. When you plug in the reader, Windows Update downloads and installs the required driver.

For other smart card readers, check the support web site of the card reader vendor for instructions on how to install it for Windows 7.

Installing the Gemalto .NET Biometric Solution

As stated earlier, this is one of the components of Gemalto's .NET solution. For details on how to install it, please consult the section "Installing the .NET Additional Components for Windows 7" in the *.NET Smart Cards in a Windows Environment Administration and User Guide*.

Uninstallation

Normally you should not need to uninstall .NET Bio as this happens automatically when you install a new version. However, if you need to uninstall it manually, the procedure is described in the section "Installing the .NET Additional Components for Windows 7" in the *.NET Smart Cards in a Windows Environment Administration and User Guide*.

User Certificate Enrollment

Before you can enroll your fingerprints and use them in a PKI context, you must enroll a user certificate in your smart card.

According to your enrollment means, ask your administrator for instructions. Check the certificate is correctly enrolled by performing a standard smart card logon, that is, non-biometric.

Note: Remember that for the "non-PKI" version described in this document, we assume that the card does not have any PKI certificates enrolled.

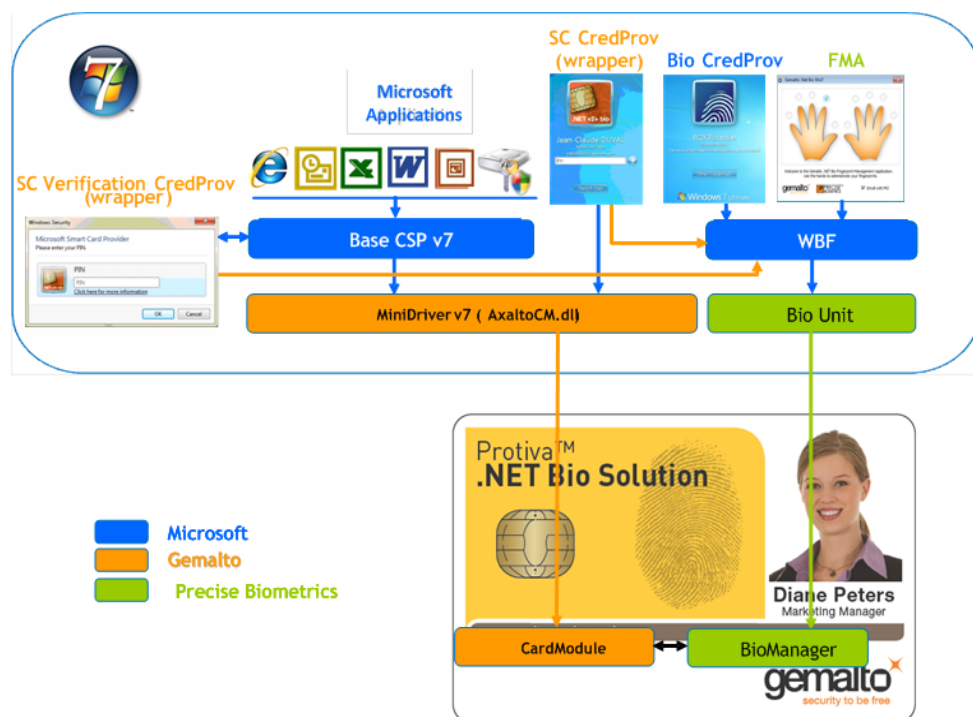
Gemalto .NET Bio Components

The architecture of the Gemalto .NET Bio Solution relies on the Microsoft Base Cryptographic Service Provider v7 (Base CSP v7) component that is native in Windows 7. The .NET Bio Solution consists of both on-card and off-card components, as shown in “Figure 1”. These include two applications that reside on the Gemalto .NET smart card itself, and some libraries that must be installed in the “Windows System” directory on the client computer. Components installed on the client PC enable the user’s biometric credentials to seamlessly interact with the Microsoft operating system and applications.

The “Windows System” directory depends on whether the version of Windows 7 is 32-bit or 64-bit:

- For 32-bit OS - All components are installed in C:\Windows\system32
- For 64-bit OS - The 64-bit components are installed in C:\Windows\system32 and the 32-bit components are installed in C:\Windows\SysWOW64.

Figure 1 - Gemalto .NET Bio On-Card and Off-Card Components



On-Card Components

Gemalto .NET Bio includes the following on-card components:

- .NET operating system and OTP - OATH assembly similar to standard Gemalto .NET smart cards
- **Card Module Assembly (Gemalto)** – This is the “oncard” module for the Minidriver. It is compliant with the Microsoft Minidriver v7 Specification and paired with the off-card minidriver library. It also implements a Bio API for communication with the other on-card application, the BioManager Server
- **BioManager Assembly (Precise)** – This is the “oncard” module for the Biometrics Unit (Engine and storage adaptors). It stores the biometric credentials and implements the matching algorithm used to verify fingerprints.

Off-Card Components

Gemalto .NET Bio requires the following client libraries to be installed in the “Windows System” directory (see previous page). Some implement a User Interface as shown in Figures 2 – 5.

- **Base CSP v7:** Minidriver based and integrated in Windows 7. This provides the standard Windows 7 Credentials GUI for user authentication.
- **WBF (Microsoft).** Based on Biometrics Unit and integrated in Windows 7, this provides the APIS for Biometrics management (enrolling and storage of FPs and Match-on-Card)
- **Minidriver (Gemalto).** This is compliant with the Microsoft Minidriver V7 specification and provides access to the .NET Bio Card Module Assembly. This is installed automatically by the windows 7 “plug-and-play” feature when you insert a .NET Bio card in the reader.
- **Biometrics Unit (Precise).** This provides the following:
 - Sensors adapter (Authentec, UPEK)
 - Engine adapter (Precise specific)
 - Storage adapter (.NET card)

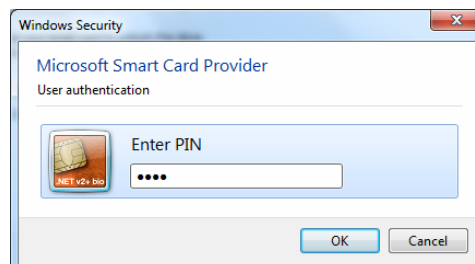
This needs to be installed by the Administrator (see “Installing the Fingerprint Sensor” on page 7). All three components are included in the WBDI driver package.

- **Smart card credential provider (CP).** This provides:
 - PKI management (done by the MS CP)
 - Minidriver access (done by the MS CP)
 - WBF access for Match-on-Card (customized by Gemalto - wrapper)
 It is the CP that manages the smart card logon. Its GUI is shown in “Figure 2”.
- **Fingerprint Management Application (Precise).** This manages:
 - Fingerprint enrollment and deletion
 - The User Verification Mode (UVM)
 - Biometric Settings (changing the fingerprint sensor if more than one is connected to the PC)

Figure 2 - The Smart Card CP User Interface

- **Smart card verification CP.** This provides:
 - PKI management (done by the MS CP)
 - Minidriver access (done by the MS CP)
 - WBF access for Match-on-Card (customized by Gemalto - wrapper)

It is this CP that manages authentication for applications such as SSL authentication (accessing secure web sites) and signing e-mails. Its GUI is shown in “Figure 3” (UVM1 example).

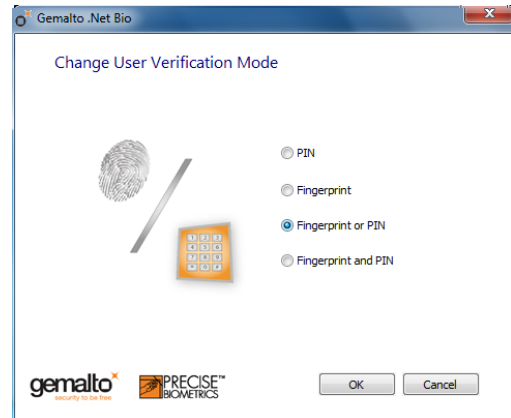
Figure 3 - The Smart Card Verification CP User Interface

- **Standard MS Biometrics CP**
 - WBF access
 - Login/Password CP (non-PKI)

Figure 4 - Standard MS Biometrics CP User Interface

- **Fingerprint Management Application (FMA)** – done by Gemalto's partner Precise Biometrics. This is started from the Windows 7 control panel and is WBF based.

Figure 5 - FMA GUI



Using the Gemalto .NET Bio Solution

This chapter describes how to perform some of the more common tasks with the Gemalto .NET Bio Solution for Windows 7 such as:

- Smart card logon
 - using one of four User Verification Modes (UVMs) in the PKI version
 - using fingerprints in the “non-PKI” version
- Fingerprint enrollment
- Fingerprint deletion
- Changing UVM (PKI version only)
- Changing a fingerprint template
- Unblocking the PIN
- Unblocking fingerprints authentication (PKI version only)
- Lock/Unlock the system
 - using one of four User Verification Modes (UVMs) in the PKI version
 - using fingerprints in the “non-PKI” version
- SSL authentication (PKI version only)
- Office document or email signature (PKI version only).

Warning: You can connect ONE .NET card reader at any one time. This includes hardware devices such as Gemalto's Smart Enterprise Guardian and Smart Guardian that contain a .NET card.

The following assumptions are used for the purpose of describing the selected use cases in this chapter:

- The person working on the PC is the end-user, and the use cases are described accordingly
- The user is working on a PC with Windows 7 installed
- .NET Bio software has been installed on the user's PC
- The biometrics settings have been enabled on the PC
- The smart card reader and fingerprint sensor are both connected and working properly
- A .NET Bio smart card is present in the card reader

- One logon/signature X.509 certificate has been already enrolled on the card
- No fingerprints have been enrolled on the card

Getting Started

The first time you use your .NET Bio smart card, it behaves like an ordinary smart card. Before you enroll any fingerprints, you can log on to your computer as normal without a smart card by typing a username and password or use the .NET Bio card to perform a smart card logon in PIN only mode (PKI version only).

The first step is to enroll at least one Fingerprint as described in “Enrolling Fingerprints for Biometric Authentication” on page 17, but Gemalto recommends that you read the following sections first.

User Verification Modes

PKI Version

In the PKI version of .NET Bio, there are four UVMs as described in the “Overview”:

- UVM1: PIN only - This is the default value for the non-PKI version
- UVM2: Fingerprint (FP) only
- UVM3: PIN or FP
- UVM4: PIN and FP

The **Set UVM** parameter sets the UVM of the card. It is this value that is modified when the user changes the UVM. It is given an initial value when the card is personalized, but this can be modified by the Administrator after personalization and before issuance to the end-user if the Administrator has a post-issuance tool, such as DAS.

The mode in which the card is operating is called the **Active UVM**. Normally this is the Set UVM value, but it is possible to differ under certain scenarios, for example if the user blocks the Biometric Credential

Note: Even if the Set UVM of a card is UVM2, UVM3 or UVM4, the Active UVM is UVM1 (PIN only) until the first FP is enrolled. When the FP is enrolled, the Active UVM will match the Set UVM.

If the Set UVM is UVM1 (PIN only), enrolling Biometric credentials has no immediate effect: The Active and the Set UVM both remain as UVM1. An explicit change in the Set UVM is required for the card to start using the biometric credentials enrolled.

Details on how to change the UVM are given in “Changing the UVM” on page 24.

Non-PKI Version

In the non-PKI version, the default value is UVM1 and it cannot be changed.

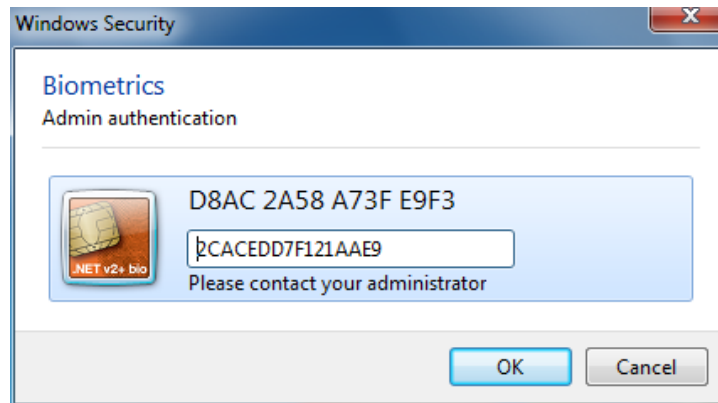
Biometrics Admin and User Authentication

In both versions of .NET Bio, when performing operations with the Fingerprint Management Application, you must authenticate yourself. This authentication differs according to whether the **Access Condition to FMA** configurable parameter is set to *admin* or *pin* (for an ordinary end-user). The authentication is described below from the end-user’s point of view.

admin

If set to *admin*, your rights are limited and you need intervention from the Administrator for sensitive operations such as **Unblock User Fingerprints** and **Change User Verification Mode**. In these cases, the **Biometrics Admin authentication** window appears as shown in “Figure 6” and you need intervention from the Administrator.

Figure 6 - Biometric Admin Authentication Window



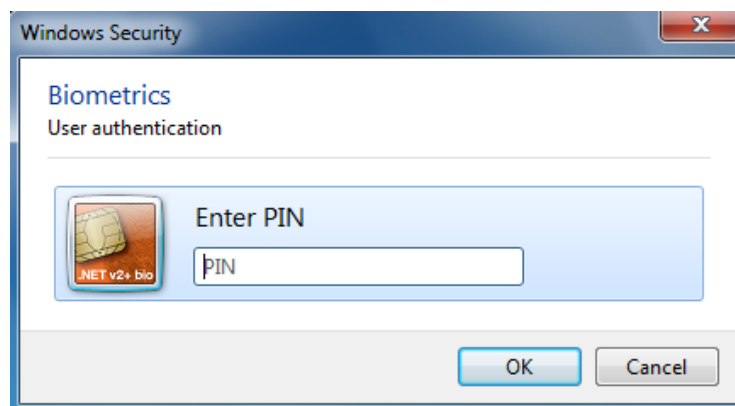
- 1 The window displays a 16-digit challenge, generated by the card. This is the hexadecimal number beginning “D8AC...” in “Figure 6” (the white box is empty when the window first appears).
- 2 Contact your system administrator, and provide this 16-digit challenge. The administrator will in return provide you with a 16-digit response.
- 3 Enter this 16-digit response in the white box (beginning 2CAC....) in the example in “Figure 6”.
- 4 Click **OK** to complete the authentication.

pin

If set to *pin*, you can perform most operations just by authenticating yourself according to the Active UVM. However the **Unblock User Fingerprints** operation does still require a response to the 16-digit challenge from the Administrator.

The **Biometrics User authentication** window appears as shown in “Figure 7”.

Figure 7 - Biometric User Authentication Window



You must authenticate yourself according to the Active UVM. In the example in “Figure 7”, this is PIN only but it could equally be any of the other UVMs.

Note: In the non-PKI version, the Active UVM is always UVM1 (PIN only). This means that you must always enter the PIN in order to access the FMA. This PIN entry is necessary because the FMA has features that update the card, such as enrolling and deleting fingerprints.

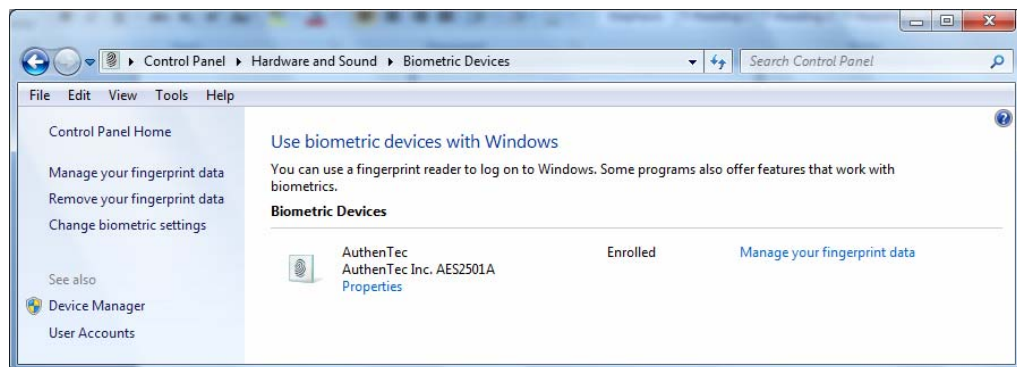
Changing the Fingerprint Sensor

If you have more than one FP sensor connected to the computer, and want to change from one to another, you will need to change the Biometric Settings.

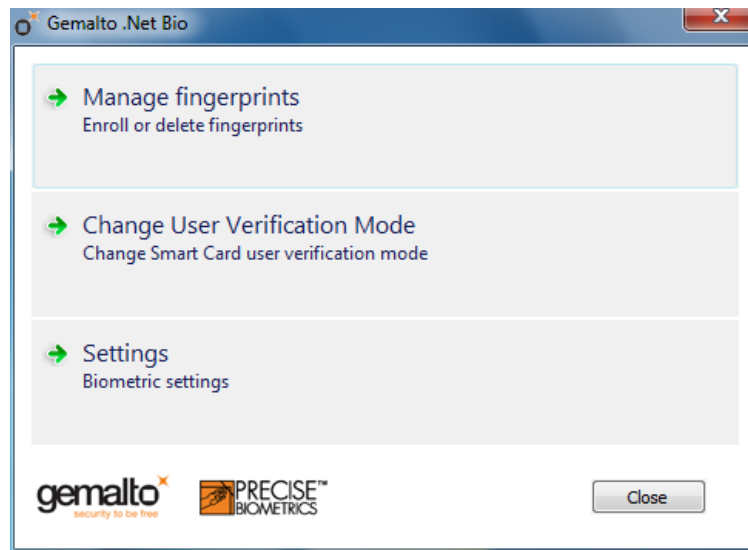
To change the Biometric Settings:

- 1 From the control panel, go to **Hardware and Sound > Biometric Devices**. This displays the window shown in “Figure 11”.

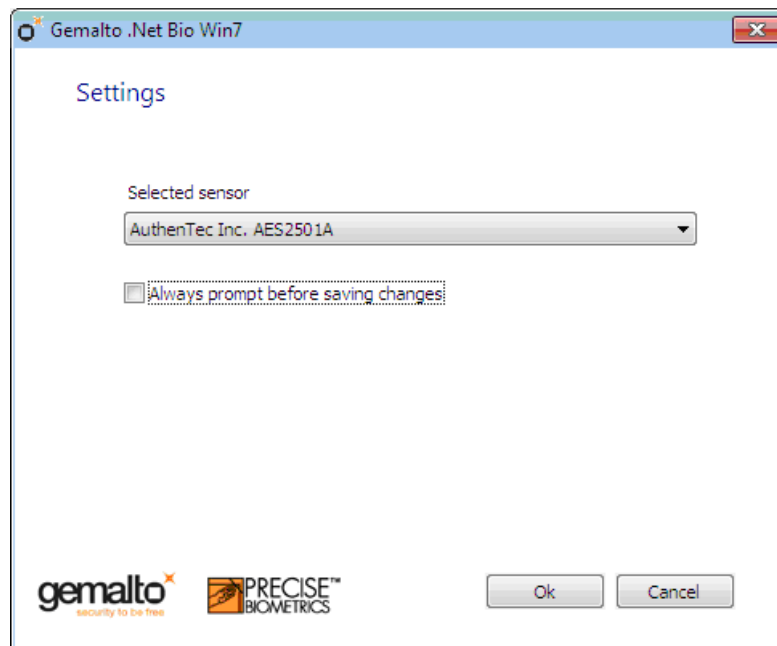
Figure 8 - Use Biometric Devices with Windows (After Enrollment)



- 2 Click **Manage Your Fingerprint Data** in either of the two places. If you have not yet enrolled any fingerprints, click **Use your fingerprint with Windows** instead.
- 3 Authenticate yourself as described in appears as shown in “Biometrics Admin and User Authentication” on page 14.
This starts the Fingerprint Management Application (FMA) as shown in “Figure 9”.

Figure 9 - Fingerprint Management Application (After FP Enrollment)

4 Click **Settings**. This displays the **Settings** window as follows:

Figure 10 - The Settings Window

5 In **Selected Sensor**, choose your new FP sensor and click **OK**.

Note: Checking the box **Always prompt before saving changes**, means that whenever you try to delete an individual fingerprint template (described in “Deleting Fingerprints” on page 22), a confirmation box appears asking if you sure.

Enrolling Fingerprints for Biometric Authentication

Before you can begin using fingerprint recognition with the Gemalto .NET Bio Solution, you first need to enroll one or more fingerprints onto the card. The fingerprint information is written to and stored on the card. You can enroll up to 10 fingerprints and then select which ones are used for verification.

The Gemalto .NET Bio Solution works with both swipe and flatbed fingerprint sensors. Fingers should be clean before scanning them. The following tips can also help ensure an optimal enrollment.

Tips for Using a Fingerprint Sensor

Swipe Sensor: To help ensure successful readings with a swipe fingerprint sensor:

- Swipe your finger flat on the sensor with constant speed.
- Make sure the whole area marked in orange is scanned.
- Do not use your fingertip.
- Do not rotate your finger while swiping.
- Do not lift your finger while swiping.

Flatbed Sensor: To help ensure successful readings with a flatbed fingerprint sensor:

- Place your finger flat on the sensor.
- Make sure that the whole area marked on the orange zone is scanned.
- Make sure you position your finger so that your cuticle is level with the center of the sensor.
- Make sure your finger is placed straight, not rotated.
- Do not place your finger too far down on the sensor.
- Avoid skewed or misaligned finger placement.

Enrolling Fingerprints

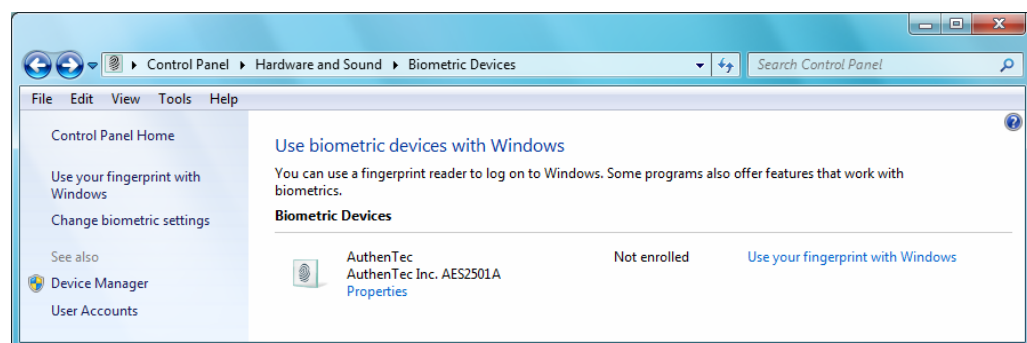
This section shows you how to enroll fingerprints.

Note: A fingerprint can be enrolled once only. To enroll several fingerprints you have to use a different finger each time.

To enroll one or more fingerprints for biometric authentication with the Gemalto .NET Bio Solution:

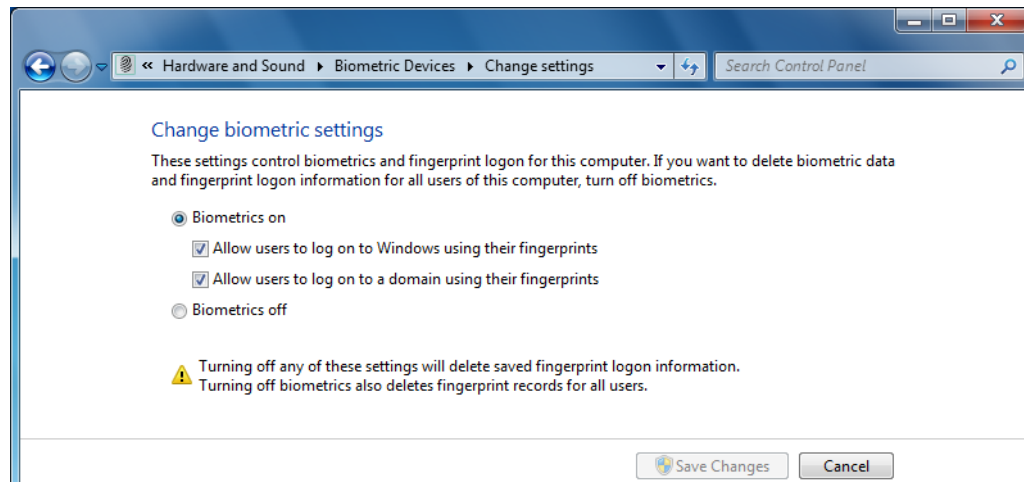
- 1 From the control panel, go to **Hardware and Sound > Biometric Devices**. This displays the window shown in “Figure 11”.

Figure 11 - Use Biometric Devices with Windows (Before Enrollment)



The sensor is present and the current state is “Not enrolled”.

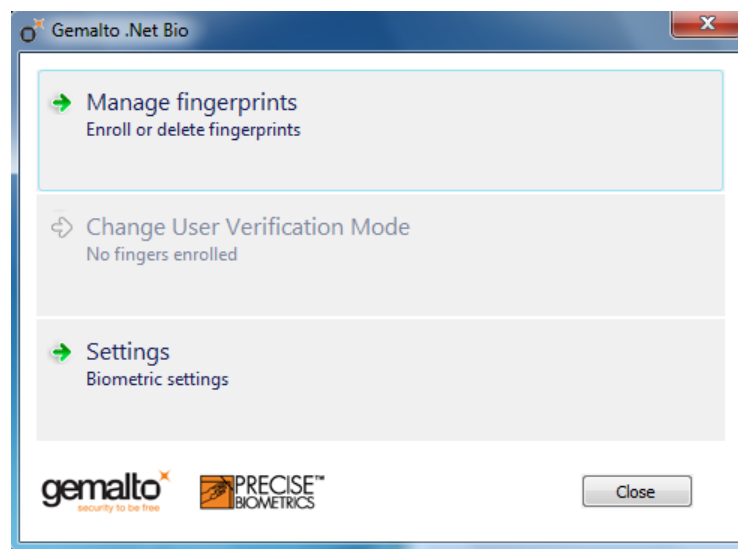
- 2 On the left side of the control panel, select **Change biometric settings**. This displays the window shown in “Figure 12”:

Figure 12 - Change Biometric Settings Window

- 3 Choose **Biometrics On** and check one or both of the “**Allow Users...**” boxes according to your requirements.
- 4 Click **Save Changes**. This returns you to the window in “Figure 11”.
- 5 Click **Use your fingerprint with Windows**, (either of the two places).
- 6 Authenticate yourself as described in appears as shown in “Biometrics Admin and User Authentication” on page 14.

Note: Since no fingerprints have yet been enrolled, the Active UVM in this case is PIN only, regardless of the Set UVM setting.

This starts the Fingerprint Management Application (FMA) as shown in “Figure 13”.

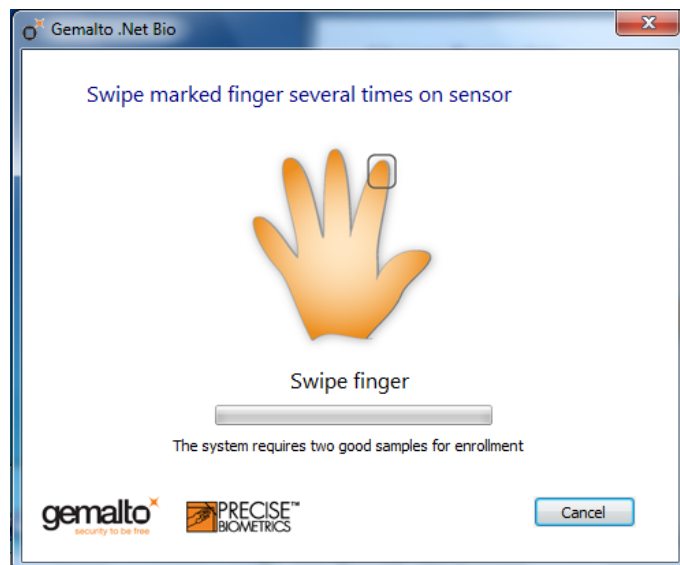
Figure 13 - Fingerprint Management Application (Before FP Enrollment)

Note: The Change User Verification Mode is not yet available because no fingerprints have yet been enrolled.

- 7 Click **Manage Fingerprints**. This displays the window shown in “Figure 14”.

Figure 14 - Manage Fingerprints Window (No FPs Enrolled)

- 8 Select the finger whose fingerprint you want to enroll. A window appears asking you to swipe the selected finger as shown in "Figure 15".

Figure 15 - Swipe Prompt

- 9 Place (or swipe) your finger on the fingerprint sensor. You are prompted to do it again to get a 2nd sample as shown in "Figure 16".

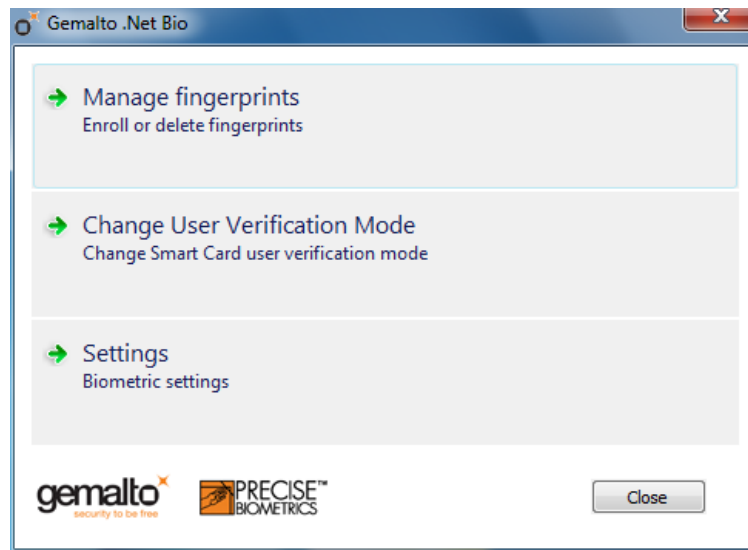
Figure 16 - Second Swipe Prompt

- 10 Swipe your finger a second time. If both samples have enough points in common, the quality check will be positive and a tick appears next to the finger as shown in “Figure 17”. Otherwise you will be asked to provide 2 new samples (known as resampling).

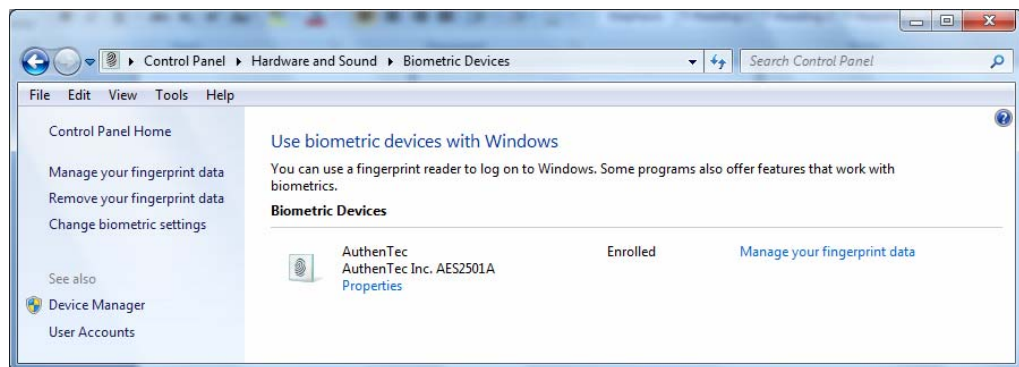
Figure 17 - Manage Fingerprints Window (One FP Enrolled)

- 11 Repeat steps 8 to 10 for each fingerprint that you want to enroll.
- 12 Click on the red cross of the **Manage Fingerprints** window to close it. This returns you to the FMA window.

Note: Now that FPs have been enrolled, the Change User Verification Mode option is available as shown in “Figure 18” on page 22.

Figure 18 - Fingerprint Management Application (After FP Enrollment)

- 13** Click **Close**. The **Use Biometric Devices with Windows** window is refreshed. Notice that “Use your fingerprint with Windows” has changed to “Manage your fingerprint data”.

Figure 19 - Use Biometric Devices with Windows (After Enrollment)

The fingerprint enrollment is now complete.

Deleting Fingerprints

This section shows you how to delete fingerprints. It is not possible to delete all the fingerprints in a single operation, they must be deleted individually.

Note: You cannot delete a fingerprint if this means you would have less than the “minimum number of FPs required” value (determined during card personalization). If you try to do this, your attempted deletion simply has no effect. Similarly if the “minimum number of FPs required” value is 1 or more, you are prevented from turning off the biometric settings, which would delete the fingerprints of all the users of the PC.

Caution: There is a situation where you can block the card if you delete the last or all FPs. This scenario is if you are in FMA mode *pin*, AND you are using UVM2 or UVM4 AND the number of FPs required” value is 0. If you leave the FMA you can no longer re-authenticate yourself as you have no FPs.

Gemalto recommends you use UVM1 or UVM3 when deleting the last or all FP. If you use UVM2 or UVM4 then you **MUST** make sure that you enroll at least one FP before leaving the FMA.

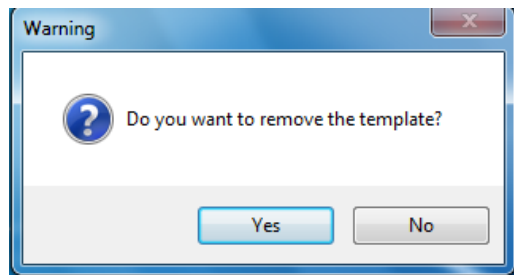
To delete the data for an individual fingerprint:

- 1 From the control panel, go to **Hardware and Sound > Biometric Devices**. As you have at least one fingerprint enrolled, the window looks like that shown in “Figure 19” on page 22.
- 2 Click **Manage your fingerprint data**.
- 3 Authenticate yourself as described in appears as shown in “Biometrics Admin and User Authentication” on page 14.
- 4 The **Fingerprint Management Application (FMA)** starts as shown in “Figure 18” on page 22. Click **Manage fingerprints**.
- 5 The **Manage fingerprints** window appears displaying the fingerprints enrolled. Pass the mouse over the fingerprint you want to delete. The FMA displays a popup to tell you that you can delete the fingerprint by clicking it as shown in “Figure 20”.

Figure 20 - Manage FP - Delete Fingerprint Prompt



- 6 Click the fingerprint.
- 7 Depending on the biometric settings (see “Figure 10” on page 17), the following warning may appear:

Figure 21 - Delete Fingerprint Template Warning

Click **Yes**.

- 8 When you have finished deleting fingerprints, click **OK** in the **Manage fingerprints** window to return to the FMA window.

Changing the UVM

This section describes how to change from one UVM to another from the user's perspective.

Note: This feature is available in the PKI version only.

To change the user verification mode:

- 1 From the control panel, go to **Hardware and Sound > Biometric Devices**. This displays the Biometric Devices window as shown in "Figure 19" on page 22.
- 2 On the left side of the control panel, select **Manage Your Fingerprint Data**.
- 3 Authenticate yourself as described in appears as shown in "Biometrics Admin and User Authentication" on page 14.
- 4 This starts the Fingerprint Management Application (FMA) as shown in "Figure 13" on page 19.
- 5 Click **Change User Verification Mode**. The **Change User Verification Mode** window ("Figure 22") appears.

Figure 22 - Figure 10: Change User Verification Mode

- 6 Select a new verification mode, Fingerprint or PIN in this example.

- 7 Click **OK**, to return to the FMA Window (“Figure 13” on page 19).
- 8 Click **Close** to close the FMA window.

Logon Scenarios

These scenarios assume that at least one fingerprint has been enrolled on the card.

PKI Version

This section describes how to perform a smart card logon with a .NET Bio card from the end-user's point of view for each of the four User Verification Modes. Remember that the UVM is determined by the value of the Active UVM.

When you log on to the PC, the Smart Card Logon icon should be a .NET Bio icon as shown in “Figure 23” on page 25.

Figure 23 - .NET Bio Smart Card Logon Icon



If a different icon appears, click **Switch User** to display the **Credentials Selector** as shown in “Figure 24”.

Figure 24 - Credentials Selector

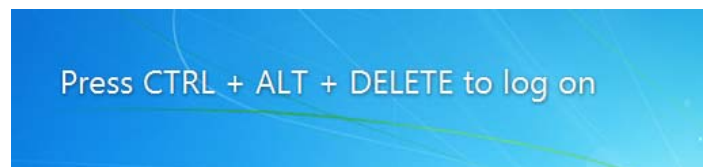
Click the .NET Bio smart card logon icon for your smart card. In the example in “Figure 24”, the left tile, without the .NET Bio icon is to perform a standard user / password authentication (without a smart card). The credentials selector displays one tile for each certificate found in the .NET Bio card (two in the example shown in “Figure 24”). Sometimes an “Other User” tile also appears.

The scenarios described here, assume that you have performed this step if it was necessary.

If the Single Sign-On (SSO) option of the PIN policy is set in the card, the user is required to authenticate himself only once with this PIN, until the card is reset or removed from the reader.

Logging on in PIN-only Mode (UVM1)

- 1 Insert the smart card into your smart card reader.
- 2 When the prompt shown in “Figure 25” appears, press <Ctrl> <Alt> .

Figure 25 - <Ctrl> <Alt> Prompt

- 3 At the Smart Card Logon Screen (“Figure 26”), type your PIN, and then press **Enter** or click the arrow to the right of the PIN box. If the PIN matches the one stored on the card, your Windows 7 desktop starts.

Figure 26 - Smart Card Logon (PIN Mode)

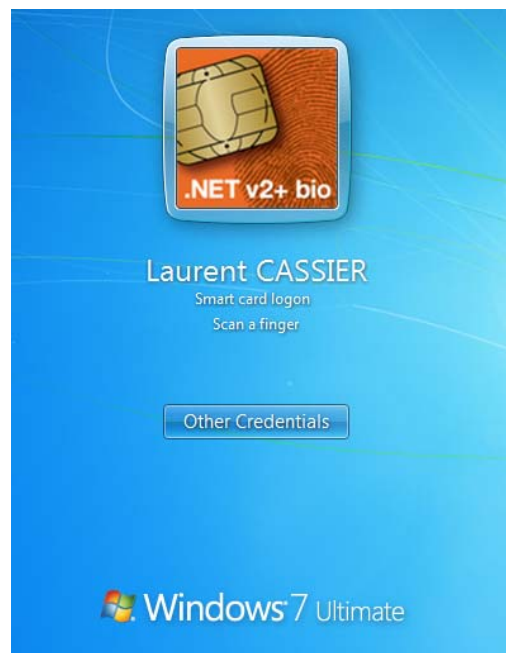


Logging on in Fingerprint-Only Mode (UVM2)

Naturally this scenario assumes that you have already enrolled fingerprints on the card, the logon process is as follows:

- 1 Insert the smart card into your smart card reader.
- 2 When prompted press <Ctrl> <Alt> .
- 3 At the Smart Card Logon Screen ("Figure 27") swipe one of the fingers that you have enrolled.

Figure 27 - Smart Card Logon (FP Only)



If the swipe is unsuccessfully captured, the .NET Bio icon turns red and a “fingerprint capture failed” message appears. In this case the swipe does not count as a failed longer and the fingerprint retries ratification counter is not decremented.

If the swipe is successfully captured, but the capture does not match the FP stored, the icon turns red, the fingerprint retries ratification counter is decremented and the number of remaining attempts is displayed.

Figure 28 - Unsuccessful Authentication (Red)



If the fingerprint authentication is successful, the icon turns green and you are logged on to the computer.

Logging on in PIN-or-Fingerprint Mode (UVM3)

If the card is set to operate in PIN OR Fingerprint mode, the logon process is as follows:

- 1 Insert the smart card into your smart card reader.
- 2 When prompted press <Ctrl> <Alt> .
- 3 At the Smart Card Logon Screen (“Figure 29”) either enter your User PIN and click the right-arrow or swipe one of the fingers that you have enrolled (no need to click the right-arrow in this case).

Figure 29 - Smart Card Logon (PIN or FP Mode)

If the authentication is successful, the .NET Bio card icon turns green. If unsuccessful, it turns red as in “Figure 28” on page 28.

Logging on in PIN-and-Fingerprint Mode (UVM4)

If the card is set to operate in PIN AND Fingerprint mode, the logon process is as follows:

- 1 Insert the smart card into your smart card reader.
- 2 When prompted press **<Ctrl> <Alt> **. The first logon screen is the one for fingerprint authentication – identical to the one used in UVM2 shown in “Figure 27” on page 27.
- 3 Swipe one of the fingers that you have enrolled.
If the authentication is successful, the .NET Bio card icon turns green and you are prompted to enter the PIN.
- 4 Type your PIN, and then press **Enter** or click the arrow to the right of the PIN box. If the PIN matches the one stored on the card, your Windows 7 desktop starts.

Note: The .NET Bio card has separate counters to record the number of remaining attempts for PIN authentications and Fingerprint authentications. If the FP authentication is successful, but the PIN authentication fails, only the PIN counter is decremented.

Non-PKI Version

When you log on to the PC, the Smart Card Logon icon should be as shown in “Figure 30”.

Figure 30 - .NET Bio Smart Card Logon (Non-PKI)



If a different icon appears, click **Switch User** to display the **Credentials Selector** as shown in “Figure 24”.

Figure 31 - Credentials Selector (Non-PKI Version)



The tiles in the Credentials Selector are as follows (from left to right)

- Standard non-smart card based logon for a named user
- Standard Smart Card Logon indicating no PKI certificates found
- Fingerprint logon using FPs stored in the .NET Bio smart card.

To logon using fingerprints:

- 1 Insert the .NET Bio card.
- 2 Swipe one of the fingers enrolled on the .NET Bio card (there is no need to click the **Fingerprint** tile).

The card checks to see if the FP matches one of those stored in its memory. This is the Match-on-Card function. If it does, the computer checks to see if the FP belong to one of those in its list of users associated with FP authentication. This is managed by the WBF in Windows 7.

- 3 One of the following occurs:
 - If successful, the **Fingerprint** tile turns green and you can access the computer.
 - If the swipe is unsuccessful (correct finger but not read correctly), the **Fingerprint** tile turns red and you must try again.
 - If the swipe is successfully read but the FP does not match one of the users “known” to the computer, (for example it is someone else’s finger) the **Fingerprint** tile turns red and a message tells you that the fingerprint is not found in the fingerprint store. In this case you must click **Switch User** to return to the Credentials Selector in “Figure 31”, from where you can choose how you want to log on.
 - If the fingerprint is successfully read and recognized as matching one on the card - but the user is not known to the computer, the normal prompt for username and password appears and the user must log on in this way. For subsequent logins to that computer, the user is recognized.

Note: There is no ratification counter for the FP authentication, so you cannot block the card by failing FP authentication.

Changing the PIN

You can change the User PIN of the smart card by using the Windows 7 Secure Desktop feature.

To change the User PIN of the smart card:

- 1 Press <Ctrl> <Alt> .
- 2 Choose **Change a password**.
- 3 Choose **Change User PIN**.
- 4 Enter the current PIN in **PIN** and the new PIN value in **New PIN** and **New PIN Confirm**, then click **OK**.

Changing Fingerprints

To add a new fingerprint, follow the instructions in “Enrolling Fingerprints” on page 18.

To remove a fingerprint, follow the instructions in “Deleting Fingerprints” on page 22.

To change an existing fingerprint, that is reswipe it, you must first delete the fingerprint, then enroll it again.

Unlocking the PIN

You can unlock the User PIN of the smart card by using the Windows 7 Secure Desktop feature.

Note: In order to be able to do this, the **Unblock Card** feature in the secure desktop user interface must be enabled in Windows 7, as described in “Appendix A - Enabling Unblock Card in Windows 7”.

To unblock the User PIN of the smart card:

- 1 Press <Ctrl> <Alt> .
- 2 Choose **Change a password**.
- 3 Choose **Unblock User PIN**. The window displays a 16-digit challenge, generated by the card as shown in “Figure 32”.

Figure 32 - Smart Card Unblock Window



- 4 Contact your system administrator, and provide this 16-digit challenge. The administrator will in return provide you with a 16-digit response.
- 5 Enter this 16-digit response in **Response** and the new PIN value in **New PIN** and **New PIN Confirmation**, then click **OK**.
- 6 Click the arrow to complete the authentication.

Unlocking Fingerprint Authentication

You can unblock the User FP of the smart card by using the Windows 7 Secure Desktop feature.

Note: This feature is available in the PKI version only.

To unblock the User FP of the smart card:

- 1 Press <Ctrl> <Alt> .
- 2 Choose **Change a password**.
- 3 Choose **Unblock User Fingerprints**. The window displays a 16-digit challenge, generated by the card, similar to the one in “Figure 32” on page 32.
- 4 Contact your system administrator, and provide this 16-digit challenge. The administrator will in return provide you with a 16-digit response.
- 5 Enter this 16-digit response in **Challenge** and click the arrow to complete the unblock operation.

Unlocking Fingerprint Authentication via the PIN

From version 7.1.0.1 of the minidriver onwards, an option is available where unblocking the PIN automatically unblocks the fingerprint authentication at the same time. This is done by setting the configurable “Unblock FP when unblock PIN” parameter to 1.

Locking/Unlocking the System

The Gemalto .NET Bio Solution can also be used to unlock the system. To lock a computer (instead of logging off), press **Ctrl+Alt+Del** to access the Secure Desktop Menu), and then select **Lock this Computer**. This action means that the computer can be unlocked only by a smart card logon. Removal of the smart card can also lock the computer if this option has been set as global policy or local computer Policy ((**Control Panel > System and Security > Administration Tools > Local Security Policy > Local Policies > Security Options / interactive Logon: Smart Card removal behavior**))

Unlocking your computer with the Gemalto .NET Bio Solution works the same way as a secure logon. Upon successful verification of the smart card PIN, fingerprint(s) or both, the session is unlocked and you return to the Windows 7 desktop in its previous state.

Using Gemalto NET Bio verification in the User Desktop

.NET Bio can be used by many applications that run in the Windows 7 user desktop, including MS Outlook for email signature and encryption, MS Word and Excel for digital signature of documents, and EFS for file and folder encryption. It can also be used with VPN clients for secure remote authentication.

Digital signatures are valuable for proving that you signed the contents of a document or message and that the contents have not been altered in transit. This is called “non-repudiation.” For additional privacy, you can also encrypt documents and messages. The message contents are encrypted using the shared digital certificates of both the sender and the recipient.

If an application works on Windows 7 and provides support for Microsoft's Smart Card Cryptographic Service Provider architecture, then the standard smart card PIN prompt can be replaced by the corresponding .NET Bio fingerprint verification prompt. For detailed information on using smart cards for two-factor authentication, digital signatures and encryption with different applications, refer to the application documentation.

The *.NET Smart Cards in a Windows Environment Administration and User Guide* provides some useful examples of the following:

- Signing mails in Microsoft Outlook and other e-mail applications
- Signing documents in Microsoft Office applications, such as Word, Excel, Powerpoint
- SSL authentication to Web sites
- Encrypting files using EFS
- Encrypting files using BitLocker To Go
- Applying a Digital Signature to an e-mail using MS Outlook

The examples in that document are for generic .NET cards. The only difference with .NET Bio is that you authenticate yourself according to the active UVM (PIN/ Fingerprint)

To digitally sign an email message with the .NET Bio Solution:


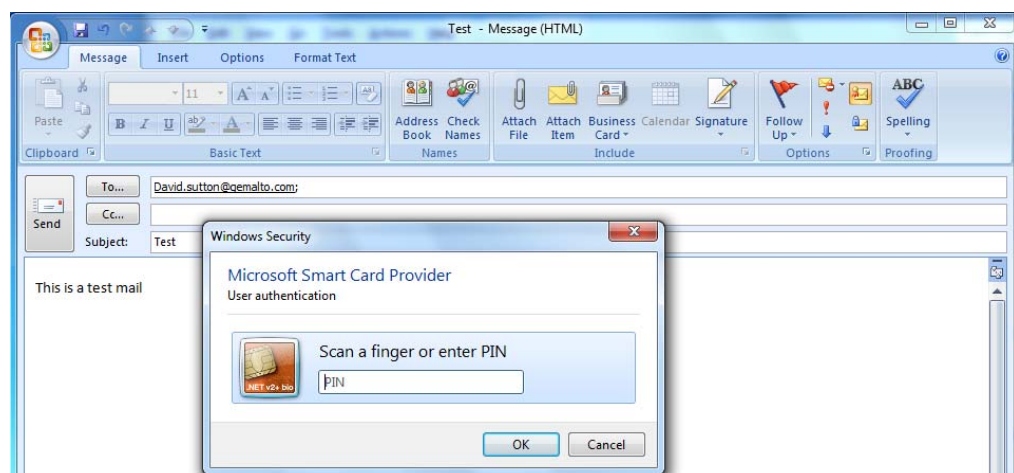
- 1 When creating the email message, go to **Message Options**. In Outlook 2007 you do this by clicking options here 
- 2 In the **Message Options** window, click **Security Settings**, then in the Security Properties window that opens, select **"Add digital signature to this message"**. If you have more than one digital certificate stored on the card, select one to use to sign the message.
- 3 Complete your message and click **Send**. The security dialog box corresponding to the Active UVM of your card appears.

Figure 33 - MS Outlook - Sign Email



- 4 Authenticate yourself (in this example swipe your finger and/or enter your PIN corresponding to UVM3), and then click **OK**. If the credentials match the ones stored on the card, your digitally signed message is sent to the recipient(s).

SSL Authentication to Secure Web Sites

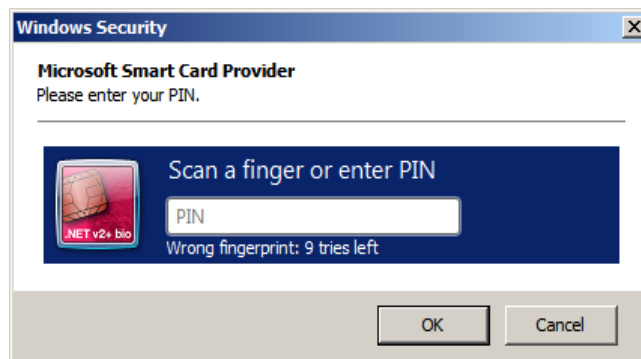
This section outlines how to use a .NET Bio smart card to authenticate yourself to a secure web site (SSL authentication)

To perform SSL authentication:

- 1 Launch Internet Explorer.
- 2 Go to your SSL web site.
- 3 If several certificates are present in your smart card, Internet Explorer asks you to select one. Select your certificate and click **OK**.
- 4 Authenticate yourself according to the Active UVM (UVM3 in our example) and click **OK**.
- 5 If the authentication is successful, the .NET Bio icon turns green, your connection is authenticated and you enter the web site.

If the authentication fails the .NET Bio icon turns red and you have to retry.

Figure 34 - Unsuccessful SSL Authentication



Encrypting a File or folder using EFS

To encrypt a file using an encryption certificate stored on the smart card:

- 1 Right-click on the file or folder and select **Properties**.
- 2 Click **Advanced**.
- 3 Select **Encrypt Contents to Secure Data** and click **OK**.
- 4 Click **OK** to encrypt the file with your smart card. The security dialog box corresponding to the current user verification mode of your card will appear.
- 5 Authenticate yourself as appropriate (swipe your finger and/or enter your PIN), and then click **OK**.
- 6 After successful verification of the PIN or fingerprint, the file will be encrypted using the encryption certificate on the card.
- 7 The file contents are now encrypted. To decrypt and open the file, the smart card inserted and the correct PIN or fingerprint is presented.

BitLocker To Go

This feature is new to Windows 7. It is available for the Windows 7 Ultimate version only. It is similar to EFS but encrypts an entire drive instead of a file or a directory. It is particularly useful to encrypt an entire external drive or USB key.

It is based on Microsoft's Base CSP, so can be used with a .NET Bio card.

Pre-requisites

To use BitLocker To Go with biometric authentication, you need the following:

- Windows Seven Ultimate
- A smart card reader and its driver (for Windows 7, the CCID driver is Inbox)
- A .NET Bio smart card and its smart card mini driver (for example, Gemalto's .NET smart card driver available from Windows Update)
- The Gemalto .NET Bio Solution must be already installed on the computer.
- A "Bitlocker" certificate (includes the object with OID 1.3.6.1.4.1.311.67.1.1) but you can also change the default policy to use the logon OID (1.6.1.4.1.311.20.2.2)

To configure BitLocker To Go to recognize the .NET Bio smart card:

- 1 Insert the .NET Bio card.
- 2 Connect the USB key or external drive to the computer.
- 3 Right-click the drive in Explorer and choose **Manage BitLocker**.
- 4 In the menu that appears, choose **Add a smart card to unlock the drive**.
- 5 Click **Close**.

To encrypt an external drive or USB key using BitLocker To Go:

- 1 Insert the .NET Bio card you configured for BitLocker To Go.
- 2 Connect the USB key or external drive to the computer.
- 3 Right-click the drive in Explorer and choose **Turn on BitLocker**.

Windows 7 encrypts the whole drive using the BitLocker certificate in the .NET Bio card.

To read an external drive or USB key encrypted using BitLocker To Go and a .NET Bio card:

- 1 Insert the .NET Bio card you configured for BitLocker To Go.
- 2 Connect the USB key or external drive to the computer. The window in "Figure 35" on page 37 should appear.

If it does not, in Explorer right-click the virtual drive for the USB key/external drive and choose **Unlock**. This displays the window in "Figure 35".

Figure 35 - External Drive Encrypted using BitLocker To Go



- 3 Click **Unlock**. The security dialog box corresponding to the Active UVM of your card appears.
- 4 Enter your PIN and/or swipe your finger as appropriate and click **OK**.
You now have full access to the data on your USB key or external drive.

Abbreviations

CCID	chip / smart card interface device
CP	credential provider
CSP	cryptographic service provider
EFS	encrypting file system
FAR	false acceptance ratio
FMA	fingerprint management application
FP	fingerprint
GUI	graphical user interface
MoC	match-on-card
MS	Microsoft
N/A	not applicable
OATH	the initiative for open authentication
OTP	one-time password
PIN	personal identification number
PKI	public key infrastructure
SSL	secure sockets layer; a protocol, v.3.0.v, for securing tcp/ip sessions
SSO	single sign-on
UI	user interface
UVM	user verification mode
VPN	virtual private network
WBDI	web based driver installer
WBF	Windows biometrics framework
WSF	Windows smart card framework