LITE VERSION
(Limitation to 10 finger templates)

BIOCERT AUTHENTICATOR 1.0 Lite

Before starting

We wish to indicate that this document is a first draft to be packaged with the release of the BioCert Authenticator toolkit. We will try to give as much information as possible and we assure that this document will continuously updated. Please do not hesitate to forward any questions or comments: marc_potvin@biometricsdirect.com

INTRODUCTION

Biometrics is a science of recognizing a person using physical characteristics using fingerprint, hand, voice, iris, retinal, DNA…

When using Biometrics, two methods are generally used. The Verification method is referred as **"One to One"** (1:1). This method consist of stating a first identification token (User ID, Smart card…) and verifying if the person is who he claims to be.

The Identification method is known as the **"One to Many"** (1:M). This technique consist in comparing the biometric template against a set of stored templates and find the identical match.

With the increasing reliability and performance, the One to many method has become a preferred technique where user identification requires only a simple touch.

The BioCert Authenticator is a Client/Server application and toolkit that performs 1:M identification. It has been designed to help programmers easily integrate Biometrics directly within their application using simple ActiveX control technology.

BIOCERT Client/Server

The BioCert toolkit is a Client/Server application that has a single purpose, Identify a user and return a basic credential to be used in any ActiveX compliant applications.

The Lite version has all the functionalities than the Pro but with a only limitation of 10 finger templates.

The Server portion is base on a OLE database connection. The default installation includes a MS Access database to start with. MS SQL and other database engine can be supported but have not yet been tested.

Installing the BioCert Server should be done on a centralized computer. The Lite Version uses a simple search pattern. Fingerprint identification is done by comparing templates starting with the first stored in the database.

This will explain why the first enrollee will always have an instantaneous identification while the last one in might be in seconds.

> ***Note: Please notice that when enrolling two fingers per user, will account for two fingerprints, if planning to enroll 100 people with their 10 fingers, you will have a potential of 1000 fingerprints !!!***
>
> ***For enhanced Identification performance, you may later upgrade to the Enterprise version using the same User database.***

The database structure is based around the Fingerprint Identification Record. The FIR is a representation of the information extract from the minutiae of a fingerprint.

> ***Important: Please note that the FIR is not a representation of a captured image of the fingerprint. Many believe that fingerprint biometrics can be used to compare against centralize records. This is very far from being reality and most impossible! The FIR contains only a sample of information of the fingerprint.***

The other values stored in the database are a Numerical field (FkNumeric), an Alpha-numerical (FkAlpha), Payload, Enable and Role.

Both FkNumeric and FkAlpha are available and should to be used as links to your existing application. In the Numerical, someone could use the social security number while the Alpha could be used for an Employee ID number.

The Payload is a very unique feature to the BioCert Authenticator. It is a data field that can only be used when enrolling and can only be extracted when the users is identified

> ***Note: The BioCert is designed in a way to limit to user information to its simplest! The FkNumeric and FkAlpha should store only a link key to your application and the Payload should be used to store a unique identifier or secret.***
>
> ***This means that if someone should hack your system and put his hands on the BioCert database, he would only get a list of Encrypted FIR with no user information to link with it !***

INSTALLATION

The **BioCert.zip** contains two installation files, the BioCert-Server and the Toolkit. You will need to extract both in a determined folders in order to install them separately.

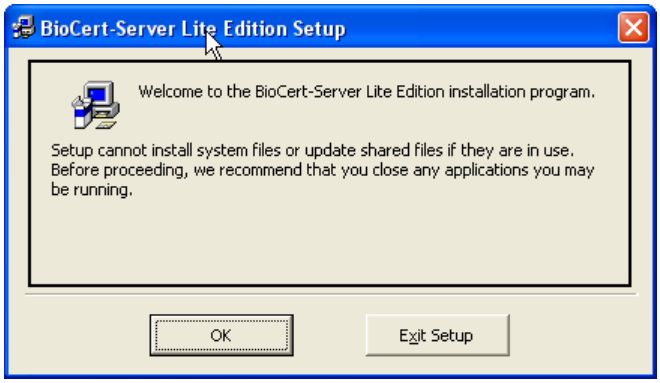
BioCert Server

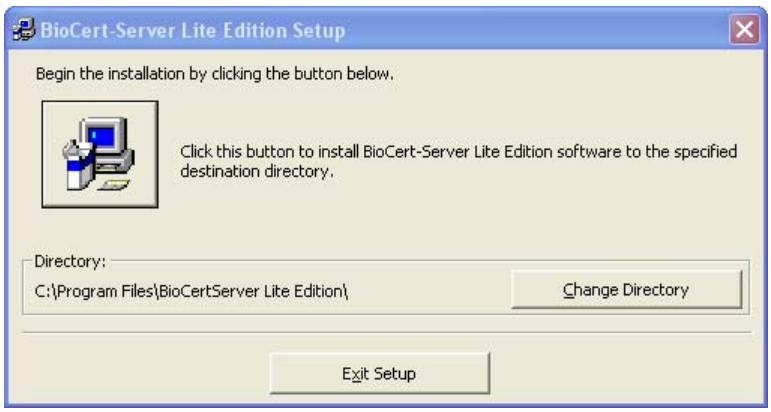
The BioCert server is a very simple application. Its only purpose is to Identify a user and connect to a single database

System requirements for the server

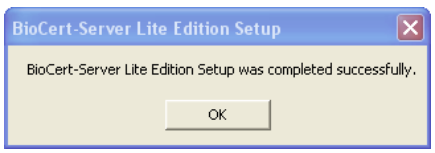
- Pentium III, or higher recommended
- Windows NT/2000
- 128 MB System memory or higher

Starting the installation:

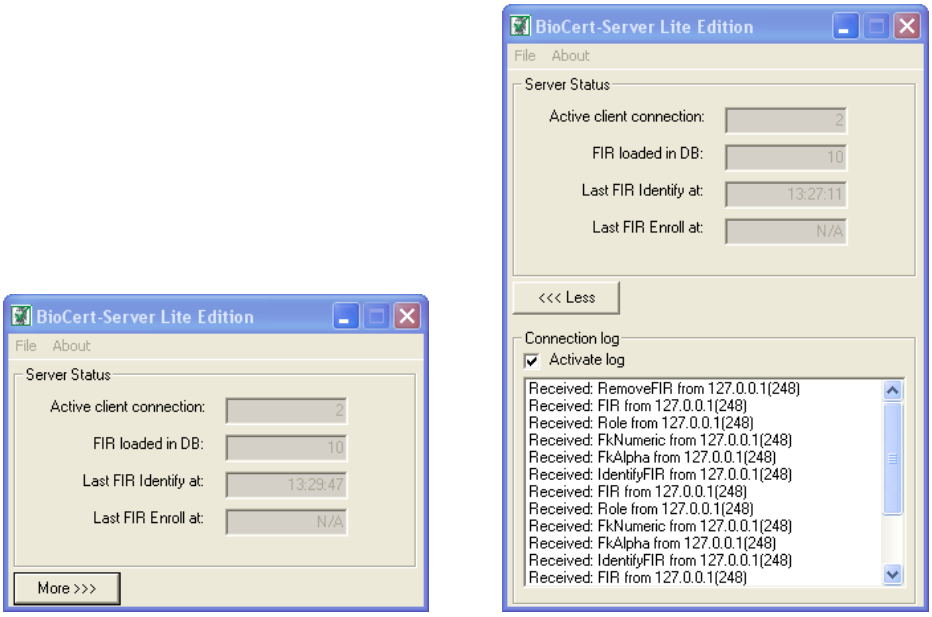




Please follow all prompts and instruction until completion.



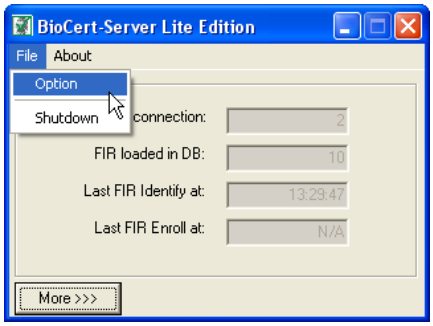
Once installed, you may start the BioCert Server.



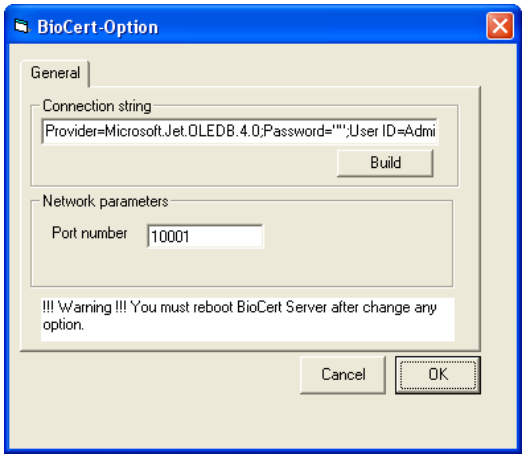
The information that is indicated are the following:

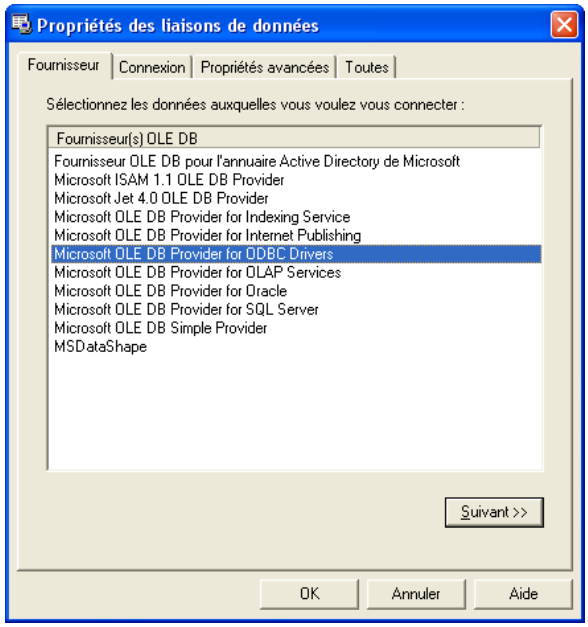
- **Active client connection**: indicates the number of client/toolkit's connected to the server.
- **FIR Loaded in memory**: This value represents the number of fingerprint templates loaded in the System memory. All fingers enrolled are counted and each FIR are loaded twice in the System memory. (*Enterprise version*)
- **FIR Loaded in DB**: Counts the number of users in the database. **(Maximum of 10 in Lite version)**
- **Last FIR identify at**: Value representing current activities on the Server.
- **Last FIR Enroll at**: Value representing current activities on the Server.
- **More>>>**: Will open an extra window showing connection logs.
    - The log window will show the last 500 connection activities.
    - These logs are intended to show current activities and are not logged in a file.

The file menu



Option:





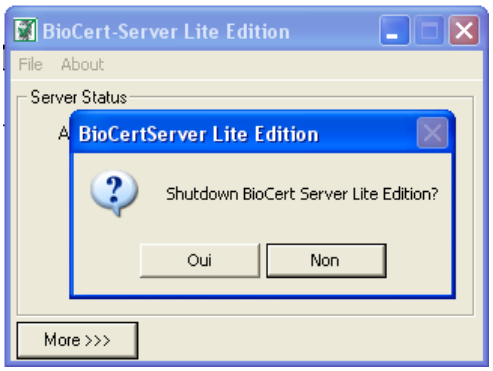
Connection string:
The BioCert Server is OLE DB compliant. In the default installation we have preconfigured a BioCert.mdb and its Connection string. For security reasons, you may easily change the database location, use a more robust Database engine and add a password for security.

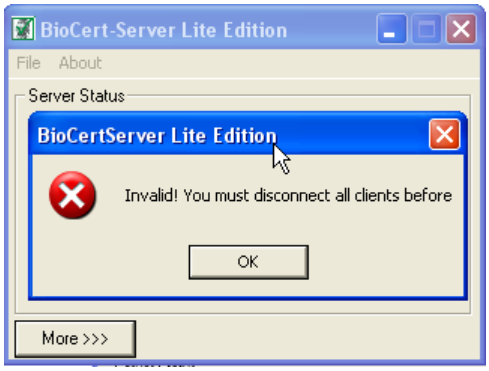
> ***Warning: Once you have applied changes to the database connection, it is recommend to shut down and restart the BioCert server.***

Network parameters:
The Port number is the TCP port value that needs to be synchronized with the toolkit. The default value is 10001 and can be changed accordingly to your network specificity.

!!! Warning !!!: All changes applied in the Option tab will require that you restart the BioCert Server for these to apply.

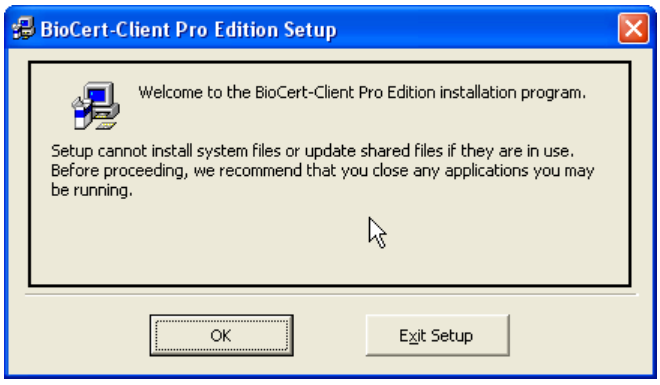
Shutdown: Shut downs the BioCert Server.



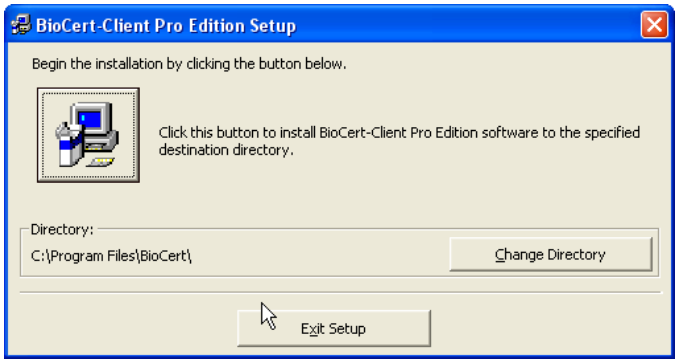


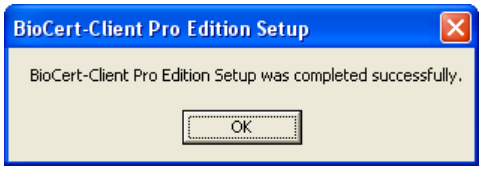
The BioCert server will not Shutdown if there is an active client still connected ! You may refer to the connection log to discover which client might be connected.

BioCert toolkit



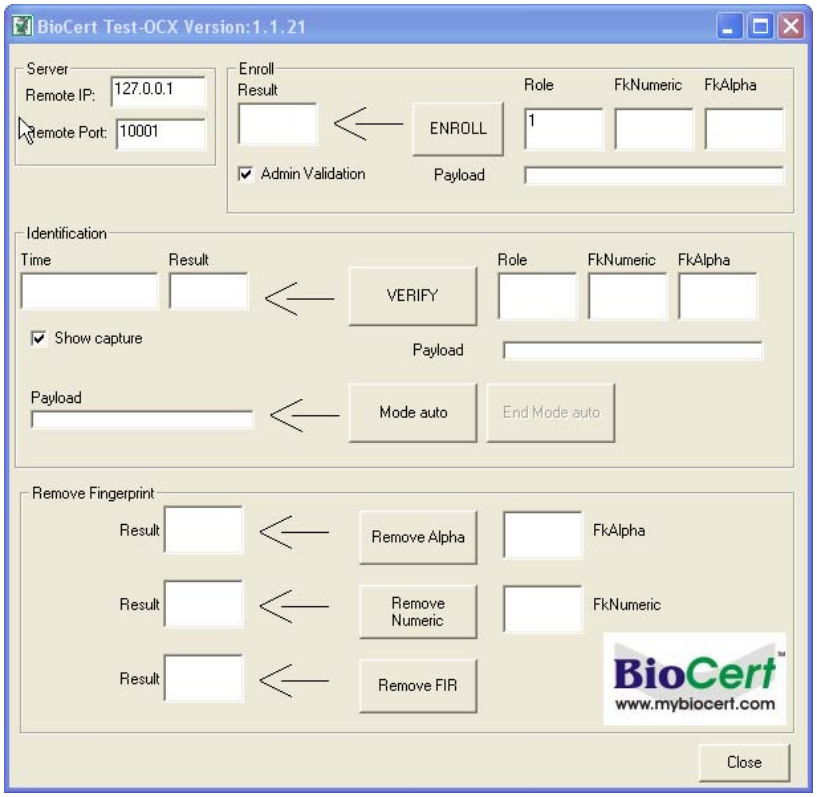
Please follow all prompts and instruction until completion.



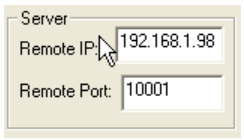


The BioCert Authenticator installation is now completed. You may run the Sample application that is included to validate the connection with the Server.

RUNNING THE SAMPLE APPLICATION

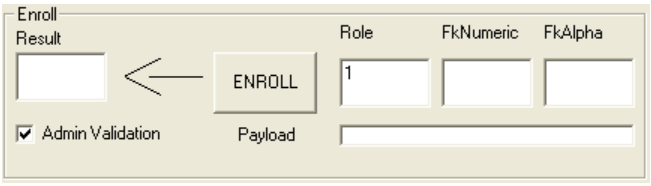


The Sample application is a representation of all the included features of the toolkit. The Visual Basic Code is available and should be found in the BioCert folder.



The server connection is the network address of the server. You can use the IP format (ie: 192.168.1.98) or the server name (ie: biocert.companyname.com). The remote port should be set to the Server's specified port.

ENROLLMENT



The Enroll button launches the Fingerprint Registration.

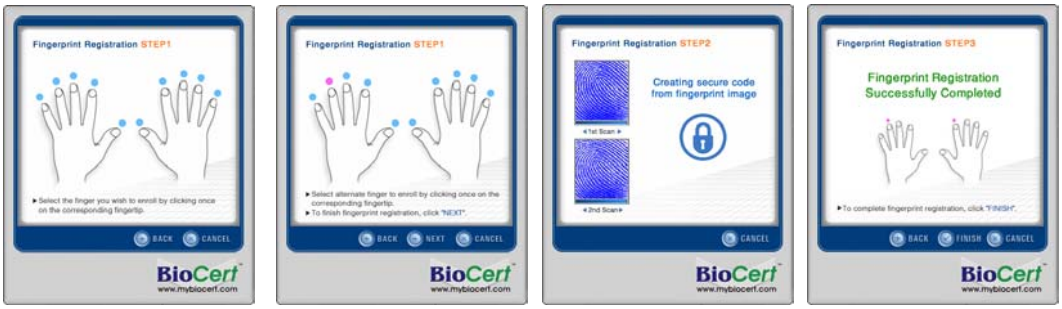
Prior to clicking on Enroll, you will need to supply identification information that will be stored with the FIR.

- For Management:
    - Role is a value that can be used to apply management policies. are made available for administration purpose. Proceeding with the First enrolment, you should uncheck this box. The first person to be enrolled will then have the role of admin and will be in turn needed to validate other users.
        - 2 = Top Admin
        - 1 = Admin
        - 0 = User
    - Checking the "Admin Validation" box is an example of such policy. When checked, no new user can enroll without having an admin fingerprint validation.

    - The FkNumeric field can be used to store a numerical value and be a link to your application.
        - Should be managed to be unique.
    - The FkAlpha field could store a name (John Smith) or member ID (JS001).
        - Should be managed to be unique.
    - The Payload is a unique feature to the BioCert Authenticator. The information will be stored and highly encrypted within the FIR itself. **Once included in the FIR it cannot be modified**. This value can represent a unique identifier or a personal secret information of the user and will only be accessible on a finger identification of the given user.

Notice: Storing the key information to your application is not a good idea since you will not be able to manage or delete a user without his fingerprint validation.

Once identifiers are specified, you can click on the Enroll button to start the Fingerprint Registration. Simply follow the instructions.

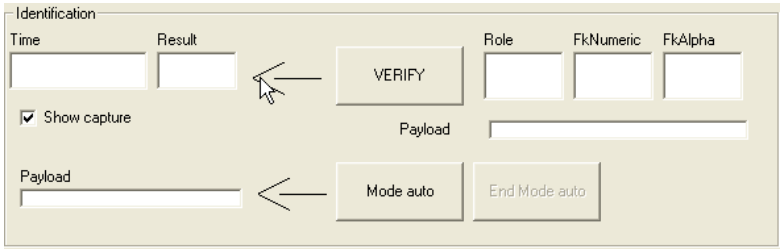


An administrator's finger will be required if the Admin Validation was checked.

And finally, you should have a result value of "0" that confirms that the enrollment process was successful.

> ***Note: The BioCert server does a verification through the database to ensure that a user is not enrolled twice. The error number will be "10701"***

IDENTIFICATION



Clicking the **VERIFY** Button will return the following information:

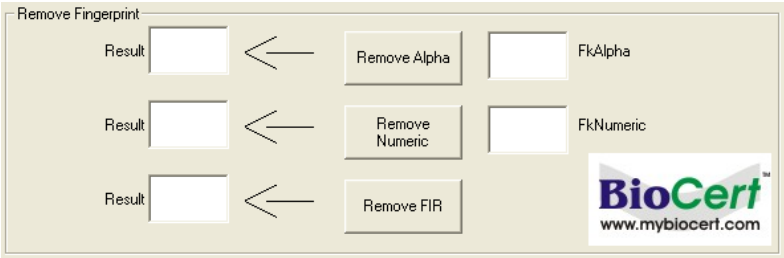
- **Time**, is a simple timer that counts the identification start to finish.
- **Result**: (example)
  - 0 is an successful Identification
  - 10202, no user identified
  - 261, device error
- **Show Capture**: Will specify if you wish to hide the BSP window on an verification process.
  - *While the fingerprint image is shown during the scan it is important to understand that the image is not captured.* The visible window should be considered has a tool to help users better understand how the finger is positioned during the scanning.
  - The "invisible" mode will avoid having the window pop-up on the screen
- **Role**

- 2 = Top Admin
- 1 = Admin
- 0 = User

- **FkNumeric**
- **FkAlpha**
- **Payload**

The **Mode Auto** button is an example of a continuous identification loop. Once the user is Identified, the Payload information is extracted and the Identification process continues.

Remove Fingerprint



Fingerprint management is limited to add and delete only.

Indicating the FkAlpha or FkNumeric will remove the user's FIR from the BioCert database and system memory.

Remove FIR will require that the user be identified. Once identified, the FIR will then be deleted in the database an system memory.

PROPERTY:

LONG CaptureTimeout
Sets the timeout value upon verification. The default value is 10,000 ms.

LONG EnrollImageQuality
Controls the quality of the image captured in enrollment. Has a value of 0 – 100, with the default set at 50.

LONG VerifyImageQuality
Controls the quality of the image captured in verification. Has a value of 0-100, with the default set at 30.

LONG SecurityLevel
Indicates the security level set for fingerprint recognition. Values range from 1 (lowest) to 9 (highe st). The default is 5 (normal).

1 = LOWEST
2 = LOWER
3 = LOW
4 = BELOW NORMAL
5 = NORMAL
6 = ABOVE NORMAL
7 = HIGH
8 = HIGHER
9 = HIGHEST

LONG DeviceTypeUser
Provides information regarding the types of devices linked to the PC. The default is 255 (auto).

1 = PARALLEL
2 = USB
255 = AUTO

LONG DeviceTypeAdmin
Provides information regarding the types of devices linked to the PC. The default is 255 (auto).

1 = PARALLEL
2 = USB
255 = AUTO

LONG DeviceIDUser
Designating a specific device number
(beginning with 0), it provides the Device ID for that number.

LONG DeviceIDAdmin
Designating a specific device number
(beginning with 0), it provides the Device ID for that number.

VARIANT Payload

Payload: Data, such as a cryptographic key, password or user ID, stored in a FIR and released only upon verification

LONG Role
Provides information regarding the role of user to enrolled or identified. The default is 0 (user).

0 = USER
1 = ADMIN
2 = TOPADMIN

INTEGER RemoteTimeOut
Sets the waiting time for server response. The default value is 60 seconds.

STRING RemoteHost
Designating the remote host server IP address. The default value is 127.0.0.1 (Local host)

LONG RemotePort
Designating the remote host server IP port number. The default value is 10001 (You have to use the same port as the server)

LONG IdentifyDisplayMode
Used to show or hide capture display on a Identify.

0 = CAPTURE_DISPLAY_ON
1 = CAPTURE_DISPLAY_OFF

METHOD:

1. Fingerprint Enrollment

Enroll()

The Enroll method is used to enroll fingerprints and store it in the database on the BioCert-server.

Output: Error code

2. Fingerprint Verification

Identify([CheckTopAdmin as boolean])

The identify method performs fingerprint verification by comparing the newly input fingerprint data with the existing fingerprint data in the server database .

Input: Optional parameter, True or False, default is False.
Output: Error code

Put true in parameter for verify if you want to check if the user is admin or top admin.

3. Remove Fingerprint

a) **removeFIR(MyFIR as string)**

Remove the existing fingerprint data in the server database with FIR comparison.

Input: FIR character string
Output: Error code

b) **removeFkAlpha(MyFkAlpha as string)**

Remove the existing fingerprint data in the server database with forward alpha key comparison.

Input: FkAlpha character string
Output: Error code

c) **removeFkNumeric(MyFkNumeric as long)**

Remove the existing fingerprint data in the server database with forward numeric key comparison.

Input: FkNumeric as long
Output: Error code

ERROR CODES AND CONSTANTS

BioCert Server

Value	Error code	Definition
0	NONE	No Error
1	NOT INITITIALIZED	Engine is not initialized
101	MEMORY OVERFLOW	Fail to memory allocation
102	ERROR TO SAVE DB	Fail to save DB
103	ERROR TO LOAD DB	Fail to load DB
104	INVALID TEMPLATE	Invalid Template
105	OVER LIMIT	Over the maximum fingerprint registration number (License)
106	IDENTIFICATION_FAIL	Input fingerprint is not identified
701	ALREADY IN DB	Fingerprint is already in the DB
702	NOT IN DB	Fingerprint is not in the DB

BioCert Toolkit

GENERALERRORS		
Error code	**Error name**	**Description**
0	BioCertERROR_NONE	Function completed successfully
16	BioCertERROR_INVALID_HANDLE	There is an invalid handle in an input function parameter or input field of a data structure
32	BioCertERROR_INVALID_POINTER	There is an invalid handle in an input function parameter or input field of a data structure
48	BioCertERROR_INVALID_TYPE	The input structure type is invalid
64	BioCertERROR_FUNCTION_FAIL	Function failed for unknown reason (internal)
80	BioCertERROR_STRUCTTYPE_NOT_MATCHED	The type of input structure does not match the request type value
96	BioCertERROR_ALREADY_PROCESSED	The template was already processed
112	BioCertERROR_EXTRACTION_OPEN_FAIL	The extraction module cannot be opened
128	BioCertERROR_VERIFICATION_OPEN_FAIL	The verification module cannot be opened
144	BioCertERROR_DATA_PROCESS_FAIL	Internal error occurred during data processing
160	BioCertERROR_MUST_BE_PROCESSED_DATA	The function requires a fully processed FIR
176	BioCertERROR_INTERNAL_CHECKSUM_FAIL	The Checksum of FIR data in an input parameter is invalid
192	BioCertERROR_ENCRYPTED_DATA_ERROR	The encrypted FIR data in an input parameter is broken
256	BioCertERROR_INIT_MAXFINGER	The maximum finger count for enrolment is invalid. Must be set in range of 1 – 10
272	BioCertERROR_INIT_SAMPLESPERFINGER	The samples per finger count for enrolment is invalid. Must be set in range of 1 – 10
288	BioCertERROR_INIT_ENROLLQUALITY	The image quality value for enrolment is invalid. Must be set in range of 1 – 100
304	BioCertERROR_INIT_VERIFYQUALITY	The image quality value for verification is invalid. Must be set in range of 1 – 100
320	BioCertERROR_INIT_IDENTIFYQUALITY	The image quality value for identification is invalid. Must be set in range of 1 – 100
336	BioCertERROR_INIT_SECURITYLEVEL	The security level value is invalid.

Device Errors		
Value	**Error name**	**Description**
4096	BioCertERROR_DEVICE_OPEN_FAIL	Device could not be opened
4112	BioCertERROR_INVALID_DEVICE_ID	The device ID in an input parameter is invlaid
4128	BioCertERROR_WRONG_DEVICE_ID	The device ID in an input parameter refers to a different device
4144	BioCertERROR_DEVICE_ALREADY_OPENED	The device in an input parameter is already opened
4160	BioCertERROR_DEVICE_NOT_OPENED	The device in an input parameter is not yet opened
4176	BioCertERROR_DEVICE_BRIGHTNESS	The brightness value is invalid. Must be set in range of 1 - 100
4192	BioCertERROR_DEVICE_CONTRAST	The contract value is invalid. Must be set in range of 1 - 100
4208	BioCertERROR_DEVICE_GAIN	The gain value is invalid. Must be set to 1, 2, 4, or 8.

USER INTERFACE ERRORS		
513	BioCertERROR_USER_CANCEL	Use of “Cancel” button closed function
515	BioCertERROR_CAPTURE_TIMEOUT	Fingerprint capture process timed out
10202	BioCertERROR_IDENTIFICATION_FAIL	Input fingerprint is not identified
10701	BioCertERROR_ALREADY_IN_DB	Fingerprint is already in the DB
10703	BioCertERROR_SERVER_TIMEOUT	Server response timeout. Verify that the server is running.
10704	BioCertERROR_SERVER_NOT_CONNECTED	No server response. This may happen if the Port number is not well set in the server or at the client side.
10705		