

# WhoIsIt Biometric Technology Introduction

Electronic signatures and passwords have been used routinely by most of us for quite some time, most notably in relation with bank accounts. You use a simple form of electronic signature every time you use your ATM card: The PIN code you enter into the ATM machine acts as your electronic signature.

A PIN code is convenient and works well as long as you have only one PIN code to remember. But as electronic signatures make their way into new areas of everyday life, the number of PIN codes you must remember quickly becomes unacceptable. This presentation focuses on various ways to employ *biometrics* as an alternative to PIN codes. Several alternative biometric strategies will be presented. They vary in cost and the level of security they provide. The WhoIsIt product from Qvoice can be used to realize all these different biometric strategies.

The idea behind passwords and PIN codes is very simple and intuitive. However, a biometric solution with the same degree of security and cost efficiency is surprisingly difficult to build. This is especially true if you want to start using biometrics with legacy software that supports only password authentication. After nine years in the biometric security market, WhoIsIt has matured to the point where it provides a multidimensional solution space that can accommodate most security requirements and can be tailored to fit your budget.

# WhoIsIt Biometric Technology Introduction

## ***Security concerns with biometric lockboxes***

Several solutions exist that will remember your passwords and automatically type them for you once your identity has been verified with biometrics such as fingerprint. These *biometric lockbox* applications eliminate the need for remembering passwords. Another benefit of these solutions is that there is no need to rewrite an application to eliminate its password entry dialog box. The biometric lockbox types the password for us. Sounds like a good idea. However, there are important security concerns with these solutions. We will take a look at some of the weak points of biometric password lockbox solutions and show how WhoIsIt offers a better, significantly more secure solution.

## ***Storing passwords securely in a lockbox***

A password lockbox needs to store the passwords somewhere so that you do not need to remember them. Obviously, this storage needs to be secured so that they can not be compromised by hackers. The standard way to secure information like this is to encrypt it. We can simply encrypt the password lockbox. If a hacker is able to steal your password lockbox they won't be of much use to him because they are encrypted.

Note that encryption requires a cryptographic key, and decryption is only possible by using the *exact* same key. So whenever we want to retrieve a password from an encrypted lockbox following successful biometric authentication, the lockbox software must somehow come up with the exact cryptographic key in order to decrypt the passwords in the lockbox. The problem is that a biometric matching algorithm does not generate any exact information from your fingerprint - it simply compares two fingerprints and computes the *probability* that they come from the same finger. Thus biometrics can not be used to unlock an encrypted lockbox because they do not produce the required cryptographic key. So how do the current biometric lockboxes on the market work? There are several solutions. We will explore them below.

# WhoIsIt Biometric Technology Introduction

## ***Encrypting the lockbox with a secret key***

The simplest solution to storing passwords securely in a lockbox is to encrypt the lockbox with a secret encryption key that is known only to the lockbox program (stored in the lockbox program code). In response to successful biometric matching, the lockbox software will use the secret key to decrypt the lockbox contents and paste the password so you don't have to type it.

This is highly vulnerable to hackers since they can reverse engineer the lockbox program code to find the secret key and use it to decrypt any lockbox. *This is just as secure as storing the key to your front door under your doormat –in other words not very secure.* Note that investing in a massive front door (ie strong encryption) does not improve the situation.

The benefit of this approach is the low cost it achieves by making use of hardware you already have (typically the local harddrive) to store the lockbox data. It doesn't require any fancy hardware, and as long as your computer is stored in a location where access is limited (for example inside your home), the danger posed by hackers may be ignored.

This is the most common way to implement a biometric lockbox, and it is supported by WhoIsIt. However, you should carefully consider the security risks of using this type of lockbox. WhoIsIt offers several alternatives at the cost of additional hardware.

# WhoIsIt Biometric Technology Introduction

## ***Carrying the lockbox with you***

The approach described above relied on encryption to prevent hackers from reading the passwords out of your lockbox in clear text. However, a good hacker will be able to decrypt the lockbox contents by reverse engineering the lockbox software. A much more secure solution is to take the lockbox with you so that no encrypted lockbox data is left around on your machine for the hacker to find and decrypt.

With the proliferation of USB, there are now many devices that can be used to carry your lockbox data around just like you carry a keychain. There are several variants of USB drives, small USB devices that fit on a keychain and behave like a portable disk drive. If you simply move the lockbox data away from the local hard drive and onto a USB drive, you will be carrying your lockbox with you, moving it out of reach from hackers who break into your machine.

## ***Storing the lockbox on a smart device***

Storing the lockbox on a standard USB drive works fine until you lose the USB drive. That would be similar to losing your key chain. You wouldn't feel very comfortable unless you changed all your locks (changed all your passwords). Only in this case the situation is even worse - you might not be able to change all your passwords because the finder of the USB drive beat you to it – he changed your passwords before you did, and has effectively assumed your identity.

# **DiskOnKey Biometric ID USB Device**

## **The Ultimate is user Authentication**

If everything from logging on to your PC to accessing your bank account hinges on your password or biometric record could someone copy your fingerprint and steal your passwords?

- Are your private keys used for authentication and to sign documents safe?
- If your private keys are stored on your PC or laptop are they secure?
- Are your private keys and passwords vulnerable to copying, hacking or being guessed or are they easily accessed? If the answer is yes then they are not safe
- Do you know that fingerprint templates and passwords when sent to PC, servers and applications can be intercepted, copied and otherwise manipulated leading to unauthorized use of a person's biometric template and passwords.
- Do you know that biometrics templates, passwords and private keys stored in a tamper proof container, hand carried and controlled by the individual user and not stored on a PC or company / government database assures the user the safest method of protecting oneself from hackers and biometric privacy concerns?

# WhoIsIt Biometric Technology Introduction

## Placing Biometrics, Passwords and Private Keys in a Hand Carried Tamper Proof Container

What we need is a USB drive that cannot be read at all until you have unlocked it with biometrics. If you lose your USB drive and someone finds it they will not be able to read anything out of it (not even encrypted data). This requires that the USB device has an onboard CPU with some protected storage that can only be read by that CPU. The trick is to store the WhoIsIt biometric database in the protected memory region. A PC cannot read this memory region directly over USB, it can do so only indirectly by communicating with the onboard CPU. The onboard CPU will deny any request to read the protected memory until you have performed a fingerprint match first.

WhoIsIt offers this type of solution using the DiskOnKey product from M-Systems Inc. DiskOnKey Biometric ID device is a USB drive with some extra hardware inside – some protected storage that can only be accessed by an onboard CPU. The CPU is powerful enough to carry out fingerprint matching.

In order to gain access to the information in the WhoIsIt biometric database stored in the DiskOnKey Biometric ID device, you must first plug the DiskOnKey Biometric ID device into the USB port of your PC and then place your finger on a fingerprint sensor connected to the same PC. The fingerprint acquired from the sensor is then sent to the CPU on the DiskOnKey Biometric ID device which in turn matches it against the authorized fingerprints that are stored securely on the DiskOnKey Biometric ID device. If there is a match the CPU will allow the PC to read data from the WhoIsIt database.

Even if you lose your DiskOnKey Biometric ID device you can rest assured that nobody will be able to read anything out of it.

# DiskOnKey Biometric ID

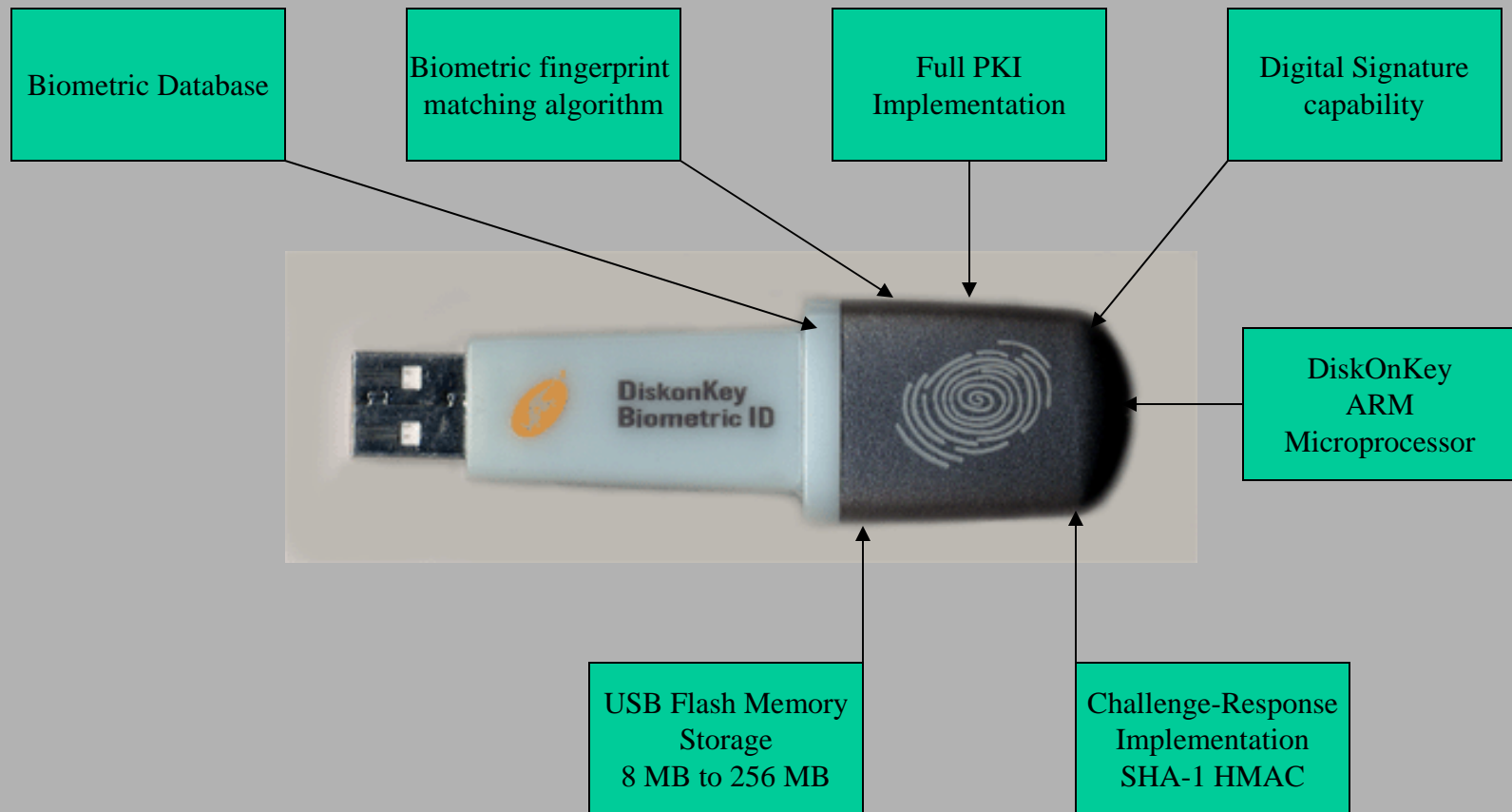
## Carry Your Passwords, Digital Signature and Fingerprint Matching With You

The DiskOnKey Biometric ID device verifies its owner through fingerprint identification. Enrolling your fingerprint to a database on a server creates a privacy dilemma – your fingerprint template is in the possession of someone else. This privacy concern is no longer an issue with the DiskOnKey Biometric ID device since the user's fingerprint template is stored and matched on the device using its protected biometric database and built in microprocessor. The enrolled fingerprint and stored secrets (passwords) never leave the device. Just plug the DiskOnKey Biometric ID device into a standard USB port, place your finger on any supported fingerprint sensor to authenticate and access company servers, web based applications and single sign on programs from anywhere.

- Fingerprint template never leaves the device.
- Fingerprint template is stored, matched and verified on device.
- Fingerprint identification algorithm executes fingerprint matching using the onboard microprocessor.
- Biometric privacy is assured with built-in-privacy-protecting-technologies. Fingerprint templates can not be compromised or spoofed with fake data, templates, passwords; digital keys never leave the DiskOnKey. They're in your possession at all times. Hackers can not gain access to the biometric database
- The DiskOnKey Biometric ID device eliminates the need to be a member of a specific PC or server biometric database because you carry your DiskOnKey biometric database and secrets with you at all times.

# DiskOnKey Biometric ID

WhoIsIt Firmware Feature set



# DiskOnKey Biometric ID

**Biometric Database** - The WhoIsIt biometric database is located in a protected memory area on the DiskOnKey device accessed only by the onboard CPU. The WhoIsIt biometric database contains the authorized user's fingerprint templates, passwords, user attributes, digital signature, certificates and public and private keys.

**Fingerprint Matching Algorithm.** – WhoIsIt performs a fingerprint match between two templates resulting in a score indicating the software's confidence in whether or not the templates are from the same finger. The results can then be used by WhoIsIt Firmware to decide whether or not to:

1. Unlock the user data located and stored on the DiskOnKey biometric Device.
2. Authenticate the user for Windows desktop, network logon and / or single sign-on programs.
3. Authenticate the user for web based and legacy applications.
4. Authenticate the user before computing a Response from a Challenge received from an application.
5. Authenticate the user before PKI encryption/decryption takes place.
6. Authenticate the user before digitally signing documents.
7. Authenticate the user as to who he or she claims to be to confirm proof of personal identification.

**USB Flash Memory Storage-** The DiskOnKey Biometric ID is a fully portable flash storage device designed for people on the move. Store everything from business documents, financial and medical records to personal files, music and e-mail. The storage capacity from 8 MB to 256 MB.

# DiskOnKey Biometric ID Capabilities

**PKI Implementation.** WhoIsIt generates private and public keys directly on the DiskOnKey Biometric ID device. WhoIsIt firmware will encrypt and decrypt data using the users stored keys only after passing fingerprint identification. A user's private keys will never be released from the DiskOnKey Biometric ID device. Private keys are safe guarded by the WhoIsIt firmware on the DiskOnKey Biometric ID device.

**Digital Signatures-** WhoIsIt firmware can generate a digital signature and sign documents using the protected private key stored on the DiskOnKey Biometric ID device. WhoIsIt will digitally sign a document only after the user has submitted and passed fingerprint authentication. Sign documents anywhere anytime.

**Challenge Response Algorithm** — The WhoIsIt firmware located on the DiskOnKey Biometric ID can compute a response from challenge issued by a server and / or application once the user has been authenticated through fingerprint identification. The WhoIsIt firmware contains industry standard SHA-1 HMAC Challenge Response algorithm.

- The Challenge Response algorithm on the DiskOnKey can be used to authenticate a user to any application from any PC equipped with a fingerprint sensor simply by inserting the DiskOnKey Biometric ID device into a USB port.
- The user's passwords, digital signature and private keys can never be compromised because the passwords, private keys and digital signature stored on the DiskOnKey never leave the DiskOnKey device .

# WhoIsIt Biometric Lockbox and Wallet

**The days of remembering passwords are gone.** The Diskonkey Biometric ID is a portable password repository for people with multiple passwords. Because passwords are hard to remember users choose small and simple passwords that are easily decoded.

**Lockbox** The WhoIsIt biometric Lockbox will encrypt, store and remember large complex passwords that are difficult to remember and hard to crack. When an application or web page requests a password simply insert the Diskonkey biometric ID device into the USB port and place your finger on the fingerprint sensor. When verified, the WhoIsIt accesses the stored password sequence, decrypts it and then automatically pastes it into the application dialog box granting the user access.

**Wallet** The WhoIsIt wallet can interact with an application or web page by sending the correct password and user name programmatically to the application thereby eliminating the need for the user to interact with or paste a password into a password dialog box. The password and user name is parsed to the application for authentication and not pasted into the application's password dialog box. This operation is completely transparent to the user and application. It all works under the hood.

The WhoIsIt biometric database stored on the DiskOnKey device increases security and eliminates the responsibility of remembering passwords.



WhoIsIt Biometric Disk on Key Authentication

WhoIsIt Biometric database stored on Key containing  
Secrets and Fingerprint Templates

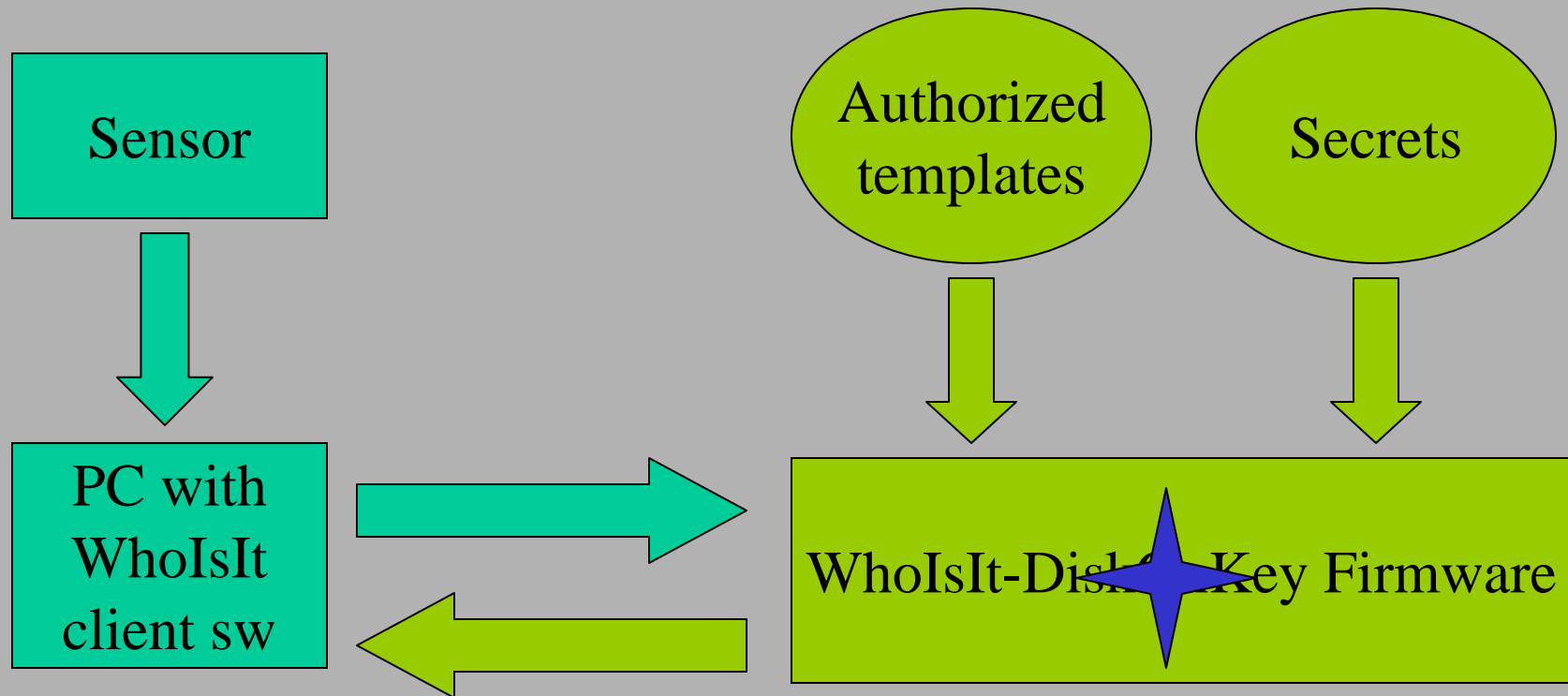
All Fingerprint Matching done on Key

WhoIsIt Biometric Database

|           |                   |                                    |                      |                         |                      |
|-----------|-------------------|------------------------------------|----------------------|-------------------------|----------------------|
| User Name | Override Password | Application and Web page passwords | Fingerprint Template | Public and Private keys | Digital Certificates |
|-----------|-------------------|------------------------------------|----------------------|-------------------------|----------------------|

|  |                               |
|--|-------------------------------|
| Challenge Response Algorithm<br>SHA-1 HMAC | Digital Signature capability. |
|--|-------------------------------|

# Data flow during matching



# WhoIsIt Lockbox/Wallet Integrating Biometrics into Applications

## Application Output

Medical Records Application

**Application sends an Identifier as output to WhoIsIt firmware on DiskOnKey**

1. The application calls WhoIsIt API
2. WhoIsIt API (QVfend or QVocx)Active X control receives the Identifier sent by application user..
3. The identifier is used to retrieve the correct password from the WhoIsIt biometric database stored on the DiskOnKey device.

**Application Output Identifier**

## Application input from DiskOnKey

### DiskOnKey Output

User name & password released from DiskOnKey and pasted into password dialog box or parsed directly into application.



1. WhoIsIt receives Identifier
2. Matches fingerprint
3. Releases password & user name

# WhoIsIt Challenge/Response Explained

To better understand how we can implement a highly useful password lockbox/wallet that never releases its passwords, we will now look at what happens when you log on to your local area network fileserver in the standard way using a username and password entered at your workstation login screen. When you submit your username and password in the login dialog box, your workstation does not actually send the password to the server. This may be somewhat surprising and forms the basis for implementing a password lockbox/wallet that works without releasing the actual password.

In most login implementations, instead of sending the password to the fileserver, the workstation first requests a random bitpattern from the server. This is known as a *challenge*. The client then appends the password to the challenge. The result is run through an irreversible hash function; for example SHA (Secure Hash Algorithm). The SHA result is sent back to the server and is known as the *response*. Since the server knows the correct password and also the challenge it has sent to the client, it can independently compute the response and check that it is the same as the response received from the client. If there is a match the server knows that the client knows the correct password. Note that as long as the fileserver or application program never sends the client the same challenge twice, it is not possible for a hacker to reuse the response to gain access to the server or application even if he has successfully obtained the response using some kind of network sniffer. The server or application will send us a different challenge the next time so that any previous responses will not work the next time around.

**Note** Before the WhoIsIt firmware can compute the response the user must be authenticated. This is accomplished by placing a finger on the fingerprint sensor. The template from the sensor is extracted and sent to the DiskOnKey to be matched against the stored authorized template. The DiskOnKey microprocessor will only compute the response for the challenge after the user has been authenticated.

# WhoIsIt Challenge/Response on DiskOnKey Biometric ID

Now that we have explained how WhoIsIt pasts passwords into password dialog boxes and / or programitacly parses passwords directly to applications for authentication, we will look at how we can use the DiskOnKey Biometric ID to implement an authentication scheme that eliminates not only the user's need to parse or type passwords as illustrated above, but the need to send passwords between software components. This improves security by eliminating the possibility that password are compromised when passed around. Our approach requires modifying the client side implementation of the challenge/response implementation. The server side of the challenge/response implementation can remain unchanged.

With our scheme, the password can never be compromised because it can not be read out from the DiskOnKey Biometric ID. To compute the response, the workstation simply passes the challenge it received from the server on to the DiskOnKey Biometric ID over USB. The CPU on the DiskOnKey Biometric ID will retrieve the password from its protected storage area, but will not send the password to the PC. Instead it computes the response using the challenge and the password and sends the response over USB to the workstation. The workstation then forwards the response over the network to the fileserver or application it tries to authenticate with. The trick is that it is not possible to read passwords out from the protected storage area on the DiskOnKey Biometric ID. Thus passwords remain under tight control of the DiskOnKey Biometric ID and can never be compromised by fake application password dialog boxes or login screens etc.

Note that the application (or in this case the login process) needs to be modified to let the DiskOnKey Biometric ID compute the response from the challenge instead of insisting on computing the response itself.

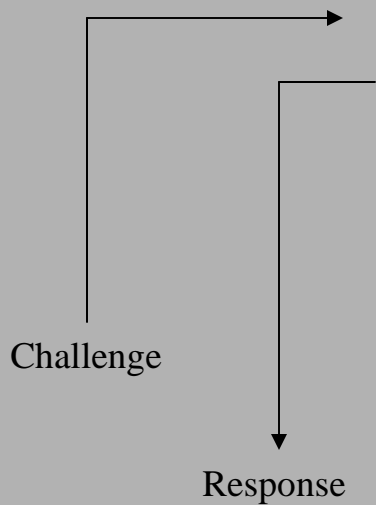
## **Challenge/Response algorithms supported by the WhoIsIt DiskOnKey Firmware**

The DiskOnKey Biometric ID implements the HMAC-SHA1 challenge/response algorithm as described in Network Working Group documents RFC-2104 and RFC-3174. SHA1 is a secure hashing function adopted by the US Government in Federal Information Processing Standard 180-1 (FIPS180-1). The DiskOnKey Biometric ID uses SHA1 to compute a Hashed Message Authentication Code (HMAC) as decribed in RFC-2104.

# Integration with applications using Challenge Response technology



**Built in ARM microprocessor**  
**Password Storage**  
**Matching**  
**Challenge - Response SHA-1 HMAC**



Client GUI - Gatekeeper

Biable  
High lever API Frontend  
QVfend  
Active X Control

WhoIsIt high level API allows applications to use biometrics as the authentication method.

Visual Basic or C++

Java Applet

ActiveX

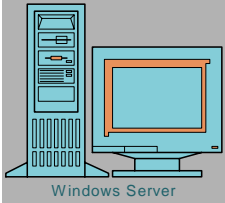
Web page or Legacy Application

# Modifying software to use DiskOnKey Biometric ID challenge/response

As pointed out above, the client part of a challenge/response system needs to be modified so that the client software delegates to the DiskOnKey Biometric ID to compute the HMAC-SHA1 response based on the challenge from the server. WhoIsIt offers two APIs that programmers can use in their modified client software.

- WhoIsIt offers an ActiveX control that will handle all communication with the DiskOnKey Biometric ID over USB as well as communication with a range of fingerprint sensors. The ActiveX control can be embedded in any application or web page and makes it simple to modify any client software to rely on the DiskOnKey Biometric ID to compute the response to a challenge from a server or web page application.
- WhoIsIt also offers the QVFEND programming interface that provides the same services but in a way that is somewhat easier to use than an ActiveX control. This API offers a single routine that accepts a single input parameter (the challenge) and produces a single output parameter (the response). The routine will pop up a WhoIsIt *gatekeeper* requesting the user to insert his DiskOnKey Biometric ID device and place his or her finger on the fingerprint sensor. When an authorized fingerprint is seen on the sensor, the routine will request the DiskOnKey Biometric ID to compute the response for the given challenge and return that response to the client software which in turn can send it to the server as it would normally have done if it computed the response itself.

# DiskOnKey WhoIsIt Challenge - Response



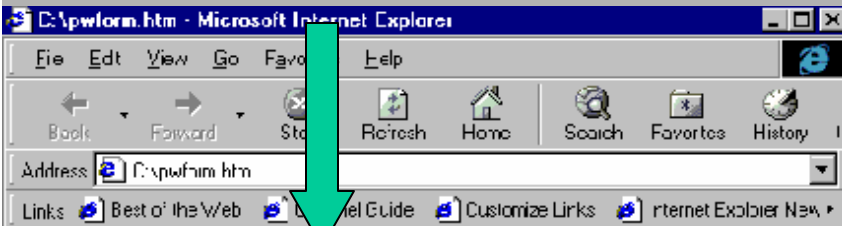
Windows Server

Web page biometric authentication using Challenge/Response



SSL

Server or application requesting authentication computes a random challenge. Challenge is sent to the WhoIsIt Active X control scripted into the web page



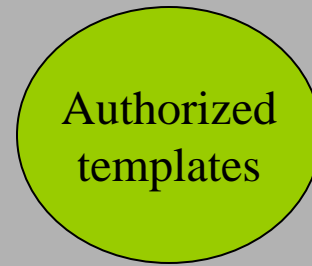
WhoIsIt Active X Control receives challenge from server or application..

WhoIsIt Active X Control extracts fingerprint template. Fingerprint template and challenge are sent to the DiskOnKey to compute the response from the challenge



Fingerprint rejected

Place finger on fingerprint sensor



The authorized template is matched against the template extracted from the sensor



WhoIsIt appends password to Challenge to Compute Response using standard Challenge Response SHA-1 HMAC Algorithm



DiskOnKey returns Response to the server or application indicating that it knows the password.

# DiskOnKey Biometric ID Security



1. Contains WhoIsIt firmware in protected area.
2. Contains IControl matching algorithm.
3. Contains ARM Microprocessor.
4. Contains WhoIsIt Lockbox - paste passwords into password dialog boxes.
5. Contains WhoIsIt wallet. Integrate biometrics into legacy applications.
6. Contains SHA-1 HMAC Challenge/Response algorithm.
7. Computes a response from a challenge.
8. Stores user's fingerprint templates in protected area.
9. Matches fingerprint templates on device.
10. Fingerprint templates never leave DiskOnKey Biometric ID device.
11. Stores user's passwords. Passwords never leave DiskOnKey Biometric ID device.
12. Generates and stores user's public and private keys on device.
13. Private keys never leave DiskOnKey Biometric ID device.
14. Generates and stores user's digital signature. Signature key never leaves device.
15. Plugs into any USB device.
16. Hand carry biometrics and passwords in tamper proof device.
17. Authenticate to any application, logon program.
18. Fits on a Key chain. If lost, passwords and templates cannot be compromised.

## Supported Fingerprint Sensors



IControl swipe fingerprint sensor

AuthenTec fingerprint sensors - DEFCON from Targus and Acer

Secugen optical sensors – Mouse and Hamster

Fujitsu sensors

DIGITUS PCMCIA fingerprint sensor – FIC 200

Identex – Pods and PCMCIA fingerprint sensor for Windows 95 and 98

Billionton – PCMCIA fingerprint sensor AuthenTec chip

SCM - PCMCIA fingerprint sensor AuthenTec chip

KYE mouse – AuthenTec chip

Veridicom sensor

**Note** WhoIsIt DiskOnKey firmware can store face templates. Matching for face recognition on Client PC

# *Summary*

We have seen how WhoIsIt offers many different levels of biometric security depending on end user requirements.

It is often possible to use a lockbox to implement fairly good security for password based legacy applications without modifying those applications. However, for better security, an application may be modified to let the DiskOnKey Biometric ID or Qvoice biometric server compute the response used in the application's challenge/response algorithm. This ensures that the password can not be compromised by a fake password entry dialog box.

Users can hand carry all the necessary authentication credentials with them at all times.

Digital keys, digital signatures, logon and application passwords can not be compromised.

Biometric template privacy is assured. Your fingerprint template need not be on some distant database.

**The DiskOnKey Biometric ID device is the most secure biometric authentication device available**