

A SutiSoft White Paper



4984 El Camino Real,
Suite 200
Los Altos, CA 9402
Phone: 650-969-7884
Fax: 650-969-2783
www.sutisoft.com

SECURED BioPass™ Standalone: Fingerprint-based Access Control for the Standalone Systems

Contents

Introduction	3
Need for Better Access Controls	3
The Password Problem	3
The Biometrics Advantage	3
SECURED BioPass™ Standalone:	4
BioPass™ Standalone	5
Robust Security	5
Best in class fingerprint algorithms	5
Your fingerprints are secure	5
Simple Sign-On™ Utility	5
Sensor Agnostic	5
Encryption / Decryption Utility	6
Summary	6
Value Proposition	6
Security	6
References	6
Time Saving	6



Introduction

In today's world, protection against information theft has become a major concern. The loss of valuable information can lead to a number of personal and legal issues.

As a result, people are increasingly concerned about securing access to their PC's. More attention is being paid towards stringent identity enforcement mechanisms to provide guaranteed privacy and confidentiality of information access.

The Password Problem

The most common way of controlling access to systems has always been using passwords. Each authorized user is allocated a user-id and an initial password. The users are expected to change their initial passwords the first time they login to the system.

As long as the user has one or two accounts or applications to manage, this approach is simple and easy to implement. But when the number of accounts become large, the problems begins to surface. Users find it very difficult to remember all the user-ids and associated passwords for their various application accounts.

When burdened with remembering so many user-ids and passwords, some users make a list of their user-id's and passwords and store them into the system or some of them make sticky notes and paste them in and around their working area. In addition, some users also share their account information with their family, friends and co-workers.

Some users even use same passwords for different applications while others use the names of their loved ones as their passwords thus making them easily vulnerable to hackers. As a result, security of the system is compromised.

Need for Better Access Controls

The most common (user-id and password) way of implementing access control is easy to implement, but requires the user to take extreme care to safeguard this information. It also becomes cumbersome to manage on a large scale across many applications with many different user-ids and passwords.

In an effort to implement more strict rules on password-based access controls, many applications or websites require passwords to be strong (combination of numbers, letters, and characters). These passwords end up being complicated. Users trying to adhere to such policies have a difficult time memorizing the passwords and typing them as well.

The use of biometrics for access control can lessen many problems including the vulnerabilities, cost and inconveniences associated with the traditional password based solutions.

The Biometrics Advantage

Biometrics enables the identification of a person based on his or her physical characteristics and/or behaviour. Common biometrics include: fingerprint, voice pattern, retinal pattern and facial features. Among this large variety of biometric possibilities, the use of fingerprint for identification and verification dominates the market. There are many reasons for this including the low cost, high-reliability and fast-response of the fingerprint technology and systems.

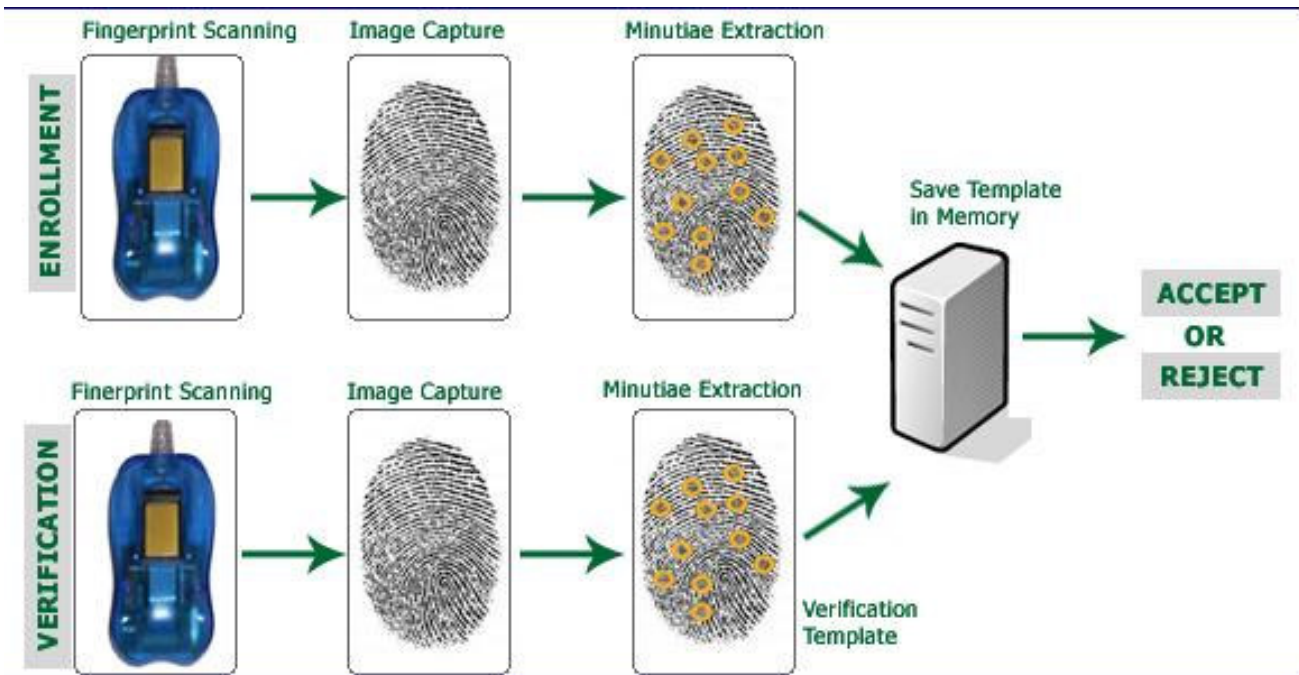
The use of fingerprints for user authentication has been on the rise as people have discovered many problems with password and hardware token-based systems.

Fingerprint-based authentication provides a rather elegant solution to all of the problems associated with passwords and hardware tokens. Since fingerprint technology has become affordable and is reliable, its use in user authentication is rapidly increasing. It is much easier and faster for users to provide their fingerprint than to remember and type in their passwords or to carry tokens around.

SECURED BioPass™ Standalone from SutiSoft does an elegant job of using fingerprints for logical access control.

SECURED BioPass™ Standalone: Fingerprint based access control for your System

SECURED BioPass™ Standalone provides effective access control for individual systems by requiring registered users to authenticate themselves with their fingerprints rather than by passwords. By doing so, it addresses the vulnerabilities associated with password-based authentication by combining the biometric identity verification technologies and the best-in-class extraction/matching techniques.



Credentials of the users are securely stored in the local cache. On a SECURED BioPass™ Standalone enabled system, when users want to login to the system, they need to provide their user-id and fingerprints.

Each user's fingerprint is matched against his registered fingerprints stored in the system cache. In case of a mismatch, the user is denied access to the system

In case of a successful match, the user login is permitted. From this point onwards, user experience is identical to their everyday experience with the system.

SECURED BioPass™ Standalone provides local authentication i.e. user is authenticated for local access to the system. It allows registration of fingerprint templates and their update to be done at the time of windows login.



The various features and benefits of SECURED BioPass™ Standalone include:

Robust Security

By using fingerprint-based access control, it eliminates the vulnerabilities associated with simple user-id/password. SECURED BioPass™ Standalone provides rock solid security access control to the system.

Best in class fingerprint algorithms

SECURED BioPass™ Standalone uses the best-in-class fingerprint algorithms developed by NEC. NIST (National Institute of Standards and Technology), in their evaluation of many fingerprint technologies, has clearly placed NEC as the leader (NIST, 2003). As the fingerprint algorithms form the heart of any fingerprint-based authentication system, the quality of the algorithms is the most important factor.

Your fingerprints are secure

SECURED BioPass™ Standalone does not store or transmit the image of the user fingerprints. It extracts salient points from the image, called minutiae points, and uses them for authentication purpose. While the minutiae can be extracted from a fingerprint image, one cannot take the minutiae and develop the original fingerprint image. This eliminates the chance of fingerprint image being lost, stolen or misused.

Sensor Agnostic

SECURED BioPass™ Standalone is sensor agnostic and can work with a variety of fingerprint sensors available in the market. Within a single installation of SECURED BioPass™ Standalone, several different types of sensors can be used. Fingerprint registration of a user can be done by one type of sensor and verification can be done by another.

BioPass™ Standalone

SECURED BioPass™ Standalone is installed on the user PC and is used by the user at the time of logging in to the system. It captures the user-id, fingerprint and stores in them in the local cache. The same are verified against the registered templates.

SECURED BioPass™ Standalone replaces the existing Microsoft graphical user interface for login and puts its own interface in place of MS-GINA (a Microsoft Windows DLL that does the authentication function).

SECURED BioPass™ Standalone provides a number of useful utilities which enable the users to extract more value from their investment in fingerprint sensors and systems.

The two most useful utilities include Simple Sign-On™ (SSO) and File/Folder Encryption/Decryption.

Simple Sign-On™ Utility

SSO enables users to register their user-id's and passwords used to access web-based services. Once these are registered, the user can logon to these services using their fingerprint, thus eliminating the need to remember user-ids and passwords.

In this scenario, when the web page or application pops up on the screen, SECURED BioPass™ Standalone displays the fingerprint authentication screen. Upon successful verification of the user-id and fingerprint with the server, it automatically populates the user-id and password fields of the web page or application. Then all the user has to do is to press enter to accept the user-id and password and continue with the log-in process.



Encryption / Decryption Utility

Encryption/Decryption utility, as the name suggests, enables the user to encrypt and decrypt files and folders by using their fingerprint as the key. This eliminates need for the user to remember long keys or passwords for encrypting files and folders.

Value Proposition

There are a number of convincing reasons for using SECURED BioPass™ Standalone for an individual system which includes security, and time saving. These value propositions are outlined below.

Security

Most importantly, SECURED BioPass™ Standalone provides a rather robust level of security access for the systems resources. Fingerprint-based authentication insures that the user is who he/she claims to be as users cannot “lend” or share their fingerprints with anyone.

Time Saving

It is considerably faster to provide fingerprint for authentication than to type in passwords.

Generally passwords are required to be long and cryptic strings of alpha, numeric and special characters. For such passwords, not only is the time to type in long but users often have to retype them as errors are easily made in typing such passwords.

Sometimes, after a user attempts to log in 3 or more times unsuccessfully, the system rejects the user. The user in this case has to reset his account. This leads to wasted time and frustration for the users.

SECURED BioPass™ Standalone provides a much faster and convenient way to provide secure authentication information.

Summary

SECURED BioPass™ Standalone provides fingerprint-based access control for standalone systems. It addresses the vulnerabilities associated with password-based authentication.

SECURED BioPass™ Standalone uses the best-in class algorithms for fingerprint matching resulting in unmatched performance and accuracy. In addition, SECURED BioPass™ Standalone is fingerprint sensor agnostic. This enables users to use sensors that best match their needs.

References

NIST (2003). *Fingerprint Vendor Technology Evaluation 2003: Summary of Results*



U.S. Office Address:

SutiSoft, 4984 El
Camino Real Suite 200
Los Altos, CA 94022
(650) 969-SUTI (7884)
Fax: (650) 969-2783
info@sutisoft.com

Japan Office Address:

SutiSoft, KK
Minato Bldg 4F
1-1-12 Minato, Chuo-ku
Tokyo 104-0043 Japan