



# SECURED BioPass™ Standalone

Fingerprint Based Access Control for your system.  
Powered by NEC



## Supported Configurations:

**System OSs:** WinXP (Home and Pro), Windows 2000, Windows 2003, Windows Vista, Windows 2008, and Windows 7

**Fingerprint Sensor:** UPEK, Validity 201, Validity 301, and AuthenTec 1610.

**Fingerprint Template Extraction and Matching:** NEC

**Smartcard Reader:** HP USB SMARTCARD READER

**Smartcards:** ACOS3

SutiSoft's SECURED BioPass™ Standalone product provides fingerprint / Smartcard based access control for standalone systems. By combining the Smartcard based authentication, biometric identity verification technologies and the best-in-class extraction / matching techniques, SECURED BioPass™ Standalone provides a rock solid access control mechanism for a system. Before a user can connect to the system, he needs to be authenticated either by using Smartcards or by using his fingerprints.



## Smartcard Authentication



In a SECURED BioPass™ Standalone enabled enterprise, when users want to login to the system, they need to select the type of authentication: Smartcard Authentication or Biometric Authentication.

On selecting Smartcard Authentication, users' need to insert the smartcard in the reader, enter the PIN to authenticate themselves.

Each user's PIN and User Details are matched with the same stored in the smartcard. 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.

SutiSoft, Inc  
4984 El Camino Real #200  
Los Altos, CA 94022

Phone: 650 969-7884  
Email: [info@sutisoft.com](mailto:info@sutisoft.com)



# SECURED BioPass™ Standalone

Fingerprint Based Access Control for your system.  
Powered by NEC

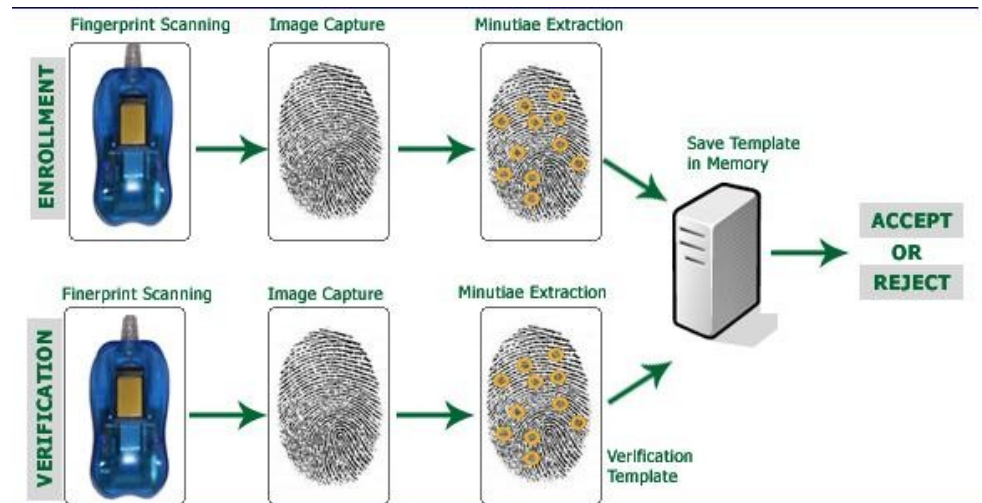


## Users:

The No. of users permitted to register on to BioPass Standalone depends on Windows capability

On selecting Biometric Authentication, users need to provide their user-id and fingerprints.

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



## Benefits:

- Robust security—you have to be who you claim to be!.
- Convenience—no need to remember always-changing, impossible to remember passwords.
- Speed—no need to type in cryptic passwords.
- Cost-effective—pays for itself (in six months) by eliminating high password maintenance costs.
- Easy migration—easily “bolted on” to existing enterprise IT infrastructure.
- Best-in-class fingerprint software—powered by NEC’s fingerprint engine, recognized by NIST as a leader in fingerprint algorithms.
- Fingerprint sensor agnostic—get the best value for money.

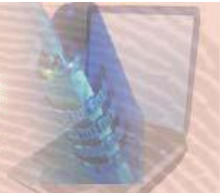
SutiSoft, Inc  
4984 El Camino Real #200  
Los Altos, CA 94022

Phone: 650 969-7884  
Email: info@sutisoft.com



## SECURED BioPass™ Standalone

Fingerprint Based Access Control for your system.  
Powered by NEC



SECURED BioPass™ Standalone is a standalone solution for fingerprint, smartcard-based authentication. Credentials of all the legitimate users are stored in the smartcard / local cache. Every time a user wants to login to the system, his identity information is collected by the SECURED BioPass™ Standalone Client and sent to the smartcard / local cache for authentication. Access is permitted or denied based on the results of this authentication.



### Features:

- Fingerprint / Smartcard based authentication – BioPass Standalone allows a user to secure this system either by using smartcards or BioMetric authentication technology.
- Multi-factor Authentication – BioPass allows users to authenticate themselves by using a combination of password, PIN, or password, password/fingerprint or fingerprint only.
- Login Time Registration – Users can register their fingerprints even at the time of windows login.
- No Server Required – BioPass Standalone uses the local cache to store passwords and fingerprints and hence does not require a server.
- Windows Clients – BioPass Standalone supports WinXP (Home and Pro), Windows 2000, Windows 2003, Windows Vista, Windows 2008, and Windows 7 clients.
- Simple Sign-On –Allows users to manage their passwords for web-based applications, and fingerprint- based file and folder encryption and decryption.
- Fingerprint sensor agnostic – BioPass Standalone allows users to register with one fingerprint sensor and authenticate with another.
- Easy Migration – Organizations can implement smartcard / fingerprint based authentication at their pace depending upon their budget and the availability of smartcards / fingerprint sensors.



SutiSoft, Inc  
4984 El Camino Real #200  
Los Altos, CA 94022

Phone: 650 969-7884  
Email: [info@sutisoft.com](mailto:info@sutisoft.com)

Explore

Contact



<http://www.sutisoft.com>