SECURED BioPass™

Fingerpringt Based Access Control to your corporate Network

Powered by NEC

Supported Configurations:

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

Server OSs: WinXP Pro, Windows, 2000, 2003, Linux (available soon)

Server Software: Java 2 SDK v1.5, 1.6, Apache Tomcat, HSQL

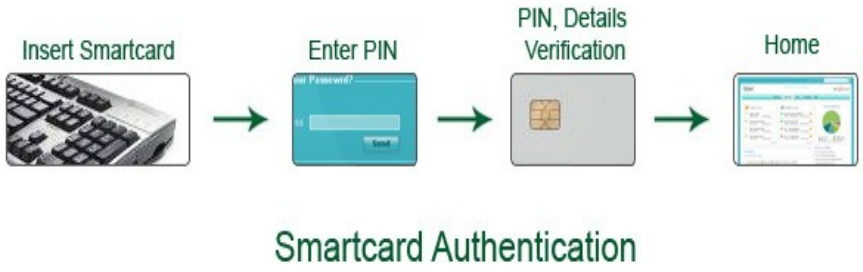
Fingerprint Sensor: UPEK, Validity 201, Validity 301, and AuthenTec 1610.

Fingerprint Template Extraction and Matching: NEC

Smartcard Reader: HP USB SMARTCARD READER

Smartcards: ACOS3

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



Smartcard Authentication

In a SECURED BioPass™ 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' needs 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 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.

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

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

SECURED BioPass™

Fingerpringt Based Access Control to your corporate Network

Powered by NEC

Users:

SECURED BioPass™ comes in the following user configurations:

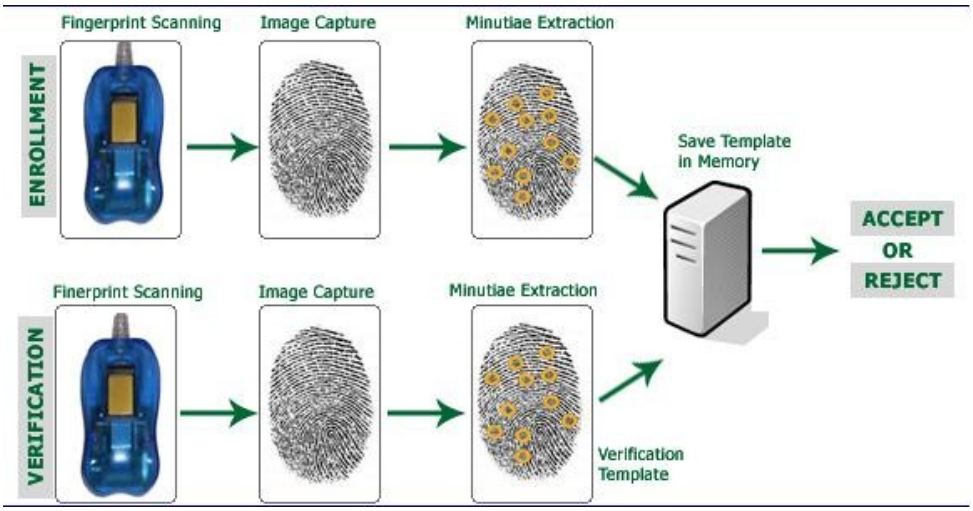
- 50 users
- 100 users
- 250 users
- 500 users
- 1000+ users

For other configurations, please contact SutiSoft, Inc.

The system is capable of scaling up to handle much larger number of users.

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.



Remote users can authenticate with SECURED BioPass™ Server just as they would in the enterprise provided they have access to internet.

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™

Fingerpringt Based Access Control to your corporate Network

Powered by NEC

SECURED BioPass™ is a client-server solution for fingerprint / smartcard based authentication. Credentials of all the legitimate users are stored in the smartcard / SECURED BioPass™ Server. Every time a user wants to connect to the enterprise network and access its resources, his identity information is collected by the SECURED BioPass™ Client and sent to the smartcard / SECURED BioPass™ Server for authentication. Access is permitted or denied based on the results of this authentication.

Features:

- Fingerprint / Smartcard based authentication – BioPass allows an organization to secure their corporate network resources 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.
- Local Caching – BioPass provides a local caching feature so that users can be granted access even when the server is unavailable.
- Fail-safe operation – Whenever there is a hardware failure in the primary server, authentication is automatically done from the secondary server in a completely seamless manner.
- Windows Clients – BioPass client 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.
- Remote, web-based administration – BioPass can be administered using a web based administration console that can be accessed from anywhere in the network using a web browser.
- Fingerprint sensor agnostic – BioPass 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

Explore Contact SHARE