



VST™ with True User Identification® Software Development Kit

IDENTIFY POPULATIONS OF ANY SIZE WITH CERTAINTY

Key Benefits

Development Support

Mature SDK with over 90 functions

C, C++, VB, .NET and Java API support

Implement at client and/or on server

Proprietary or Commercial DB support for Identification

Sample applications included

Support for Windows, Linux and Windows CE

Standard Support

NIST-validated, AFIS-grade fingerprint algorithms

NIST-validated, ANSI/INCITS fingerprint standard support

INCITS 378 support

INCITS 381 support

ISO 19794-2 Support

WSQ compression support

FIPS 201 (GSA-APL) Support

NFIQ Support

Interoperable between ISO and INCITS templates



3349 Highway 138,
Building D, Suite A
Wall, NJ 07719, USA
866.846.2594
information@bio-key.com
www.bio-key.com

PRODUCT OVERVIEW

BIO-key's patented Vector Segment Technology™ (VST) with True User Identification (TUI™) is a fingerprint algorithm and database development toolset that allows you to tightly integrate biometric verification and/or identification into new or existing applications and middleware.

VST with TUI includes all the tools needed by developers and integrators to quickly and easily add secure and super-scalable fingerprint verification and identification functionality to applications and product platforms, giving them complete control over the user environment and authentication processes.

FEATURES

The VST software development kit includes libraries: application program interfaces, device drivers, sample code and fingerprint database tools to integrate fingerprint image capture, fingerprint image quality assurance, fingerprint template extraction and fingerprint template matching and searching routines into virtually any application.

VST offers complete reader interoperability, supporting devices from every major fingerprint reader manufacturer. With this capability, users ENROLL ONCE on any of the supported readers, and can subsequently use readers from every major reader manufacturer to establish their identity.

The advanced minutiae and vector based fingerprint algorithms that are the core of VST deliver superior accuracy, are ideally suited for large population verification or identification applications. Additionally VST includes **support for FBI, NIST, ANSI and ISO fingerprint standards.**

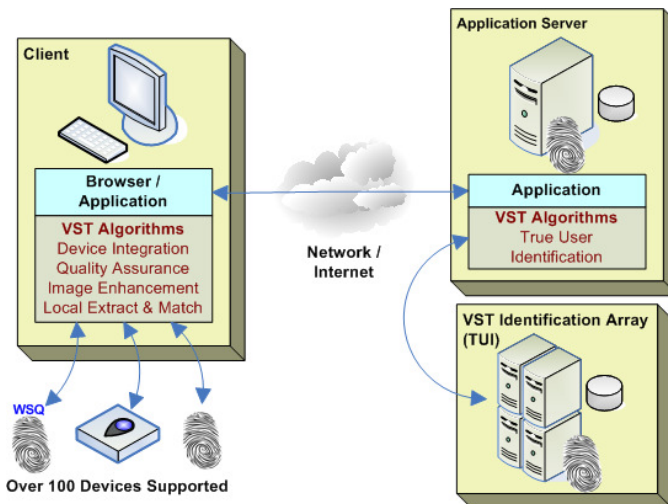
True User Identification (TUI) is a scalable Intelligent Image Indexing™ technology for identification systems of any size. Its performance speed of **more than 6 million fingerprint matches per second** has been validated at Oracle's Partner Technology Center.

SIMPLE, SECURE, CONVENIENT- VST is ideal for rapidly integrating fingerprint verification and/or identification functionality into any application.

Protect Identities

VST can store each user's fingerprint as a mathematical template, eliminating the need to store the user's fingerprint image on a computer or in a database.

This proprietary mathematical template cannot be reverse-engineered to reconstruct the fingerprint.



Device & Image Support

Over 100 fingerprint-enabled devices incorporating over 30 sensor types

- Full device interoperability (Enroll on device A and match or search using device B)
- Stand-alone device support, keyboards, mice, laptop computers, point-of-sale devices, access control units and handheld devices

Standard image input file formats include BMP, RAW, and WSQ

Ability to use fingerprint data direct from EFT file formats

Fingerprint Functionality

Low false match and false non-match rates with unique 41 level fingerprint image quality assurance filter

Supports plain, segmented slap, rolled & latent fingerprints

Intuitive user experience with GUI visual feedback of fingerprint during capture process improves overall system performance

Verification, alias prevention and identification modes

Integrate Rapidly

The VST software development kit is easy-to-use and ships with sample applications and straight-forward API's. It supports .NET, C, C++, VB and Java development environments. Environments including PowerBuilder, Cold Fusion and others have also been supported with these general use API's.

Passwords Optional

Passwords continue to be problematic for enterprise authentication. With VST, you incorporate strong authentication, while eliminating the need for users to reset and record passwords, access codes, IDs and PINs that can be easily compromised. With VST, users can establish identity with or without tokens or cards (e.g. FIPS 201) in a client or client-server application.

Accurate ISO/ANSI Algorithms

VST accuracy has been validated by the National Institute of Standards and Technology (NIST), the US government's independent testing laboratory and standards body, in two key testing programs:

- Large Scale SDK test and
- Minutiae Interoperability Exchange Test (MINEX).

NIST MINEX Participant 1J - BIO-key International, Inc.			
BIO-key Template Create & Match Equal Error Rate		3 rd Party Template Match Equal Error Rate	
Mean	Median	Mean	Median
0.0046	0.0046	0.0049	0.0046

SPEED, ACCURACY, SCALABILITY- Identify Large Populations

VST is unique in its ability to accommodate large and very large civilian or customer populations without compromising system speed or accuracy.

Millions of Matches per Second

Leveraging BIO-key's Intelligent Image Indexing™ Technology, VST delivers blistering speeds on commercial hardware, operating systems and database software. More than 6 million fingerprint matches per second have been achieved running on as few as ten (10) commercial (COTS) servers.

Better Than 99% Accurate with Just Two Fingers

NIST, using test databases of more than 11 million people, validated VST performance in more than 3.3 trillion match operations. The largest test database, collected by the US Department of Homeland Security via the US-VISIT program, yielded a true match rate for VST of 99.33% using just a two finger match set.

Scale Infinitely

BIO-key's VST with TUI technology delivers an extensible development framework capable of managing hundreds of millions of fingerprints for alias prevention, verification and identification purposes.

Applications

Financial/E-Commerce	Transportation
Healthcare	Loyalty/Membership
Government	Application Service Providers
Education	Corporate Intranets/Extranets