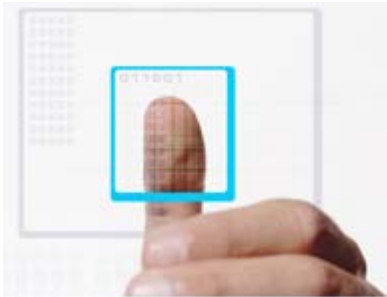




True User Identification®



Your fingerprint contains enough data to positively identify you to any system. True User Identification from BIO-key eliminates the need for an associated user ID, PIN or smart card.

BIO-key measures up:

- BIO-key's solutions can identify users in seconds—even when searching databases of millions of fingers!

- Using our patented VST, we analyze from 1500 to 2000 data points from a fingerprint, far more than traditional algorithms!

- True User Identification performs false alias checks across databases to reduce or eliminate fraud typically resulting from users having more than one identity!

- True User Identification employs VST's support for full biometric reader independence, offering great flexibility.

3349 Highway 138,
Building D, Suite A
Wall, NJ 07719, USA
866.846-2594
support@bio-key.com
www.bio-key.com

SCALABLE & TRUE BIOMETRIC IDENTIFICATION

BIO-key International has revolutionized biometric finger identification systems. With the True User Identification framework from BIO-key, an Oracle database running on industry standard hardware can perform true fingerprint biometric identification that scales to the millions of records, opening the door to many applications.

WHAT IS IDENTIFICATION?

Biometric identification is the ability of a system to recognize, or identify a user based on the biometric fingerprint data alone. Most biometric systems today are merely verification systems that first require an identifier; like a card, PIN, user ID or other token. Identification systems deliver more—the ability to do large scale false alias checks to determine if the same user is in the database multiple times, under different names.

WHY BIO-KEY IS DIFFERENT

BIO-key's identification technology focuses on the ability to do true identification, not just binning or speed searches. BIO-key has defined a unique set of index data points from a fingerprint that can be mapped into an Oracle database. This unique indexing algorithm lets your database system go directly to the right set of records, eliminating the need to do a large number of comparisons in order to find a list of candidate matches, quickly and accurately.

This replaces the typical binning search methodologies that invoke errors when the global binning characteristics are lost or 'confused'. Additionally, traditional search techniques generally start at the 'top' and work their way until they find a match. This is often not the best match and could easily result in a false accept.

THE PROOF IS IN THE METRICS

BIO-key's biometric performance numbers are off the charts in the three most reliable performance indicators of a biometric identification algorithm: *false acceptance rate* (FAR), *false rejection rate* (FRR) and *failure to enroll rate* (FER).

The FAR measures how often the system mistakes an impostor for an authorized user—the worst-case scenario in a secure environment. In tests, BIO-key's FAR was measured at better than 1 in 200 million!

The FRR measures how often the system rejects an authorized user, a situation that can inconvenience users but that poses no direct security risk. In practice, FRRs are dependent on environmental conditions and the resulting quality of the finger models. BIO-key's FRR can be controlled to near zero by following our guidelines for obtaining high-quality finger scans.

The FER measures the ability to enroll a true population. BIO-key can enroll more than 99.9% of any population set.

CONFIGURATIONS

The BIO-key True User Identification framework utilizes Oracle 9i or 10g for the database engine. This framework is a series of schemas, extensible indexes, and stored procedures that enable the application to effectively 'identify' a biometric sample with a simple SQL statement. Much of the interaction with the True User Identification framework is with simple SQL commands, and can be combined with any other forms of data to create complex queries.

Shopping for a biometric security solution?

Ask these questions about the solutions you are considering:

- √ *Is the system based upon open standards, including:*
 - *Complete scanner independence?*
 - *Full support of SQL databases, such as Oracle 9i & 10g?*
 - *Operating system support, including Microsoft and Linux?*

- √ *Is there an option to store or completely destroy the fingerprint image?*
- √ *Does the system store the biometric data in a format that is impossible to reverse engineer into a fingerprint?*
- √ *While providing biometric identification does the system invoke the biometric in a completely secure environment?*

If the answer to any of these questions is NO, you should be talking to BIO-key!

The simplicity of the True User Identification framework veils the inherent complexity of database management and configurations. The overall management of the Oracle database can make the difference between a fast system and a sluggish one. BIO-key representatives can work with your system administrators to help effectively tune the partitions, clusters, and related data to provide the fastest and most streamlined system possible.

IDENTITY PROTECTION

No security system can achieve total security as long as a user's identity data can be stolen or duplicated. Whereas a user ID, a password or even a scanned fingerprint image can be compromised, BIO-key's advanced security plugs the security holes. Once your finger is scanned and converted to an encrypted mathematical model, the scanned image can be destroyed. All that remains is the model, which cannot be decoded to obtain the original fingerprint image.

IDENTIFICATION IN PRACTICE

Within a security or authentication application, BIO-key's identification technology can be implanted in a wide variety of uses:

- True User Identification's manageable application size and platform independence enable deployment in a wide variety of environments.
- Your application can be tuned to offer different degrees of security and or speed by adjusting the various settings and thresholds.
- True User Identification is ideally suited for client/server models, offering the ultimate convenience to users while providing the ultimate security to the server application.
- True User Identification is embedded as optional components in BIO-key products and offerings, including the state-of-the-art authentication solution, WEB-key, or in the robust Vector Segment Technology SDK.

True User Identification uses a staged indexed approach to 'search' the database in the fastest and most accurate way possible. Hundreds of data index points are checked in each search.

Optional Tailgating Monitor