How it works

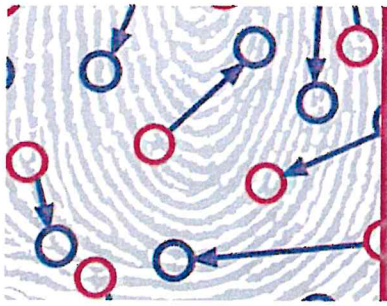
identiMetrics™
Simplify your school day

The identiMetrics™ Finger Scanning Process



Finger is scanned

In order to be enrolled in the computer software, the person's finger is scanned by the biometric finger scanner. The computer software develops a grid of intersection points from the swirls and arcs of the scanned finger.



Unique points identified

A template is created by the software that shows the intersection of unique points on the finger. The fingerprint image is destroyed. The template is converted to a binary number. The binary number is then encrypted and stored.



Points converted to unique binary number

When the person returns to be identified, the finger scanner again scans the finger. The computer software now compares the new template with the other templates in the database. When a matching template is found, the person is identified.

This identification and matching process takes under one second to complete.



Encrypted binary number linked to ID

No fingerprint image is ever stored. No fingerprints can be recreated from the template.

Just like the iPhone!



Differences Between Identification Software and Law Enforcement Applications

Identification Software	Law Enforcement Applications
Uses flat images of only two fingers to create templates.	Captures rolled images of all 10 fingers.
Flat images reveal the center of the finger and require only a minimum of unique identifying points in order to make a match.	Rolled images capture unique identifying points on the entire finger surface in order to collect the maximum number of unique identifying points.
The purpose is to identify a person already enrolled in the software.	The purpose is to identify suspects based on fingerprint images directly taken from a crime scene.

Frequently Asked Questions

Q: What is biometric identification? A: Biometrics are automated methods of recognizing a person based on a physiological or behavioral characteristic. They include face, fingerprint, hand geometry, handwriting, iris, retina, vein and voice – anything that's a part of you.

Q: Why choose finger scanning for identification? A: Because it's fast, accurate, cost-effective and secure.

Q: Can my fingerprint be given to anyone else? A: No. There are no fingerprint images stored. Only encrypted numerical representations of the unique points of the fingerprint are stored.

Q: Can my fingerprint data be taken off the computer and used to re-create my fingerprint? A: No. identiMetrics never takes your fingerprint, only unique points. The actual fingerprint cannot be recreated from the encrypted template.

Q: Can my fingerprints be taken from the computer software and used on another fingerprinting system? A: No. identiMetrics™ uses a proprietary algorithm that can only be used with identiMetrics software.

Q: Can my fingerprints be copied or used by anyone else? A: No. It is impossible to duplicate or falsify fingerprints from the information stored in the identiMetrics software.

Q: Can anyone get into the identiMetrics database and extract a fingerprint image or a digital template and associate it to a particular person? A: According to Dr. Stephanie Schuckers, Director for the Center for Identification Technology Research at Clarkson University, the biometric software does not store the user's fingerprint image. The images are destroyed after they are used to build a unique mathematical model using both minutia based and vector analysis. That encrypted digital template cannot be de-encrypted and decoded to obtain the minutia based template and consequently recreate the original fingerprint image.

Q: Do twins have the same fingerprints? A: No. Every person has unique fingerprints, even twins.

Q: Do finger scanners spread germs? A: According to a Purdue University study, biometric sensors are no dirtier than doorknobs.

Q: Why Biometrics in Schools? A: Many areas in an organization require identification. The most common kinds of identification currently in use are picture ID cards, PINs, and, of course, visual identification. Each of these methods creates its own issues and is a drain on time and resources.

Cards are regularly forgotten, lost, mutilated and shared; PINs are easily forgotten, swapped or stolen. Also, visual identification is a poor solution, especially with today's considerable security concerns and reporting issues. By using biometrics for identification, the problems and costs associated with the current methods can be avoided and new standards of accountability can be put into place.

Q: What about Parent privacy concerns? A: Parents need to trust both schools and the service providers that work with schools. In an effort to ensure that parents can be confident in how organizations use student data, the Future of Privacy Forum and the Software & Information Industry Association have developed a Student Privacy Pledge that education service providers are signing to show their commitment to safeguarding student privacy. identiMetrics was an early signatory of the Student Privacy Pledge www.studentprivacypledge.org.

Need more information? Please visit our website www.identiMetrics.net