



Imprivata OneSign & Finger Biometrics

Imprivata OneSign & Finger Biometrics Overview

Introduction

These days, each of us has a growing awareness of the risks involved in protecting IT-based resources from identity theft, malicious outside attacks, or generally inappropriate use. We are also seeing government and industry regulators issue strict mandates requiring companies to take significant steps to strengthen defenses against these misuses. As a result, many corporations are implementing strong multi-factor authentication policies that are much stronger than the password schemes that had been so commonplace in the past.

Strong authentication is the use of at least two factors to authenticate a user based on “what the user knows”, “what the user has”, and “who the user is”. Implementations include the use of strong password schemes, ID tokens, proximity cards, smart cards, and biometrics.

This overview outlines the advantages and complexities of using finger biometrics as one form of strong authentication.

Biometrics

Biometrics - the measurement of one or more physical or behavioral characteristics of an individual - is used to increase a system's security level dramatically without increasing the complexity. Biometric identifiers are highly reliable since they cannot be easily faked, altered, or misappropriated.

Biometric identifiers include both physical (fingerprints, hand geometry, eye patterns, facial features) and behavioral (voice prints and signatures). Behavioral identifiers are more subjective than physical identifiers. They can vary because of external conditions such as illness, and can conceivably be imitated. Physical identifiers are virtually impossible to replicate, and are considered to be the more reliable of the two identifiers.

The most technically advanced, proven and recognized physical identifier is the fingerprint. These were first used for positive personal identification more than one hundred years ago, when it was proven that each finger of every individual has a unique arrangement of ridge detail. In the years that followed, organizations throughout the world have had growing requirements for positive identification systems resistant to high technology fraud. This requirement has created increased interest in biometrics, and fingerprint technology has remained the most effective, economical, and widely used biometric identification system.

There are two basic methods of authenticating a person's identity using biometrics:

Biometric identification is a process of authenticating a person's identity by comparing measurements of some physical characteristic against ALL measurements filed in a reference database. Only biometric characteristics are used to locate the person in the reference database and confirm his or her identity. This process is often called a "one-to-many" comparison.

Biometric verification is the process of authenticating a person's identity by comparing measurements of some physical characteristic against one or a few predetermined records filed in a reference database. This process is often called “one-to-one” comparison because some demographic information is used to first find the person's record from the reference database before identity is confirmed.

Several key factors need to be considered which affect a system's biometric authentication system's performance and accuracy.

Fingers Fingerprint readings can be impacted by several factors associated with the finger itself – the density of the fingerprint, the thickness of the print's ridges, the skin's wetness/dryness, the age/sex/occupation of the person, and the physical size of the finger. Users can affect a system's accuracy simply by how they present a finger to the sensor. If they rotate the finger relative to that stored as a reference, the system must compensate by "looking harder" at the reference information to increase the confidence in the match. If the user varies his translational finger placement upon the sensor, he may not present the system with enough area of overlap with the enrolled feature maps. A lack of overlap decreases the confidence of the attempted match.

The enrollment process itself will impact a biometric authentication system's accuracy. This process must manage the quality of the stored feature information. Several impressions of each finger to be enrolled are taken, the feature information checked for internal consistency, and, finally, a live authentication is attempted so that a user can be certain that the enrollment is accepted.

Sensors As a rule of thumb, sensors which capture images at 300 DPI or higher will perform better. Most government systems work at 500 dpi range. High-end "forensic grade" systems must be at least 0.75" x 0.75" @ 500 DPI @ 128-gray levels and contain a minimum of 10-13 matching minutia points. These partial print requirements are legally acceptable for use in evidence gathering. All commercial systems work at smaller area than this. A typical user will generate between 18-35 normal print points to be matched, where some people may generate anywhere from 10 to 12 to 50+ points ... the more the better. Larger images lead to more accurate captures.

Fingerprint reading sensors vary in quality and price. Simple optical devices can be purchased at \$30/unit. However, these low-end units are susceptible to grease on platin and to dry or damp fingers. They are also susceptible to being spoofed, such as a piece of tape with toner on it. OneSign supports Upek sensors that utilize a silicon-based sensor to capture fingerprint images using active-capacitance sensing technology. Each sensor cell (pixel) contains an active capacitive feedback circuit whose effective feedback capacitance is modulated by the presence of live skin close to the surface of the sensor. This active sensing approach provides much higher immunity to parasitic effects. This ensures a higher signal-to-noise ratio and greater capacity to capture a wider range of fingerprints than other silicon-based technologies such as passive capacitive sensing.

Commercial v. Government quality levels People often associate fingerprinting with a very sophisticated, carefully monitored environment – like the Department of Motor Vehicles or the FBI. These once in a lifetime use-cases require trained personnel along with significantly more time and money spent on the technology and the process. These are considered Government-level implementations.

Fingerprint biometrics are widely used in commercial situations today where specialized training isn't required or available, and where equipment costs are much lower and the time availability for the entire fingerprint biometric processes is much less. Examples include hospitals and financial services organizations where administrators require strong authorization and maximum convenience. The introduction of built-in notebook computer sensors has recently facilitated the use of encrypted shared disk drives.

One significant difference between "government" and "commercial" usage is that commercial algorithms need to adapt to less-than-ideal circumstances than government-grade systems, including:

- Day-to-day users who are untrained and unsupervised. They want to swipe a finger once, and quickly have the system accept them.
- Lots of finger motion and distortion, even during the enrollment phase
- Administrators without biometric expertise, as a DOD or RMV official would have
- Pressure differences in the finger when pressed onto the sensor
- Moisture or humidity differences in the finger when pressed onto the sensor

WORKING WITH FINGER BIOMETRICS & ONESIGN ADVANTAGES

Background

Imprivata architects have significant experience in implementing digital fingerprint technology. Team members have implemented state-wide large-scale driver license programs in Colorado, Texas, Georgia, West Virginia and the Connecticut DSS that included finger imaging. This team has also implemented finger imaging as part of the Mexico Voter ID, Brazil Alien Identification Program, the Honduras Voter ID Program, and the Philippines Social Security System.

Features

- OneSign matches each user by correlating against known set of references, taking into account:
 - Variations in pressure and density
 - Aging or dirt induced variations in the print
 - Orientation of finger on the sensor
- OneSign's capture algorithm:
 - Captures images at higher speeds, resulting in less image blur distortion
 - Normalizes for humidity variations in the finger
 - Is "device neutral", and not associated with a specific sensor or reader
- Credentials are stored centrally, using strong security and privacy safeguards by:
 - Ensuring that each captured fingerprint image is destroyed and cannot be misused
 - Maintaining mathematical descriptions of a print's landmarks, but not the actual print itself
 - Never shipping a username with the template
 - Storing username in a double-blind alias mechanism on server
- While OneSign has been tested with a number of sensors, Imprivata integrates with and resells the Upek TouchChip USB Fingerprint Reader.

Performance

- No other ESSO vendor does biometric "Identification". Imprivata embedded high-end image processing technology into a commercial product at a price that no other competitor can match.
- OneSign's failure rate, or "False Accepts" and "False Rejects", is at a rate of <1 in 1 million reads
- OneSign has a 2.5 times higher verification speed than the next fastest competitor
- OneSign can handle a wider range of finger image presentation with higher accuracy. Most algorithms allow a finger to be +/-10 degrees off-center. OneSign supports +/- 30 degrees.

HOW DOES IT WORK? ONESIGN & FINGER BIOMETRICS

The OneSign Agent uses Imprivata Secure Exchange (ISX) technology to manage the secure sessions between the appliance and the user's enabled applications. The OneSign Agent captures and proxies all credentials, handles sign-on to enabled applications, and permits authentication of users through finger biometrics, ID tokens, smart cards, proximity cards, or passwords. Authenticated users have single sign-on access to all OneSign-enabled applications.

Enrollment

Setting Up the Capability

The OneSign administrator designates which users are authorized for finger biometric reading. The administrator then sets parameters to indicate (1) whether to allow more fingerprints to be scanned after an initial enrollment, and (2) the number of authentication attempts to allow before triggering a failure event. Lower "attempt" settings are less convenient to users, but offer higher security.

Installing Readers

Each workstation intended to implement finger biometric authentication must be equipped with a fingerprint scanner. This is a USB device that connects to the local computer and contains a transparent scanning area on which the user places the pad of the fingertip being scanned. As long as one enrolled finger is clean and unscarred, fingerprint scanning is highly reproducible and reliable. The scanner has no moving parts. The important part is the scanner window. As long as the window is clean, finger biometric authentication can be simple and reliable.

Enrolling Individual Users

Users who will be authorized for finger biometric authentication (or, for optional fingerprint identification) get an opportunity to enroll when logging into OneSign. To enroll, each user (1) logs into the computer and authenticates, (2) responds to prompts to enroll for finger biometrics, and (3) places the pad of each chosen fingertip flat on the scanning window to ensure a good scan. After three successful scans of the finger, the enrollment process is completed.

Authenticating Users

To authenticate via fingerprint scanner, a user (1) logs in via the OneSign logon window and selects "Fingerprint", (2) places the pad of an enrolled finger on the scanner's sensor area, and (3) waits for the system to acknowledge the scan. The user is authenticated after the system accepts the fingerprint.

Identifying Users

OneSign's optional Fingerprint *identification* feature identifies the user by comparing the fingerprint to all other fingerprint records. Upon unique identification, the user will be authenticated. No typing is required.

SUMMARY

Any finger biometric solution choice needs to consider the critical factors - usability and convenience, system performance, security and user privacy, and cost. The OneSign technology is the end-result of an experienced team of image processing experts delivering a secure and high-performing system for fast, everyday use.



10 Maguire Road
Building 2
Lexington, MA 02421
v 781 674 2700
f 781 674 2760

1.877.ONESIGN

Imprivata Europe
Forsyth House
77 Clarendon Road
Watford
Herts, WD17 1LE
United Kingdom
v+44 1923 813511
f+44 1923 813501

www.imprivata.com