KRONOS

DATASHEET

Privacy and the Kronos 4500 Touch ID Option

"Unlike systems used by government and law enforcement agencies, Kronos 4500 Touch ID technology does not store actual fingerprint images. Instead, it scans and converts the employee's fingerprint ***... into an encrypted mathematical representation.***"

How to Alleviate Employee Concerns

Most of us witnessed the "magic" of finger-scanning technology for the first time in the movie theater — enthralled with the spies and evil geniuses who used these space-age gizmos to gain entry to their secret chambers. Times change, however: Now finger-scanning technology is far from being the stuff of fiction. But even though finger-scanning devices have long proven themselves in the workplace and in industrial settings, an aura of mystery still manages to hover over the technology.

Wary employees

So, while the benefits of the Kronos® 4500 Touch ID™ finger-scanning option for the Kronos 4500™ terminal have been widely experienced by customers across numerous sectors of the economy, employees in some of the organizations in these sectors have raised concerns about how this apparently mysterious technology might affect their privacy. At Kronos, we take employee privacy concerns seriously. Which is why the 4500 Touch ID finger-scanning option is specifically designed to safeguard that privacy.

Kronos 4500 Touch ID: No fingerprints captured or stored

Unlike Integrated Automated Fingerprint Identification Systems (IAFIS) used by government agencies for forensic and law enforcement purposes, Kronos Touch ID technology does not store hard-copy fingerprint images. In fact, no images are stored at all with the Kronos system. Instead, the Kronos 4500 terminal equipped with the Touch ID option scans the employee's finger, then converts the fingerprint image into a mathematical representation, which it stores in an encrypted format. As a result, it's practically impossible to reproduce the original image — a fact that greatly promotes the cause of employee privacy.

Kronos 4500 Touch ID and government technology don't mix

The knowledge of the incompatibility (on several levels) of Kronos finger-scanning technology with government and law enforcement IAFIS fingerprinting devices should go a long way toward calming employees' privacy concerns. In fact, Kronos Touch ID finger-scanning technology uses a unique algorithm, resolution, and capture size. These things combine to make the encrypted fingerprint data stored in the Kronos system irresolvable by government IAFIS technology.

Alleviate employees' concerns with finger-scanning technology

Step 1:
Employees' fingerprints are scanned — not stored — before biometric data is converted.

1 0 1 1 0 1 0 1
0 1 1 0 1 0 1 1
1 1 0 1 0 0 0 1
0 0 1 0 1 1 0 0
1 0 0 1 0 1 1 0
0 1 0 0 0 1 1 1

Step 2:
The image is converted to an encrypted mathematical representation, which can't be used to re-create the actual fingerprint.

In a nutshell: Why IAFIS devices can't access Touch ID-encrypted fingerprint data

Ridge vs. minutiae algorithm	Kronos finger-scanning technology relies on the *ridge* patterns in the core of the scanned finger. IAFIS devices, on the other hand, look at the entire rolled fingertip image to capture *minutiae* points in and around the core of the fingertip.
Lower resolution	The resolution required to define the fingertip image ridge pattern for the Kronos 4500 Touch ID finger-scanning option is 160 dots per inch (dpi); this resolution is much lower than the 500 dpi required by IAFIS devices.
Smaller capture size	The Kronos terminal uses solid-state sensors with active areas of less than ¾ of an inch by ¾ of an inch. IAFIS devices, by contrast, require the full measure of the fingertip — typically a rolled fingertip image.

Of particular relevance, with respect to the incompatibility between Kronos finger-scanning and government fingerprinting technologies, are the critical differences between the ridge and minutiae algorithms used by Kronos and IAFIS devices:

- **Ridge algorithm:** Kronos finger-scanning technology preserves and enhances the ridge pattern from an employee's finger. Features such as scars, cuts, or creases are removed, since they can appear or disappear from measurement to measurement — and degrade the accuracy of the comparison.
- **Minutiae algorithm:** IAFIS devices employ minutiae-based comparison techniques — which take scars, for example, into consideration — as part of the comparison process. Since these minutiae are removed during the Kronos enhancement and compression process, the mathematical representation that serves as a template in the Kronos system is unsuitable for, and incompatible with, IAFIS identification systems.

Proof positive: concerns debunked

And finally, in addition to all the evidence offered above, academic sources have recently reduced any remaining concern over privacy, civil liberties, and even hygiene with respect to biometric and finger-scanning devices. A recent study at Purdue University found that biometric devices are less likely to transmit germs, viruses, or bacteria than the door handles employees touch again and again every day. Moreover, the study found, biometrics is actually a privacy-enhancing technology when deployed appropriately. This is particularly true in Kronos time and attendance applications where finger-scanning technology employs encryption and other techniques to protect employee labor and identity information.

FINGER SCANNING FOR ACCURACY AND INTEGRITY

In addition to promoting employee privacy, Kronos 4500 Touch ID finger-scanning technology is highly accurate and provides security measures that are extremely difficult to circumvent. For example, the fingertip sensor includes a dynamic optimization feature that provides high image resolution, which in turn produces very low false acceptance rates.

Subsurface technology. The Kronos 4500 Touch ID option uses an image-capture technology that images below the surface layer of the skin. Contrary to the case with DC capacitive technology, for example, skin surface conditions do not limit the ability of the sensor in the Touch ID-equipped Kronos 4500 terminal to capture fingertip data, because the Kronos subsurface technology captures the employee's live fingertip image from beneath the surface. Calluses, dryness, dirt, moisture, the effects of aging, and even contaminants, therefore, have little or no effect.

Anti-spoofing. What's more, with its active anti-spoofing technology, the Touch ID-equipped Kronos 4500 terminal immediately rejects fake fingers. Rubber stamps, finger molds, latex fingers, and the like are rejected instantly whenever the system's subsurface technology fails to detect an actual fingertip.

Kronos Incorporated 297 Billerica Road Chelmsford, MA 01824 +1 800 225 1561 +1 978 250 9800 www.kronos.com

More information about Kronos customer success stories may be found at **www.kronos.com/library-search.aspx.**

33802-89905