



Worried About Privacy with Biometric Technology?

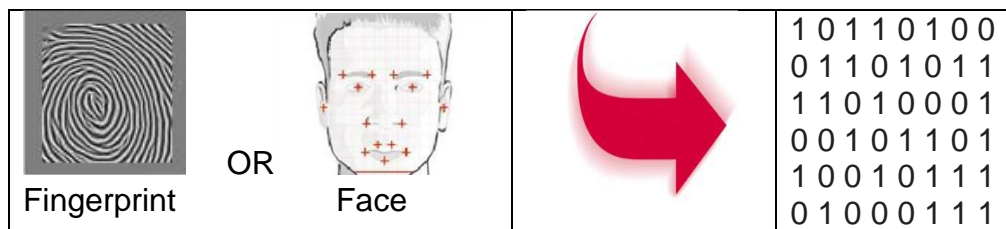
With ZKAccess, you can relax.

Biometric technology helps create more secure workplaces by verifying the identity of employees as part of the access control process.

But while the benefits of biometrics are well documented, some employees may still be concerned about the misperceived privacy issues surrounding this technology.

Fingerprint and/or Facial Recognition for the Workplace

Unlike the technology used by Automated Fingerprint Identification Systems (AFIS) for law enforcement purposes, ZKAccess' biometric devices do not capture and store actual fingerprint and face images. Instead, ZKAccess devices collect only a small sub-set of sample data (aka minutia points), convert it into binary data using mathematical algorithms and then store only a digital representation of the fingerprint and/or face (not an actual image). Having only minutia data makes it virtually impossible to recreate the original image.



Bottom-line: There are no privacy issues related to BIOMETRIC identification and verification

Proven technology

ZKAccess is committed to providing the most secure biometric solutions possible and is constantly developing & enhancing our sensor technologies and firmware which are incorporated into our security devices.

Significant differences between AFIS devices and ZKAccess devices include:


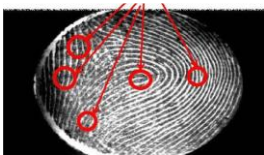

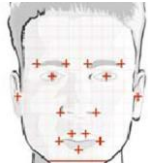
Image vs. Minutia Analysis –

ZKAccess devices rely upon only minutia data and NOT the actual image of the scanned fingerprint nor face. Conversely, AFIS-type devices use the entire rolled fingerprint image containing the ridge patterns of the fingerprint and facial images.



Image size –

ZKAccess devices use small, 3/4” x 3/4” optical sensors; AFIS devices require a full measure of the fingerprint, which is typically a rolled fingerprint image. Same with face images.

Fingerprint image	Fingerprint minutia	Face image	Face minutia
			

ZKAccess Biometrics: Accuracy and Integrity

ZKAccess biometric devices are extremely accurate and near impossible to deceive, thanks to the integrated security components within our sensors and firmware. These technologies combine to form one of the most powerful fingerprint and facial security solutions in the industry.

For maximum accuracy, ZKAccess devices have a dynamic optimization process, enabling high fingerprint and facial image resolution and quality with low false acceptance rates. Additionally, some of ZKAccess fingerprint scanners use a sub-surface multispectral imaging technology which can see beneath the outermost layer of the skin (epidermis) and view the live layer of the skin (dermis) where the true fingerprint resides. This means that conditions on the outer skin’s surface (such as calluses, dryness, dirt or contaminants, moisture, or the effects of aging) do not limit the ability of the sensor to capture fingerprint minutia data. Some scanners have anti-spoofing technology, in which a fake fingerprint (formed from rubber stamps, finger molds, latex fingers, etc.) is immediately rejected.

No fingerprint nor facial image is saved!

Fingerprint & facial images are converted to mathematical representations BEFORE storing.

Incompatible with AFIS technology

Because of the different resolution, fingerprint/facial size, and image enhancement processes of the two technologies, the fingerprint and facial data collected by a ZK device is virtually unusable by AFIS.

Accurate —

ZKAccess biometric devices ensure fast, accurate identification