M2SYS Biometric
Security Overview

A natural reaction to the use of biometric technology is the perceived risk of personal privacy invasion – what exactly is being done with my biometric information? Who can access it? How is it being used? Can it be used by an outside party?

As one of the largest biometric system providers to the commercial marketplace, M2SYS recognizes the sensitive nature of its technology. Consequently, we employ several important security features to ensure the privacy of those using the system is fully protected:

Captured images (face, fingerprint, etc..) are NOT stored, unless requested by customers

Biometric data is stored in a proprietary format unique to the M2SYS system

All biometric data is secured both in transit and at rest using AES 256-bit encryption

Advanced Encryption Standard (AES), also known as Rijndael, is a block cipher adopted as an encryption standard by the U.S. government. It is used worldwide and has been analyzed extensively, as was the case with its predecessor, the Data Encryption Standard (DES). AES was adopted by the National Institute of Standards and Technology (NIST) as U.S. FIPS PUB 197 in November 2001 after a 5-year standardization process. AES 256-bit is the most secure version of the AES algorithm, and the safest encryption standard on the planet *(www.clickssl.net/blog/256-bit-encryption)*.

When a person is enrolled in the M2SYS biometric recognition system, the software extracts the unique identification data from the captured image and stores this information in the form of a proprietary identity template. An actual copy of the captured image itself is NOT stored (unless requested by customers). The system then uses the identity template to recognize that person on an ongoing basis. The identity template is simply a binary data file that cannot be used to reconstruct the original image. Without a copy of the image itself, no one could perform analysis or comparison of the biometric data stored within the M2SYS system.