

Fully Secured Fingerprint Recognition, PERIOD.

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? How can it be used by an outside party?

As one of the largest fingerprint recognition 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:

- Fingerprint images are **NOT** stored
- Fingerprint data is stored in a **proprietary format** unique to the M2SYS system
- All fingerprint data is stored using **the AES 128 bit encryption** algorithm

Advanced Encryption Standard (AES), also known as Rijndael, is a block cipher adopted as an encryption standard by the U.S. government. It is expected to be 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.

When a person is enrolled in the M2SYS fingerprint recognition system, the software extracts the person's unique identification data (minutiae) and stores this information in the form of a proprietary identity template. An actual copy of the fingerprint image itself is NOT stored. The system then uses the identity template to recognize that person on an ongoing basis. The identity template is simply a data file, a series of zeros and ones that cannot be used to reconstruct the actual fingerprint image. Without a copy of the image itself, no one could perform analysis or comparison of the fingerprint.

To learn more about this topic and the steps M2SYS is taking to protect personal information, please contact your Account Executive.

