ADVANTAGES

AES 256-bit Encryption & RSA Algorithm

AES 256-bit Encryption & RSA Algorithm

Integrated Biometrics' integration of 256-bit AES encryption and the RSA Algorithm ensures that biometric data captured by IB scanners is protected by one of the most robust encryption standards available. This enhancement offers customers:

- **Enhanced Data Security:** The 256-bit AES encryption safeguards sensitive biometric information, protecting it from unauthorized access and ensuring compliance with stringent data protection regulations.
- **Increased Trust and Reliability:** By securing data at the point of acquisition and during transmission, customers can confidently deploy scanners in high-stakes environments like law enforcement, border control, and financial services.

Encryption provides communications between the scanner and external devices or applications using 256-bit AES keys and RSA algorithms. This closed loop approach protects biometric data at the point of acquisition, across field wiring, and into the host application. By combining private/public key structures, and industry best practices, this ensures that sensitive personal information receives the highest level of scanner encryption currently available.

Encrypted IB scanners also protect against physical tampering. Each scanner contains a unique calibration file installed in each serialized unit during production. Attempts to disassemble security protections by disassembling the unit or inappropriately accessing the hardware alters the device's calibration, rendering that device's imagery unacceptable.

The AES Standard

The AES (Advanced Encryption Standard) was created and adopted by the US National Institute of Standards and Technology (NIST) to protect sensitive information, particularly against the increasingly prevalent brute force attacks. Adopted in 2002, AES replaced the outdated and vulnerable Data Encryption Standard (DES). Though originally developed by the US government, AES encryption is now the industry standard for commercial and personal data security

AES: How it Works

AES (Advanced Encryption Standard) is a symmetric block cipher that encrypts data in blocks of 128 bits using keys of 128, 192, or 256 bits. These "pieces' of data are encrypted numerous times, and multiple changes are made to the bits, including swapping, mixing in plain text and rearranging, to make the data harder to decrypt without the correct key.

Though multiple variations of AES exist, AES-256 provides the highest level of security. AES-256 uses a 256-bit key length for encryption and decryption, resulting in 14 rounds of encryption with 1.1 x 1077 different potential combinations. AES-128 uses a shorter 128-bit length key and applies 10 rounds of encryption, making it less secure. Many applications still use AES-128. IB encourages clients that need data security to confirm that AES-256 is being utilized.

In addition to security, AES-256 is efficient and suitable for large volumes of data.

The RSA Algorithm

To provide even greater security, Integrated Biometrics uses RSA (Rivest–Shamir–Adleman), an asymmetric encryption, for the secure key exchange. Unlike AES, a symmetric algorithm that uses the same key for encryption and decryption, RSA uses a public key for encryption and a private key for decryption.

This hybrid approach enhances security and performance; RSA provides the secure key exchange, while AES efficiently encrypts the actual data.

Encryption is available with Integrated Biometrics' Kojak, Five-0, Danno and Watson scanners.