# Key File Generation Requirements

## **(3M Confidential)**

## Customer provided

**Key ring**: The encrypted key ring of size 256\*size (256) bits in binary format. There are 256 keys in the key ring. The encrypted key ring is generated by encrypting the plain text key ring using 256 bit AES (Advanced Encryption Standard) with CBC (Cipher Block Chaining). If desired, customers can generate their own key ring and encrypt it with their Key and IV (initialization vector). The key should be 32 bytes (256 bits), IV should be 16 bytes (128 bits). Customer then sends the encrypted key ring to 3M for creating key files. When importing key files in readers, the Key and IV (used when generating customer key ring) need to be specified. The total key ring size includes 16 bytes of AES residue for a total of 8208 bytes.

**sig2**: The signature of the key ring, an 8 bit CRC (CRC-8-CCITT) of the plain text key ring. The CRC is initialized to zero. CRC-8-CCITT specifies use of polynomial x^8 + x^2 + x^1 + x^0 which is represented by value 0x107.

**Key:** a hex-encoded ASCII string (64 characters long) of the 32-byte customer key used to encrypt the key ring. More information is needed in how to securely transfer this data to 3M.

**IV: initialization vector** a hex-encoded ASCII string (32 characters long) containing the 16-byte customer IV used to encrypt the key ring. More information is needed in how to securely transfer this data to 3M.

List of reader MAC addresses that will read secure tags (or 3M provided based on reader order data).

TID mask and value (or provided by 3M based on tag order information)

Password authentication (enabled or not enabled)

Tag filter enable (3M recommended usage)

EPC flags (permalock, write lock)

User block flags (permalock, write lock, read lock). Each block is 64 bits (4 words). There are eight blocks, 0-7, with Block 0 reserved for tag security and always write protected. Each block can have a unique setting for read lock or permalock but if block 0 is write locked, all user blocks are write locked.

## 3M internally provided

Key file labeling

Key ring ID

Configuration command file based on above parameters

## 3M supplied to customer

Signed key ring file for importing into the reader