INTRODUCING

machineQ SECURITY

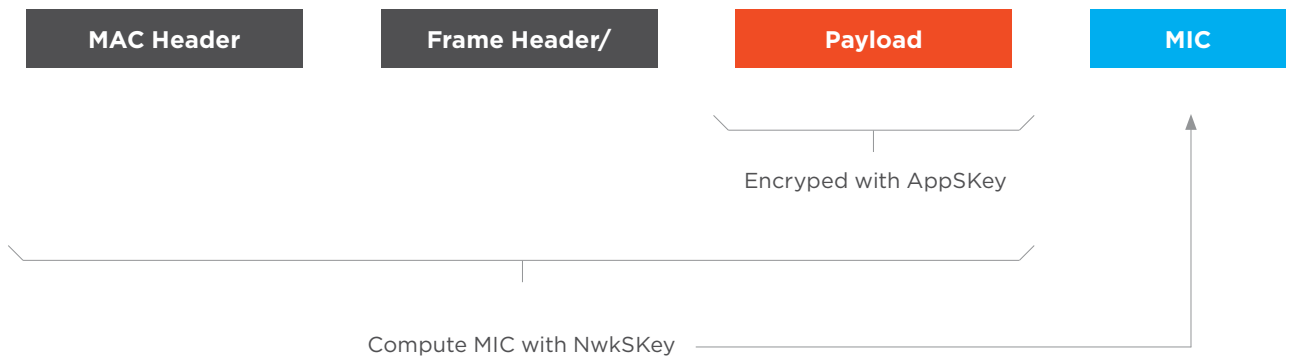
DESIGNED INTO THE SYSTEM AS A TOP PRIORITY

IoT customers will be building their businesses on their IoT systems. These systems need to be robust, secure, and resilient. machineQ combines the world class end to end security design of the LoRaWAN standard with industry best practices on each element to provide the best possible security and data integrity to our customers.

The National Institute of Standards and Technology (NIST) recommendation for key management approves AES-128 bit encryption beyond 2031. This is the same level of recommendation for AES-256 and the strongest recommendation they offer.
-NIST Special Publication 800-57 Part 1 Revision 4: Recommendation for Key Management Part 1: General

LoRaWAN end to end security model protects the data in flight

- ✓ 128 bit AES encryption and authentication applied on a per-device basis
- ✓ Two independent master keys: one for the network payload (NwkKey) and one for the application payload (AppKey).
- ✓ In LoRaWAN 1.1, the customer can choose to manage her own application keys, and nobody else can access the decrypted data. She can also choose to delegate key management to machineQ.
- ✓ Each device is individually keyed, reducing the attack surface and increasing resiliency



Backend Systems Security protects the systems that process the data

- ✓ Leveraging Comcast's vast experience running Carrier Grade systems
- ✓ HTTPS and VPN technologies are used for securing the communication among these critical infrastructure elements