**Cyber Security**

The requirements listed below will conform to the air interface protocol requirements in mission critical security standards including IEC-62443, CIP 005-5, DO-377 SER-08 and FIPS 140-3

1. The air interface protocol shall support the following options for data encryption/decryption algorithms and key sizes (amendment to 802.16-2017, section 7.5.1):

|  |  |  |  |
| --- | --- | --- | --- |
| Algorithm | Mode | key length | Reference in 802.16-2017 |
| AES (NIST.FIPS.197) | CBC (NIST.SP.800-38A) | 128, 192, 256 | Add to 802.16 |
|  | CCM / CTR (NIST.SP.800-38C) | 128,  Add: 192, 256 | 7.5.1.2, 7. 5.1.3 |
|  | GCM (NIST.SP.800-38D) | 128, 192, 256 | Add to 802.16 |
|  | XTS-AES (NIST.SP.800-38E) | 128,  Add: 192, 256 | Add to 802.16 |
|  | CBC with key wrapping (NIST.SP.800-38F) | 128, 192, 256 | 7.5.1.4 |
| DES | Remove option |  | 7.5.1.1 |

1. The air interface protocol shall support the following algorithms options for TEK encryption (amendment to 802.16-2017, section 7.5.2)

|  |  |  |  |
| --- | --- | --- | --- |
| Algorithm | Mode | key length | Reference in 802.16-2017 |
| TDEA (3-DES)  NIST.SP.800-67r2 | CBC (NIST.SP.800-38A/F)  Disallowed after 2023 | 128 | 7.5.2.1 |
| RSA |  | 1024  Add: 2048, 4096 | 7.5.2.2 |
| AES (NIST.FIPS.197) | ECB (NIST.SP.800-38A) | 128,  Add: 192, 256 | 7.5.2.3 |
|  | CBC with key wrapping (NIST.SP.800-38F) | 128, 192, 256 | 7.5.2.4 |

1. The air interface protocol shall support HMAC authentication with 112 bits key length or higher. HMAC (amendment to 802.16-2017, section 7.5.3) shall be calculated using SHA-2 (NIST.FIPS.180-4) or SHA-3 (NIST.FIPS.202) with key length ≥224
2. The air interface protocol shall support CMAC-AES or GMAC-AES for message authentication.
3. The air interface protocol shall support the following public key encryption/decryption algorithm options for AK encryption (amendment to 802.16-2017, section 7.5.8):

|  |  |  |
| --- | --- | --- |
| Algorithm | Key length | Reference in 802.16-2017 |
| RSA | Remove: 1024,  Add: 2048, 4096 | 7.5.8 |
| ECC | 224 or higher | Add to protocol |

1. Key management: the air interface protocol shall support PKMv2 (amendment to 802.16-2017, section 7.2.2). It will not support PKMv1 only (amendment to 802.16-2017, section 7.2.1)
2. Authentication mode (amendment to 802.16-2017, section 7.8.2): mutual authentication mode will be used. The base station shall send its X.509 certificate in the Authorization Reply message.

**Glossary**

|  |  |  |
| --- | --- | --- |
| **ACRONYMS** | **Acronym Expansion** | **Definition** |
| AES | Advanced Encryption Standard | A U.S. government approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information.  SOURCE: FIPS 197 |
| AMTS | Automated Maritime Telecommunications System | A commercial mobile radio service in the USA. It offers voice and data communications to maritime customers. |
| CIP 005-5 | Critical Infrastructure Protection 005-5 | An electronic security perimeter around cyber assets. |
| DES | Data Encryption Standard | A symmetric block cipher algorithm for the encryption of digital data. |
| ECC | Elliptic-curve cryptography | Asymmetric public key cryptographic methods used for authentication and encryption |
| FIPS 140-3 | Federal Information Processing Standard 140-3 | Security requirements for cryptographic modules. |
| HMAC | Hash-based message authentication code | A message authentication code with cryptographic hash function and a secret cryptographic key. |
| IEC-62443 | International Electrotechnical Commission-62443 | A set of security standards used to defend industrial networks from cyber threats. |
| RSA | Rivest–Shamir–Adleman | An asymmetric public key signature algorithm that may also be used for encryption and decryption. |
| SHA | Security Hash Algorithm | A family of cryptographic hash functions. |