EN 18031-1 clause	Mapped EN 303 645 clause(s)	Requirement (paraphrased)	Y / N / NA	Notes / evidence
ACM-1	5.5-4, 5.5-5	Use access-control mechanisms to protect security and network assets	Y	
ACM-2	5.5-5, 5.6-7	Enforce least-privilege security configuration	Y	
AUM-1	5.5-4, 5.5-5	Access control mechanisms required per ACM-1 shall use authentication mechanisms	Y	
AUM-2	5.1-3	Authentication has at least one element of the categories knowledge, possession and inherence (one factor authentication).	Y	
AUM-3	N/A	Validate all relevant properties of the used authenticators	Y	Crypto / checksum fails on incomplete auth
AUM-4	5.1-4	Allow changes to authentication mechanisms, including tokens	Y	
AUM-5	5.1-2, 5.1-3	Enforce strong secrets (length, complexity) and use best-practice cryptography	Y	
AUM-6	5.1-5	Throttle or lock out after repeated authentication failures	Y	aum6.js, maximum brute force speed 1 / s
SUM-1	5.3-1, 5.3-2, 5.3-15	Implement secure update mechanisms for components, including replacement strategy	Y	
SUM-2	5.3-9, 5.3-10	Guarantee authenticity and integrity of updates, especially via network	Y	
SUM-3	5.3-3, 5.3-4, 5.3-5, 5.3-6	Provide automatic, user-transparent update processes with periodic checks	Y	
SSM-1	5.4-1, 5.6-3	Use secure storage for security assets and protect them physically	Y*	Security through physical means, e.g. access controlled office or home
SSM-2	5.4-1, 5.4-2	Protect security parameters against tampering and ensure integrity	Y*	Security through physical means, e.g. access controlled office or home
SSM-3	5.4-1	Ensure secure storage mechanisms for all security parameters	Y*	Security through physical means, e.g. access controlled office or home
SCM-1	5.5-6, 5.5-7	Secure communication mechanisms for communicating security assets and network assets with other entities via network interfaces	Y	
SCM-2	N/A	Apply best practices to protect the integrity and authenticity of the security assets communicated	Y	Public-key + symmetric cryptography for sensitive assets
SCM-3	5.5-6, 5.5-7	Encrypt critical security parameters during transmission	Y	
SCM-4	5.5-1	Use cryptography resilient against replay attacks	Y	
RLM-1	5.9-1	Design resilience against DoS and support graceful degradation	Y	
NMM-1	N/A	Implement network monitoring and detection mechanisms	Y	Data from relayed devices is aggregated to a constant interval / size
TCM-1	N/A	Rate-limit traffic to prevent resource abuse	Y	Traffic separation from BLE to IP traffic, data aggregated rather than forwarded as-is
CCK-1	N/A	Cryptographic credential minimum strength	Y**	CCKs that are solely used by a specific security mechanism excepted, 64 bit password / signing root. Signed messages time-limited (forward secrecy)
CCK-2	5.1-3	Generation of confidential cryptographic keys shall adhere to best practice cryptography	Y	
CCK-3	5.1-1, 5.4-4	Ensure credentials are unique	Y	
GEC-1	5.2-1, 5.2-2, 5.2-3	Implement secure development lifecycle processes	Y	
GEC-2	5.6-1, 5.6-5	Limit exposure of services via related network interfaces	Y	
GEC-3	N/A	Optional network interfaces / services can be disabled	Y	Configuration UI can be disabled, all services configurable
GEC-4	N/A	Documentation of exposed network interfaces and services	Y	https://docs.ruuvi.com/gw-open-ports-services If document is moved, contact support@ruuvi.com for up to date address
GEC-5	5.6-1, 5.6-3	Disable unused functionality and secure physical interfaces	Y	
GEC-6	5.13-1	Validate inputs to prevent improper data	Y	
CRY-1	5.1-3, 5.3-7, 5.5-1, 5.5-2, 5.5-3	Use reviewed cryptography, support crypto agility, and secure communications/updates	Y	

* Product is open source Bluetooth Gateway, installing and running custom software is a core feature of the product. Attacker with physical access can install a firmware to print out security assets