ETSI EN 303 645 clause	Mandatory, Recommendation, Conditional	Requirement (paraphrased)	Status	Notes / evidence
5.0-1	M	Provide a mechanism for reporting security implementation details	Y	This document
5.1-1	M	Ensure no device ships with a universal default password	Y	64-bit random password
5.1-2	M	Generate unique default passwords using a CSPRNG	Y	https://devzone.nordicsemi.com/f/nordic-q-a/66858/is-device-id-in-nrf52832-random-generated-fips-compliant-as-nrf51822/294795
5.1-2A	R	Passwords should not be used for machine-to-machine authentication	Y	64-bit random password
5.1-3	M	Enforce best-practice cryptography for authentication secrets	Y	Asymmetric + symmetric crypto for authentication, messaging sensitive information
5.1-4	M	Allow users to change authentication credentials securely	Y	Browser-based UI for changing authentication
5.1-5	M	Protect against brute-force attacks (e.g., lockout, rate-limit)	Y	Ratelimited by processing capacity of device to ~1/s attempts
5.2-1	M	Implement a vulnerability reporting process	Y	Vulnerability Disclosure Policy is published at manufacturer website
5.2-2	R	Disclosed vulnerabilities should be acted on in a timely manner	Y	VDP governs response times to reports
5.2-3	R	Document and track incoming vulnerability reports	Y	Static analysis of software supply chain against known CVEs
5.3-1	R	Ensure update mechanisms are available	Y	Bootloader, updates over the internet or over USB
5.3-2	M	Secure updates unless constraints prohibit them	Y	Software updates are downloaded over DNS + TLS protected sources, ”integrity protected communication channel”
5.3-3	M	Make update process simple from a user perspective	Y	Browser UI + automatic updates by default
5.3-4A	R	Support automatic updates without user intervention	Y	Automatic download of updates by default
5.3-4B	R	Automated update at initialisation after user consent	Y	Browser setup wizards checks for and asks for permission to install update
5.3-5	R	Check for updates on startup and periodically	Y	12 hr check cycle
5.3-6A	R	User should be able to enable and disable the automatic update mechanism	Y	Browser UI allows for maintenance windows, disable, enable, custom FW, beta updates
5.3-6B	R (C)	Notify user on update failures	N/A	Updates are not notified, not applicable
5.3-7	M	Use cryptographic mechanisms to verify updates	Y	SSL / TLS is used as a core component of firmware updates
5.3-8	M	Security updates shall be timely	Y	Updates can be made available in 12 hours to all devices configured to accept autoupdates
5.3-9	R	Ensure authenticity and integrity of updates	Y	See 5.3-10
5.3-10	M	Verify authenticity/integrity of network-delivered updates	Y	Trust relationship is established through authenticated communication channel, DNS + TLS
5.3-11	R	Inform user that a security update is required	N	There is no separate information channel for updates; updates are automatic unless disabled
5.3-12	R	Notify when update will disrupt the basic functioning of the device.	N	There is no separate information channel for updates; if necessary users can be emailed of maintenance window
5.3-13	M	The manufacturer shall publish defined support period	Y	Lifecycle promises are maintained in manufacturer website
5.3-14	R (C)	For devices that cannot have their software updated, the rationale for the absence of software updates, should be published	N/A	Software is updateable, N/A
5.3-15A	R (C)	For devices that cannot have their software updated, the device should be isolable	N/A	Software is updateable, N/A
5.3-15B	R (C)	For devices that cannot have their software updated, The hardware should be replaceable	N/A	Software is updateable, N/A
5.3-16	M	The model designation of the device shall be recognizable	Y	Only one model in product series
5.4-1	M	Securely store sensitive security parameters	N	Security of sensitive parameters depends on physical security of device
5.4-2	M	Hard-coded unique per device identity resists tampering	Y	Identity is based on read-only register, authenticated on backend
5.4-3	M	Hard-coded critical security parameters source code shall not be used	Y	
5.4-4	M	Ensure uniqueness of security parameters	Y	See 5-1
5.5-1	M	Encrypt all sensitive communications	Y	
5.5-2	R	Prefer evaluated cryptographic modules	Y	Mbed-tls API is certified, https://products.psacertified.org/products/mbed-tls. Backend implementations are not certified
5.5-3	R	Support crypto-agility to replace algorithms	Y	Hardware implementations can be replaced with generic SW implementations
5.5-4	R	Use access-control to protect network and security assets	Y	Secure-by-default configuration
5.5-5	M	Security-relevant changes in configuration via a network interface shall only be accessible after authentication	Y	
5.5-6	R	Encrypt critical security parameters in transit	Y	
5.5-7	M	Protect confidentiality of critical security parameters	Y	Critical security parameters are no accessible over network
5.5-8	M	Secure management processes for critical security parameters	Y	Security parameters are not transmitted over network in normal use; encrypted registration; encrypted at rest database
5.6-1	M	Disable all unnecessary services and ports	Y	
5.6-2	M	Network interfaces minimize the disclosure of security information.	N	Version information is accessible without authentication
5.6-3	R	Protect physical interfaces from unauthorized access	Y	USB interface is accessible for debug and intentional custom firmware uploads
5.6-4A	M	Logical debug interfaces shall be disabled or protected	Y	No networked debug interface available
5.6-4B	R	Debug interfaces that are physical ports should be physically protected by the device	Y	USB interface is accessible for debug and intentional custom firmware uploads, other physical ports require opening of enclosure with
5.6-5	R	Restrict device functionality to intended use only	Y	Constrained device
5.6-6	R	Code should be minimized to the functionality necessary	Y	Constrained device, compile flags for used features
5.6-7	R	Software should run with least necessary privileges	N/A	Constrained device
5.6-8	R	Include a hardware-level access control mechanism for memory	N	
5.6-9	R	Follow secure development processes	Y	CI/CD, unit, integration and manual testing, security scans, version control
5.7-1	R	Device should verify its software	N	
5.7-2	R	Alert if an unauthorized change is detected	N	
5.8-1	R	Data transiting between the device and associated services should be protected with best practice cryptography	Y	
5.8-2	M	Sensitive data transiting between the device and associated services should be protected with best practice cryptography	N/A	Data is not sensitive, but protected as per 5-8.1
5.8-3	M	All external sensing capabilities shall be documented	Y	Bluetooth gateway, collection is documented and configurable
5.9-1	R	Design systems to be resilient to outages	Y	Watchdogs, persistent memory, rollback of update on error
5.9-2	R	Provide fallback functionality during network failure	N	Local access remains, data collected during outage is lost
5.9-3	R	Device should connect to networks in an orderly fashion	Y	Retries present similar load profile as normal operation
5.10-1	R	Collect and analyze system telemetry	Y	
5.11-1	M	Allow users to delete their data easily	Y	Factory reset button
5.11-2	R	Provide tools for complete data erasure from associated service	Y	Delete account -function
5.11-3	R	Notify users how to delete their data	Y	Account deletion is displayed in account setting page
5.11-4	R	Confirm data deletion success	Y	LED signals on factory reset, delete success page on service data deletion
5.12-1	R	Simplify device installation processes	Y	Plug’n’play installation, minimal configuration and advanced configuration options
5.12-2	R	Provide users with guidance on how to securely set up their device	Y	Browser-based UI guides users through setup, plug’n’play is secure by default
5.12-3	R	Guide users on how to check whether their device is securely set up	Y	Browser-based UI explains security implications of settings, secure by default
5.13-1A	M	Validate input conforms to expected format	Y	
5.13-1B	M	Reject malformed or malicious inputs	Y	
6.1	M	Provide consumers personal data policy	Y	Privacy policy is available at manufacturer’s website
6.2	M (C)	Device shall acquire consent to process personal data	N/A	Personal data is not processed
6.3A	M (C)	Users can withdraw their data processing consent	N/A	Personal data is not processed
6.3B	M (C)	Store information about data processing consent	N/A	Personal data is not processed
6.4	R	Limit personal data in telemetry	Y	Telemetry data is anonymized
6.5	M	Provide users information about telemetry data	Y	Privacy policy contains section about telemetry data
6.6	M	Pseudonymize personal data where possible	Y	See 6-4
6.7	R (C)	When personal data is collected for aggregation, collected data retention period should be minimized	N/A	Personal data is not processed
6.8	R (C)	Data anonymisation protects private data	N/A	Personal data is not processed