DECT NR+ PROTOCOL STACK · NORDIC NRF9151

BFi91NR7DLCVG

MAC, DLC and Convergence layers as one product. ETSI specifies them separately; we deliver them as a single device — one radio timeline, one set of counters, one service surface. Written to ETSI TS 103 636 V2.2.1 (Release 2) and licensed as software IP for the Nordic nRF9151 System-in-Package.

TS 103 636	MAC → CVG	31%	55%	915 / 1.9
V2.2.1 RELEASE 2	ONE PRODUCT	OF 1 MB FLASH	OF 256 KB RAM	MHZ & GHZ NR+

MEASURED ON OUR REFERENCE BUILD

541 µs
Security processing / PDU
AES-128 CMAC integrity and AES-128 CTR ciphering, hardware-accelerated.

22 ms
Delivery confirmation, typical
Per SDU, acknowledged send: 22 ms average, 14 ms best, 94 ms worst. One delivery result per accepted send — success or failure, never silence.

39–43 ms
Make-before-break handover
No link downtime. The new link is up before the old one goes.

4 s
Discovery → association
Cross-channel. A device that wakes on the wrong channel finds the cluster itself.

0
Idle CPU wake-ups
With no active role the stack does not wake the application core at all.

64
Associations per node
Up to six granted data channels; further peers join as RACH-only members with a working uplink.

Every platform measures differently. These figures come from our own reference build on the nRF9151 and move as the stack changes. Silicon revision, build profile, clock and power configuration, antenna and RF environment, host interface and your own application load all shift them, in either direction. What governs for a given product is what is measured on that product. They are not protocol conformance results and carry no regulatory meaning. The firmware is under continuous optimisation, so these figures can change without notice; the version shipped with an order, and the datasheet issued against it, are what govern.

FAILURE SEMANTICS

A link that loses a message without saying so is usable for telemetry and unusable for anything that must act on what it receives. The stack is built so the layer above always knows where it stands.

Exactly one result per send
Every accepted send returns one delivery result. Not zero, not two. No application has to infer from a timeout whether something arrived.

No silent-drop path
No code path discards a packet without reporting it. Losses are visible, with a reason attached, everywhere they can occur.

Integrity measured on air
Security Mode 1 verified on captured traffic rather than assumed from source. NIST SP 800-38A/38B known-answer tests run through the production cipher path.

Counters survive a reboot
Cipher counters stay unique across power cycles; a restarted device never reuses a spent keystream. Absence of reuse is measured on the ciphertext.

What this is, and what it is not. These are the delivery and failure semantics an IEC 61508-style black channel needs from the transport beneath it. The channel makes no safety claim of its own and holds no functional-safety certification; it gives an end-to-end integrity protocol what that protocol needs in order to make its own claim.

PROTOCOL CAPABILITY

MAC (TS 103 636-4)	All 13 clause-5 procedure groups exercised on air. Fixed and portable termination roles, and both at once as a mesh relay.
Access	Random access with contention-window backoff; scheduled access with per-link grants and repetition; HARQ with closed-loop feedback, redundancy-version cycling and a bounded give-up.
Mobility & mesh	Neighbour tracking, count-to-trigger and make-before-break handover. Relaying with route cost and source routing; group assignment, paging and reconfiguration.
Cognitive radio	The operating channel is measured continuously; a cluster that finds it loaded announces a move and takes its devices with it. Load and occupancy are reported to associated devices.
DLC (TS 103 636-5)	Service types 0–3 with segmentation, reassembly and lifetime control. Implicit ARQ over the MAC's HARQ results.
Routing services	Uplink to a backend, downlink, RD-to-RD flooding with a hop budget, and Selective Source Routing.
Convergence	Service types 0–4 with flow-control windows and full ARQ feedback carrying segment-level NACKs. Endpoint and Mux-Tag multiplexing in both wire forms; duplicate removal and in-sequence delivery.
Security	Security Mode 1 per flow: AES-128 CMAC integrity and AES-128 CTR ciphering, hardware-accelerated through the secure-side crypto service.
Access profile	TS 103 874-2 (AP2) V2.1.1 — Table 7.1-1 mandatory set, Secure Joining (10.3) end to end. Configuration Data Distribution (Annex C) verified including relay leg and offline self-heal.
Bands	Band 1 (1880–1900 MHz) and Band 4 (902–928 MHz) both air-verified from the same image; the band group is a start-up parameter. Licence-exempt — no base station, no operator, no SIM. Throughput and range at 915 MHz not yet characterised.
Verified on air	43/43 applicable TS 104 047-2 MAC test purposes; 8/8 DLC and 4/4 CVG purposes. Star, tree at depth 2 and chain at depth 3 with end-to-end security through two keyless relays. Not verified beyond depth 3. TS 104 047-1 not claimed.

TWO WAYS TO INTEGRATE

On the nRF9151 itself

A C API for applications running on the SiP's own 64 MHz Cortex-M33. Your code and the stack share the part; nothing else is needed in the design.

Beside your own MCU

A byte-addressable register map over UART at 1 Mbaud, CRC-protected. Your host keeps its architecture, toolchain and application — the radio becomes a peripheral it reads and writes. No Nordic toolchain required on your side. SPI slave planned.

RESOURCES AND BUILD PROFILES

Embedded profile	31% of the part's flash and 55% of its RAM, application and TF-M together. No host interface, console or logging.
Companion-chip profile	34% of flash and 57% of RAM, adding the UART host register map. Your application runs on your own MCU.
Allocation	No heap allocation anywhere in the data plane. Link, grant, scheduler and buffer pools are fixed at build time.
Target	Nordic nRF9151 System-in-Package — 1 MB flash, 256 KB RAM. Percentages are of the whole part.

APPLICATIONS

- Mission-critical transport carrying an end-to-end integrity protocol as a black channel — industrial safety, transaction integrity
- Industrial sensor and actuator networks
- Automated guided vehicles and mobile robotics
- Utility metering and smart energy; building and infrastructure monitoring
- Intercom-class voice and alarm devices; mesh telemetry over extended sites

WHERE THIS STANDS

The stack is written to ETSI TS 103 636 Release 2 and has been exercised against the corresponding test specification on our own bench, including against interference sources and passive monitors we build ourselves. It has **not** been submitted for formal conformance testing. Nothing in this document is a claim of protocol conformance, interoperability certification or regulatory approval.

Full specification, under NDA

This brief is the public summary. The complete product specification — per-mode memory tables, measured timing tables with the test report behind each row, the clause coverage audit, integration guides and the host register map — is released under a mutual non-disclosure agreement.

Request it at **flsemi.us** — select **DECT NR+ MAC IP** and tick **Send the full specification under NDA**. We reply with a mutual NDA; the specification follows once it is signed.