CENTRI Protected Sessions

IoT Data Protection from Creation to Consumption

CENTRI Protected Sessions – Secure your IoT data from creation to consumption, through every mile along the way. Protected Sessions changes the game by giving you data security for bi-directional communications while freeing you from the limitations of multiple network protocols and a mixed IoT topology. Session lifecycles are IoT-friendly by design – by working within the constraints of low-power MCU devices using low-power networks that may have intermittent network access, Protected Sessions can maintain the security of your communications channel through lifespans from seconds to months! Using heavyweight industry-standard encryption, CENTRI Protected Sessions is optimized for lightweight devices with data compression and a tiny footprint, providing both security and efficiency between the endpoint device and the back of the cloud.

Advantages of Protected Sessions

EVERY MILE SECURITY – Protected Sessions secures bi-directional communications between your IoT devices and your application server/cloud. Keep your data safe while it is in transition through gateways, compute engines, and midpoint/fog devices in-between encrypted network segments.

NETWORK AGNOSTIC – Runs across ANY network or combination of different networks/protocols. And because it only requires integration at the two ends, the device and the application server, you can change out network topologies without re-coding your Protected Sessions implementation.

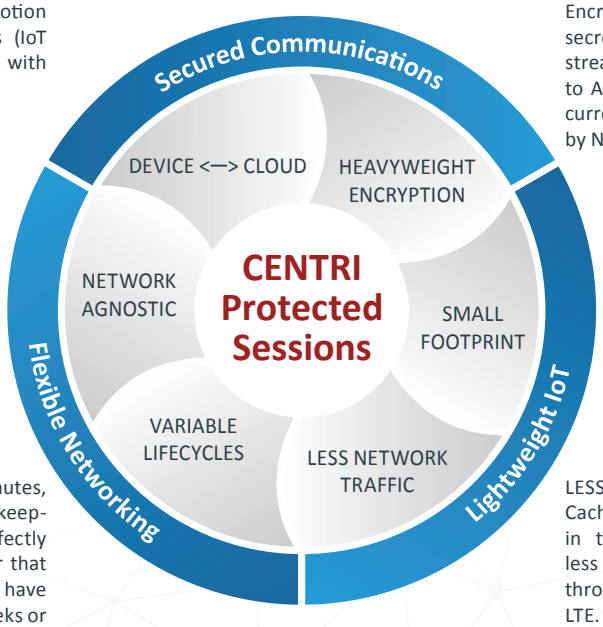
IoT-SIZED – Small footprint libraries and session lifecycles that fit the unique requirements of IoT devices and networks with intermittent connectivity. Set your session length to seconds, minutes, hours, days, months, or even the total number of data transmissions – flexible variables coupled with low-latency help extend battery life.

FOR IoT DEVELOPERS – Simple, straight forward security. Endpoint libraries for your embedded device and session manager libraries for your application server provide flexible, easy-to-use, consistent interfaces in multiple C-based languages.

DEVICE <—> CLOUD – Full security for bi-directional communications protects your data both in motion and at rest, between two secure endpoints (IoT device and application server). Authentication with hardware ID on IoT device.

NETWORK AGNOSTIC – No network or protocol dependency allows for unlimited flexibility. Works across any combination of networks, protocols, hubs – standard or proprietary. BLE, LTE, MQTT(S), TLS, HTTP(S), WiFi, cURL, SCP, FTP(S), File Sharing, USB, Thread, LoRa, Zigbee, Z-Wave, etc.

VARIABLE SESSION LIFECYCLES – Seconds, minutes, hours, days, weeks, or even months. With no keep-alives, sessions can have lifecycles that fit perfectly with the unique requirements of IoT. A sensor that powers its antenna only once per hour can now have a persistent protected session that lasts for weeks or even months. Perfect for networks with intermittent connectivity.



HEAVYWEIGHT ENCRYPTION – Industry Standard Encryption. ECHDE key exchange, perfect forward secrecy, SHA-512 Symmetric Session Keys. Salsa20 streaming cypher perfect for IoT and equivalent to AES-128 (Salsa20 has never been broken and is currently used by Google, Apple, EU, recommended by NIST, NSA, etc.).

SMALL FOOTPRINT – Designed for small IoT devices, libraries run on Arm Cortex M4 MCUs and need only ~26K FlashROM and ~10K RAM. Reduce your battery usage with highly optimized CENTRI libraries (hand optimized assembly for Arm) and reduce your network operating expenses (LTE, etc.) through CENTRI's patented single-pass encryption plus compression.

LESS NETWORK TRAFFIC – Patented Single-Pass Cache-Mapped Encryption & Compression occurs in tandem (parallel not serial), requires ~40% less bandwidth than BLE, TLS, and creates faster throughput while lowering operating costs over LTE. Initial handshake completed in one roundtrip of ~550 bytes.

CENTRI
Advanced Security for IoT

DATASHEET
Protected Sessions

Protected Sessions Uses Widely Accepted Cryptographic Standards

Device Identity	Key Exchange	Data Encryption	Key Derivation Function
Hardware-based ID to guarantee IoT device authenticity	Elliptic Curve Diffie-Hellman Cryptography (ECDH) 25519 used by Apple iOS	Salsa20 symmetric key cipher certified by EU eStream	SHA-512 (FIPS 180-2 publication) cryptographic hash function designed by the National Security Agency

Heavyweight First/Last Mile and Every Mile In-Between Security for Lightweight IoT

SECURE DATA ON YOUR ENDPOINT DEVICE

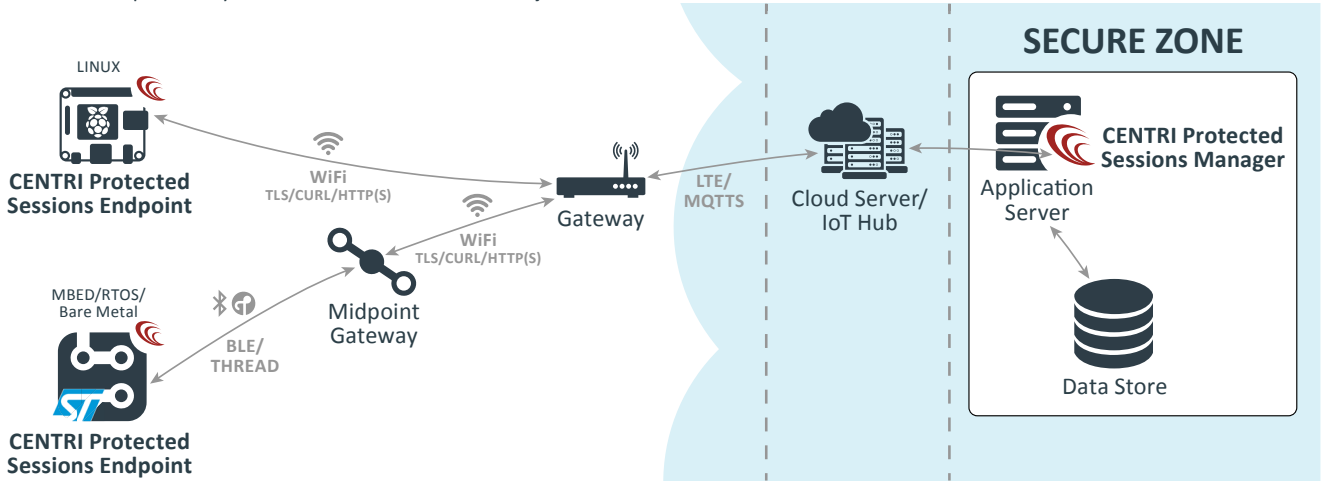
Low power, small devices, even without TCP/IP stacks – Protected Sessions keeps your data secured within any communications environment. Data can be protected immediately following creation before it even hits the first network leg. ***True first mile security.***

SECURE TRANSMISSION WITHIN COMMUNICATIONS CHANNEL

Regardless of which network(s) exist in-between your IoT device and application server, your data is protected both in transit and while it is being transferred between networks at gateways, mid-points and compute engines. ***True every mile security for the entire journey.***

SECURE DELIVERY INSIDE YOUR APPLICATION SERVER

Data is decrypted and decompressed in the CENTRI library that resides *inside* your application server. No unencrypted data goes across any network link – not even the loopback on your server! ***True last mile security.***



Technical Specifications

	Platforms Supported	Footprint
IoT Endpoint	• Embedded: Arm Cortex M4/M3, bare metal, Mbed, FreeRTOS, etc. • Linux devices	• ~26K Flash, ~10K RAM depending on platform and architecture
Application Server	• Linux • AWS, Azure, etc.	• Less than 2MB depending on platform and architecture

About CENTRI

CENTRI provides advanced data security for the Internet of Things. Our flexible, software-only product provides IoT professionals, developers and device makers with the means to quickly get to market with purpose-built IoT security, protecting data from creation to consumption. CENTRI enables you to mitigate today's data communication risks in a standards-based network infrastructure with heavyweight industry-standard encryption and compression, packed into a lightweight small footprint ideal for low-power IoT endpoint devices.

arm MBED Partner

/centritech /centritechnology /company/centri-technology

www.centritechnology.com | +1 206.395.2793 | sales@centritechnology.com