

# BEAST – Embedded Medical Secure Platform: Securing Data from the SoC up to the Cloud

M. I. Ben Salah, D. Vizár, J.-M. Koller, A. Dherse, P. Liechti, J.-N. Pfeuti, D. Hoover, A. Farnier

*There's more and more medical IoT devices exchanging personal data with many stakeholders over unsecure networks and storage, which creates security and confidentiality issues. We propose a solution providing easy to use end to end security and confidentiality from the sensor node up to the cloud, based on COTS hardware components.*

CSEM developed an end-to-end secure, yet practical and easy to deploy, communication and data exchange platform codenamed *BEAST* based on the Nordic nRF5340 chip, taking advantage of CSEM know-how on security and on PPG (Photoplethysmography) acquisition & processing. This platform suits particularly well the requirements of applications acquiring and exchanging sensitive data, e.g. personal information in medical and healthcare applications

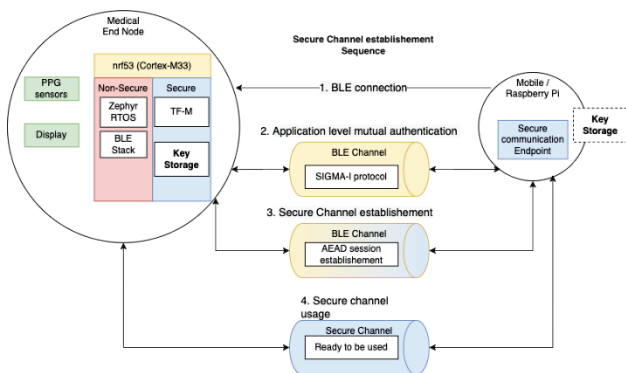


Figure 1: Secure end to end Channel establishment.

BLE wireless communication typically imposes a cumbersome pairing procedure, which is impractical in an application handling sensitive data with a large number of everchanging stakeholders (e.g. patients in a hospital), in particular because of the time it takes to launch and ensure that the BLE pairing code is correct. Security is required at two levels of the application, to ensure the transfer of sensitive data only to a trusted infrastructure (from device to the cloud, through gateways) and to prevent a third-party application could eavesdrop and intercept sensitive data when using mobile applications to retrieve medical data.

The CSEM BEAST secure IoT platform addresses these issues by implementing a custom transport layer over Bluetooth Low Energy (BLE) and a security protocol and key management architecture with their implementation on all stakeholder endpoints, typically made of the End Nodes running Zephyr, with Trusted-Firmware-M (TF-M), and the Gateways running Linux, with Python on a Raspberry Pi 5.

It automatically secures the connection, based on device trust, obtained through cryptographic verification and establishes a secure channel based on SIGMA-R protocol. This guarantees the mutual authentication where both devices ensure that they interact with an authorized device. Furthermore, the Authenticated Encryption Authenticated Decryption (AEAD) session establishment ensures that whatever payload is transmitted is cryptographically validated and authenticated at the decryption. Once the AEAD session is established, the secure channel can be used for transmitting the sensitive payload.

The BEAST transport layer allows to transmit payload over BLE and takes care of framing/splitting of data, retransmission and missing data notification. It also indicates the status either for an

error during the reception or during the security processing. The gateway/infrastructure can also transmit data to the end node, through a 'command' endpoint.

The security architecture is based on a mutual authentication protocol based on a four rounds version of SIGMA-R with a minimal subset of persistent keys and a device certificate, for minimal overhead when it comes to deployment. A successful mutual authentication allows the gateway & the device to communicate securely. The second element of the security architecture is a digital certificate PKI hierarchy, made of a root certificate (Cert<sub>R</sub>), a device certificate (Cert<sub>EN</sub>), a gateway certificate (Cert<sub>GW</sub>) and a cloud certificate (Cert<sub>CL</sub>). These certificates allow each party to identify that they're under the same certificate authority and to trust each other using the beforementioned security protocol.

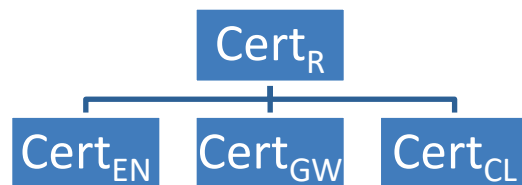


Figure 2: BEAST Public key Infrastructure (PKI) Hierarchy.

A proof-of-concept system demonstrator, based on nRF5340 and a Zephyr compatible PPG library for the medical end node and a Raspberry Pi 5 for the gateway, has been realized and successfully evaluated, demonstrating secure channel establishment and transmission of medical heartrate data in a secure manner and showcasing it through a visualization. The BEAST end node runs the Zephyr RTOS, on which the PPG acquisition operates together with the processing library integrated to the Zephyr DeviceTree. The Zephyr BLE stack provides wireless connectivity. Finally, the BEAST security library, based on the Trusted-Firmware-M, implements the security protocol, the key management and the secure storage of the device certificates. By using TF-M, this solution is portable to any TF-M compliant MCUs. On the gateway side, the implementation of the secure node is based on Linux using BlueZ for the BLE part and the BEAST security endpoint application is a python-based solution (for the cryptography and the BLE interface) and web technologies for the visualization (javascript + MQTT).

In conjunction to the demonstrator 2 reference documents are available: (i) BEAST security specification & (ii) BEAST software architecture document. The BEAST demonstrator can form the basis for many deployments involving the data acquisition, transmission, sharing and processing of sensitive data.