

# User-centric Key Management for End-to-End IoT Security and Privacy

D. Vizár, C. Kassapoglou-Faist, R. Berguerand

The extensive sensing of the human beings in internet of things (IoT) applications generates large volumes of personal data. The large attack surface of IoT systems made of constrained, (inter)connected embedded devices systems, calls for end to end-to-end (E2E) encryption, but the difficult key management -hampers adoption. CSEM designed a unique solution that integrates E2E encryption and electronic data sharing in the spirit of GDPR.

The internet of things (IoT) technologies enable new features or even new applications in numerous markets. However, the IoT architecture also exposes a large attack surface, spanning the cloud and the heterogeneous connected devices and connection technologies (often with inadequate security), with attacks on devices already on the rise [1]. A user has no choice but to trust an ever-growing number of applications with handling their data securely and to accept data processing requests, where fine granularity and user control is often at odds with flexibility and data reusability. The so-far presented results [2] do not fully address the security requirements and IoT constraints and end-to-end (E2E) authenticated encryption (from device to the cloud application), a robust security solution, seldom sees deployment in practice because of the difficulty of distributing encryption keys.

acts as a personal key manager, securely storing a long-term master key. Mid-term *data protection keys* derived from the master key are provisioned to the IoT devices (2), which run a lightweight, configurable multi-stage key-schedule to derive encryption keys deterministically (3). E.g., encryption keys may be rotated once per day, derived through two intermediate secrets rotated each week and month, respectively. The encrypted data is sent to the cloud *with no keys* (4), enhanced with metadata that fully determine the derivation of the encryption key. A cloud application then issues a non-repudiable *digitally signed sharing request*, detailing both the desired secrets (by the key metadata) and the intent of the processing. The structure of the key schedule enables both fine-grained and bulk access, by requesting encryption keys, the appropriate intermediate secrets or even data protection keys. Subject to user's consent, the key manager can then provision the requested secrets to the requesting processing application (5). In the example above, two months-worth of data would correspond to two, short binary metadata strings for both the request and response.

The design is scalable (in amount of data. Nr. of sensors and nr. of patients), with only a small footprint on both the devices and the key manager, ensuring a perfect fit with the constraints of IoT. Apart from the robustness afforded by E2E encryption, the framework also provides privacy well beyond the state of the art, empowering the user with a direct, technical control over the data they own, in a fashion that is along the principles of GDPR. This increase of personal control may, paradoxically, increase the likelihood that users would agree to (re)share reasonable subsets of their data, unlocking even more value form the data being collected. For example, a patient may agree for encrypted, key-less data to be stored long-term and then electronically agree to use data from a month for the development of a new, life improving drug. The framework has been implemented (Figure 1) and successfully demonstrated using CSEM's ultra-low-power platform Wisenode and  $\mu 111$  operating system. Further extensions of the technology are identified, such as using User-Managed Access (UMA) tools to alleviate the need of the users' personal trusted device to be online whenever a sharing request is sent, or the integration of the processing application and the data processor module in a Trusted Execution Environment to ensure that data is decrypted within an isolated, secure environment and never needs to leave it.

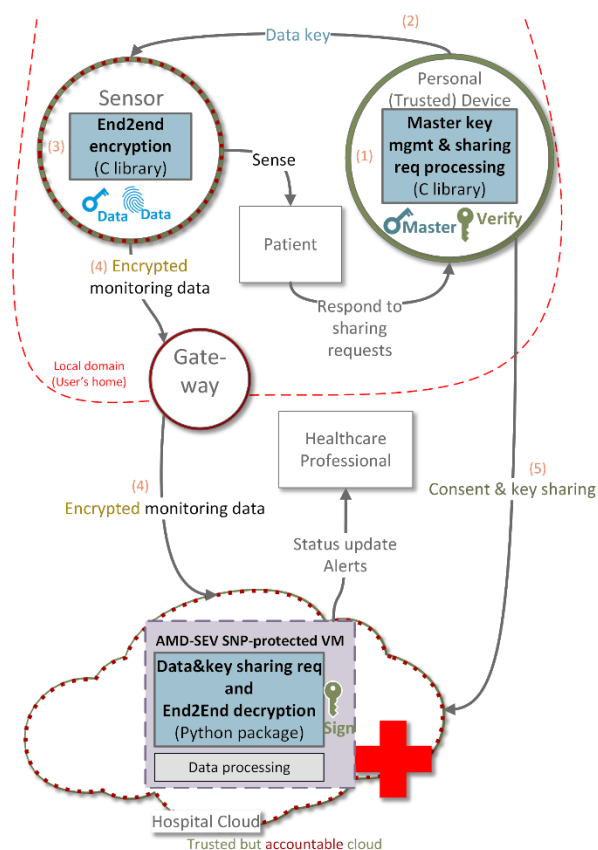


Figure 1: Remote patient monitoring with end-to-end security and privacy.

An E2E framework [3] has been designed at CSEM in the scope of the EU project Moore4Medical [4], primarily for continuous patient monitoring applications (Figure 1, orange numbers link to the description). It proposes a *trusted personal device* (1), a dedicated wearable or a virtual device in the smartphone, which

In conclusion, the novel E2E security and privacy solution designed and implemented at CSEM is an ideal mean of affording robust, E2E security and privacy to data in any IoT-like application. An adaptation to industry 4.0 is already in progress. Provable security of the solution is currently being investigated.

[1] C. Cimpanu, "New HEH botnet can wipe routers and IoT devices", ZDNet, 2020.  
 [2] S. Sridhar and S. Smys, "Intelligent security framework for iot devices cryptography based end-to-end security architecture," ICISC 2017.

[3] M. de Ree, D. Vizár, G. Mantas, J. Bastos, C. Kassapoglou-Faist, Corinne, J. Rodriguez "A Key Management Framework to Secure IoMT-enabled Healthcare Systems" CAMAD52502.2021.9617796.  
 [4] EU project Moore4Medical. (2020) <https://moore4medical.eu/>