

# Extending End-to-end Data Encryption & Sharing Technology with Microledger Audit Trails

C. Bühner, D. Vizár

CSEM's Encryptflow technology extends the end-to-end data encryption and sharing in IoT to generate non-repudiable audit trails for each sharing transaction. This allows traceable resharing and to ensure that the data processors always get the original data, paving the way to a trusted data economy.

The ongoing digitalization together with the expansion of the Internet of Things (IoT) paradigm result in immense quantities of data being collected in virtually all verticals. In most cases, the data collected by a particular organization has a potential value for the ecosystem of the organization that is far greater than the value extracted through the primary processing. Yet, such a secondary data valorization in the ecosystem rarely happens, due to lack of trust. In digital health, patient data collected in diagnostic monitoring are rarely reused at scale to further improve diagnostic, drug development or treatments, due to complex regulation and patients' privacy concerns. Due to fear of uncontrolled data dissemination, data produced by advanced manufacturing machines is rarely reused to increase the power of predictive maintenance models or the efficiency of support from the component suppliers. Similar situation arises in complex logistic ecosystems, for which data could help improve the overall efficiency but instead is remaining siloed.

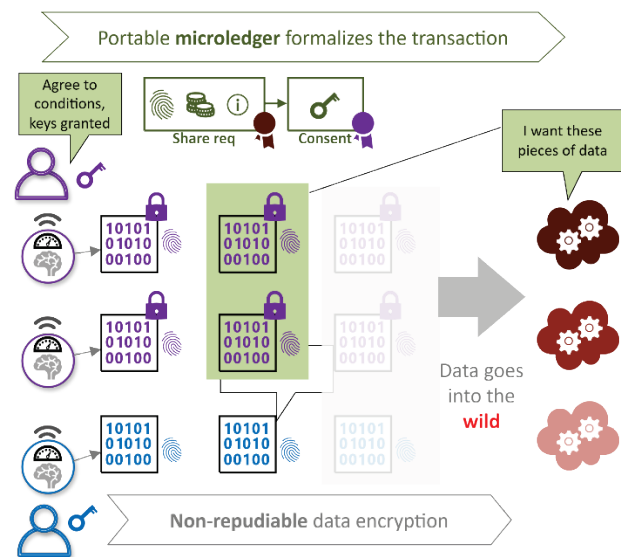


Figure 1: Data protection and controlled sharing with EncryptFlow.

To address these issues, CSEM has previously developed an advanced technology, representing the first step towards advanced data valorization, allowing data to be protected, confidently advertised and then flexibly shared with processors that needn't be identified at the time of encryption. It integrates end-to-end data encryption and transparent data sharing where a data owner retains a fine-grained control over who gets what access, designed and optimized to scale up to IoT proportions<sup>[1]</sup>. It encrypts (not only) IoT data directly at source with very low overhead. The data then stay protected until needed for processing, no matter what the underlying transmission and storage infrastructure is. In particular, the decryption keys are not provisioned to any party. Any would-be processor needing

access can compute a succinct, signed electronic request to access the exactly needed data points (e.g. readings of a sensor from a certain day, week or month), thanks to clever metadata that characterizes keys used to encrypt each data point. Only upon the data owner's consent (explicit or preconfigured) are decryption keys provisioned.

However, fully addressing the issues standing in the way to a data economy requires crucial missing features. On one hand, it is desirable that each data access request granted shall generate an audit trail, i.e., a strong, cryptographically non-repudiable evidence. On the other hand, ensuring that data owners cannot selectively reveal real or dummy, useless data upon key provisioning is needed to extend the trust in the transaction both ways (reassuring data "buyer").

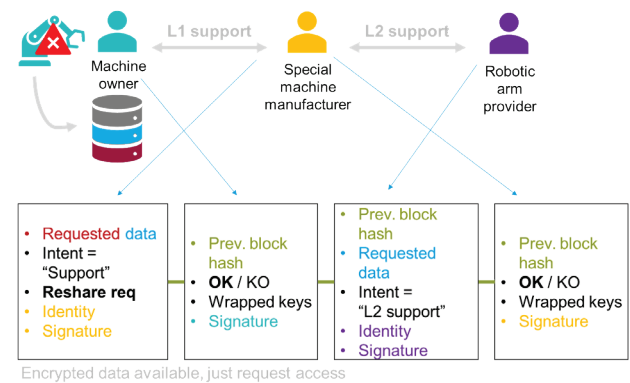


Figure 2: Microledgers allow controlled data forwarding with audit trails.

To address these remaining problems, CSEM has extended the data encryption technology and dubbed it EncryptFlow (Figure 1). The first improvement in EncryptFlow is the use of committing encryption, which protects the data confidentiality but also ensures that, once encrypted data is released, it can only be decrypted to the original plaintext with the original key. The second improvement is that the sharing request and response are now embedded in a microledger, i.e., a hash-chain<sup>[2]</sup> with digitally signed blocks. This way, the interaction automatically produces an audit trail available to both parties at the end of the transaction, as the request and response are sequentialized and digital signatures provide non-repudiation. The design of the microledger allows data processors to open any single microledger to a third-party auditor, allowing for an impartial resolution of disputes. A primary sharing microledger can also be extended with a request block made to the primary data processor for resharing (if authorized). This enables flexible, yet transparent data forwarding for level-2 machine support for example, with audit trails for the full path data travels (Figure 2).

[1] D. Vizár, C. Kassapoglou-Faist, R. Berguerand, User-Centric Key Management for End-to-End IoT Security and Privacy, [CSEM Scientific & Technical Report \(2022\), 20](#)

[2] D. Horne, Hash Chain, Encyclopedia of Cryptography, Security and Privacy. Springer, [https://doi.org/10.1007/978-3-642-27739-9\\_780-2](https://doi.org/10.1007/978-3-642-27739-9_780-2)