



Report on kNotary (a.k.a. kSecure) Technical Basis: The integrity protocol


By request of Kinamik Data Integrity S.L., we are providing an informal security assessment of the Kinamik Secure Audit Vault *integrity protocol*, also known as *kSecure*. This report is solely based on Kinamik's *kNotary* (a.k.a. KSecure) *Technical Basis* (KTB) about its secure register architecture, Version 1.5-RC2 dated November 2008.

Assuming the following conditions: all keys (private and session) are kept secure, the cryptographic algorithms, the hardened servers and the Time Stamp Server (TSS) are not compromised, and the protocol is tightly implemented, we have not found any weakness in Kinamik's integrity protocol. Specifically, the graceful close registers have the following properties: tamper evidence, message-level granularity and message confidentiality. The abnormal close registers and live registers have tamper evidence and message-level granularity form the first entry (open entry) to the last signed entry (for instance, the last metronome entry). Furthermore, both registers (abnormal and live) have message confidentiality.

Based on the previous assumptions, the addition, modification and deletion of register entries have been evaluated for the tamper evidence and the message-level granularity. The confidentiality was studied when the attackers want to access to the secret information of the register.

The integrity of the graceful close register can be verified by the auditor. If messages are encrypted it is not necessary to decrypt them in the integrity verification process; this means that the auditor can be external and does not need to have access to the encryption keys. Furthermore, the scheme is more efficient in computation, communication and storage than to signing every message.

In conclusion, assuming the conditions described above we see that the claims asserted by Kinamik are sound and we have not found security flaws in the integrity protocol based on the kNotary (KSecure) Technical Basis (KTB) Version 1.5-RC2, dated November 2008, provided by Kinamik Data Integrity S.L.



Jordi Castellà-Roca, PhD
Tenure-track lecturer
Departament d'Enginyeria Informàtica i Matemàtiques
Universitat Rovira i Virgili