Trusted Timestamps – A new (Old) Tool to Ensure Integrity and Authenticity of Research and Clinical Data

Authors: Matthias Görges, PhD[1], Christian L Petersen, PhD[2], and J Mark Ansermino, MBBCh, FRCPC[2]
1) Pediatric Anesthesia Research Team, Child and Family Research Institute, Vancouver, Canada , 2) Department of Anesthesiology, Pharmacology & Therapeutics, The University of British Columbia, Vancouver, Canada

Background: Trusted timestamps [1] are digital markers that can be used to prove the existence of data before a specific time and preventing the owner from modifying the data at a later time without invalidating the timestamp. Trusted timestamps are issued by a third party, typically a certificate authority. Their integrity is based on the application of hash functions (to summarize the data content without revealing its content) and digital signatures (to prove the validity of an issued timestamp). As such, they provide strong evidence that data files have not been altered since the time they were protected with the trusted timestamp.

This idea was first used by Robert Hooke in 1660 who published an anagram of what eventually became Hooke's law. Without disclosing its content at a specific time he was able to claim priority to his finding [2]. Nowadays, trusted timestamps are used to claim priority of code, inventions and other documents. Yet, they also have applications relevant to clinical research and medicine in general: a) to verify data integrity in sponsored research studies, and b) to ensure the integrity of data collected as part of a patient's medical record. Of particular relevance to anesthesia are vital signs data, drug administration records, and descriptions of other interventions as documented in an anesthesia information management system.

Methods: We use the LambdaNative software development framework [3] to integrate Trusted Timestamps with our existing medical data collection software, to provide a modular software block that can be dropped into future research projects and/or back-ported into our existing data collection systems. The implementation uses industry standard public key encryption and cryptographic hashing technology and provides a mechanism for securely submitting requests to a time stamp authority and for verifying the returned timestamps.

Results: We have implemented trusted time stamping, using the German National Research and Education Network (DFN), Time Stamp Authority server (zeitstempel.dfn.de, freely available for non-commercial use) and made it publicly available under a liberal open source license [4]. The software enables trends and waveforms files to have trusted timestamps automatically applied at the time of collection. Using this technology will therefore inherently ensure data integrity from the source at a specific point in time and potentially eliminate the need for medical records affidavits and other means of certifying the validity of medical data after the fact.

Conclusion: Trusted timestamps serve an increasingly important role in many areas of society, but have yet to become an integral component of data collection and management in medicine. Use of this technology in anesthesia may prove to be a useful way to safeguard against accidental and/or intentional alteration of research and clinical data, to strengthen litigation evidence, and to improve the overall quality of data in the field. We encourage all medical researchers to consider adopting this technology in their data collection systems.

References: [1] C Adams, P Cain, D Pinkas, R Zuccherato, Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP), *Internet Engineering Task Force*, 2001:RFC 3161; [2] H Petroski, Invention by Design: How Engineers Get from Thought to Thing, *Harvard University Press*, 1996:10-11; [3] CL Petersen, M Görges, D Dunsmuir, M Ansermino, GA Dumont, Experience report: functional programming of mHealth applications, *Proc 18th ACM SIGPLAN Int Conf Funct Program*, 2013:357–62 [4] https://github.com/part-cw/lambdanative/wiki/Index-of-Module-timestamp