

Brian McFarland
Guardtime Federal, LLC

Keyless Signature Infrastructure for Secure Systems Engineering

Systems Engineering is highly collaborative across multiple organizations for complex systems, yet National Security Systems are required to be protected from the Insider Threat. The Insider Threat can extend into the design and development engineering processes, thus organizations need controls in place to efficiently provide accountability for engineering activities as well as securely tracking compliance. Digital signatures provided by Keyless Signature Infrastructure (KSI) efficiently provides both accountability as well data integrity for compliance data. KSI utilizes a unique non-bitcoin based permissioned blockchain to generate digital signatures without private keys. KSI aggregates signatures once per second into a binary Merkel tree and periodically publishes the root hash. The resulting signatures are intrinsically timestamped based upon the aggregation round. The resulting highly scalable structure supports rapid verification of signature attributes embedded in the immutable blockchain with trust rooted in a widely publicized root hash. The ability to verify KSI signatures and their associated timestamps simply through access to the widely publicized root hash makes KSI ideal for highly collaborative environments.