

What is Kinamik's Data SafeSealer™ technology?

Data SafeSealer software from Kinamik is advanced electronic data signature technology that is designed to be integrated with third party software products to bring all the benefits of assured information and tamper evidence to any digital binary data. It enables high-performance, realtime protection of streaming audio, video and network traffic data with minimal computational overhead, providing irrefutable proof of the data's authenticity and integrity using strong cryptographic key management, increasing its evidential weight and facilitating data protection and security compliance requirements.

What are the business benefits of using Kinamik's Data SafeSealer technology?

- ▶ Allows third-party software solutions to add unique tamper-evident properties to data.
- ▶ Supports litigation in a Court of Law by increasing the evidential weight of streaming records.
- ▶ Augments financial and privacy regulatory compliance processes by delivering independently verifiable, trustworthy data.
- ▶ Reduces the risk of unwanted or malicious manipulation by providing end-to-end trust and extends the data's chain-of-custody from capture or generation to export.
- ▶ Meets or exceeds the most stringent anti-tampering regulatory and best practices measures (e.g. BSI10008, HIPAA, PCI-DSS, FISMA, etc.).
- ▶ Mitigates the risk of insider and privileged user abuse in untrusted environments.

Information today is increasingly becoming more and more liquid

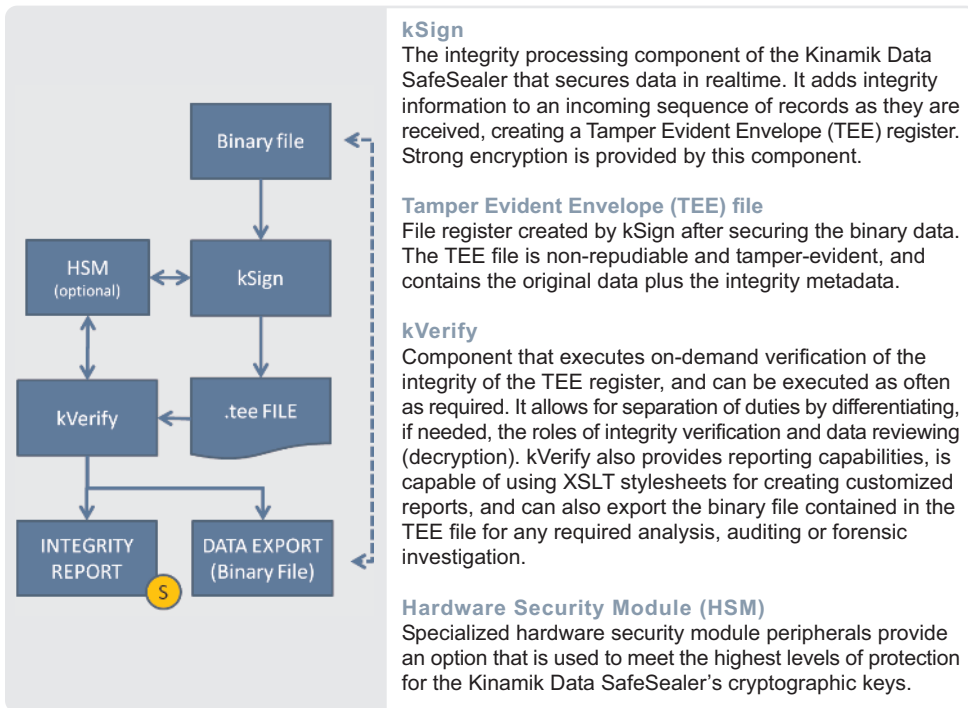
Information processing environments are being challenged by a fundamental change in the way that an ever-increasing torrent of potentially sensitive data is being handled. Current protection and assurance methods are not particularly well-suited for this paradigm shift. Simply put: streaming data is subject to an infinite number of potential internal and external man-in-the-middle attacks, and cannot therefore be fully trusted.

In addition, recent trends such as Cloud Computing, the widespread adoption of mobile devices and the consumerization of IT have dramatically increased the amount of data flowing in and out of the organization. These trends, as well as the sheer volume of information being created, influence how information has morphed from individually isolated files to a more liquid form (e.g. video surveillance, lawful intercepted data, audio records, etc) that must be assured. The value of this sensitive data is also on the rise due to its extensive use in supporting data retention and e-evidence requirements, forensic-level investigations, compliance or auditing processes, and executive decision-making.

A certain loss of confidence in an ever-increasing torrent of sensitive data

Current anti-tamper measures often require grouping streaming data into files or introduce delays before being applied. These delays can create a degree of doubt as to whether any of the data has been tampered with before these protective methods were utilized. And if any single record is compromised, severe consequences can result, making all of the data stream less valuable for any subsequent use.

- ▶ For Cloud environments: The uncertainty of just who is accessing, managing and storing all corporate data and the inability to demonstrate due standard of care illustrate a certain lack of transparency in cloud environments today. Compliance and security officers find themselves unable to trust their external cloud providers with their data, and are reluctant to allow sensitive data migration to the Cloud.
- ▶ For Lawful intercept providers: These solutions can be subject to potential abuse by internal employees and external hackers. Ineffective controls to protect and preserve the confidentiality and integrity of both sensitive system audit logs and lawful intercept data can have significant privacy infringement, trust and compliance impacts, and can also undermine the evidential weight of the collected data.
- ▶ For Identity and Access Management (IdAM) records: Building an assured and irrefutable association to an electronic identity record is a foundational security element. However, many IdAM implementations can be compromised by rogue users whose aim is to access legitimate electronic identity files and substitute bogus credentials.
- ▶ For Video/audio surveillance information: The evidential weight of audio and video surveillance digital data is largely dependent upon proof of the authenticity and integrity of data and its chain of custody. Furthermore, dealing with digital data increases opportunities for internal or external users to undetectably modify video and audio data.



Kinamik Data SafeSealer · Product Architecture

Kinamik Data SafeSealer™: the advanced information assurance solution for increasingly liquid data

Kinamik Data SafeSealer (kDSS) technology is used effectively in a variety of information processing scenarios, including Cloud Computing, lawful intercept, Identity and Access Management and video/audio recording and surveillance. It can be seamlessly integrated with third-party solutions, allowing these technologies to offer unrivalled tamper-evidence properties and delivering completely trustworthy data. For Cloud environments, kDSS brings a "flight data recorder" capability by securing sensitive data in realtime at the highest level of granularity, offering assurance that system audit logs are trustworthy and delivering digital evidence-ready proof that data hasn't been tampered with. For Lawful Intercept solutions kDSS delivers an always-on irrefutable record of all transactions, allowing the ability to demonstrate the authenticity and integrity of the intercepted data and ensuring that it retains its chain-of-custody with verifiable evidential weight and protection from even the most privileged user. Deployed within Identity and Access Management (IdAM) environments kDSS secures all sensitive data as it is being generated, providing irrefutable proof that it hasn't been tampered with from the moment of creation, resulting in complete end-to-end trust. For video surveillance and audio recording, kDSS is capable of protecting the integrity of any streaming digital data so that any subsequent verification can prove its authenticity and integrity protection, leaving it ready for evidentiary use.

Selected features

- ▶ **Lightweight:** with a minimal computational footprint, kDSS can be easily installed within the existing infrastructure without requiring complex architectural adaptations.
- ▶ **Data agnostic and safe:** kDSS' signing and verification processes do not require to understand the data's content or structure, therefore respecting the sensitive data's confidentiality.
- ▶ **User-configurable:** kDSS provides for fine-grained, user-adjustable integrity and authenticity (non-repudiation) in realtime, allowing a balance between granularity and available computational power.
- ▶ **Multi-platform support:** compatible with any operating system and platform that supports Java (e.g. Linux/Unix, Solaris, Windows, etc.).
- ▶ **Strong encryption:** the received data can be optionally encrypted with keys independent from the integrity verification process, so tamper-evidence can be verified without decrypting sensitive information.
- ▶ **HSM-integrated:** kDSS provides for the ability to use Hardware Security Modules (HSM) to protect and store keys, and leverage cryptographic accelerators.

Advanced Kinamik technology in an embedded solution for OEMs

Kinamik technologies are available as an application program interface (API), allowing easy and fast integration with third-party technologies. The embedded solution enables the delivery of real-time data integrity assurance to virtually any product or solution, enhancing their ability to successfully address security, data governance and compliance requirements.



Kinamik Data Integrity, Inc.
303 Twin Dolphin Drive
Redwood City, CA 94065, USA
Tel: (+1) 650 632 4408
Fax: (+1) 650 551 9901

Kinamik Data Integrity, S.L.
Diputació 238, àtic 5
08007, Barcelona, Spain
Tel: (+34) 931 835 814
Fax: (+34) 933 041 681
www.kinamik.com
info@kinamik.com



About Kinamik Data Integrity, Inc.

Kinamik technology protects digital records at rest or in flight from being altered. We provide a Centralized Audit Vault repository for sensitive data that adds integrity and authenticity at a fine grain level, creating in the digital world a level of evidence that is analogous to paper-based records. Kinamik's solutions deter, detect and demonstrate data manipulation to guarantee the authenticity and assurance of digital information.

Our mission is to bring a higher level of trust, accountability and privacy protection to data in mission-critical industries that deal with large volumes of high-value data and sensitive information. We provide advanced data integrity assurance capabilities to industries such as financial, health, life sciences, transportation, public sector agencies and IT hosting sectors.

Kinamik is a McAfee SIA Partner and a Sun Startup Essential Partner

Kinamik is a trademark of Kinamik Data Integrity, Inc. All other trademarks contained herein are the property of their respective owners.

© 2011, Kinamik Data Integrity, Inc.