

Case study

Scytl Secure Electronic Voting provides complete and trustworthy auditability to their clients using Kinamik technology

Benefits

- ▶ Full audit trail and log files auditability.
- ▶ Ability to unquestionably prove log files integrity.
- ▶ Full data integrity protection by making log files tamper-evident.
- ▶ Auditability and security provides Scytl with a unique differentiator.

The Company

Scytl Secure Electronic Voting is a worldwide leader in the development of secure solutions for electoral modernization. The solutions provided incorporate unique cryptographic protocols that enable to carry out all types of electoral modernization processes and elections in a completely secure and auditable manner. Scytl's advanced electoral security technology positions the company as a leader in electoral modernization industry.

Scytl's innovative technology has received many international awards, including the ICT Prize, the European Venture Contest Prize, the RedHerring 100 granted by RedHerring magazine and the Global Innovator granted by Guidewire Group.

Scytl's clients are both in the private and public sector, including governments in Spain, USA, France, Austria and Switzerland, among others.



“Kinamik’s expertise in the development of immutable log solutions has allowed us to enhance the auditability of the elections managed by Scytl’s solutions. The incorporation of immutable logs is a clear differentiator in environments with critical audit and security demands like e-voting elections. We are extremely pleased to collaborate with Kinamik in the implementation of immutable logs for e-voting environments.”

Jordi Puiggali,
VP Research & Development
Scytl Electronic Voting

The Challenge

Implementing an e-voting system is a complex project both from a technical and social perspective. Voters must accept these new disruptive technologies in a very sensitive field: the exercise of their political rights.

Public opinion's acceptance and e-voting process confidence are key factors for the success of an e-voting initiative implementation. For achieving this, assigned representatives and independent auditors must be able to verify that the system works flawlessly and honestly. Auditability is usually considered as a decisive factor for gaining trust in an e-voting system and, since electronic voting is in essence a paperless ballot, the lack of accurate and trustworthy audit trails is commonly deemed as a factor that could diminish the trustworthiness of the electoral process. Immutable audit trails then arise as the solution for solving these accuracy and trust issues by giving the ability to demonstrate that a voter has effectively cast the vote, and by allowing that assigned authorities are able to verify and audit that the system works properly and audit trails are accurate and trustworthy (i.e., they have not been manipulated).

One of Scytl's key differentiators is precisely its capability of delivering easily auditable electoral processes. This is achieved by providing a verifiable immutable trail of the whole electoral process by creating tamper-evident audit trails. By providing secure, trustworthy and verifiable electoral processes to any auditing authority, Scytl's implementation of Kinamik underlying technology sets them apart of their competition.

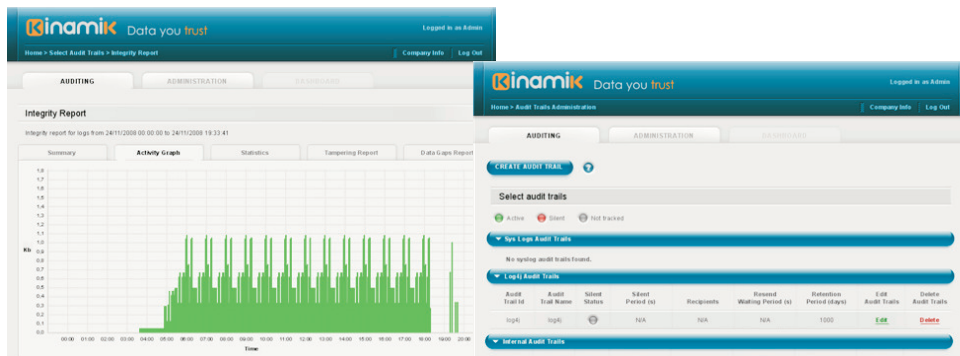
Using its implementation of Kinamik's technology, Scytl has provided a secure e-voting environment for approximately 1.000.000 users in various projects worldwide, including high-profile electoral events such as the 2008 US Presidential election and the 2009 process for the election of the representatives to the Assembly of the French living abroad. In many of these electronic voting cases, security and auditability issues were raised and successfully tackled by Scytl's products, in part thanks to the full data integrity protection technology applied to the election's audit trails obtained by the technology they share with Kinamik.

Scytl continues to be the leader in providing e-voting solutions. Kinamik is proud to help Scytl in consolidating its offering, providing world-class e-voting solutions and consolidating as a worldwide leader in its sector.

Kinamik Secure Audit Vault selected features

- ▶ Messages in transit compression: reduce bandwidth usage by compressing up to 70% messages sent to the integrity processing component.
- ▶ Optional data encryption: using strong industry standard protocols for encryption, all the data existing in the secured audit vault can be rendered confidential.
- ▶ TSA compatible: for achieving a higher level of security and integrity protection, the Kinamik Secure Audit Vault is fully compatible with external time stamping authorities (TSA).
- ▶ Data Retention Policy tool: Kinamik Secure Audit Vault allows users to define different retention policies for each independent data source, enabling compliance with laws, regulations and standards (e.g. PCI-DSS, HIPAA, Basel II, SOX, MiFID, etc.) that mandate specific data retention periods.
- ▶ Regular expressions text search within centralized repository: use web-based search capabilities for an exact localization of specific text strings and expressions within the secured data.
- ▶ Easy-to-interpret comprehensive integrity report: evaluate trust level of data with one simple snapshot. Pinpoint any integrity infringement down to the event level.
- ▶ Archival and storage compression capabilities: reduce storage and archiving costs with the Kinamik Secure Audit Vault's archiving compression capabilities, with up 5:1 compressing ratio.
- ▶ High performance: Kinamik Secure Audit Vault's technology is capable of processing and securing up to 40.000 EPS (events per second)*

*kSecure signing capability. Results may vary depending on various factors such as system configuration.



Kinamik Secure Audit Vault · Integrity Report Activity Graph and Administration Console

About Kinamik

Kinamik software protects digital records from being altered. We build a Centralized Audit Vault for sensitive data with integrity and authenticity at a fine granular level, creating in the digital world a similar level of evidence than to traditional paper-based records. Kinamik deters, detects and demonstrates data manipulation to guarantee the correctness of digital information.

Our mission is to bring a higher level of trust, accountability and privacy protection to industries that deal with large volumes of sensitive information. We address data integrity mainly in financial, health, government, and IT hosting sectors.

Kinamik is a Sun Startup Essential Partner and an Oracle Partner.



What is Kinamik Secure Audit Vault?

Kinamik Secure Audit Vault is an innovative software solution that collects, secures and centralizes audit information from different sources, while providing irrefutable proof of integrity. It helps organizations reduce audit and compliance costs, mitigates insider threat and gives legal admissibility and best-evidence in case of litigation.

Supported platforms

- ▶ Linux/UNIX
- ▶ Solaris
- ▶ Windows
- ▶ Any Operating System that supports Java

Supported feeds

- ▶ Syslog messages
- ▶ Generic text files
- ▶ JDBC applications
- ▶ Log4J (for all Java applications running on a 1.4 or later JVM)
- ▶ Native BEA Weblogic 9
- ▶ Native OpenSolaris Audit
- ▶ New platforms are constantly being added and can be supported on demand



Every effort has been made to ensure that the information included in this datasheet is accurate and up-to-date at the time of going to press. Nevertheless, the products described herein are subject to continuous development and improvement and Kinamik reserves the right to change their specifications at any time. We disclaim any liability with respect to this document, and no contractual obligations are formed directly or indirectly with its contents. Kinamik is a trademark of Kinamik Data Integrity, S.L. All other trademarks contained herein are the property of their respective owners.