

ELN

Industry Insights: Security Considerations for Today's Electronic Lab Notebooks

Welcome to our latest Q&A session. For those of you not using ELNs, please don't run off! While this exchange nominally addresses concerns with various aspects of ELNs, the reality is that these concerns are valid for all types of informatics systems, both inside and outside the laboratory. The topics we examine range from options available for electronic signatures and verifiable time stamps to methods for reliably embedding external documents into an ELN. As before, we've gathered experts from some of the leading companies in the field to provide

their take on these questions and explain why they feel that way. As the best way to do something — assuming such a thing actually exists — generally varies with circumstances, the wise reader will take this explanation of "why" and examine it in light of their own processes. Of course, our experts have provided high-level views and couldn't get into all of the potential caveats affecting their answers, the critical thing here is not to find the answer, but to point you in the right direction to ask additional questions.

— John R. Joyce, Ph.D.

Q: ELN use in a regulated environment requires verifiable electronic signatures. Please describe the best available options and their relative benefits. Which do you recommend and why?

Robert Pavlis: There are three aspects to controlling electronic signatures. I recommend the following functionality:

- ▶ controlling access to data and the ability to add data to any document in ELN. This is normally done with an e-sig system that requires users to enter their name and password.
- ▶ tracking additions and changes in an audit trail system. It is important that the audit trail tracks before and after values for any change. Many ELN systems perform this function. However, very few provide the ability for the approver/auditor to easily see these values at the time the approval is being done.
- ▶ verifying any signature on a document or ELN worksheet after it is printed or displayed electronically. A very good way to do this is to provide a water mark, which proves to the viewer the signature was electronic and was authenticated at the time it was placed on the document.

Paul Denny-Gouldson: When an ELN is deployed in a regulated laboratory, there are a number of options that exist ranging from simple hash algorithm encryption signatures up to digital signatures. Hashing algorithms are used in

many industries and have been used for many years to provide tamper evidence. Digital signatures are now also useable to verify identity and provide tamper evidence and are sometimes deemed a higher level of security.



I recommend open signature systems based on public key infrastructure and other public standards.

— Jeff Spitzner
Rescentris

Jeff Spitzner: Options include commercial third-party services (SAFE, Surety, other hosted signing services), Adobe PDF solutions, and ELNs using either proprietary or open architecture enterprise digital signature systems. Commercial external (SaaS) offerings designed for signing ELN records work for signing simple documents and can benefit labs with limited IT resources. The costs may be high to utilize these strategies and there are risks that these companies may not stay in business. Online and PDF e-signature solutions may not be able to handle complex data sets and other critical lab records that establish the context of the work. Proprietary ELN systems maintain lab records safely behind the firewall, but might not be sup-

ELN

ported or have accessible data in the future for verification. I recommend open signature systems based on PKI (Public Key Infrastructure) and other public standards that ensure the time/date stamped records, digital signatures, keys and original notebook documents are all accessible in the internal ELN system and backups, such that e-signatures can be verified independent of third-party organizations but cannot be tampered with without detection. These solutions can offer future-proof, secure, and verifiable e-signatures.



SAFE BioPharma developed a trusted environment for digital signatures that allows exchanging records among different authorities.

— Thomas Schmidt
Waters

Thomas Schmidt: Principally, two kinds of electronic signatures are in use today: the one-factor user/password verification and the true digital signature. With the one-factor user/password verification, you can sign the current status of a document and the ELN application can prevent changes to the signed record. But, when you export the record, e.g., during regulatory submission, you can't assure the integrity of the signed document without a link between the signature and the record content. In contrast, with the digital signature framework, the record integrity can be guaranteed. This two-factor electronic signature requires an additional hardware token for authentication and links the signature uniquely with the record content. The SAFE BioPharma organization developed a trusted environment for digital signatures that allows exchanging records among different authorities. Because the signature is directly attached to the content, the receiver can unambiguously verify the authenticity of the signer and the integrity of the content.



Electronic signatures can be split into several categories. Each one of them brings different security elements.

— François Beillouin
Agilent Technologies

François Beillouin: Electronic signatures can be split into several categories. Each one of them brings different security elements, but also constraints. The general mechanism consists of signing a document checksum with a trusted certificate. When the certificate is a company one, used server side (when we consider enterprise systems), the maintenance is easy, but the individual authorship proof mechanism relies

both on the certificate itself and on the procedure used inside the software to activate and track signatures.

When the certificate is an individual one, this is no doubt the easiest way to prove the identity of the signer and, so, the author and witness of an experiment. However, this option requires a lot of efforts regarding certificates management and security. There's one variation on this mode with SAFE certificates which adds a way to trust electronic records when exchanging them between different companies. The choice between these options has to be debated and accepted with the legal department, and both can be very well adapted depending on the company activity. As these needs can also evolve with time, it's important to select an ELN that can accommodate all different options.

Steven Neri: In a regulated environment, all records should be audited and should also be preserved in encrypted electronic record form. The implementer should then have the option to selectively determine where and to what extent electronic signatures will be enforced. This approach of combining system-generated electronic records capture with configurable e-sig determination is strongly recommended because it provides a comprehensive audit history, while at the same time enabling the customer to selectively manage the way that electronic signatures effect the user experience.

Q: Time stamping ELN records is critical to any legal challenges, but can be especially tricky when operating across multiple locations and time zones. What steps do you recommend to minimize the risks of alterability of records and to avoid potential legal challenges?

Mats Kihlén: Global systems are, to an increasing extent, operated from a single corporate data center. While the server obviously holds a central time, each ELN client needs to keep track of the local time when an experiment is created or signed. I recommend that the ELN records are stamped for clarity with either UTC or GMT, as well as the local time. In case of ambiguity, e.g. due to erroneous client computer settings, the central time will overrule the local.



Time stamps from trusted sources should be used in combination with e-signatures to maximize security ... of records and audit trails.

— Paul Denny-Gouldson, IDBS

Paul Denny-Gouldson: Timestamps are critical, and the problem has been solved by other industries, such as banking. There

ELN

are standards that are used to provide a unified time format coupled with the time zone information about where the user was when the time stamp was applied. There are also well-documented methods and services (GPS time servers) to provide central timestamps that other systems can reference. The time stamps obtained from “trusted sources” should be used in combination with e-signatures / digital signatures to maximize the security and auditability of records and audit trails.

Jeff Spitzner: I recommend only using the time stamp of a single server — not local to the client computer or end-user — for ELN records. The server should be synchronized with remote time servers and there should be policies in place for verification of the single official ‘system time.’ The time stamp is added to records from the server as part of the record transaction to avoid any chance that users change their computer time. The location and time zone of the user can be tracked but does not really matter, because the time is absolute not relative. The sequence of events, records and sequential assignment of globally unique identifiers make it nearly impossible to alter a record without detection or without having to change all the data in the system — which should be impossible without a major conspiracy and a system that is not built for compliance. The audit trail will demonstrate that all records are created and managed in proper order and this can be readily verified.



It is critical to use a centralized, common system for all ELN record versioning and time stamps.

—*Dominic John*
Symyx Technologies

Dominic John: It is critical to use a centralized, common system for all ELN record versioning and time stamps. Time

stamps should be generated at the database, reconciled to coordinated universal time (UTC), and recorded with the client’s local time zone offset (from UTC). This ensures consistent time stamps while also preserving the ability to record the local time the action was taken. Signatures should be required when committing an ELN record to the database. The signature should require the user’s credentials, reasons for the change and optional comments. This ensures that the correct person is committing the ELN record to the system.



Time stamps that provide unequivocal reference to UTC time may be implemented by recording three components of the reference clock.

— *William Buote, VelQuest*

William Buote: Time stamping all records and changes to records, as well as electronic signatures is required to support the chronology of activities. Time stamps that provide unequivocal reference to UTC time (commonly referred to as GMT) may be implemented by recording three components of the reference clock. These are the day, time and time-zone bias. Using these three components, the actual chronology of events may be determined, even for those events happening in different time zones. In addition to the data recorded in the time stamp, the referenced clock must be controlled and synchronized.

Thomas Schmidt: To obtain comparable time stamps in international ELN deployments, the time stamps should be stored in a standard time format such as UTC, the coordinated universal time. Nevertheless, for the convenience of the user, the ELN user interface should also display the time stamps in the local time. Very often, the application server time, i.e., the time originating from the customers on-site server, is taken as the source for the

PARTICIPANTS

François Beillouin

ELN Professional Services Manager
Agilent Technologies

Mats Kihlén

ELN Specialist
Contur Software

Paul Denny-Gouldson, Ph.D.

Product Manager, E-WorkBook Suite
IDBS

Robert Pavlis

President
Labtronics

Steven Neri

Director of Pharmaceutical Business Development
LabWare

Jeff Spitzner

President and Chief Science Officer
Rescentris

Dominic John

Director of Software Marketing
Symyx Technologies

William Buote

Senior Vice President and Chief Technical Officer
VelQuest

Thomas Schmidt, Ph.D.

Informatics Senior Product Manager
Waters