ClickCommerce

21CFR Part 11 Compliance

Approval Processes, Security and 21 CFR Part 11

When applying 21CFR Part 11 guidelines to IRB and / or IACUC approval processes, it's important to know that a vendor's technology can stand up to requirements. Click Commerce's extranet-level security and product practices provide IRBs and IACUCs a compliant, configurable product base that satisfies 21CFR Part 11 requirements for a "closed" system. Though higher levels of add-on security technologies exist in the market today, they are primarily intended for "open" system use, exceed the practical needs of the IRB and add unnecessary costs. Click Extranet's security system is comprised of several essential elements to meet 21CFR Part 11 requirements:

- Strong authentication (e.g. passwords containing both letters and numbers).
- Password rotation (e.g. password expiration after a configurable period of time such as 90 days).
- A flexible software platform whose security is configured to each institution's compliance operating policies and fully tested through multiple alpha and beta tests prior to deployment; all secure signature processes are documented in workflow charts.
- Signing activities restricted by several attributes in Boolean combinations (e.g. by an individual's role AND department; individual's role OR institution, etc.).
- Audit logs that cannot be altered that track review / approval signatures time and the nature of an item's disposition.
- Data transport protection from unauthorized "eavesdropping" through the use Secured Sockets Layer (SSL) and certificate authorities.

When combined with an institution's continuing education policies on password protection, secured physical access to server hardware and other IT – related institutional SOPs, Click Extranet provides a secure product base for managing any institution's human or animal research subject oversight program.

21CFR Part 11 Review

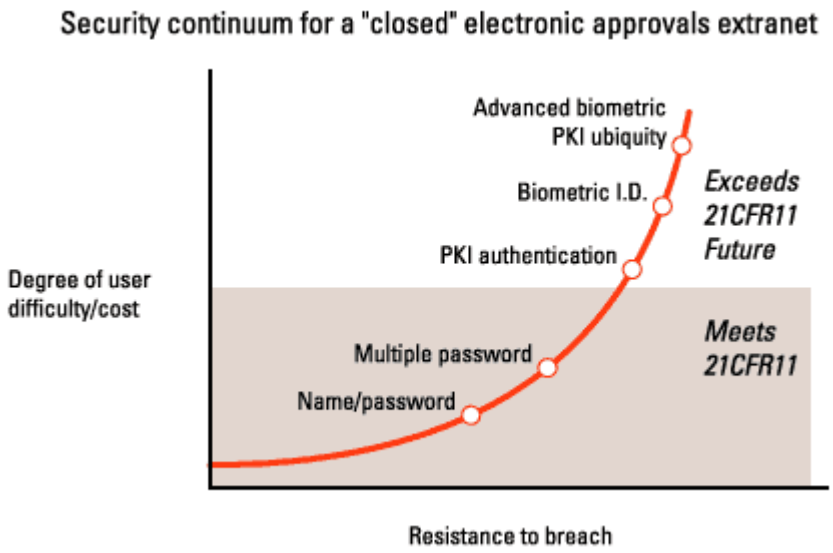
Verification and auditing capability (auditabilty) are at the core of every approvals system: institutions must be able to prove that any person taking action with the system is who they say they are. Furthermore, document submissions, reviews and approvals must be recorded reliably and cannot be changed without documentation: electronic signatures are the key to achieving this. The issues here really boil down to how much access security is satisfactory given the environment in which the system operates, whether "open" or "closed".

Closed System Policies and Access Security

A discussion about security should begin with the assumptions about the system operating environment. In the case of an approvals management system, the operating assumption is that the system is "closed": e.g. that the grant applications or research proposals and associated approval document data will be maintained within the same institution who is governing the process. Closed systems address some of the data integrity and confidentiality issues through an assumed level of trust among employees that is backed up with SOPs. For example, an SOP might forbid employees from writing down system passwords on notes near their workstations while, in parallel the automation system policy might require rotating to a new password every 90 days. Both work together to ensure data integrity and confidentiality.

With Internet technologies such as browsers and servers with extranet security, it's now possible for external companies, such as sponsors or commercial IRB personnel, to play a role in approval processes. Document and content security make it easily possible to accommodate external participants while hosting the system centrally within the Institution and still maintain a "closed" system context. But, exactly what should be the access security for such a system and how extensive must it be to meet the requirements of 21CFR Part 11? Figure 1 introduces a model of cost/benefits for escalating levels of security that could be used to implement a closed system such as would be used for automating approvals.

Figure 1



Different from an "open" system where 21CFR Part 11 requires stronger authentication involving digital signatures, a closed system might use a combination of identification code (name)/password pairs or, optionally, multiple passwords for certain electronic signature actions. Note the distinction between "digital signatures" and "electronic signatures"; some security technologies that implement the former—several of which are still unproven—present cumbersome usage and cost challenges. For practical purposes of IRB, IACUC and ancillary committee approvals, Click implements only name/password and, where requested, multiple password authentication. Reviewing each starting from the low end:

- Name/password: the most widespread authentication scheme for electronic signatures, this scheme has the advantage of being familiar to anyone who has ever touched a computer. When abutted by SOPs that ensure proper password administration and conscientious employee use, name/password schemes provide an appropriate first-level of system access and operation. In addition, when combined with “strong” passwords (those involving both letters and numbers) and rotation schemes to force password changes every 90 days, resistance to breach becomes greater still and presents users with minimal password complexity.
- Multiple passwords: requiring a 2nd "signature" password for comments, changes and approvals provides added protection against careless or deliberate unauthorized use of the system. After signing-in with a system-wide password, certain creation, modification or approval actions can require the use of a 2nd password before the system will record the user's action. Adding complexity to the administration and usage process, multiple passwords now must be rotated on a similar basis to the conventional ones, but only to a select audience of users who, for their part, need to retain the confidentiality of a 2nd key. This approach involves more effort for users (to retain password safely and to recall them) as well as for administrators (to issue and track passwords and to reset passwords when they have been lost or forgotten). Though definitely manageable, the efficacy of such a system depends upon the diligence of the users and the responsiveness of the administrators; however, its value depends on the overall reduction in risk of fraudulent approvals that the institution perceives is gained through a 2nd signature compared to the administrative costs of gaining the signature.
- Public Key Infrastructure (PKI) authentication: PKI document encryption with private and public keys is arguably the most comprehensive and secure means of ensuring the identity of an author and tying it irrefutably to a singular edition of a document. However, PKI technology also complicates system design, performance and user experience. With digital certificates, users are typically tied to their workstations for signing operations, which eliminates the cost advantages of universal browser access: each time a user wishes to work from a different machine, a process to transfer the certificates to the new machine adds complications. In addition, like passwords, the loss or theft of a private key can result in impersonation. Finally, additional care must be used in determining the performance characteristics of a system where thousands of users are taking actions involving digital certificates: authentication traffic involving public/private key decoding can present significant computing overhead. Pilot testing the use of PKI on a small population of users would seem to be a prudent means of observing its characteristics (and costs) before widespread roll-out in a production setting.
- Biometric identification: using physical data as an authentication means continues to raise legal questions as well as questions of efficacy. Fingerprints, facial scans, voice recognition technologies have repeatedly gained press for spectacular failures. For example, read this recent BBC article: http://news.bbc.co.uk/hi/english/sci/tech/newsid_2016000/2016788.stm. Also, with the costs involved in adding hardware, it seems likely that biometric identification's adoption will be limited to applications where multiple means of verifying identity are required (e.g. military or national security applications).
- Future: the legal issues of collecting biological identity data aside, at some point in the future, hardware costs for effective biometric monitors may come down and PKI issues eased with the familiarity that comes

from widespread exposure. At that time, the distinctions between authentication for closed and open systems may well blur as costs and usage difficulty become insignificant.

Summary

An Institution must choose the right technologies that encourage automation system adoption by the constituents who need it most: the PIs, the IRBs and Department personnel. Security for any approvals system is a constant decision-making process that must balance SOPs for physical system access with the use of appropriate, available electronic technologies that resist breach, but encourage easy-to-use steady-state operation. Click Commerce's Compliance Extranet meets or exceeds the requirements in 21CFR Part 11 for "closed" systems by providing manageable name/password administration, strong passwords with rotation options and optional 2nd password signatures when desired for specific approval actions and comprehensive audit logs to track all signatories' activities within electronic processes.