



Electronic Submissions in Compliance with Regulatory Requirements for the Global Pharmaceutical Industry

Bridging the Gap Between Document Management and High Security

Table of Contents

Introduction	2
The Technology Behind the Process	2
Choosing the Right Tool for the Job	3
Adobe Self-Sign Capability	3
Livelink from Open Text	3
Kyberpass TrustPlatform – Squaring the Circle	3
SAFE	4
Summary	5

Introduction

Many businesses today are seeking to reduce costs and improve efficiencies through a re-engineering of their business processes. The Life Sciences industry is no exception to this trend. A notable case-in-point is the documentation chain for new drug application (NDA) submissions. To bring a new drug to market now costs on average about \$800 million. It has been estimated that 30 % to 40% of that cost arises from the paperwork associated with an NDA. To put this in perspective, the documentation paper trail for an NDA consists of between 500,000 and 1 million pieces of paper, enough to fill several trucks. This is clearly a burdensome undertaking, and a prime candidate for business process re-engineering.

Several years ago, the US Food & Drug Administration (FDA) took the initiative, to encourage electronic filing of NDAs. This was not a mandatory change, but created an opportunity for the industry to substantially reduce the cost, and more importantly the time taken, to submit NDAs. In view of the enormous cost of the approvals process, even small improvements in the time to market with a new drug represent many millions of dollars of savings on each drug. The economic argument is compelling if one considers that every day saved in the NDA submittal process translates into \$2 to \$3 million dollars of revenue generation.

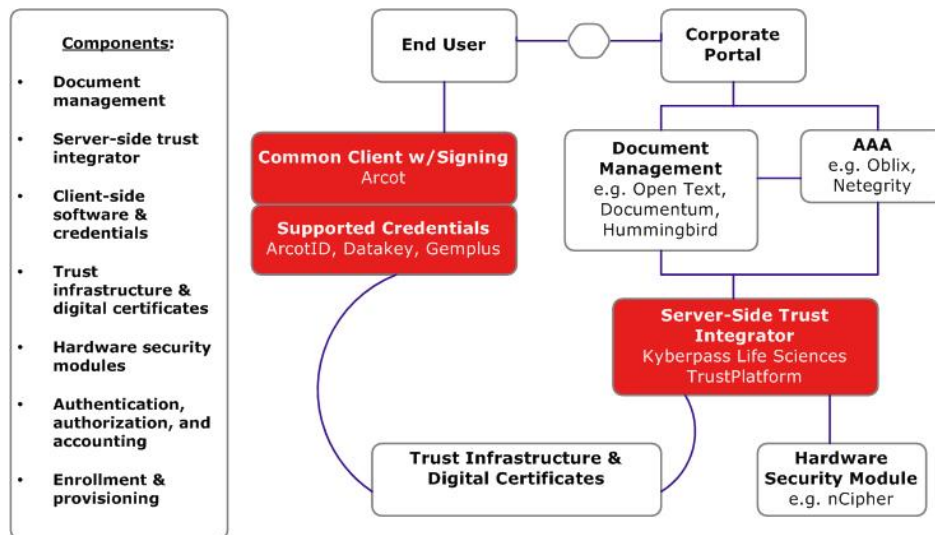
The Technology Behind the Process

A complete end-to-end electronic submission is not a simple matter. Not only must companies automate their document management process, but they must also ensure that the entire chain is secure and auditable. However, all the components required to complete this task exist and are proven. The challenge is to integrate all the pieces into a compelling and manageable solution. To be truly complete, such a solution relies on a trusted third party (TTP) to ensure that users are who they say they are and that they are authorized to sign the appropriate documents at the time of the submission. With this in place, you have a legally binding electronic submission, including the signature page, and no requirement for paper documents or physical storage.

Another critical aspect of a complete solution is a seamless integration of the component parts of the process. This means that document management systems, often already deployed in a Life Sciences company, are integrated with the tools needed for authentication, authorization and accounting (AAA), and that all of these applications are tightly integrated with an appropriate underlying trust infrastructure.

The trust infrastructure itself must be compliant with established and recognized standards that meet the legal and regulatory requirements of the pharmaceutical industry. This leads in turn to a requirement for other technologies, such as digital certificates, hardware security modules (HSMs) and Public Key Infrastructure (PKI) to complete the solution set.

A Complete End-to-End Solution



Choosing the Right Tool for the Job

According to their use, documents may require different levels of trust. Today there exist a number of products to meet the trust criteria for a specific document. Some of these options are illustrated below:

Adobe Self-Sign Capability

Adobe Acrobat provides a Self-Signing function, which allows users to sign, verify the signatures of other users and build a Trusted Certificate list. The user certificate is a separate file exported from Acrobat for verification. Acrobat also contains a hidden part, which contains a mechanism for binding the signature to the Adobe Portable Document Format (PDF) file.

While this does supply a moderate level of security, there is no validation of the certificate by a trusted third party to ensure that the person who signed the document is who they claim to be and is authorized to do so. This signing capability is limited to PDF documents and cannot be used, for example, to sign extensible markup language (XML) documents.

Livelink from Open Text

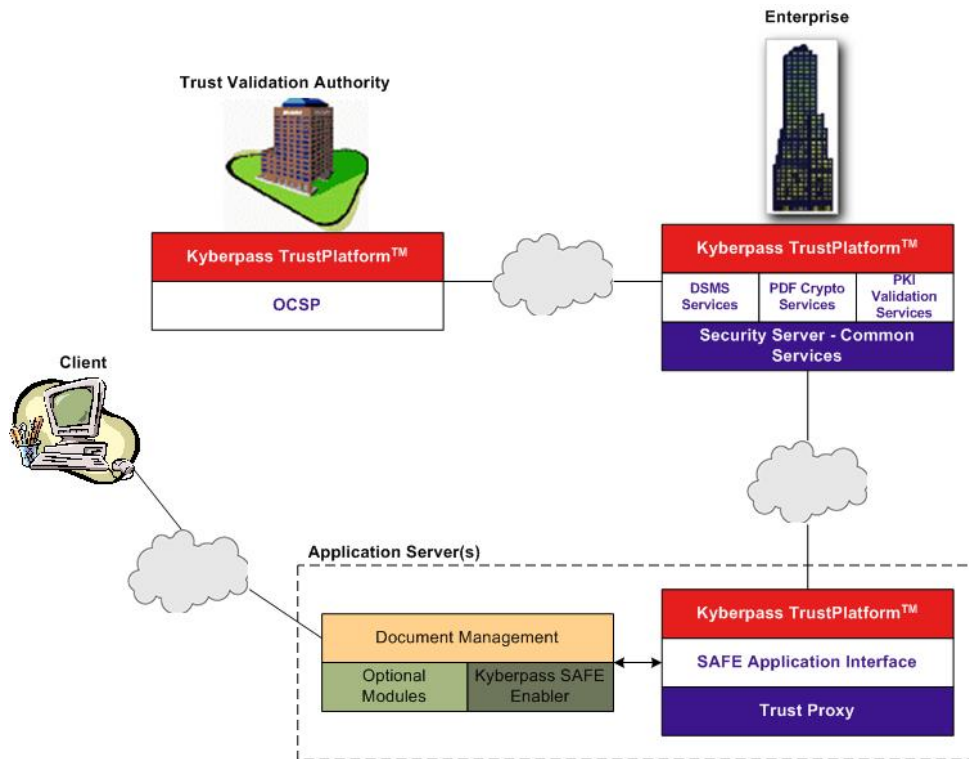
Livelink eSign™ is a sophisticated document management (DM) product, which supports workflow procedures, permissions, document integrity, and many other features found in quality DM software packages. But it does not support digital signatures. Rather, Livelink relies on policies and procedures to guarantee that security requirements and regulatory compliance are met.

For cases where a legally binding signature is required, Livelink provides an audit trail, a workflow map and the ability to generate a letter attesting to the legal validity of the electronic signatures.

Livelink can also generate an XML header file containing a digital certificate to accompany a document. This file is not bound to the document, however, and is not compliant with the signature requirements of the FDA's regulation 21 CFR Part 11. Moreover, these digital signatures cannot be validated through a trusted third party.

Kyberpass TrustPlatform – Squaring the Circle

The Kyberpass Life Sciences TrustPlatform provides a security framework that DM and other applications can use to provide the high-trust component of an electronic submission and other documents. The platform provides a seamless connection between popular DM applications (e.g. Documentum, Open Text, Hummingbird, Adobe) and a standards-based trust infrastructure. The net result of this effort is to enable such products to work with **Legally Admissible Digital Signatures** in compliance with the FDA's 21 CFR Part 11 regulations. *Legally binding* derives from Part 11.100-b "Before an organization establishes, assigns, certifies, or otherwise sanctions an individual signature, the organization shall verify the identity of the individual". The Kyberpass TrustPlatform provides for this verification step.



Vendors of DM systems, and many other applications for that matter, have tried to add security as an after-thought, some time after their products were originally developed. Since security was not a conscious part of their design, compromises have frequently had to be made. In contrast, when Kyberpass set out to create a high-trust electronic collaboration environment, its architectural approach treated security as a fundamental design criterion. Kyberpass has created a clean application programming interface (API) enabling customers to connect to their underlying security infrastructure via the Kyberpass TrustPlatform with minimal disruption to existing applications.

SAFE

About three years ago Pfizer, one of the world's leading pharmaceutical companies, began what has now become a shared, industry-wide initiative to develop and agree an identity management scheme that would address the security needs of regulatory bodies around the globe. The scheme will provide a basis for secure information exchange both internally, within Pfizer, and on a wider cross-industry basis. The initiative is called **SAFE** - Secure Access For Everyone - and is now widely endorsed and actively financed by 15-20 of the world's largest pharmaceutical companies.

Based on guidelines established by the FDA, the SAFE initiative is defining digital credentials, which will satisfy the requirements of the FDA's 21 CFR Part 11, EMEA and the national regulatory authorities of a number of key countries around the world. The credentials are expected to be based on a superset of the globally recognized, bank-backed, Identrus trust standard. But significantly, while the Identrus standard meets the requirements of the global banking environment, it is not currently sufficiently stringent (in terms of archiving legal accountability, etc) to meet the SAFE specification. Nevertheless, Identrus provides a substantial building block on which to create SAFE, and a number of leading Identrus banks are promoting this approach.

Like all infrastructures, however, the value of SAFE comes in its use not simply in its definition. In the coming months, SAFE compliance will be built into a wide range of applications and transactions. Any application that has a requirement for a legally binding, standards-compliant digital signature as part of its business functionality is a candidate for the Kyberpass TrustPlatform. Work is proceeding on a number of fronts to make SAFE compliance generally available to the industry. Kyberpass, together with its partners, has taken a leadership position in making this happen.

Summary

There is a number of compelling business reasons for drug companies to comply with 21 CFR Part 11 and the requirements of the leading regulatory authorities worldwide:

- The savings in time and paperwork associated with electronic submissions is enormous with paybacks being measured in days rather than months
- With improved efficiencies in the submissions process, the volume of NDAs being processed can be increased substantially without adding additional administrative overhead
- As the economics of bringing drugs to market is improved, drugs not previously considered cost effective can be re-considered
- All businesses need to improve their cost structures and streamline their processes to remain competitive. Electronic submissions are a good example of applying this principle to the pharmaceutical industry

Kyberpass and its partners are collaborating to deliver an entirely new business process with minimal disruption to established procedures. Over the next few years SAFE will become an established methodology of business for the Life Sciences industry with substantial financial benefits for all parties in the supply chain.

©2004 Kyberpass Corporation
1111 Prince of Wales Drive, Ottawa, ON K2C 3T2 Canada • www.kyberpass.com

ALL RIGHTS RESERVED. THIS DOCUMENT IS PROTECTED BY COPYRIGHT.

THIS PUBLICATION IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR NON-INFRINGEMENT.

THIS PUBLICATION COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN; THESE CHANGES WILL BE INCORPORATED IN NEW EDITIONS OF THE DOCUMENT. KYBERPASS CORPORATION MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE PRODUCT(S), AND/OR THE PROGRAM(S) DESCRIBED IN THIS DOCUMENT AT ANY TIME

<MWP600_03.0604>