PKI Adoption Case Study (for the OASIS PKIA TC)

ClinPhone Complies with FDA Regulations Using PKI-based Digital Signatures

PKI Project Title	Digital Signatures for ClinPhone
Organisation concerned	ClinPhone
Timeframe of implementation	24 hours
Date went live	March 2005
Case study author	Uri Resnitzky
Contact details	uri@arx.com

1. Business background

ClinPhone is the world's leading Clinical Technology Organization (CTO) providing innovative and proven solutions for global clinical trials. ClinPhone has been serving the pharmaceutical and biotechnology industries for 15 years; evolving from a small, local company in Nottingham, UK to a large, global provider of clinical technology products. Today, ClinPhone's customers range from small biotech's to the world's top pharmaceutical companies. From globalization to cost containment to increased regulations – ClinPhone is a customer-driven organization, continuing to develop, refine, and evolve their product offerings based on research and feedback from their customers.

ClinPhone's experience spans from Phase I to Phase IV studies, ranging from single center studies with 20 patients to 'mega trials' with over 40,000 patients. The company has over 15 years of unrivaled track record for innovation in the development of clinical trial technology, over 2,000 studies, in 90 countries and over 70 languages. ClinPhone undergoes between 40 – 50 audits annually.

More information about ClinPhone is available here: http://www.clinphone.com

2. Objectives for the PKI Project

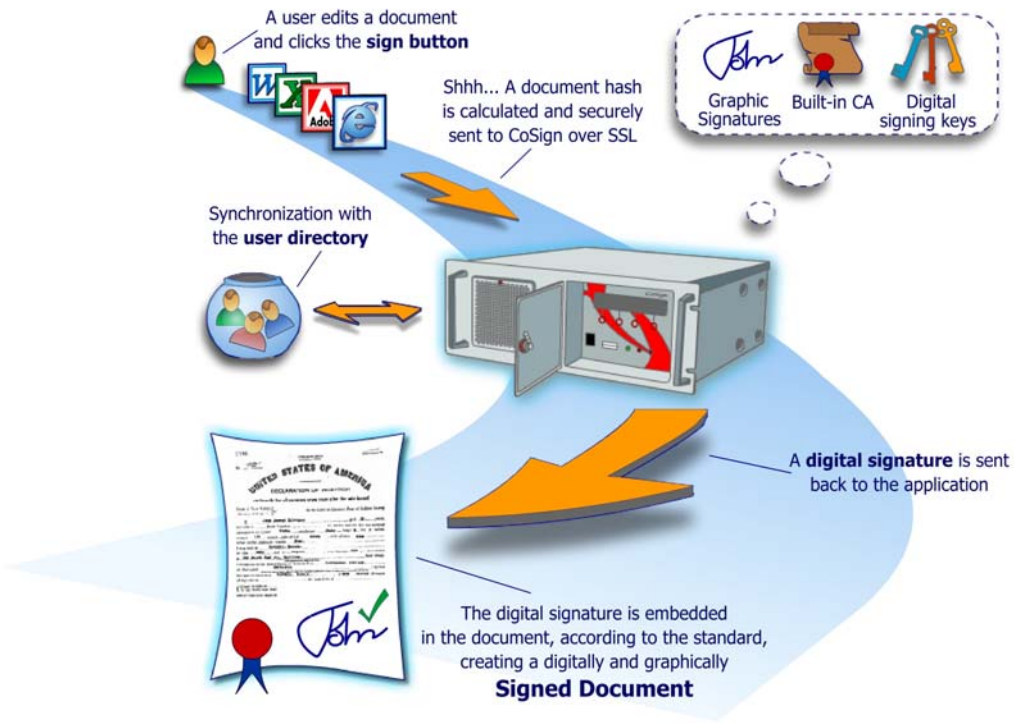
- *As part of the move from paper to electronic documents ClinPhone sought a digital signature solution that would enable compliance with stringent industry regulations. These include the US FDA's Title 21 CFR Part 11 – federal regulation for the use of electronic records and electronic signatures, GxP - a set of pharmaceutical industry quality guidelines and best practices including GMP (Good Manufacturing Practice), GCP (Good Clinical Practice), GLP (Good Laboratory Practice) and GAMP (Good Automated Manufacturing Practice), Computer System Validation, and others.*

- *The underlying motivation for the paperless initiative was improving ClinPhone's internal business process efficiencies: for example a paper-based approval processes could take 2 weeks to get signatures from 3 people in 3 different offices around the world. Delays in documents issuing and filing and the logistics of transferring documents between sites are among the issues identified by ClinPhone as associated with paper documents signed with 'wet ink'.*
- *Target users included 600 employees in three worldwide offices (UK, Belgium & USA) creating a large number of Microsoft Word & Acrobat PDF documents the majority of which are needed to meet regulatory requirements, demonstrating that ClinPhone's systems are validated and controlled. Many of these documents (such as Standard Operating Procedures (SOPs) and Audit Reports) have to be signed by several people.*

3. System notes

PKI Implementation

- *ClinPhone chose to implement its PKI-based digital signature system using an enterprise version of the ARX CoSign appliance. CoSign is a tamper-evident, hardware appliance offering centralized key generation and storage, and server-side signing operations for any authenticated user on the network. (see illustration; more information about CoSign is available here: http://www.arx.com)*



- *ClinPhone chose to operate its own insourced stand-alone root certificate authority which is installed within the appliance.*
- *ClinPhone uses Microsoft Active Directory for identity management, and has procedures in place to ensure that the identity of an individual has been established before their network logon credentials are assigned. Therefore it was decided to leverage the existing identity proofing policies to automatically drive the PKI key-generation and certificate issuing processes. To accomplish this the appliance was configured such that whenever authorized administrators create a new user in the Directory, the appliance automatically generates a signing key and issues a certificate for that user.*
- *ClinPhone chose to leverage the existing Active Directory authentication infrastructure (based on the Kerberos protocol) to control users' access to their signing keys. This means that once a user is logged into the corporate network, client side applications can securely prove the user's identity to the appliance using the Single Sign On features of the Kerberos protocol. This allows the appliance to select the correct certificate for the logged-in user from the many certificates it may have stored.*
- *Following specific guidance in the FDA 21 CFR 11 regulations, ClinPhone chose to augment the security by configuring the appliance to require manual username and password entry and enforce correct validation against the Active Directory each time before a signing key is allowed to be used. Note that verification against the Active Directory preserves ClinPhone's existing investment in password aging mechanisms which is required by 21 CFR 11, and helps user acceptance by not requiring a separate password / PIN to be memorized for signing purposes.*
- *To support high availability requirements, ClinPhone installed a secondary appliance in its data centre which is kept synchronized with the primary appliance using secure replication. This means that users can continue to sign documents (a mission critical function) even if one appliance fails.*

Application Integration

ClinPhone's users use Microsoft Windows based desktops & laptops as well as remotely accessing Citrix servers. Digital signature functionality was provided to users as an add-on to the Microsoft Office products which are used to create the regulated documents. This off-the-shelf add-on which is part of the ARX CoSign client software allows users to add signature fields into the documents, configure the signature appearance and of-course sign and validate signature fields. PDF files are signed using Adobe Acrobat which supports the MS-CAPI interface. ClinPhone configured the system so that each signature includes the full name, a graphical representation of the hand written signature (captured once using an electronic pad and stored within the appliance tied to the user's signing key), the date and time of the signature (taken from the appliance's clock which is synchronized with a reliable time source) and the reason for the signature (chosen from a pre-configured list). This ensures that ClinPhone complies with appropriate

regulatory requirements including the electronic signature requirements of 21 CFR part 11. Templates were prepared for frequently used document types (such as SOPs) which already include approval pages with built-in signature fields ready to be signed by the various managers once the document is complete.

The digitally signed documents are stored centrally in specified write-protected directories comprising a secure archive. The electronic version held on the network is considered the source document and printed documents are for working use only.

4. Business impacts

The Approval process was sped up. Previously, obtaining an approval on a project required staff to fax documents from ClinPhone's HQ in the UK to branches around the world. The approval process could take anywhere between three to four weeks to secure signatures from all the parties. After implementing the PKI digital signature solution an approval process can be completed in 10 minutes. The increased productivity benefits to the company are obvious.

Digitally signing documents also reduced the need for every document to be printed, filed, microfilmed and archived. Documents only need to be printed when specifically required. Source documents are now available on the corporate network at all sites 24/7 reducing the need for faxing, making certified copies and the number of original documents that have to be couriered between locations. The impact of this is a reduction in expenses related to paper documents.

Due to centralized nature of the deployed PKI solution, it is possible to quantify the use of digital signatures within ClinPhone by analyzing the audit log generated within the appliance. From this analysis we can see an extremely quick adoption of the system and consistent use exceeding 1,500 signatures per month all through the first year of deployment (with each user signing on average once every 3.5 working days).

Because of the system-in-a-box characteristics of the deployed PKI system, ClinPhone's IT staff and business process owners could quickly install, configure, deploy and maintain the system throughout the company with no specialized knowledge or training in PKI.

5. Next steps and suggested improvements

ClinPhone's deployment of a PKI-based system was driven by the need for electronic signatures. Currently the signatures are mainly verified inside ClinPhone offices and used for internal processes. In the future, it is possible that a need to exchange signed document with ClinPhone's customers will arise, which will require working out procedure for trusted distribution of ClinPhone's root certificate. Note however that due to the centralized nature of the system, instant revocation is available simply by disabling or removing

the revoked user's Directory account, reducing the need to handle issuing, publication and distribution of a CRL.

On a wider perspective, moving from paper to electronic documents presents new challenges and potential benefits which can be better realized using a Document Management system in order to better control archiving, versioning, indexing and retrieval of electronic documents as well as automating workflows. ClinPhone has decided to start with the implementation of the electronic signature project before implementing a Document Management system which is the main reason that a PKI based solution was chosen over point solutions available with some Document Management systems. One of the mandatory requirement of any evaluated Document Management system is its ability to process digitally signed files without invalidating the signatures, and Document Management systems that can be made digital signature aware are considered.

Others implementing PKI should try to base their choices on their specific business requirements rather on everything the technology can provide – balancing ease of use and security.

6. Suggestions to the PKI industry

- *To facilitate adoption, the PKI industry should concentrate on making systems easy to use, manage and deploy.*
- *It may be prudent to concentrate on solutions to specific business problems, such as digital signatures for compliance in internal company processes, rather on building a generic infrastructure.*
- *Systems that require specialized personnel, high per-user cost, and working with several different vendors and service providers have a lower chance of being adopted successfully.*
- *For digital signature systems within organizations, server-side signing combined with leveraging of existing infrastructure for user identity management and authentication provides a sound basis. This has to be augmented with tight integration on client desktops which should be as transparent as possible providing support within applications users work with every day.*