White Paper

Research collaboration in the cloud:
How NCI and Research Partners are using Interoperable Digital Identities, Digital Signatures and Cloud Computing to Accelerate Drug Development

Contributors:

Executive Summary

A 2010 pilot study involving government and industry cancer researchers indicates that using interoperable digital identities, digital signatures and cloud computing will accelerate initiation of a clinical trial while lowering its costs. They participated in the first phase of a pilot study examining use of interoperable digital identities and cloud-based digital signatures to eliminate reliance on paper forms in clinical trials.

The ongoing study involves researchers at the National Cancer Institute's Cancer Therapy Evaluation Program (NCI/CTEP) and Bristol-Myers Squibb Company. NCI/CTEP is the world's largest sponsor of cancer treatment clinical trials.

The researchers were provisioned with interoperable digital identity credentials, a form of software installed on a computer, cell phone or other device, which establishes a close link with the user's proven identity and allows for the application of digital signatures to electronic documents. Unlike their simple electronic counterparts, digital signatures cryptographically guarantee the integrity of documents to which they are affixed. In the pilot study, the electronic documents were placed in the cloud, where the researchers were able to access and sign them immediately. Prior to the study, the signature process was delayed by use of courier service, fax, travel, etc.

The digital credentials exist within legally-binding and regulatory-compliant cyber-communities, known as identity trust hubs.

- All US federal agencies are served by the Federal Bridge identity trust hub, which provided the NCI researchers with their digital identity credentials.
- The biopharmaceutical and healthcare industries are served by an identity trust hub known as SAFE-BioPharma, through which the Bristol-Myers Squibb researchers received their credentials.

The Federal Bridge and SAFE-BioPharma cross-certified to become interoperable, allowing a digital identity asserted by one to be trusted by the other. Both the Federal Bridge and SAFE-BioPharma are part of a matrix of identity trust hubs serving governments, industry sectors and higher education. These identity trust hubs are affiliated through the Four Bridges Forum (www.the4BF.com).

Phase I (July 2010 – October 2010) demonstrated the use of digital identities for authentication and the application of digital signatures to electronic documents

Phase II (underway) expanded the study to include researchers in sanofi-aventis.

Phase III (expected to start mid-year) will include researchers at universities and academic cancer research centers. Their digital identities will be part of the Research Education Bridge Certification Authority (REBCA), an identity trust hub serving the country's higher education sector and which currently is in the process of cross-certifying with other trusted cyber-communities.

The pilot successfully demonstrated the ease with which interoperable digital identities could be deployed and used to access electronic documents and apply digital signatures to them. It eliminated use of paper copies and allowed signed documents to be exchanged rapidly and securely on-line for business processes initiated by the NCI/CTEP's Protocol and Information Office (PIO).

Background

Numerous forces are driving public and private sectors to exchange confidential documents via Internet faster, more economically and with greater security. Pharmaceutical companies are highly collaborative and require a constant flow of confidential information with researchers, healthcare providers, and regulators worldwide. R&D productivity is one of the major challenges facing life sciences. Time lost in starting or conducting clinical trials results in substantial financial losses and delays delivery of new therapies to patients. NCI has been mandated to more quickly initiate clinical trials to patient accrual, to reduce costs, to streamline document management while assuring greater document security, and to have environmentally sound procedures.

SAFE-BioPharma and Federal Bridge Certification Authorities

The SAFE-BioPharma standard and the Federal Bridge Certification Authority (FBCA)use public key infrastructure (PKI) technology. PKI is used by numerous stakeholders (particularly governments and regulated industries) to verify identities and to protect information exchanged via the Internet. When PKI communities, also known as “identity trust hubs,” cross-certify with each other, they become **interoperable**, thereby allowing a digital identity asserted by a user from one community to be relied upon and accepted by a relying party from another community.

Among other trust hubs, SAFE-BioPharma is interoperable with FBCA, the U.S. government’s PKI-based system serving U.S. federal agencies.

SAFE-BioPharma -- The SAFE-BioPharma standard requires that the signatory’s proven identity is captured in a digital certificate and made available to apply digital signatures. The standard also requires each digital identity to adhere to rules that guide and regulate its uses.

SAFE-BioPharma digital signatures offer a greater level of protection than other forms of electronic signature. They provide authentication, non-repudiation and data integrity across every single bit of the information to which the signature is applied. In simple terms this means that if any component of the signed document is ever changed, the signature will be invalidated. The contract-based standard requires all members and users to meet technical requirements, to accept each others’ SAFE-BioPharma identities and signatures, and to enter into the community’s risk mitigation system.

SAFE-BioPharma was created specifically for use in the global biopharmaceutical industry and in the healthcare arena. The US Food and Drug Administration (FDA) and European Medicines Agency (EMA) have been and continue to be active participants in the standard’s development and evolution. SAFE-BioPharma digital identities are recognized and trusted within the SAFE-BioPharma community.

SAFE-BioPharma credentials can be provisioned from a variety of certificate authority infrastructures including Citibank, Exostar, IdenTrust, PGP TrustCenter, Trans Sped, and the SAFE-BioPharma system operated by Verizon Business Systems.

Federal Bridge -- The Federal Bridge Certification Authority is an identity trust hub used by NCI/CTEP. *FBCA and SAFE-BioPharma have formalized relationships with each other and each asserts the identity of its participants across the entire federation*. This relationship allows biopharmaceutical companies that use the SAFE-BioPharma standard and US Federal agencies that use FBCA to recognize and accept documents that carry each other's digital signature. This demonstrates the efficiency and security of cross-jurisdictional credentials usable by all participants and secured through a PKI-based infrastructure

The Federal Bridge and the Federal Public Key Infrastructure Policy Authority (FPKIPA) are, in part, based on standards/guidance provided by NIST.

NCI/CTEP

NCI/CTEP is the world's largest sponsor of cancer treatment clinical trials, reflecting its mission to improve the lives of cancer patients by finding better ways to treat, control and cure cancer.

The program currently has 900+ active clinical trials testing new cancer treatment regimens. It activates approximately 130 new protocols per year. During the protocol lifecycle, from concept to closure, each protocol produces many signed and exchanged documents among multiple participants, including cooperative groups -- groups of physicians and/or medical institutions cooperating to investigate new treatments, cancer centers and academic institutions.

To pilot the digital signature process, NCI/CTEP selected its randomized Phase 2 and Phase 3 trials conducted through Cooperative Groups.

The protocol process follows:

- A Cooperative Group submits a Concept/ Letter of Intent (LOI) for CTEP review and approval
- After CTEP review a signed letter is sent to the cooperative group along with a consensus review of suggested changes.
- The collaborating pharmaceutical company receives a copy of the LOI or concept and submits a signed drug approval letter allowing CTEP to approve the LOI/Concept so the group can author and submit a protocol.
- Upon CTEP receipt of the protocol, a signed acknowledgement letter is sent to the Cooperative Group.
- Once the protocol is reviewed by CTEP; a signed comment letter is sent back to the Cooperative Group.
- A revised protocol is then resubmitted (there may be multiple revisions before final protocol approval is granted).
- CTEP approval or disapproval of the revised protocol is sent via signed letter.
- Amendments to protocols follow the same last few steps for review, revision, and notification of approval or disapproval.

Business Need

The pilot demonstrated dramatic time savings for all document flows that require multiple signatures from participants working on or off-site. It demonstrated how an all electronic workflow including digital signatures improves the business process flow and thus improves the ability of NCI to speed up research and be more responsive to public health needs.

Documents

The first step was to develop digital signature and workflow capabilities for the following documents:

- Protocol receipt Acknowledgement Letter
- Protocol Approval/Disapproval
- Clinical Trial Agreements
- Contracts

Streamlining the signature workflow of these documents allowed research to get underway more quickly. Depending upon specific documents involved, it eliminated hours to weeks to months in the document workflow process.

Digital Signature Service

The enhanced services were provided by utilizing FBCA cross-certified, PKI-based, digital certificates with existing SAFE-BioPharma members. In subsequent phases, these certificates will be deployed to all cooperative groups and drug suppliers.

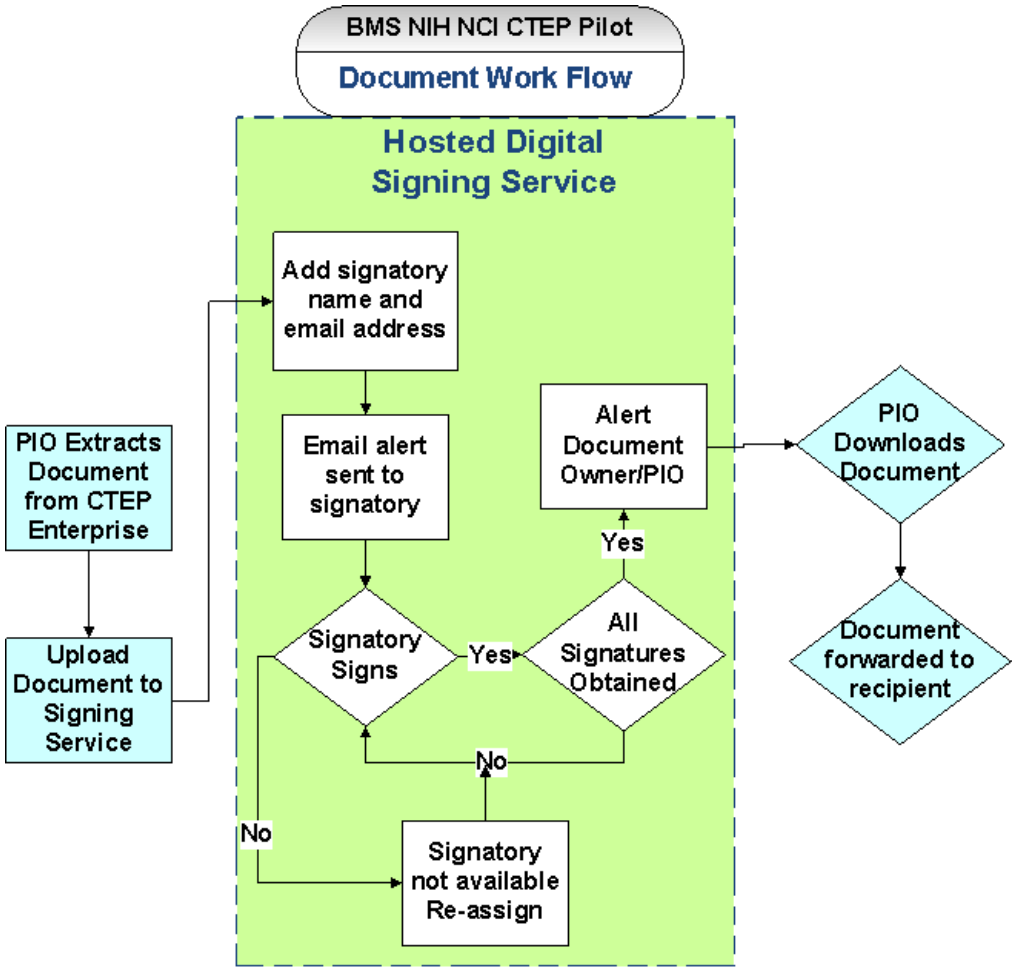
The architecture consists of each signatory having Internet access and a FBCA or SAFE-BioPharma cross-certified digital credential and access to a digital signature service. This project leverages an existing Safe-BioPharma hosted digital signature service (DSS), which replaces handwritten signatures and paper based document routing services such as courier and/or fax. The documents are available only to people signing the documents, with access controlled through a self-provisioned user account based on each user's email address. Because the address must match the email address in the digital credential, only digital credentials issued from approved Certification Authorities are accepted. Once provisioned, access can be controlled via strong 2-factor authentication.

1

The DSS works as follows:

- A document requiring signatures is uploaded to the DSS.
- Signatories are alerted via email that a document is awaiting signature.
- Once all signatures are obtained, the document originator is alerted to download the document.

The DSS provides significant value while enhancing security and respecting state and federal privacy laws. The following diagram illustrates the system-level document workflow topology:



Identity Proofing

E-Authentication identity proofing/assurance levels are defined by NIST SP 800-63-1 and cover four assurance levels. Levels 1-2 are single factor with different identity proofing methods as follow:

- Level 1 does not require identity proofing, i.e. the credential holder asserts his identity and proof is not required.
- Level 2 requires proof.
- Levels 3-4 are 2-factor authentication with more rigorous identity proofing methods. Government identification documents with requirements (Level 4) must be provided to prove the source.

The Federal Bridge Certification Authority – Certificate Policy (FBCA-CP) allows for five different assurance levels (Rudimentary, Basic, Medium, Medium Hardware, and High) for public key certificates. These FBCA-CP assurance levels are a combination of an appropriate identity proofing and credentials, e.g. FIPS 140-2 encryption. (Source: FBCA_CP_RFC3647.pdf).

The different assurance levels, aligning NIST SP 800-63-1 and the FBCA-CP, require coordination and can be verified with the FPKIPA and its Certificate Policy Working Group. SAFE-BioPharma Association sits on both committees, as a non-voting member, through the FBCA cross-certification.

Additionally, the FPKIPA requires an annual audit by all participants to verify effective implementation of the FBCA-CP. The FBCA-CP is the aligning document that all FBCA participants, e.g. DHHS, DoD and all cross-certified issuers (i.e. SAFE-BioPharma Association), must adhere to in implementing their respective PKI structures and policies.

Results

Cost Savings

Substantial cost savings are anticipated as the pilot moves to production. Using paper forms, an average 10% of the documents are shipped overnight and 10% are shipped by courier service. Using digital signing, those costs are eliminated.

Time Savings

The time savings are significant. Paper processes are time consuming and often require physically shipping documents to signatories. Typically it takes 3 to 5 business days per signature. The pilot demonstrates that each signature can take minutes. Furthermore, NCI/CTEP estimates that in 2010 documents comprising almost 100,000 pages were used to develop and correspond on its clinical trials. While the unit does not track the time involved in scanning, organizing and sending these paper documents to the FDA, it reports that it is extremely labor intensive and, once digitized, will be greatly simplified.

Document Loss

The pilot demonstrates elimination of lost or misplaced documents. Using digital signatures establishes an audit trail of when the document was uploaded, of the email sent to alert the signatory that the document is available for signature, and when the document was actually signed.

Reduced Environmental Impact
Besides saving money, time and reducing document loss, the pilot also is reducing the carbon footprint. Moving to an electronic process eliminates use of paper and ink, eliminates document shipment, and minimizes storage and retrieval needs.

Next Steps
Phase 1 of the pilot was determined a success and Phase II is being initiated with sanofi-aventis and additional BMS staff. Additionally, business workflow processes will expand to include NCI's Regulatory Affairs Branch. Phase III is under development with requests for involvement going out to Cooperative Groups that are REBCA members.

Summary

Use of interoperable FBCA digital credentials and those based on the SAFE-BioPharma digital standard facilitated the successful implementation of a public/private pilot that showed how paper processes can be eliminated from initiating a clinical trial. As the pilot expands to include other companies and university-associated cancer treatment centers [via the Research Education Bridge Certification Authority], the use of interoperable digital credentials and digital signatures to sign research-associated documents will expand. As a result, medical and clinical trial research will be conducted with greater efficiency and therapeutics will be delivered faster and with lowered environmental impacts.

This white paper can be downloaded at http://www.safe-biopharma.org/infocenter/whitepaper_ResearchCollaborationInTheCloud.pdf

For additional information contact SAFE-BioPharma Association • 1 Bridge Plaza, Suite 275 • Fort Lee, NJ 07024 • Phone: 201-849-4545 • Email: info@safe-biopharma.org.