



SAFE-BioPharma Association
Secure Access For Everyone

Meeting the Need for a Global Identity Management System in the Life Sciences Industry White Paper



Authored by:

s t e f l e x

June 2005

TABLE OF CONTENTS

1.	INTRODUCTION	3
2.	EXECUTIVE SUMMARY	4
3.	WHY A GLOBAL ELECTRONIC IDENTITY MANAGEMENT SYSTEM?	5
	3.1 Global Identity and Access Management	5
	3.2 Global Identity Assurance	7
4.	WHAT IS SAFE?	8
5.	SAFE APPROACH	9
6.	SAFE IMPLEMENTATION	11
	6.1 SAFE Model	11
	6.2 SAFE-Pfizer Implementation	12
	6.3 SAFE-GlaxoSmithKline	13
	6.4 SAFE-Merck	14
7.	FUTURE OF SAFE	15
8.	CONCLUSION	16
	APPENDIX A - VALUE TO MEMBERS	17
	APPENDIX B - VALUE TO VENDORS	19
	APPENDIX C – MEMBERSHIP OPTIONS	21

About the Authors:

Fern McBee:

Fern McBee is a Microsoft Certified Systems Administrator (MCSA: Security) and CompTIA Network Certified Professional (Network+) with an Associate Degree in Business. Ms. McBee has experience in providing Information Technology regulatory compliance consulting services for the Pharmaceutical industry. She specializes in securing IT infrastructures and bringing them into regulatory compliance.

Manish Ingle:

Manish Ingle has a MS in Biomedical Engineering, and an MBA in Finance. Mr. Ingle is a PMI Certified Project Management Professional (PMP) and ASQ Certified Software Quality Engineer (CSQE) with 12 years of industry experience including 10 years in Project Management, Quality Assurance and Information Technology. He has extensive knowledge in FDA regulated (GxP) and non-regulated areas related to pharmaceuticals and medical devices with proven ability to verify, validate, conduct software and process quality assessments and perform auditing including audits and assessments under the Sarbanes Oxley (SOX) law.

About Stelex:

Stelex – The Validation Group, Inc. (Stelex) provides enterprise-wide compliance solutions to regulated industries in the pharmaceutical, medical device, diagnostic and biotechnology sectors. The firm delivers a comprehensive suite of validation, technology, regulatory and business solutions. In addition to Quality Auditing Services, Stelex offers Sarbanes-Oxley Compliance consulting, System Integration and Implementation, Security & PKI services, Computer System Validation, Process Validation, Equipment Qualification, Infrastructure Qualification, Program Management and Best Practice Consulting. We offer ComplianceBuilder™, the compliance infrastructure solution for ERES compliance requirements. We also provide a broad range of technical training and professional education through our fully accredited Stelex University.

Acknowledgement:

The Authors would like to thank Dan Matlis, *Vice President* of Stelex for his advisory guidance and input to this White Paper. Special thanks to Chris Haughney at Stelex; Tony Gazikas and Scott Potter at Pfizer; Colleen McMahon at GlaxoSmithKline; Pamela Fusco and Keith Heilner at Merck, Ashley Evans and Rick Krohn at SAFE.

1. Introduction

One of the biggest challenges facing the Life Sciences Industry is the migration from paper to electronic records. To fully leverage the benefits of paperless records and to conduct information exchanges, the industry must establish a virtual environment that is secure and trusted. The foundation of this “digital transformation” is the ability to create and manage a cost-effective global Identity Management System that can be leveraged by trusted partners across disparate domains worldwide. The decision to adopt a paperless operating environment is often based on business case needs, strategic initiatives, or other factors. To date, inconsistencies in technical standards, issues of privacy, data security, and confidentiality have hampered the switch to electronic records. The topic of this White Paper is the development and implementation of a global Identity Management infrastructure that delivers electronic identity credentials for legally enforceable and regulatory-compliant digital signatures. In addition, it takes a critical look at three major biopharmaceutical companies that are adopting a global identity management infrastructure including challenges faced during implementation. From these industry profiles insight is gained into the decision to participate in this global initiative and the lessons learned from their experiences.

2. Executive Summary

Electronic information exchange on a global scale requires a highly secure trust environment where Life Sciences companies and business partners can efficiently use electronic processes to conduct business transactions. Public confidence in the validity, integrity, and reliability of electronic records depends on a common security framework that is uniform, regulatory compliant, and delivers sustainable return on investment. Information exchanges that are subject to regulatory compliance must be considered trustworthy, reliable, and essentially equivalent to paper records. Organizations will save valuable time and resources by moving to digitally signed records and enjoy immediate cost reductions in provisioning and handling identity credentials.

In the business-to-business and business-to-regulatory world, secure electronic business transactions related to identity management have been slow to take off. Driven by the need to improve efficiency of operations while managing regulatory security mandates, the Life Sciences industry, including but not limited to Biopharmaceutical, Medical Device, Diagnostic, and Biotechnology companies spend over \$1 billion per year on independent electronic identity credentialing models that have proven to be difficult to develop, maintain, and integrate.

In 2004, Pharmaceutical Research and Manufacturers of American (PhRMA) reported that approximately 40% of all Research and Development costs are attributed to paper based business processes (\$9 Billion in the U.S. alone). Utilizing digital signatures to sign regulatory documents opens the door for the industry to leverage identity management and electronic information exchange for all paperless transactions, and to recapture many of the costs (ex. duplication, records maintenance), associated with paper based processes.

There is a dramatic change approaching in the way Life Sciences organizations and their business partners exchange information. This change will ultimately benefit everyone by adding significant cost savings and value to the industry. However, online user authentication techniques have not yet translated into industry-wide electronically negotiated transactions. The lack of legally enforceable Digital Signatures prevents the elimination of paper.

Identity infrastructures in companies today are not interoperable. Identity credentials for employees and business partners are gaining acceptance within the Life Sciences industry. A practical approach to streamlining identity management and achieving interoperability involves utilizing a single credential platform that is easy and straightforward to use for employees and business partners alike. There is a significant return on investment that can be achieved by:

- Reducing password-based authentication to corporate networks and applications.
- Simplifying the process of ensuring proper levels of security for users and groups.
- Eliminating the complexity of employees and business partners who have the burden of managing multiple identity credentials.
- Reducing ROI due to paper reduction
- Streamlining the workflow
- Uniformity of standard identity infrastructure

Organizations continue to embrace new technologies designed to improve the flow of data, and lower IT costs. Technological breakthroughs eliminate the need for multiple user ID credentials and costly paper-based business processes. Identity Management is a foundation upon which many of these breakthroughs can be built. This paper concentrates on the driving force behind an innovative global Digital Identity and Access Management system poised to become the industry standard for Life Sciences companies.

3. Why a Global Electronic Identity Management System?

There is a need in the Life Sciences industry for secure electronic business transactions, confidential information sharing, and electronic funds transfer over the Internet. One key barrier to global collaboration is the lack of an Electronic Identity Management system that establishes trust between Internet communities. The current Internet security model is open to everyone with various levels of security. For example, there are popular online eCommerce services that are open to the general public to buy and sell goods with the only criteria being online personal profile registration and a credit card number. The true identity of the person using the card is not verifiable. Unfortunately, sophisticated computer hacking has left confidential information accessible and vulnerable to misuse. Life Sciences information exchanged electronically must be compliant with international regulatory requirements, contain strong security features, and be legally enforceable across borders. Companies and their business partners are relying on independent trust relationships to exchange sensitive information.

With the proliferation of unsolicited e-mail and privacy invasion concerns, *“We are going to see the World Wide Web evolve from an open system where everyone is trusted to a closed system where no one is trusted without some type of identification credential that is verifiable”*, forecasts Tony Gazikas, Vice President World Wide Development Informatics at Pfizer. Industries are responding to the need to leverage the Internet for electronic transactions while protecting their valuable information assets.

For global electronic trust, the external network infrastructure must be a closed-user system for credentialed members and based on a common security standard. A global identity management system is the foundation upon which to build global trust for electronic interactions. The system must be cost effective, and comply with established and recognized standards that satisfy legal and regulatory requirements. The global trust challenge is predicated on a collaborative security framework that supports a broad array of participants across a multitude of applications, resources, and domains. There is a need for a standards-based trust infrastructure that ensures interoperability between companies, on-line privacy of medical data, authentication, and digital signing. The solution should include a web-based platform that will enhance business process efficiency involving regulatory data collection and exchange. Along with research and development documents and submissions, it will automate the registration process with regulatory agencies and sponsors streamline processes involving clinical investigations, and financial transactions and disclosures.

3.1 Global Identity and Access Management

IT security teams worldwide are encountering the same user authentication issues with little or no collaboration. Additionally, user access to system applications often requires multiple user IDs and/or security tokens within a single company. More Life Sciences organizations are embracing the idea of replacing their multiple user identification and access control model with one unique identity credential that is secure, multi-purpose, and convenient for employees and business partners.

The key to inter-industry collaboration and identity management is to apply the common security standard to the internal infrastructure. Build upon the internal identity authentication scheme by aligning applications and business processes with the same security standard. Once companies are capable of establishing a strong internal security model that can be applied in a uniform manner

throughout the organization, then the trust domain can expand beyond the boundaries of the corporate infrastructure.

Unique Identity Credential

The industry is recognizing the need to improve regulatory business interactions by establishing a global digital identity assurance system that verifies that a person actually is who they say they are. The global adoption of a uniform security standard for electronic identity credentials enables seamless interoperability for access control to physical premises, mission-critical information systems, and applications at the security level. Standardized systems provide much needed flexibility and cost relief by migrating from a company-specific security standard to an industry-based model. In today's drug development environment, for example, clinical investigator sites, university medical centers, and medical labs all use different identity credentials for remote access to sponsors' information systems. For clinical investigators, this means multiple credentials to access various systems. Many of these inflexible systems have independent security models that are expensive to setup and administer.

For global identity credentialing and trust to be established, it is essential to align a company's internal employee identification system and business processes by linking them with a unified security framework. Ideally, a multi-purpose electronic identity credential needs to be portable, offer cryptographic functionality, and link multiple credentials to one hardware device which holds the unique identity credential. To ensure a higher level of security, the security platform for the electronic token should be based on two-factor authentication (what you know and what you have).

Physical Access

Regulatory requirements and corporate security concerns of Life Sciences IT professionals have resulted in the need for stronger security controls. As a result, companies have deployed an identity management system that authorizes employee access to the company's premises which is restricted by location. The ability to authenticate an employee's identity electronically between corporate locations is not being implemented in today's environment. Deploying a single User ID badge for all employees that is based on a common security standard will increase convenience without compromising security by standardizing physical access across different sites. For example, off-site meetings with regulatory agencies from around the world that require verification of the participants' identity will be simplified. A unified system improves operational efficiencies, enhances productivity, increases user satisfaction, reduces administration costs, and eliminates the need for additional security screening. Once a local identity management system is in place, which is based on a common security standard, then participation in a global identity management infrastructure becomes possible because it is based on the same security standard.

Single Sign-on

Public Key Infrastructure (PKI) is the electronic security infrastructure that is recommended for Single Sign-on (SSO) using Secure Sockets Layer (SSL) which allows for authenticated and encrypted communication. PKI SSO streamlines the authentication process and simplifies the process of ensuring proper levels of security for users and groups. SSO architecture reduces the cost of end user issues handled by the Help Desk. SSO enables end users to authenticate once from any workstation and have access to those applications for which they are authorized to access without the need to re-authenticate. For global single sign-on capability, digital identity

credentials need to be interoperable, deployed throughout the entire corporate infrastructure, meet regulatory requirements, and be aligned within a common security framework.

The strategic approach of a unified security standard applied uniformly throughout an organization allows for innovation. Companies are now rolling out PKI- based identity credentials for secure building access, computer single sign-on, digital document signing, executing contracts, and transfer of funds.

3.2 Global Identity Assurance

The use of Digital Signatures in Life Sciences-related business transactions is still in an early stage, primarily due to trust and privacy concerns. For Life Sciences professionals, a Digital Signature solution used to support electronic submissions must conform to a higher standard of trust and security, and should appeal to a global audience. There is a tremendous need for a consistent, industry-wide legally enforceable identity assurance architecture that will streamline business-to-business and business-to-regulator transactions. The challenge: A digital identity assurance standard needs to be developed for the industry that will remove regulatory barriers to wide-spread adoption and reduce the costs to both large and small participants by limiting the required internal infrastructure costs.

Electronic Signatures are legally admissible when backed by a contract that binds the signatory. Public Key Infrastructure (PKI) provides the security, infrastructure that ensures trust, and is typically hosted internally within the end-user organization's local network, or through a third party Certificate Authority (CA). To use Digital Certificates, business software capable of signing and verifying certificates is required. When connected to a standards-based security infrastructure, it enables verification of records and interoperability among global business partners.

The risk of using a generic electronic signature model (that may have no security feature) while seeking the most cost effective way to leverage the Internet for authentication and electronic records processing, is the concern of any stakeholder considering an eSignature solution. Generic eSignature models do not guarantee the identity of the signatory or link the identity of the signatory to the electronic record.

In order to meet a wide variety of regulatory compliance mandates, the Life Sciences industry has come together to develop, implement, and enforce policies and procedures using the concepts of digital identity authentication, access management, and global identity assurance that specifically satisfies the requirements of regulatory agencies such as, but not limited to the Food & Drug Administration (FDA), the European Medicines Evaluation Agency (EMA), the European Federation of Pharmaceutical Industries and Associations (EFPIA), Security and Exchange Commission (SEC), and Pharmaceutical Research & Manufacturers of America (PhRMA). This coalition has formed a not-for-profit, member-owned organization called SAFE Bio-Pharma, LLC.

4. WHAT is SAFE?

Secure Access For Everyone (SAFE) is a global identity management coalition that resulted from a need to provide a consistent and industry-wide method for managing and utilizing digital signatures. The SAFE framework gives companies the ability to sign regulatory and commercial transactions in a legally enforceable way. SAFE is designed for the purpose of simplifying, securing, and streamlining business-to-business and business-to-regulatory information exchange. The SAFE framework allows companies to implement a model where identity is trusted. SAFE is sponsored by the Pharmaceutical Research and Manufacturers of America (PhRMA) and European Federation of Pharmaceutical Industries and Associations (EFPIA) trade organizations with funding and leadership from eight global pharmaceutical organizations: AstraZeneca, Bristol-Myers Squibb Co., GlaxoSmithKline Inc., Johnson & Johnson, Merck & Co. Inc., Pfizer, Inc., Procter & Gamble, and Sanofi-Aventis.

SAFE provides the security and legally enforced standards for business processes and applications that fall within regulatory oversight. SAFE enables a secure, reliable means of communicating and executing transactions over public and private networks. The SAFE security standard enables seamless connections between mission-critical applications and a standards-based trust infrastructure. The unique SAFE credential uses PKI technology for global identity badges and Digital Certificates for legally binding and regulatory compliant document signing and encryption for business-to-business and business-to-regulator transactions.

SAFE incorporates the standards from Internet Engineering Task Force (IETF) Request for Comments (RFCs), Federal Information Processing Standards (FIPS), and RSA Security – Public-Key Cryptography Standards (PKCS). To meet regulatory and functional requirements, the SAFE standard utilizes Public-Key Infrastructure (PKI) encrypted key-based authentication that is based on two-factor authentication, in accordance with FDA rule 21 Code of Federal Regulation (CFR) Part 11 Section 11.30 (Controls for Open Systems). The SAFE security infrastructure facilitates global access control, authentication, confidentiality, integrity, and non-repudiation of digital information.

The SAFE standard, End-User Systems Technical Specification (EUSSPEC), provides a platform for a single unique identity credential in which all identity credentials of an individual are centralized on one hardware device.

The technology components of SAFE End-User Systems:

- A *hardware token* which may be a smart card, Universal Serial Bus (USB) token, or other hardware device that supports the generation, protection, and storage of a private signing key corresponding to a public key found in a Digital Certificate.
- The *standard Interface* to the Token. Depending on the format of the hardware token, a separate reader may be required (e.g. a smart card reader) or the token itself may interface with a standard computer port.

5. SAFE Approach

An international precedent already exists for global identity assurance for financial institutions where identity is critical. SAFE-BioPharma, LLC has partnered with Identrus to provide the legal and technical infrastructure for global identity assurance for the Life Sciences industry.

The SAFE credential (Digital Certificate) is unique because it is legally enforceable with formal liability and risk allocation. SAFE's business model is based on shared-cost and shared-service with operational and contractual accountability, administration, and management. SAFE provides members uniformity of compliance and standardized service levels. SAFE offers support documentation including: legal, policy, liability, and technical interoperability.

There are three primary reasons to join SAFE-BioPharma Association and to implement the SAFE infrastructure.

1. Reduced Cost and Workflow Efficiencies. The biopharmaceutical industry spends more than a billion dollars per year on independent identity credentialing models, and nearly 40 percent of all R & D costs can be attributed to paper-based business processes. SAFE members reap the benefits of short and long-term infrastructure cost savings. A single credential for all employees and business partners will result in a cost savings of 38 percent--approximately \$100 per user. SAFE benefits are scalable: as more processes are converted from paper to electronic using SAFE, the more a company eliminates paper, saves time, and reduces expenses.

2. Shared Implementation Lessons and Information Assets. SAFE members can reduce implementation time and risks based on best practices from concurrent implementations. In addition, SAFE has created an arsenal of tools and implementation support documentation to speed and streamline implementation. SAFE information assets include legal briefs, reference implementation, working groups, credentials, compliance tools, best practices, implementation checklist, and a vendor partner program.

3. Network of Industry Leaders. SAFE members gain entry to an industry network that includes market leading biopharmaceutical companies, CROs, health systems, clinical investigators, regulators, and vendors. SAFE and its members have ongoing programs with the FDA, EMEA and the National Cancer Institute. For example, SAFE is working with a dedicated team of FDA resources to ensure that SAFE meets 21 CFR Part 11 requirements and to address the challenges created by electronic submissions. And in a pilot program that includes EMEA and EFPIA, SAFE is being applied to EMEA's Eudralink application for access control and document signing.

SAFE, as an industry standard, is vendor agnostic. Industry collaboration and interoperability is the key to making this work (e.g. open standards for software that can make and validate digital signatures). Market demand, business processes, and regulatory mandates will encourage vendors to follow the lead of Life Sciences companies. Vendors must enable their products to meet an emerging global security standard in order to do business in the Life Science verticals. Ultimately, this capability will be built into off-the-shelf products.

The SAFE community includes members from the Biopharmaceutical, Financial, Regulatory industries and vendors who take an active role in the SAFE initiative by participating in ongoing pilot programs with the FDA, EMEA, and National Cancer Institute (NCI). As market leaders,

they are participating in profound change to the industry. The benefits derived from global collaboration and removing dependency upon paper are intuitive to each member. Everyone sees the same benefits; however, the approach is different for each organization.



Before SAFE...

- Overwhelmed by Paper
- Too Much Complexity
- Painful Audits
- Information Loss
- Sleepless Nights



After SAFE...

- Less Paper
- Simplicity
- Effortless Audits
- Never Lose an Essential Document Again
- Sleep Well

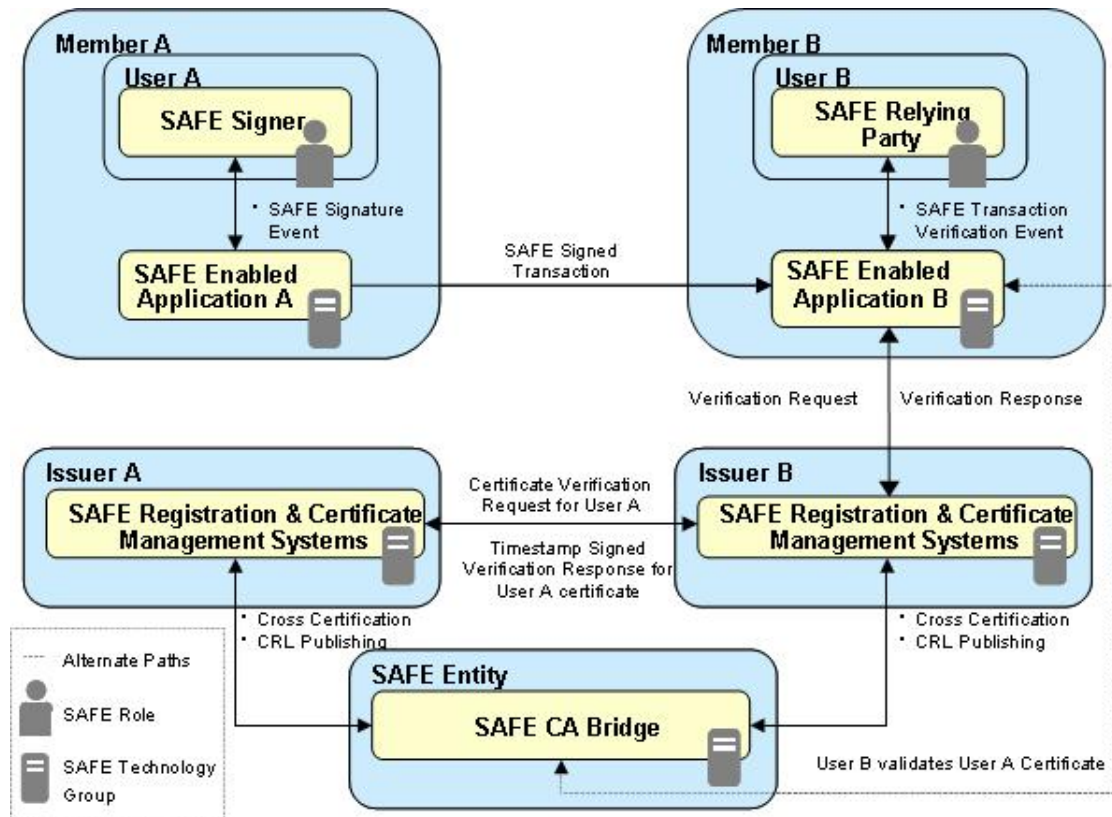
SAFE has adopted a “we” approach for reducing identity assurance and access control costs by operating a shared-cost model with membership fees. “*The whole is greater than the few*”, said Scott Potter, SAFE Project Manager at Pfizer. Members provide input into the implementation of the SAFE standard, and share information with other members to address challenges faced during their SAFE implementation.

Although the concept of a global trust community is not new, it is new for the Life Sciences industry. According to Pfizer’s Tony Gazikas, “*It is not a question of ‘if’ but ‘when’ the SAFE standard will become the required industry standard for electronic records and signatures.*”

6. SAFE Implementation

6.1 SAFE Model

The SAFE system is a combination of hardware, software, people, and processes that provide a secure digital environment to issue, revoke, archive, and recover digital certificates. The following diagram illustrates how SAFE provides a common trust bridge among the stakeholders that result in the ability to make and validate legally enforceable Digital Signatures.



Consider two Users; User A and User B who are members of SAFE. The process starts with a signature event that triggers User A to sign an object.

1. User A uses SAFE identity credential to sign the object using SAFE enabled smart card. This signed object is posted by User A on a SAFE Enabled application A as shown.
2. The SAFE enabled application A is interfaced with another SAFE enabled application B for SAFE signature verification.
3. SAFE enabled application B verifies the SAFE transaction with User B, a SAFE relying party. User B validates certificate of User A by sending a signed request to its Issuer- CA.
4. Issuer B sends a request to Issuer A to validate the certificate for User A.
5. Issuer A sends a timestamp signed response validating the certificate to Issuer B.
6. Issuer B completes the signature event by informing User B that User A certificate is valid.

6.2 SAFE-Pfizer Implementation

Pfizer is a leading pharmaceutical company with more than 250 business partners in academia and industry. Pfizer is one of the founding members of SAFE-BioPharma Association. Pfizer has provided input into the development of SAFE and has deployed a full-scale SAFE implementation based on the SAFE standard throughout the organization. As an industry leader, Pfizer and the SAFE community will fundamentally change the way the Life Sciences industry conducts business. According to Scott Potter, Pfizer manages identity credentials for over 200,000 employees and contractors; and it spends an estimated \$10 million per year for password resets. Every digital signature utilized for regulatory and non-regulatory transactions eliminates the cost of approximately \$125 required per equivalent wet signature.

The decision point that influenced Pfizer to become involved with the SAFE project was the replacement of multiple ID architectures that were in place with a common internal identity management framework. SAFE uniquely aligns identity credentials with secure information exchange. Pfizer chose a unified identity model that links multiple credentials onto one cryptographic hardware device (Smart Card). The unique ID badge provides a consistent user experience for access control and digital signing.

The rationale for adopting a holistic approach was as a business enabler that resulted in the elimination of costly paper-based business processes and the deployment of universal identity badges. They decided to implement SAFE quickly and robustly. Pfizer embarked upon a full-scale systems reengineering and identity management solution that impacted every Pfizer employee and contractor.

One of the implementation challenges Pfizer faced was adopting an identity management strategy, and linking multiple identity credentials to one token. Another challenge was keeping up with the demand for identity badges once employees realized the convenience of using a single ID badge. One of the early implementation successes was the convenience of Pfizer employees and contractors being able to have their identity authenticated at remote Pfizer locations without having to ride over to the visitor's station for additional screening.

For those members new to SAFE, Pfizer's Tony Gazikas has several recommendations regarding deployment. *"It is important to attack the hardest issues first. Educate high-level personnel about the SAFE concept and vision to dispel fear, uncertainty, and doubt. Get the financial, legal, and regulatory stakeholders on board early. Finally, chose the implementation model best suited for your organization, and then start brainstorming the right path to get there,"* suggests Gazikas.

6.3 SAFE-GlaxoSmithKline

GlaxoSmithKline (GSK) is a leading pharmaceutical company with over 100,000 world wide employees. GSK is one of the founding members of SAFE BioPharma. As an industry leader, *“GSK embraced the SAFE initiative for the opportunity to create fundamental change in electronic information exchange and identity assurance. We were also attracted to the time and cost savings from decreased paper management, improved operational proficiency, and increased productivity,”* said Colleen McMahon, Technology and Business Effectiveness Manager at GSK.

GSK’s implementation strategy is geared to accelerate secure information exchange during clinical trials by leveraging the SAFE standard for clinical investigators to improve efficiencies throughout the clinical trials process. The point solution was determined based on a 12-month ROI timeline that needed to produce a quantifiable payback.

GSK developed an identity assurance model to automate the registration process for clinical investigators that removes paper-based latency and infrastructure costs. The GSK approach was to standardize the investigation registry and develop an electronic infrastructure to support all electronic submissions where information exchange is not visible to other parties. From a web-based platform, secure logon and digital signing of regulatory transactions is made possible. The identity of the clinical investigator is registered, updated, and authenticated to increase process efficiency and ease business-to-business transactions. Investigators are able to produce reports, gather and submit information online with SAFE providing the trust infrastructure.

The implementation challenges GSK faced were strategic and operational. Getting corporate Business, IT and Legal stakeholders on board with implementing SAFE proved to be a challenge. The concept of eliminating a paper-based business process from their system was received well, but met with multiple challenges during implementation. Changing from User ID and password to Digital Signatures was one of the challenges. Staff education was another issue. Lack of knowledge of the difference between electronic signatures and digital signatures contributed to the perception that the system already in place was adequate.

According to Colleen McMahon, *“It is important to keep in mind that SAFE-accredited vendors should maintain the regulatory quality compliance documentation for their products. This may ease the process of validating the vendor product. Additionally, SAFE members would benefit from having baseline standards for Standard Operating Procedures around change management, identity credential deployment, and digital signature usage which can be internalized by the members”*.

Based on the ROI achieved in this project, GSK plans to build upon their SAFE infrastructure to include additional SAFE-enabled applications, single identity badges, and electronic business processes. GSK is attracted to the idea of global collaboration, electronic laboratory notebooks, and electronic data capture.

6.4 SAFE-Merck

Merck is a leading pharmaceutical company with approximately 72,000 employees worldwide and a founding member of the SAFE coalition. Their interest is in the SAFE trust infrastructure and a common framework that enables global collaboration, alliances, and partnerships. According to Keith Heilner, Director of Information Security at Merck, *“The biopharmaceutical industry is breaking up and outsourcing many processes. As a result, it is creating many new business partnerships that must be managed. SAFE streamlines those partnerships.”*

At Merck, the business justification for implementing SAFE was qualitative. Merck believes that the industry is moving in the direction of automation for regulatory and non-regulatory business transactions. Faced with the choice to lead, follow, or try to catch up, Merck decided to move forward into the 21st Century as an industry leader with an eye on global alliances and enterprise-wide services development. *“Digital signatures are going to take off like Google and AOL. SAFE is a true federated environment that will allow Merck to move from paper process to the automated equivalent,”* believes Pamela Fusco, CISO, Executive Director, Information Security at Merck.

Merck has taken a practical approach to implementing SAFE. They are implementing pilot programs to minimize the impact on approvals and submissions of electronic data while meeting global requirements. Merck is addressing the technical and legal aspects of electronic information exchange across multiple regions. The comprehensive technology that is needed to switch from paper-based practices and processes to an automated electronic process is the focus of the SAFE-Merck implementation model.

Some of the implementation challenges they faced:

- Articulating to key personnel the SAFE concept and vision.
- Communicating the legal and regulatory differences between the U.S. and other regions of the world.
- Defining legally binding electronic signatures vs. electronic approvals.

Suggestions for those companies embarking upon a SAFE implementation model *“start higher in the food chain. It can be challenge to sell cutting edge technology strategically, a more advantageous implementation lies within our business units,”* said Pamela Fusco.

Merck is planning a robust enhancement of their business processes utilizing the SAFE standard in the areas of access management related to identity credentialing, access management, and Digital Signatures.

7. Future of SAFE

To achieve the vision of global adoption of Digital Signatures, SAFE-BioPharma has taken the lead in creating a robust, regulatory compliant, secure, and legally binding trust infrastructure to expand beyond clinical trials and investigators to other areas common to the industry, such as post market RX samples, pre-market access control for partners, E-lab notebooks, and manufacturing QA labs. The SAFE member community is “a powerful demonstration of how the industry and global regulators can work together toward a common set of goals that will benefit the entire process of developing new drugs,” said Alan Goldhammer, Associate Vice President, Science and Regulatory Affairs at PhRMA.

The SAFE strategy for global success:

- Leverage the leadership qualities of all members in a SAFE Working-Group environment
- Promote and educate the Life Sciences community of the benefits of using a common security standard for identity credentials and information exchange
- Foster cooperation among SAFE members to effectively market the SAFE community
- Illuminate the value of participating in a shared-cost model

One of the reasons for the early successes of SAFE is the global network of people working together to launch the SAFE standard - the visionaries of the SAFE concept, the developers the SAFE technical specifications and policies, the regulatory advisors, and the early adopters of the SAFE standard.

Leading Biopharmaceutical companies and government organizations have been strategically involved, along with regulators, in the development and delivery of the SAFE standard leveraging key entities from the financial, legal, and regulatory sectors to support the SAFE initiative. Focus areas for the SAFE coalition are:

- Global operational logistics
- Membership procurement, maintenance, and growth
- Examination of existing and emerging business processes
- Common application enablement

8. Conclusion

Life Sciences professionals are committed to advancing the public health by helping to speed innovations that make medicines more effective, safer, and affordable. It is important that they get accurate, science-based information needed for medicines and treatments. Currently, providers interact with regulators using different security models for different transactions. A compliant, standards-based trust infrastructure is a critical component to enhancing inter-industry collaboration and information exchange. A common security framework will allow legally enforceable, regulatory compliant Digital Signatures to be used outside of the originating systems, and still be verifiable.

Companies must become members in order to use the system for electronic transactions. The SAFE shared-service/shared cost model will be the springboard for:

- Legally enforceable Digital Signatures worldwide
- Global regulatory compliance
- Identity-based scalability
- Uniform risk and liability management
- Broad utilization
- Reasonable implementation and support costs

When considering SAFE membership, commitment to the mission should be a key motivator. Members will have the opportunity to work with other Life Sciences professionals. Overall, participation and support of the SAFE initiative will benefit the entire industry. The greatest level of contributions will be from those individuals that have an understanding of the problems facing the industry and want to work toward a common goal.

Pfizer saw enough benefit to move forward with a global identity management system. Scott Potter at Pfizer equated global participation in the SAFE initiative to a telephone system: *“An internal phone system, where people can talk to each other has a benefit; but there is significantly more value to having a phone system that enables people to talk to the rest of the world.”*

“How long do we continue to develop point solutions that promote isolated and incompatible infrastructures that add complexity and risk to the Life Sciences community? We now have the opportunity to establish a shared common identity foundation, and we can all leverage and build from it now, the right way, versus forcing a legacy problem in the future,” suggests Ashley Evans, SAFE Industry Standard Program Manager.

APPENDIX A - Value to Members

The SAFE initiative is focused on developing a single unique identity and digital signature credential that can be deployed in a uniform manner for global use by the regulated industries in the, but not limited to, Pharmaceutical, Medical Device, Diagnostic, and Biotechnology sectors. The SAFE standard is a convergence of physical and digital security on one platform for access control and electronic document signing. Having one electronic credential for each employee and business partner will help eliminate the use of proprietary digital identity models, lower the costs for electronic collaboration, and provide a common methodology and approach to provisioning, deployment, and validation of credentials.

One key barrier to doing business online and sharing confidential information is the lack of a uniform standard and trust between Internet communities. Life Science companies currently rely on independent trust relationships to exchange information. A unique aspect to the SAFE collaboration is the common trusted community framework that provides cross certification of trust domains, strong security for sensitive information, and meets the strictest requirements for authentication, non-repudiation, integrity, liability, privacy, and legal enforcement. SAFE's real-time Internet based services offers identity assurance for each user and relying party. The SAFE standard has been developed for optimized regulatory compliance. The whole clinical trial process will be automated and secure. SAFE provides a consistent industry-wide method of managing and utilizing legally enforceable electronic signatures to sign and encrypt regulatory documents for submissions and review.

The challenge of replacing costly paper-based drug trial submissions is the final obstacle in the quest to eliminate the inefficiencies and expense associated with paper transactions. A compound passing through a Phase III clinical trial to a regulatory agency for submission and approval can produce over 6 million pages of paper. SAFE has created a low-cost electronic identity credentialing standard that reduces the cost of creating, maintaining, and submitting documents. SAFE-trusted Digital Certificates will enable the Life Sciences industry and their business partners to replace paper as the official record for both regulatory and business transactions. The Food and Drug Administration (FDA), and the European Medicines Agency (EMA) provide guidance for the SAFE initiative because of their interest in the acceptance and use of electronic drug trial and drug application submissions. Both the FDA and EMA have provided input into the development of the SAFE standard, and the implementation of an electronic life cycle for documents that support drug development and post marketing activities. Regulators will greatly benefit from reduced paper handling and credentialing costs and eliminate the inefficiencies and inaccuracies of paper-based records keeping. The SAFE, easy and straight forward approach to identity validation and verification will speed the flow of electronic documents and the approval process for new drugs.

The SAFE standard has been designed to help meet various regulatory, technical, and operating compliance requirements such as those specified in 21 CFR Part 11, as well as other similar local and regional regulations around the world (HIPAA, SOX, GMP, and GLP). SAFE certified software vendors that provide applications that are regulatory compliant right out of the box will relieve the cost pressures of conducting individual vendor audits. While Commercial Off-The-Shelf (COTS) software will provide for a more consistent, predictable user experience, software validation is still required to comply with FDA regulations. Competitive vendor supply sources that are SAFE certified is an important aspect of the SAFE approach. Multiple SAFE-enabled business applications will be commercially available. No one vendor will have a monopoly. The

net result will be fulfilling cost reduction directives while maximizing flexibility. Long term benefits of SAFE compliance:

- Reduce the cost of developing digital signature and electronic identity infrastructures
- Extend the trust community through global acceptance of a single standard
- Interoperability between global business partners
- Participating in a shared-cost model
- Competitive vendor supply sources that are SAFE certified

The SAFE identity assurance standard lowers the cost of credentialing and electronic collaboration among industry members, business partners, and regulatory agencies. SAFE members will improve business productivity by shifting credential management away from users to a uniform identity assurance standard that can be used across organizations. Cross utilization of credentials will result in industry-wide cost savings within a shared business model. SAFE simplifies compliance, user identity, and access control.

SAFE's vision is the global adoption of the SAFE standard, best practice guidelines, and business processes that go beyond biopharmaceutical companies, clinical trials, and investigators to all Life Science entities.

APPENDIX B - Value to Vendors

Mission-critical applications requiring digital credentials need to be seamlessly interoperable within the SAFE-certified community. Application suppliers from the vendor community are seeking users to market their products. The SAFE standard is finally leveling the playing field for vendors regarding security. Vendors no longer need to be concerned with adjusting their applications to meet each company's security requirements. SAFE-compliant applications have security requirements that are consistent with the security standards of their customer's right out of the box.

The vendor selection process is eased when vendors are SAFE certified. The SAFE Vendor Certification Program includes a vendor audit for compliance to regulatory technical specifications. Application vendors have an enormous advantage in delivering applications that have SAFE compliance built into them; suppliers can concentrate on being best-of-the-business application solutions. The result is cost savings to the customer and application supplier. The vendor can market their SAFE-compliant products as an additional asset to their customers. SAFE-certified vendors facilitate technological interoperability among SAFE members and their global business partners.

Collaboration between the SAFE community and Vendor community creates an alliance that will stimulate demand for software that can make, and validate electronic signatures, and promote widespread use throughout the Life Sciences community. A growing number of application software vendors is working right now to leverage the SAFE standard in the industry. Once SAFE is adopted as the industry standard, companies will require vendors that do business with them to be SAFE certified.

Application Areas Based on Member Implementation Objectives

- eLab Notebooks
- Biotech Interactions
- Manufacturing Batch Record Signatures
- Site Study Initiation Packages
- eLabeling
- Adverse Event and Safety Reporting
- Informed Consent Forms
- Sales Force Automation and Commercial Operations
- GMP, GLP, GCP Signatures
- Patient Case Books
- Advertising and Promotional Submissions
- Contract Signatures
- Internal Standard Operating Procedure and Policy Signatures
- Financial and Procurement Transactions
- Human Resources
- Industrial Operations
- eArchiving

The SAFE Vendor Certification Program uses Best Practice guidelines for systems integration throughout the product lifecycle. Although SAFE encourages vendors to adjust their products to meet the SAFE standard, in most cases doing so should not require substantial changes to existing products. The vendors that have adopted the SAFE standard will provide the seamless integration of business assets for the Life Sciences industry and their business partners. The biopharmaceutical sector, alone, has thousands of supplier relationships, and their business processes are becoming more automated. These companies welcome the added assurance that their software vendors have been certified and their SAFE-enabled applications are regulatory compliant right out of the box.

APPENDIX C – Membership Options

SAFE-BioPharma, LLC offers four primary membership options for organizations seeking to join the SAFE standard:

SAFE Full Members: SAFE Full Members have the ability to use the SAFE Standard in their production operations globally. In addition, Full Members will be able to access and leverage the SAFE-BioPharma information assets such as legal briefs, white papers, and SAFE best practice compliance and implementation guidelines. Full Members will pay annual membership fees tiered based on company size (either global revenues or R&D spending depending on company type).

SAFE Founding Members: SAFE Founding Members are those entities that have participated in the initial funding of SAFE-BioPharma, Inc. and launch of the SAFE Standard. For this early stage funding commitment, Founding Members will be granted a 25% discount on SAFE annual membership fees (according to their associated pricing tier) and they are able to appoint a representative to the SAFE-BioPharma Board of Directors for the first two years of the Company's operations. From a System usage and information access perspective, Founding Members have the same system use rights as Full Members.

SAFE Government Members: The SAFE Government membership option is reserved for government research sites (e.g., NCI) and regulatory agencies (e.g., FDA or EMEA). This membership category requires that government agencies or non-profits using SAFE are bound to the SAFE rules; however, they have the option to be voting or non-voting members as local laws allow for their participation in the governance of both SAFE-BioPharma and the SAFE Standard. Government Members can leverage the SAFE information assets and participate in the SAFE working groups. With the exception of Regulators, all Government Members will pay annual membership fees tiered based on annual expenditure levels.

Associate Members: This is a special membership option that is controlled by the SAFE-BioPharma Board. This membership category is reserved for clinical investigators or research organizations that have been requested to use SAFE by members or agencies for a limited implementation. Associate members will not pay an annual membership fee, but will be required to be bound to the SAFE rules. Associate Members will not participate in the governance of SAFE.