AstraZeneca Implementation of SAFE Digital Signatures

25-FEB-2007

Version 1

Contents

EXECUTIVE SUMMARY **2**

ASTRAZENECA "DISCOVERS" SAFE **3**

DIAGNOSING AND LEARNING MORE **3**

ASSESSING AND DOCUMENTING READINESS **4**

BUSINESS ASPECTS 4
Operating Procedures *5*
Managing Credential Ownership *5*
Defining System Ownership *5*
Ensuring Organizational Buy-in *5*
Working within Budget and Time Constraints *5*
Leveraging Expertise *6*
TECHNICAL ISSUES 6
Identity Management *6*
Adobe Configurations *6*
Firewall Access *7*
Change Management *7*
Vendor Audits *8*
Planning for Support *8*

DECIDING TO IMPLEMENT THE SAFE STANDARD **8**

DELIVERING THE SAFE SOLUTION **9**

ENABLING AN APPLICATION 9
SELECTING A CREDENTIAL ISSUER 9
DELIVERING CREDENTIALS AND TRAINING USERS 10
SUBMITTING TO THE FDA—A LANDMARK MILESTONE 11

SAFE TODAY AND INTO THE FUTURE AT ASTRAZENECA **12**

MORE ON ASTRAZENECA 13
MORE ON SAFE-BIOPHARMA ASSOCIATION 14
MORE ON ELECTRONIC AND DIGITAL SIGNATURES 15

Executive Summary

On September 18, 2006, AstraZeneca U.S. Regulatory Affairs submitted the first electronic original 356h form to the FDA. In the past, paper originals were the only way to comply with regulations. By using SAFE signatures and the FDA Electronic Submissions Gateway, AstraZeneca completed a landmark milestone. No paper original of the 356h exists.

As background, AstraZeneca U.S. Regulatory Affairs was implementing the FDA Electronic Submissions Gateway (ESG). At the same time, AstraZeneca IT colleagues were participating in ongoing development of SAFE digital signatures. The Regulatory Information Strategy Group became aware of the need for digital signatures, and saw the ESG project as an opportunity to implement SAFE signatures. Combining the two efforts would lead to the business benefit of a completely electronic submission, eliminating the overhead activities to create, sign, store, and maintain paper originals. Another business benefit was increased flexibility, because AstraZeneca colleagues could apply SAFE digital signatures to documents from anywhere with an Internet connection. When these colleagues travel, this flexibility can lead to increased speed as well, because documents can be digitally signed immediately rather than waiting for colleagues to return to an AstraZeneca site.

AstraZeneca formed two teams to implement the ESG and SAFE signatures. The teams faced a tight time schedule, starting in April 2006 with a delivery date in early fall. The teams faced both business and IT challenges. Business challenges included developing operating procedures, managing credential ownership, defining system ownership, ensuring organizational buy-in, and working within budget and time constraints. Technical challenges included enabling an application, selecting a credential issuer, performing internal validation, planning for support, and delivering credentials to users. This paper discusses the details of these challenges and how the teams resolved the issues.

As part of lessons learned, the teams identified the key elements of project success as:

- Business leaders as champions for the project.
- Small, focused team.
- Department-level scope for SOPs, training, and support activities.
- Limited number of users (80) to be provided with SAFE credentials and training.
- Delivery focused on SAFE signatures, not on company-wide identity management.
- Leveraging experiences, tools, and templates from SAFE, other members, and consultants.
- Rigorous structured process for application development, testing, and delivery.

All of these elements combined for a successful on-time and on-budget delivery.

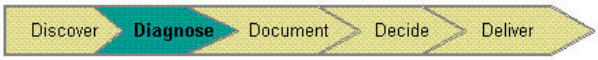
As a founding member of the SAFE-BioPharma Association, AstraZeneca understood the potential benefits of digital signatures, and had participated in developing the policies, procedures, and technical specifications. However, as an early adopter AstraZeneca faced unique issues in their implementation. This paper discusses the phases of implementing SAFE signatures and the activities in each phase. The last section of the paper discusses the vision for expanding use of SAFE signatures to internal AstraZeneca transactions. Joe Waldron (Executive Director, US Region, Global Drug Development Information Services) describes the vision as “anywhere we do wet ink signatures today is a place where we can be leveraging SAFE digital signatures tomorrow, and begin to reduce the burden associated with managing paper.”

AstraZeneca "Discovers" SAFE

Today, companies often learn about the SAFE standard from colleagues in other companies, at a conference, or by reading a news release. After learning about the standard and the SAFE-BioPharma Association, companies typically perform initial research. The goal of this research is to explore how others have implemented the standard and begin to develop a business case in their company.

AstraZeneca took a different approach. As a founding member, AstraZeneca participated in early activities through the Pharmaceutical Research and Manufacturers of America (PhRMA). When the concepts grew into the first standard in 2004, the Leadership within AstraZeneca built a business case for joining the Association. AstraZeneca recognized SAFE as a valuable idea for the future, and made a decision to learn more about the standard and how to convert the concept to reality.

Diagnosing and Learning More



When learning more about the SAFE standard, companies usually do a high-level diagnosis to understand the business case for implementing the standard. The business case explores the cost of the existing approach with ink signatures ("wet" signatures), and the cost of the solution to implement SAFE digital signatures. (See "Key Benefits of SAFE Signatures" for a brief overview.) Now, SAFE members collaborate with each other to learn about existing tools.

As an early adopter, AstraZeneca couldn't point to a successful example of their planned implementation. Rich Ware (Principal IS Business Consultant for Regulatory Affairs) explains that "our biggest challenge was convincing people that SAFE was real. It was so new, and some saw a higher risk because of that." AstraZeneca needed to develop their own tools and operating procedures, because they were among the first SAFE members to implement the SAFE standard.

AstraZeneca US Regulatory Affairs was implementing the FDA Electronic Submissions Gateway (ESG). A group at AstraZeneca was actively testing the process. Eileen Poland (Associate Director, Regulatory Information Strategy, Regulatory Affairs and Project Manager for the ESG Project) explains that the Regulatory Information Strategy Group became aware of the need for digital signatures, and saw the ESG project as an opportunity to take advantage of the SAFE solution to advance AstraZeneca's implementation of ESG. "We had a dilemma and asked Rich Ware for advice, to be able to tap into his wealth of experience with SAFE and leverage what he knew." Regulatory Affairs knew that the ESG needed a CFR Part ll compliant solution, but also wanted to gain benefits beyond the pilot. Eileen Poland explains, "we saw the ESG Pilot as a good opportunity because there were only about 80 people who needed credentials." AstraZeneca also needed to move quickly, with a planned submission date of summer 2006.

Key Benefits of SAFE Signatures
☑ **Legal enforceability.** SAFE digital signatures are the legal equivalent of an ink-based signature. SAFE signatures meet three key legal criteria. With authentication, you are sure of the identity of the person who provided the signature. With integrity, you are sure the document has not been altered since it was signed. With non-repudiation, you are sure that the sender cannot deny signing the document.
☑ **Regulatory compliance.** The SAFE standard meets or exceeds regulatory guidelines for 21 CFR Part 11 and HIPAA. SAFE designed the standard to meet similar international guidelines, and ensures that new versions comply with emerging regulations.
☑ **Strong Security.** The SAFE standard ensures security and data integrity. With two-factor authentication, users need both their SAFE credential and their passcode to digitally sign a document. This is similar to automatic teller machines, which require people to provide both their ATM card and their PIN. The standard uses public key infrastructure (PKI) to apply digital signatures to documents and to assure the integrity of their content.
☑ **Global.** SAFE members are global companies and require a global standard, both for internal and external use.

AstraZeneca US Regulatory Affairs Leaders embraced the direction of using ESG and SAFE signatures. Their strong support was vital to the eventual success of the project. Rich Ware explains that a key point for success is "the business chose us. Regulatory Information Strategy was knowledgeable about SAFE and championed the use of SAFE to their Regulatory Affairs leadership. Since they had already decided to use SAFE, it was our job in IT to make it happen. As long as the costs didn't get out of hand, we knew AstraZeneca US Regulatory Affairs wanted to go forward with SAFE signatures." AstraZeneca avoided the challenges faced by IT groups who must convince their colleagues about the benefits of SAFE signatures.

Assessing and Documenting Readiness

In general, the next step is for a company to assess internal readiness for SAFE signatures. This may require aligning with existing approaches for electronic signatures or with other IT activities. It requires developing a detailed understanding of the SAFE-BioPharma Association, and of the business and technical aspects for implementation. For most companies, assessing readiness also involves developing internal alignment among multiple groups. These groups include Legal, Regulatory Affairs, Compliance and Security, Records Management, and IT. This phase of assessing and documenting readiness is composed of two overlapping aspects for business and IT activities.

Business Aspects

Because AstraZeneca had been involved with SAFE from the beginning, the company already had a detailed understanding of the SAFE policies, procedures, and technical specifications. After all, AstraZeneca staff members helped build these documents. As a result, AstraZeneca did not face a learning curve that other companies might face. The team needed to solve business issues for internal operating procedures, managing credential ownership, defining system ownership, ensuring

organizational buy-in, completing within the budget and time constraints, and leveraging expertise from consultants and other SAFE members. The next several topics discuss these business issues.

Operating Procedures

AstraZeneca needed to develop a full set of SOPs around SAFE signatures. The policy framework provided by SAFE helped the team accelerate their activities to meet the aggressive timeline. AstraZeneca used this framework to define the internal policies and SOPs needed. (The SAFE web site describes this framework in detail; see www.safe-biopharma.org.) The team also learned from the experiences of other SAFE members in developing SOPs.

For simplicity and speed, the team developed department-specific SOPs for Regulatory Affairs. This enabled a quicker development and review path, as compared to the broader reviews and approvals needed for company-wide SOPs. While the approach limited the ownership and application for SAFE signatures to a single focused activity, this approach met the project needs. Later, after success, the team could decide whether to scale the SOPs to other activities.

Managing Credential Ownership

In addition to SOPs around SAFE signatures, the team required operating procedures to define the responsibilities with the ESG and with SAFE credentials. For example, the team needed to identify how to revoke credentials for employees who left the company or lost their token.

Defining System Ownership

To move quickly and meet the timing for the submission, AstraZeneca US Regulatory Affairs became the temporary system owners. The company is now assessing long-term system ownership.

Ensuring Organizational Buy-in

AstraZeneca US Regulatory Affairs and IT leaders were strong supporters of the SAFE implementation from the beginning. The team was responsible for ensuring buy-in from other internal groups. These groups included AstraZeneca Legal, Risk Management, Records Management, and Validation, Security, Quality and Compliance.

One potential obstacle in obtaining organizational buy-in was what Eileen Poland calls the “mire of explaining SAFE”. Explaining the technical underpinnings to non-IT staff can be a challenge. More importantly, providing such a detailed explanation isn’t necessary and wastes time. The team adopted an approach of providing a succinct description of SAFE signatures, emphasizing the importance to the business. In doing so, the training presentations and materials compared SAFE credentials to both ATM cards and to wet ink signatures. Also, the team found that linking SAFE to the ESG was useful, because using the ESG was a key goal of AstraZeneca US Regulatory Affairs.

Another potential obstacle was translating between IT Service, Validation, and business needs. As a solution, the Validation group, led by Mary Opromolla, served as effective IT-to-business translators. These colleagues were familiar with the business needs as well as who to engage within IT Service for infrastructure and quality issues. By engaging in the process early in the planning phase, they were able to minimize the impact of this obstacle.

Another potential obstacle was providing focused information to appropriate organizations. The team was able to leverage resources that SAFE provides to its members. For example, the SAFE team shared the SAFE-provided Legal Overview with the internal Legal group. This document helped AstraZeneca attorneys assess potential issues for SAFE signatures on a FDA submission. Team members described the attorneys as receptive and interested in the new technology.

Working within Budget and Time Constraints

The project was on both a tight timeline and a limited budget. AstraZeneca US Regulatory Affairs wanted to show the business benefits of using the ESG, without a huge budget or a long time to implement. In reviewing lessons learned, team members cited the project’s small size as a key to success in working within the constraints. For reference, the project began in April and completed the

primary goal with a sNDA submission in September. Eileen Poland explained that the team was clear on their goal of developing a speedy and inexpensive solution. This project needed to show a tangible business benefit for the combined activities of using the ESG and SAFE signatures.

Leveraging Expertise

Part of the success of SAFE comes from members helping other members. Rich Ware pointed out that AstraZeneca received support from other members and is now returning the favor. AstraZeneca has provided examples of validation documentation for other members to use in their implementations. Rich Ware summarizes, “If we help each other, everyone benefits and no one needs to start from scratch with a new solution.”

Another aspect of success comes from vendor support. Team members commented that the consultants added an external business perspective to the project, augmenting the expertise of AstraZeneca IT staff. Eileen Poland described how staff was particularly valuable in developing training materials, and was key to the project success by “putting all the pieces of the puzzle into the right place at the right time.” Vendors also saw the AstraZeneca project as an opportunity to expand into a new business area. Mary Opromolla (TOP Manager, Computer Validation) summarizes, "Our consultants were very motivated and provided valuable help by assisting with the implementation of the SAFE project through to success.”

Technical Issues

In late 2005, the IT team ran a small Proof of Concept (POC) activity. Rich Ware describes this as a technical POC focusing exclusively on IT issues. AstraZeneca needed to be sure that their planned approach worked with the existing network, servers, and firewalls. Also, since the company didn’t have an existing PKI infrastructure, the team’s goal was to test the concept with a few users. Rich Ware explains that “we wanted to get our feet wet with the technology and understand how SAFE implemented that technology. And we wanted to do so with just a few users.” The POC activity uncovered some issues to be resolved. The IT group was considering a second POC when AstraZeneca US Regulatory Affairs contacted them about implementing SAFE digital signatures in conjunction with the implementation of the FDA Electronic Submissions Gateway. The team was then able to apply lessons from the first POC to the production implementation of both business and IT aspects of implementing the SAFE standard.

The technical issues included identity management, Adobe configurations, and firewall access. The technical team also focused on business process issues, including vendor audits, internal validation, change management, and planning for support.

Identity Management

The team made a conscious decision not to focus on the identity management aspects of the SAFE system. First, the business need focused on digital signatures. The team needed to maintain their focus on the end goal of a digitally signed 356h form. Second, like most companies, AstraZeneca already had more than one form of identity management in place. Expanding the focus from SAFE signatures to SAFE as an identity management tool would have required changes to multiple systems, agreement among multiple groups in the company, and credentials for many more users. In addition, team members commented that the project would not have succeeded in the timeframe and budget if the team had expanded from SAFE signatures to using the SAFE credentials for identity management.

Adobe Configurations

The three key technical components required are the token drivers, Arcot drivers, and Adobe Acrobat Professional 6 or above. The technical team faced a challenge with the required version of Adobe Acrobat. The standard desktop and laptop build at AstraZeneca used an earlier version of Acrobat than required for the SAFE solution. The technical team determined that they would utilize Acrobat 7 Professional. Adding this new software caused some disruption to user’s PCs. The risk/benefit issue

for a few users who were highly motivated to sign documents with SAFE signatures fell on the 'benefit' side.

Firewall Access

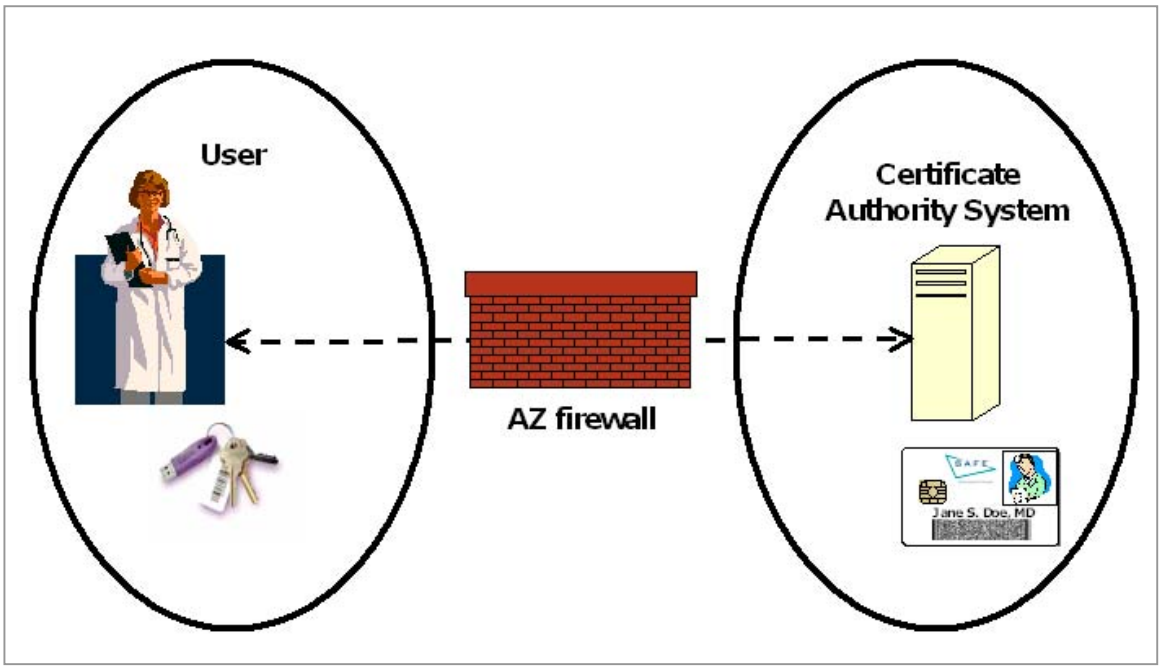
Another technical challenge involved firewall configurations. Completing authentication of the SAFE certificate requires an exchange of information between the user and the SAFE site. This in turn requires exiting from the AstraZeneca network to the SAFE site. Figure 1 depicts the process, where arrows between the Certificate Authority System and the User cross a firewall. SAFE developers had tested access through the firewall in the Pfizer environment (another SAFE founding member). However, AstraZeneca faced different issues. The lesson learned was to ensure adequate time to test and resolve technical issues. In addition, SAFE learned about how to improve their technical testing process from the AstraZeneca implementation.

Change Management

AstraZeneca's IT staff conducts "Change weekends" when infrastructure changes are implemented. Since the planned infrastructure changes can affect the software installed on servers, the SAFE technical team needed to understand all implications of upcoming "Change weekends." In addition, AstraZeneca needed to update their SLA's with support and infrastructure vendors. This ensured that vendors were aware of the implications of planned changes.

Another aspect of change management was planning for change management to the SAFE solution after delivery. The IS Change Coordinators at AstraZeneca have the benefit of visibility into all groups impacted by a planned change. The Change Coordinators also understand the business processes, SOPs, and SLAs of all impacted organizations. As a result, these coordinators are instrumental in ensuring that all compliance elements are performed for any planned change.

Figure 1 Exchanging Authentication Information across the Firewall



Internal Validation

This validation effort included typical validation activities, along with activities unique to the SAFE solution. The general AstraZeneca approach is to validate all applications, including COTS (Commercial Off the Shelf) applications. During the project, a complicating factor for the internal validation effort was the change in credential issuers. The team developed a validation strategy for the initial issuer and then needed to revise the strategy for the final issuer, Registration and Certificate Configuration Authority (RACCA). For more on credential issuers, see "Selecting a Credential Issuer" later in the paper.

Vendor Audits

AstraZeneca performed a vendor audit of Arcot, the software developer for the plug-in that integrates with Adobe Acrobat to create the digital signature. In performing the audit, AstraZeneca assessed Arcot's Quality Management System (QMS) against regulatory expectations and their adherence to their QMS and regulations such as 21 CFR Part 11.

Planning for Support

On the technical side, support for the SAFE implementation is managed through the IT help desk. For the business side, each area has a SAFE business expert. These experts support users by answering business questions, sitting with users for first time use, and assisting with training for new staff.

Deciding to Implement the SAFE Standard

AstraZeneca US Regulatory Affairs was the driving force behind using SAFE signatures. Two project teams were created to implement the FDA ESG and SAFE digital signatures. Within AstraZeneca, the teams consisted of representatives from the Business, IS and Validation. In addition, the SAFE Project Team also utilized external consultants. Eileen Poland summarizes, "SAFE was the right solution at the right time for a key business need. Because of our early experiences with SAFE, it was a perfect solution because we could leverage our existing experience."

These teams needed to develop a strategy for handling legal, records management, and compliance issues.

The ESG team ensured that AstraZeneca infrastructure was capable of handling the size of a full NDA submission. The SAFE Team was responsible for providing a solution to create digital signatures for the FDA forms. Although the two teams had different user requirements and different end-user groups, they shared the common goal of implementing both the ESG and the SAFE standard.

The parallel teams used an alignment map to track roles and responsibilities. For some team members, working on the project was a full-time activity. Other team members participated part-time, and continued their regular activities. Some team members were AstraZeneca employees and others were consultants. Paul Donfried, a consultant, described the parallel teams as "synchronized and symbiotic."

The teams held weekly joint meetings to update the project plan and discuss concerns, issues and obstacles. As Michael Gayle (US GDD IS Change Coordinator) notes, "our tightly structured approach was a key strength. The technical team could pinpoint issues and unclear requirements, and then work to find a solution. AstraZeneca's 'one IT' model was valuable in completing within time and budget constraints."

The first full-team meeting identified gaps in the planned activities, and developed a remediation plan to resolve the gaps. One example involved the concept of an electronic receipt as compared to the paper-based FedEx receipt for submissions. The use of the FDA ESG yields 2 electronic

receipts/acknowledgements: acknowledgement 1 indicates that the submission has arrived at the ESG, and acknowledgement 2 indicates that the submission has been received by the respective review Center (CDER or CBER). The electronic receipts are kept as part of the official record to document the time of the submission. IT and business staff determined the most efficient means of saving and archiving the electronic receipts. The teams developed a plan for handling the electronic receipts, identified people to implement the plan, and defined the timeline for implementation.

Delivering the SAFE Solution

Delivering the SAFE solution involves four key activities: selecting a credential issuer, enabling an application, training, and delivering SAFE credentials to users.

Enabling an Application

SAFE signatures needed to be applied to the PDF rendition of the FDA forms. The team faced a technical challenge with implementing SAFE signatures. Due to timelines, the team chose to implement a solution based on commercial off the shelf software (COTS). See “Technical Issues” earlier in this paper for detail on the Adobe issue.

As an overview, AstraZeneca uses a very structured process for application validation. IT staff start with a business need, progress through requirements, confirm requirements with users, select the application software, perform validation testing, and deliver the application. Before delivery, the Business Release Managers assess it. Their assessment includes reviewing the change management process, documentation, evaluating readiness of the Help Desk, evaluating readiness of hardware groups (who build end-user PCs), evaluating compliance issues, and working with an out-sourced vendor (IBM) to perform testing, packaging, and deployment.

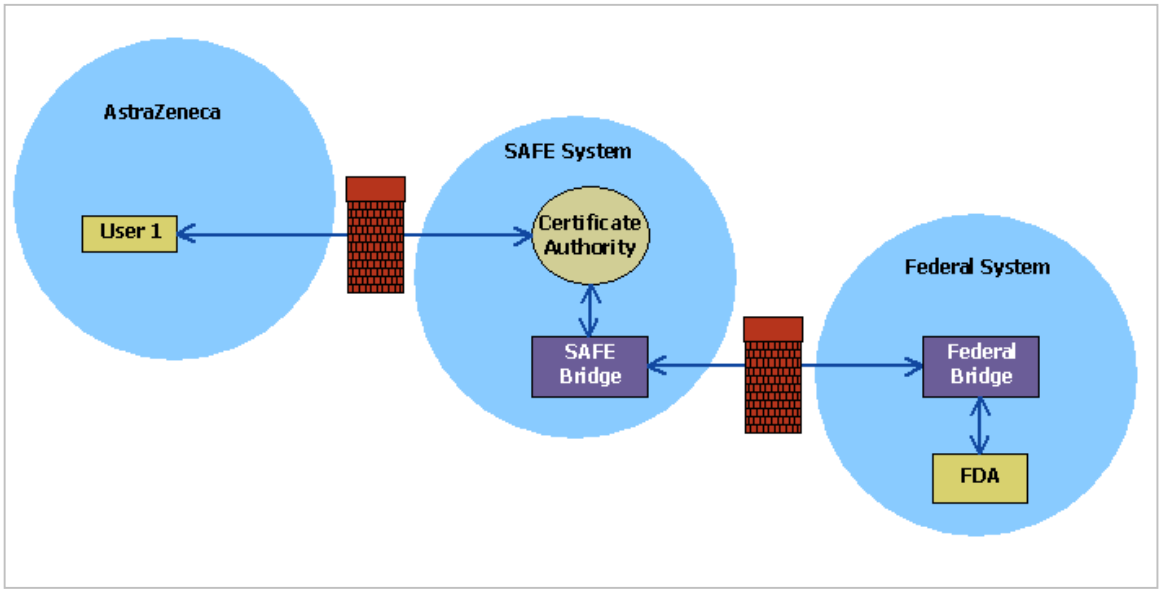
The business team relied on a key technical strength in AstraZeneca’s existing rigorous and controlled process. The business team knew the process would ensure that the new SAFE application would coexist with existing applications on user PCs. Michael Gayle refers to this process as a “non-intrusive installation.” He expands this definition by explaining; “Installing a new application on a computer must not cause problems with any existing applications already on the computer. The packaging team identifies risks for installing a new application and resolves any conflicts with the operating system (Windows 2000) or standard business applications.” By following existing processes for validating an application, the SAFE team was able to quickly enable the Acrobat application and associated tools to deliver the SAFE solution.

The digitally signed document is composed of three elements: the electronic FDA form (PDF); the SAFE Digital Signature; and the validation report. The validation report contains the certificate confirmation response from the credentialing organization (RACCA in the AstraZeneca case). The SAFE digitally signed document is archived within the electronic submission in secure storage. The AstraZeneca team consulted with Records Management to ensure that the SAFE digital signature met the requirements for long-term storage.

Selecting a Credential Issuer

For delivering credentials, companies can purchase SAFE credentials either through the SAFE BioPharma Association or through vendors. Different companies can use different credential issuers, and connect through the SAFE Bridge to each other. Figure 2 illustrates how a user at AstraZeneca can create a digital signature that can be verified at the FDA.

Figure 2 Verifying Digital Signatures Across Organizations



For providing credentials to colleagues, the team focused again on simplicity. Every company computer has a USB port, so using the USB tokens was a natural decision. This eliminated issues around purchasing card readers. Everyone involved already knew how to use a USB token. This choice helped drive AstraZeneca's choice of credential issuers.

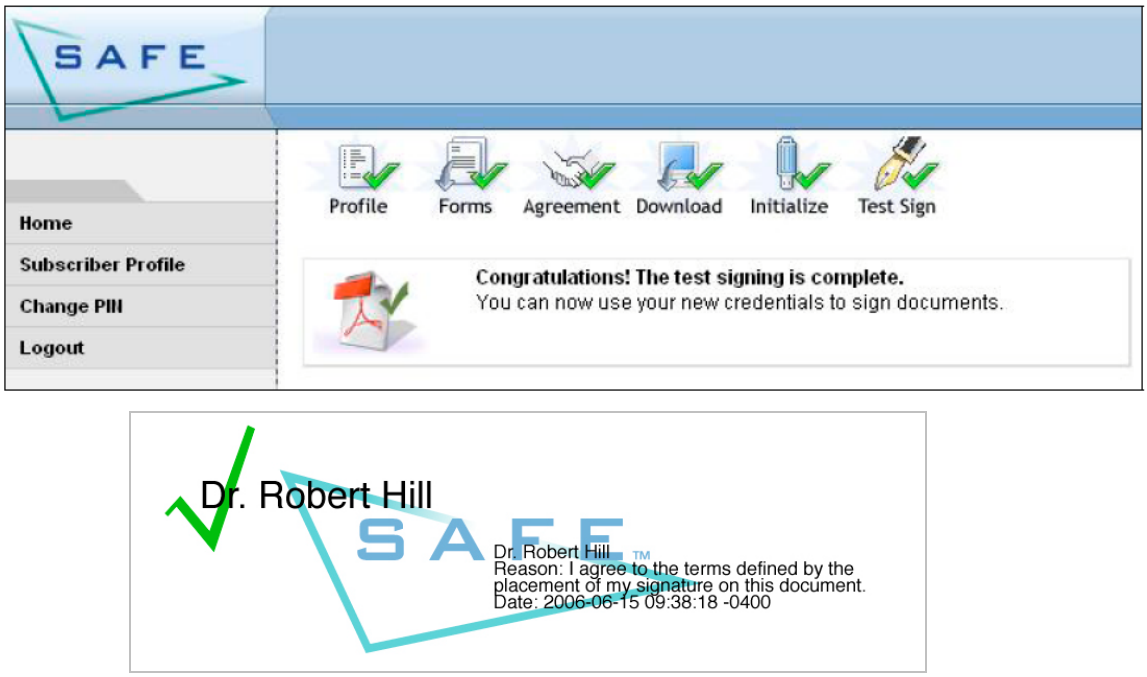
When the project began, SAFE did not provide the service of issuing SAFE credentials. The team's original plan was to use an independent SAFE certified credential issuer. While working on the project, the team learned of SAFE's decision to provide credentials, and selected SAFE as the credential issuer.

SAFE developed the RACCA application for registering SAFE users. This web-based system leads users through a six-step process to get SAFE credentials. Figure 3 shows an overview of the six steps. The green check marks indicate that the user has completed the process. Figure 3 also shows an example of a SAFE digital signature. RACCA uses either a Trusted Agent (TA) or notary approach for confirming someone's identity. A TA is a person authorized to act as a representative of SAFE in the same capacity as a notary for the purpose of confirming a user's identity during the registration process. Both approaches require face-to-face meetings, and government-issued photo id's. See "More on Digital and Electronic Signatures" for an introduction to credentialing activities.

Delivering Credentials and Training Users

The team decided to combine the activities of delivering credentials and training users. The team planned for training sessions over three weeks. Rich Ware explains that the team wanted to do everything possible to ensure success for all users. "We used what I call a RACCA-assisted approach. We arranged meetings every half-hour with a user. The Trusted Agent (TA) walked the user through the online wizard, coaching them through the six steps. We sent the users advance emails to let them know the acceptable forms of identity."

Figure 3 RACCA Steps and a SAFE Digital Signature



Most users walked out the door with their SAFE credential about 20 minutes after walking in the room. Eileen Poland commented that it was very efficient to train and credential users at the same time. “People received their credentials and were able to start using them immediately.” In the end, the team credentialed 85 SAFE users in a few days. Eileen Poland reports that end users are *extremely* positive. For reference, the team posted step-by-step instructions on the AstraZeneca intranet.

Submitting to the FDA—a Landmark Milestone

Delivering the SAFE solution to users was important, but not the end goal. AstraZeneca’s goal was to deliver the full electronic submission to the FDA via the ESG. On September 18, 2006, AstraZeneca submitted an sNDA through the FDA ESG, with SAFE-signed 356h forms. This was a landmark milestone for AstraZeneca and SAFE-BioPharma Association. Although AstraZeneca had previously delivered electronic submissions, this particular sNDA was AstraZeneca’s first digitally signed submission delivered to the FDA.

With the implementation of SAFE Digital Signatures for electronic submissions, Regulatory Affairs eliminated the need for maintaining a paper copy of the wet-ink signed FDA form. Authors create regulatory documents electronically, sign the document electronically, and create an electronic artifact. This is a significant change from hybrid paper-and-electronic submissions to a completely electronic submission. They are able to eliminate the paper itself. More importantly, they eliminate the activities to create, sign, store, and maintain the stored paper copies. Initial estimates are for substantial savings over paper originals. As use of SAFE signatures expands beyond regulatory submissions, AstraZeneca expects the savings to increase.

Users are excited about the efficiency gained by their use of SAFE digital signatures. In the past, signing of the FDA forms involved multiple steps and multiple handoffs. First, someone created the FDA form, signed the form with a wet ink signature and delivered the document to the Submissions Management Group for scanning and incorporation into the submission. Using SAFE signatures saves time and enables the Submissions Management Group to focus on overall submission quality rather than on the logistics of scanned documents. Using SAFE signatures also provides a business benefit

because the people whose signature is required are often traveling. They can review and sign the documents even when not onsite at an AstraZeneca facility. As Eileen Poland summarizes, "With SAFE signatures and the ESG, a submission can potentially be available for review earlier than if we deliver it on a CD."

SAFE Today and into the Future at AstraZeneca

Team members summarized the lessons learned by emphasizing that the limited scope increased the potential for success. As Rich Ware emphasizes, there are two keys to success. "Start small and keep it as simple as possible. Start where there's a strong need with a clear business benefit and a small number of users." Rich Ware describes "We leapt in with both feet. I would have never thought our first SAFE activity would be an FDA submission. By starting with only a few users and a targeted application, the team was able to maintain focus on simplicity. We're all continuing to learn, and saw benefit with the help of experienced consulting resources." Eileen Poland comments that she sees the keys to success as strong support from leaders, leveraging experience of SAFE consultants, providing constant communication to leaders and business users, providing excellent training, and ensuring ongoing support.

AstraZeneca sees potential benefits in expanding beyond transactions between AstraZeneca and Regulatory Authorities. Adding the ability to apply SAFE signatures to internal business transactions will provide future benefits. For this broader use, ownership of the SAFE policies and procedures will need to be transferred to the corporate IT level. For simplicity and speed, the initial implementation used department-specific SOPs. Support is also at a department level, and not scaleable to users outside the department. AstraZeneca is investigating the need for providing broader support for the use of SAFE digital signatures.

Mary Opromolla highlights the value in using industry standards for moving forward with electronic systems, saying, "From the R&D side, the SAFE implementation is a great opportunity for future expansion." There are benefits of SAFE membership. The Association goal is to support one way of working across the industry. By sharing experiences and knowledge, early adopters like AstraZeneca help new SAFE members. Michael Gayle comments "the consortium approach for SAFE is key because sharing among members helps build a feedback loop into the process." As AstraZeneca developed their solution, the team leveraged existing tools and templates from the Association. In turn, AstraZeneca shared their experience and provided samples of validation documents to other Association members.

Senior leaders at AstraZeneca recognize the value of the current SAFE implementation, and the future potential. "Utilization of the FDA ESG, along with SAFE Digital Signatures, provides a critical link in enabling AstraZeneca to transition to a fully electronic environment", says Tony Rogers, Vice President, AstraZeneca US Regulatory Affairs. Joe Waldron, (Executive Director, US Region, Global Drug Development Information Services) comments, "At AstraZeneca we have recently instituted an internal capability using SAFE as the means for digitally signing documents that we will electronically submit to the FDA through its gateway. It is our belief that this will not only benefit us internally, but equally help the agency to achieve its efficiency goals. But this is only the tip of the iceberg—SAFE has applicability throughout the value chain. Anywhere we do wet ink signatures today is a place where we can be leveraging SAFE digital signatures tomorrow, and begin to reduce the burden associated with managing paper."

More on AstraZeneca

About AstraZeneca

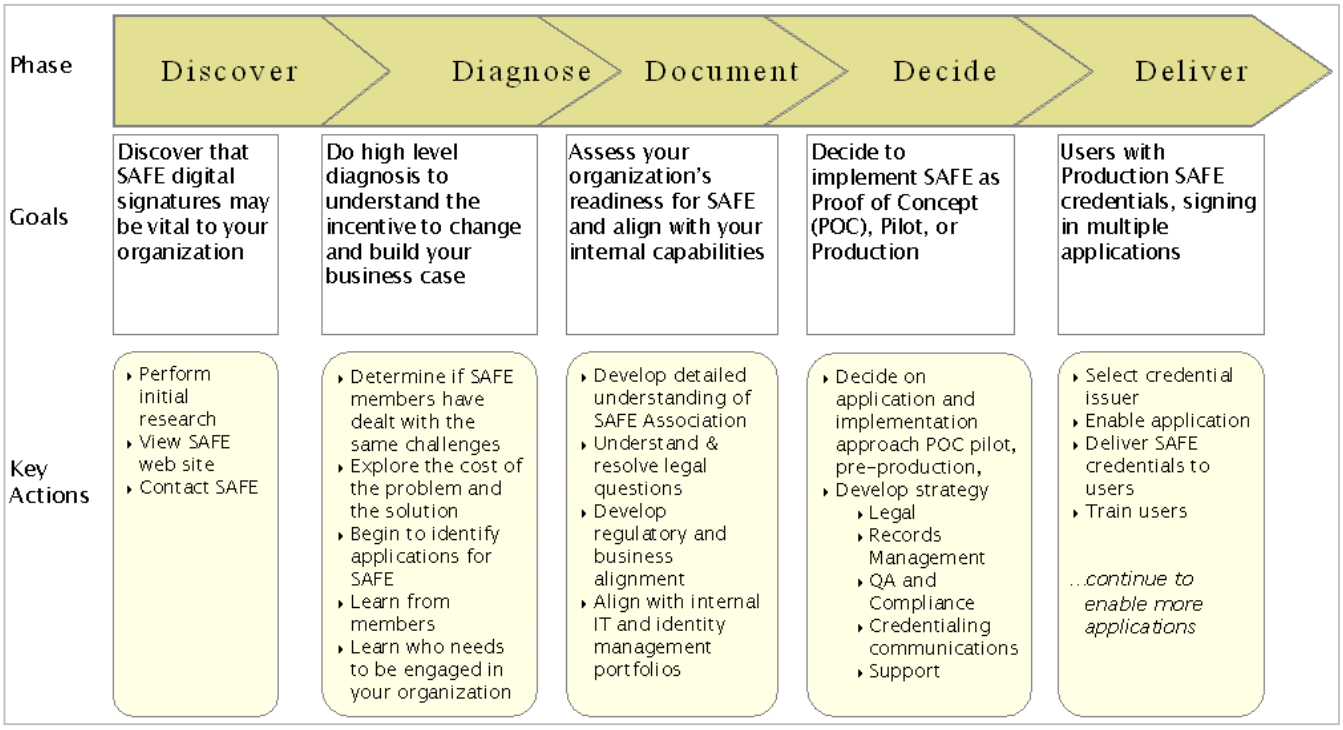
AstraZeneca is a major international healthcare business engaged in the research, development, manufacture and marketing of prescription pharmaceuticals and the supply of healthcare services. It is one of the world's leading pharmaceutical companies with healthcare sales of $23.95 billion and leading positions in sales of gastrointestinal, cardiovascular, neuroscience, respiratory, oncology and infection products. In the United States, AstraZeneca is a $10.77 billion healthcare business with more than 12,000 employees. AstraZeneca is listed in the Dow Jones Sustainability Index (Global) as well as the FTSE4Good Index. For more information about AstraZeneca, please visit: www.astrazeneca-us.com <http://www.astrazeneca-us.com>.

More on SAFE-BioPharma Association

The table below briefly summarizes aspects of SAFE Bio-Pharma Association. For more detail, visit the web site at www.safe-biopharma.org.

SAFE-BioPharma Association Overview
☑ Member-governed non-profit association
☑ Manages and promotes the SAFE standard
☑ Provides a legal and contractual framework
☑ Provides technical infrastructure to bridge different credentialing systems
☑ Provides SAFE identity credentials, both directly and through vendors
☑ Supports Vendors who supply SAFE-enabled products

The figure below shows the typical phases in implementing the SAFE standard, and identifies the goals and selected key actions for each phase.



More on Electronic and Digital Signatures

SAFE signatures are *digital* signatures. Digital signatures provide benefits beyond electronic signatures, and are a subset of electronic signatures. Most people have experience with electronic signatures. These include signing a credit card purchase with a stylus on an electronic pad or clicking on a button to make an online purchase. Just as with ink signatures, when you sign, you are indicating your intent to do something—to agree to a purchase, for example. You are also indicating your identity, confirming that you are you.

Electronic signatures typically use single-factor authentication. The most common approach is a password, something only you know. For example, when you purchase from an online store, you often login with a user name and password. The password is the one factor that authenticates who you are. If someone else knows your password, they can appear to be you. The person or company at the other end of the activity does not know for certain that you personally provided the electronic signature.

In contrast, digital signatures use two-factor authentication or strong authentication. You may hear the shorthand as "something you know and something you have." The "something you know" is usually a password, and "something you have" is a device such as a hardware token. For example, an ATM card uses two-factor authentication, because using it requires both the card and a PIN. SAFE digital signatures are similar to the ATM example. When you sign a document with your SAFE digital signature, you need a SAFE credential (stored on a hardware device) and a passphrase. The table below helps explain digital signatures by comparing activities for obtaining a SAFE credential with those for obtaining an ATM card.

ATM Card	SAFE Credential
In-person meeting at bank for first ATM card.	In-person meeting with Notary or Trusted Agent.
Provide proof of identity with government-issued photo ID. For an existing bank account, the bank required this proof of identity when you first opened the account.	Provide proof of identity with government-issued photo ID.
Sign agreement that defines your responsibility for payment and actions if the ATM card is lost or stolen.	Sign SAFE Subscriber Agreement that defines your responsibility for the token and actions if it is lost or stolen.
Receive ATM card.	Receive SAFE credential on either a USB token or a "SmartCard" badge.
Define PIN for your ATM card.	Define passphrase for your SAFE credential.
Using the ATM card requires both the card and your PIN.	Applying SAFE signatures requires both the credential and your passphrase.

SAFE signatures go a step beyond ATM cards, and use Public Key Infrastructure (PKI). PKI involves cryptography that codes and decodes your signature. This provides 100% assurance that your SAFE digital signature is yours, and that no other person added your digital signature to a document.