

Adobe solutions for the SAFE standard

Implement PDF signature technology in your digital workflow for streamlined electronic transactions



Digital signatures are enabling organizations to realize the full potential of paperless workflows. Today, fewer electronic workflows are encumbered by the need to print documents for signature approval. Instead of collecting pen-and-ink signatures and breaking fully electronic workflows, more organizations are relying on electronic signatures to reduce the time, expense, and data inaccuracies that come from scanning and rekeying information. To enable this transformation, laws, policies, and technologies around electronic signatures are converging, making electronic signatures as acceptable to corporations and governments as their paper-based counterparts.

The SAFE-BioPharma Association has developed a comprehensive business, policy, and technical model that unifies and defines all the elements of electronic signatures—identity management, certificate policy, public key infrastructure (PKI) technology, and cross-organization interoperability—binding them together into a single contractual model. The SAFE standard supports the use of digital signatures in PDF. Adobe’s support for the SAFE signature standard in Adobe® Acrobat®, Adobe Reader®, and Adobe LiveCycle® Enterprise Suite software enables companies to conduct business efficiently by streamlining the more secure movement of authenticated information across lines of business, between sponsors and clinical investigators, and among businesses and government regulators.

Table of contents

- 1 The downside of digital signatures
- 2 The SAFE-BioPharma Association
- 2 Legal and policy standards
- 2 Technical standards
- 2 Interoperability
- 3 Digital signatures in PDF
- 3 PDF signature technology
- 4 Conclusion

The downside of digital signatures

For pharmaceutical companies, one of the fundamentals of successful electronic signature implementation is harmonized identity management. As participants in clinical trials, a researcher, physician, or institution will often work with several different pharmaceutical companies, each with its own standards and credentials for identity. Some organizations may use passwords and other software certificates, while others may employ smart cards as identity mechanisms. In turn, each pharmaceutical company deals not only with clinical investigators but also with regulators from the governments of many countries, each with its own standards and technologies for identity. The result is a tangle of differing policies and technologies, each with unique user interfaces and procedures as well as varying levels of assurance and security.

These challenges are not isolated to the biopharmaceutical industry. Identity, electronic signatures, and interoperability are growing concerns in most industries as businesses and governments seek to automate their transactions more fully.

“Our Adobe solution will enable us to automate 80% of our records-related processes by 2008—up from 40% today. We believe we have the potential to improve patient care and reduce malpractice liability across Harvard hospitals by \$6 million per year, based on 30 years of claims experience with consent related issues, simply by automating patient consent forms.”

John Halamka, MD and CIO,
Beth Israel Deaconess Medical Center (BIDMC)

The SAFE-BioPharma Association

Signatures and Authentication for Everyone (SAFE) was established to address the need for identity and digital signature standards in the biopharmaceutical industry. SAFE began as a consortium of pharmaceutical companies and has expanded to include vendors of software and hardware for identity and digital signature systems. Pharmaceutical company members include Abbott Laboratories, AstraZeneca, Bristol-Myers Squibb, GlaxoSmithKline, Johnson & Johnson, Merck, Pfizer, Procter & Gamble, and sanofi-aventis. Software and PKI vendors include Adobe, Aladdin, Arcot, CoreStreet, Cybertrust, and IBM.

To accomplish its goal of establishing standards for identity management, certificate policy, digital signatures, signed documents, and software and hardware systems, SAFE facilitates interoperability among its members by accrediting SAFE-certified components and by providing a PKI Bridge that enables the cross-organizational validation of identities and signatures.

Legal and policy standards

Electronic signature legislation in the United States (E-SIGN and UETA) makes it clear that an electronic signature cannot be considered inferior to a pen-and-ink signature simply because it is electronic. However, it stops short of mandating any particular technology or level of assurance. In addition, the U.S. legislation does not address what type of electronic signature might be legally binding in any particular situation—these details are left to the implementers. Similarly, other countries around the world have developed their own legal considerations around digital signatures, and their mandates vary widely in degrees of policy and technical specification and interoperability.

To establish a baseline for legal acceptance of electronic signatures, SAFE has adopted an innovative approach. To participate in SAFE, members must adopt and reciprocally accept the SAFE policies on identity and digital signatures. In effect, they enter into a closed-contract agreement that specifies that any digital signature produced by a member that adheres to the SAFE identity and signature specification will be regarded as equal in legal standing to a handwritten signature by any other member of the consortium. The contractual nature of the agreement guarantees that the standard can be enforced in any U.S. state or any other country. It removes any legal ambiguity around electronic signatures for members and sets the stage for the SAFE technical standards to be definitive across the member companies.

Technical standards

The SAFE policies and procedures stipulate that the signature and identity technology cannot be easily subverted or circumvented, and it needs to be considered as-good or better than ink signatures in both its identification and authentication of the signing party. To this end, the members of SAFE have adopted strict PKI-based identity standards that require smart card or USB token-based credentials for users. The SAFE standards for digital signatures use PKI and encryption technologies to uniquely identify individuals and to create a digital “fingerprint” of a given document. These methods bind a user’s identity to a document’s fingerprint to create a unique signature, authenticating the signer and helping to ensure that the document cannot be altered without repercussions.

The SAFE technical specifications identify and require the use of specific types of PKI identity and signature technologies. In order for a signature to be accepted within the policy framework of SAFE, it must adhere to the technical standards. This creates a neatly closed loop of technology and policy, helping to ensure that digital signatures within the technical framework have the same (or better) legal standing as physically signed transactions.

Interoperability

Shared technology standards solve part of the signature and identity interoperability problem, but for the participating companies to create and validate each other’s SAFE-signed documents, they also need to address issues of federated trust. Enterprise-level PKI implementations are generally designed around what are known as “chains of trust.”

This means that for a digital signature to be considered valid, the application accepting the signature needs to be able to trust the identity used to create it. In PKI-based systems, this is usually achieved by having a central and secure “trust anchor,” or an entity that both parties trust. A trust anchor is often the issuer of digital identities within a company or a third-party certificate authority such as GeoTrust.

For SAFE, this means that while the technical framework and standards used in a signature may be interoperable between two companies, there may not be any relationship between their trust anchors. This can be as simple as a lack of awareness or a business agreement or as deliberate as one company being concerned that the other doesn’t use stringent enough security policies and practices. SAFE resolves these issues in two ways. First, since the SAFE specifications create a level playing field for both policy and technology, members are held to mutually acceptable standards for issuance policy and for the level and security of their PKI technology. This helps to largely eliminate the security-to-security and policy-to-policy reconciliation issues. Second, SAFE provides a PKI Bridge for its members. Bridge systems act like a higher level trust anchor for each of the member companies without requiring any of the members to abrogate or concede any of their own trust or technology. A digital signature from one company can be authenticated in another by an application traversing the SAFE Bridge to validate the signature’s certificates with the issuing certificate authority.

Digital signatures in PDF

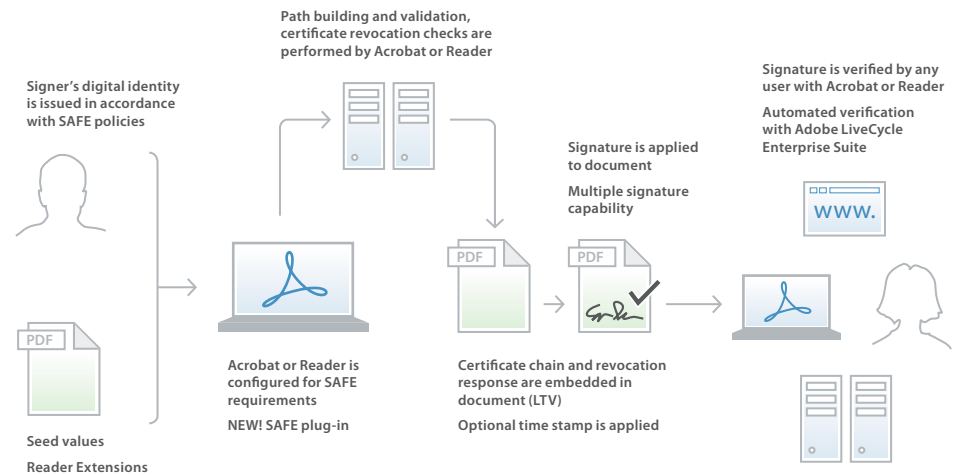
PDF is a de facto standard for document exchange and is widely adopted by life sciences and biopharmaceutical companies. The accuracy, portability, and collaborative features of PDF make it well suited to the variety of content types and platforms in biopharma workflows. PDF documents have supported digital signatures since 1999 with the release of Acrobat 4.0. In subsequent versions of the product, Acrobat support for PKI digital signature standards has steadily expanded. Acrobat 8 natively supports all the standards and specifications required for SAFE transactions. SAFE-enabled solutions can be delivered with Acrobat or Reader with a fraction of the infrastructure and expense required for other systems. Most current SAFE implementations rely heavily on several integrated server components and custom applications. None has the simplicity of signing natively in Acrobat or Reader alone. In Acrobat, the signing experience is simple, intuitive, and self-contained. There are no “receipt” files to maintain and no dependent infrastructure required to maintain them. The signature resides in the document and is always associated with it. In addition to working with conventional PDF files, the SAFE signing capability of Acrobat 8 can be incorporated into XML-based intelligent PDF forms. Intelligent PDF forms and enterprise-class document services can provide SAFE signing interface for eForms workflows.

PDF signature technology

Acrobat, Reader, and PDF include built-in support for the technologies and standards that together make up the SAFE signature standard.

Intuitive signing—For end-users, PDF signatures follow a paper-based paradigm. Signatures occur within the document and are visible on the document. Signature images can even include a SAFE logo and still be combined with sophisticated nonrepudiation and integrity technology.

PKI support—Acrobat and Reader support industry-standard X.509 certificates for signatures. They are also fully compatible with standards-based smart cards and readers and USB tokens. PDF signatures are based on industry standards like PKCS #7 and support a wide range of encryption and hash algorithms. Acrobat and Reader are extensible and support third-party software and plug-ins for the creation and validation of signatures.



Revocation checking—The built-in PKI functionality of Acrobat and Reader enables revocation checks for certificates during and after signing to help ensure that documents are being signed with a currently valid credential. Acrobat and Reader also support advanced capabilities to embed the time-stamped results of revocation checks inside a signed PDF file, capturing a snapshot of the validity of the signing certificate for long-term validation.

Time stamps (optional for SAFE)—Acrobat and Reader support industry-standard (RFC 3161) time stamps. Time stamps offer additional verification of when a transaction actually occurred and can significantly enhance the assurance level of PKI signatures.

Versioning and more secure audit trails—Multiple PDF signatures inherently create an incremental chain of signed versions of the document. This versioning capability means that users can easily determine what changes may have occurred to a document between signatures. Advanced tools, such as Acrobat Professional, even allow users to perform side-by-side visual comparisons of versions.

Together these technologies make PDF extremely well suited to standards like SAFE. The flexibility of PDF, Acrobat, and Reader means that SAFE signatures can be created and verified with little configuration and customization. The prevalence of Acrobat and Reader on the desktop means that PDF signatures can be verified by users worldwide on most operating systems.

Conclusion

SAFE has helped to significantly advance the legal, business, and technical outlook for electronic transactions worldwide. By standardizing on Adobe PDF, SAFE has also taken a significant step toward promoting the ubiquity of electronically signed documents. In turn, Adobe's built-in support for the SAFE standards demonstrates the flexibility and capability of Acrobat and Reader. Acrobat and Reader require minimal customization and interoperate directly with the standards-based PKI infrastructure of SAFE. Perhaps most important, this means that PDF signatures with Acrobat and Reader work more like traditional paper signatures than any other solution. Users can sign documents in the simple and intuitive ad hoc fashion to which they are accustomed with paper, while the more advanced PDF technologies, including LiveCycle Enterprise Suite, enable PDF documents to be incorporated directly into complex workflows with multiple users and signatures as well as enterprise systems and digital rights management solutions.

