



Signatures and Authentication For Everyone

SIGNATURES AND AUTHENTICATION FOR EVERYONE

System Documentation Glossary

1 May 2006

Version 2.1

Document Control

Area	Description
Author(s)	R. Furr
Approver(s)	SAFE-BioPharma Policy Approval Authority (PAA)
Issue Date	1 May 2006
Version	2.1
Source File	SAFE Accreditation Council Charter.doc
Security	SAFE Stakeholder confidential
Distribution	<p>The information contained in this document is intended for personnel charged with the management and operation of the SAFE System. Recipients include the SAFE-BioPharma Association, SAFE Members, SAFE Working Group Participants, SAFE Partners, and Regulatory Agencies.</p> <p>This document is controlled and managed under the authority of the SAFE Policy Approval Authority.</p>

Revision History

Revision	Date	Revised By	Summary of Changes/Comments
1.1	31 Mar 2005	R. Furr	
2.0	15 Sep 2005	R. Furr	Version 2.0, SAFE BioPharma Assn edits
2.1	16 Feb 2006	R. Furr	Update for SAFE logo change

Approval Statements

Once signed by the parties indicated below, this SAFE System Documentation Glossary has been approved by the SAFE Policy Approval Authority and has been incorporated into the SAFE Standard Document Set.

SAFE PAA Chairperson
Gary Secrest

Date

Table of Contents

1. Introduction	5
2. Audience	5
3. References	5
4. Definitions.....	6

1. Introduction

This document contains the definitions or terms accepted by SAFE.BioPharma and used through out the SAFE Standard System Documentation. The definitions in this document shall apply equally to both the singular and plural forms of the terms defined. When the context requires, any pronoun shall include the corresponding masculine, feminine and neuter forms.

Many of these terms have been previously defined and other documents are considered the reference source. Wherever possible, this has been indicated and inclusion in the SAFE Glossary is merely for convenience.

2. Audience

This document is intended for the use of members in SAFE-BioPharma and any parties contracted by them to participate in SAFE-Biopharma.

3. References

- IETF RFC 2119 <http://www.faqs.org/rfcs/rfc2119.html>
- IETF RFC 2828 <http://www.faqs.org/rfcs/rfc2828.html>
- *Merriam-Webster's English Dictionary*

4. Definitions

TERM	SAFE Meaning
21 CFR Part 11 (Part 11)	Requirements criteria under which electronic Records, Electronic Signatures, and handwritten signatures executed to electronic Records are considered equivalent to paper Records and handwritten signatures executed on paper as specified by the FDA in the US Code of Federal Regulations, Title 21, Part 11.
Access Control	A mechanism by which an operating system or application securely controls access to restricted resources.
Accreditation	The process of becoming a SAFE Accredited Issuer or a SAFE Accredited Member.
Adverse Event (AE)	A previously undetected infirmity or injury that occurs to a drug trial participant.
Affiliate	An Entity, directly or indirectly, through one or more intermediaries, controlling, controlled by, or under common control with a SAFE Member. The term "control" as used in the immediately preceding sentence shall mean either (i) the right to exercise, directly or indirectly, more than twenty-five percent (25%) of the voting rights attributable to the shares of or other ownership interests in the controlled Entity; provided that this clause (i) shall be inapplicable in the event that another unaffiliated Entity (1) holds more than fifty percent (50%) of the voting rights of the controlled Entity, or (2) has, directly or indirectly, the power to direct or cause the direction of the management or policies of the controlled Entity.
Applicant	An Entity requesting Accreditation as a SAFE Member or SAFE Issuer within the SAFE System. Once the SAFE Bridge Certification Authority is established, applicants must also request cross-certification with the SAFE Bridge Certification Authority.
Archive	A collection of data that is stored for a relatively long period of time for historical, legal, regulatory and other purposes, such as to support audit service, availability service, or system integrity service.
Audit Trail	A computer log that is automatically generated (independently of the computer's user(s)), that records activities on the computer, and that is sufficient to enable the reconstruction and examination of the sequence of environments and activities surrounding or leading to an operation, procedure, or event in a security-relevant transaction from inception to final results.
Authenticate	The use of a Public Key Infrastructure to confirm the identity of an Entity and its association with the contents of a Record.
Authorization Process	A procedure for granting Authorization.
Authorize or Authorization	To grant right(s) or permission(s) to a user to access a system resource

TERM	SAFE Meaning
B2B	Business to Business, generally in the context of collaboration, business relationships, contracts, agreements or transactions.
B2G	Business to Government, generally in the context of collaboration, business relationships, contracts, agreements or transactions.
Biometrics	A method of verifying an individual's identity based on the measurement of the individual's physical characteristic(s) or repeatable action(s) where those characteristics and/or actions are both unique to that individual and measurable.
Bridge CA (BCA)	A Certification Authority that only issues certificates to other Certification Authorities outside its PKI Domain, to support interoperability between Public Key Infrastructure Domains.
CDISC	The Clinical Data Interchange Standards Consortium.
Certificate	See "Digital Certificate".
Certificate Chain	See "Certification Path".
Certificate Policy (CP)	A specialized form of administrative policy specific to electronic transactions performed during Digital Certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromised recovery and administration of Digital Certificates.
Certificate Repository	A system, directory, database or other storage and access mechanism used by a Certification Authority to store and distribute information regarding the Digital Certificates it issues.
Certificate Revocation List (CRL)	A list maintained by a Certification Authority of the Digital Certificates that it has issued and that are revoked prior to their stated expiration date.
Certificate Status Request	An electronic Record that requests the status of a Digital Certificate to establish if the Digital Certificate is valid or invalid.
Certificate Status Response	A digitally signed Record provided by a CRL or OCSP responder in response to a Certificate Status Request.
Certification Authority (CA)	<p>An Entity trusted by one or more other Entities to create, assign, issue, and vouch for Digital Certificates.</p> <p>An Entity that issues Digital Certificates (especially x.509 Certificates) and vouches for the binding between the data items in a Certificate.</p>
Certification Path	An ordered sequence of Digital Certificates that enables a relying Entity to verify the Digital Signature on a document, file, or message. Certification Path validation is performed using the Private Key corresponding to the Public Key in the last Digital Certificate in the sequence, subject to whatever business rules or limitations the relying Entity wishes to impose on such validation.

TERM	SAFE Meaning
Certification Practices Statement (CPS)	A statement of the practices that a Certification Authority employs in managing Digital Certificates. The CPS is internal and is maintained by the Certification Authority.
Certification-Service-Provider (CSP)	An entity or a legal or natural person who issues certificates or provides other services related to electronic signatures. Term used within the European Union to refer to an entity performing the functions of an Issuer.
Consumer	An individual who obtains, through a transaction, products or services which are used primarily for personal, family, or household purposes, and also means the legal representative of such an individual.
CRL	See "Certificate Revocation List".
Cross-certification	The act or process by which two Certification Authorities establish a trust relationship by issuing each other Digital Certificates.
Digital Certificate	A Record in the form of a digital data object used by a computer that at a minimum (1) identifies the Certification Authority using it, (2) names or identifies a Subscriber, (3) contains the Subscriber's Public Key, (4) identifies its validity period, and (5) contains the Digital Signature of the Certification Authority using it.
Digital Signature	Data associated with a Record as a result of processing the Record using PKI, which data can be used to determine: (1) whether the data was created using the Private Key that corresponds to the Public Key in the signing Entity's Digital Certificate; and (2) whether the message has been altered since the Digital Signature was associated with the Record.
EFPIA	The European Federation of Pharmaceutical Industries and Associations.
EMA	The European Medicines Agency.
Employee	Any person employed by an Entity or contractually bound to act on behalf of the organization.
End-User	See "User".
Entity	A corporation, partnership, trust, limited liability company, limited liability partnership, association or other organization or entity or sole proprietorship or individuals acting in their professional capacity.
eSig, eSignature, Electronic Signature	An electronic sound, symbol, or process, attached to or logically associated with a contract or other Record and executed or adopted by a person with the intent to sign the Record.
FDA	Food and Drug Association: The Food and Drug Administration of the U.S. Department of Health and Human Services.

TERM	SAFE Meaning
Government Organization	A branch or agency of government. In the SAFE context, there are two categories of Government organization: <ol style="list-style-type: none"> 1. a regulatory agency or organization 2. any other Government agency or organization.
HL7	An international standard for clinical and administrative data promulgated by Health Level Seven, Inc., an ANSI-accredited standards developing organization.
ICH	The International Conference on Harmonization of Technical Requirements for Registration of Pharmaceuticals for Human Use.
Informed Consent	With respect to a study, a process of information exchange that provides potential study subjects with sufficient knowledge and comprehension about the study (including risks, benefits, alternatives, etc.) to freely and voluntarily consent to join the study, if the subject so desires.
Issuer	See "SAFE Issuer".
Key Compromise	A security incident in which a Private Key is exposed to potential unauthorized access, such that unauthorized disclosure, use, or alteration of the Private Key may have occurred.
Key Interface	A standard way for Signature Clients and Verifying Applications to initiate a cryptographic operation using a SAFE Credential, for the purposes of applying a Digital Signature, verifying a Digital Signature or authenticating a User.
Key Module	A hardware or software object that can be used securely to: (1) generate Key Pairs or permit an externally generated Private Key to be securely stored and (2) access the Private Key to perform cryptographic functions. Key Modules currently can be implemented in hardware (e.g., smart cards or USB tokens) or software (e.g., as files on a laptop hard drive).
Key Pair	A pair of mathematically related Keys – a Public Key and a Private Key – that are used for PKI cryptography and are generated in a way that makes it computationally infeasible to derive the Private Key from only the Public Key.
Key, or Cryptographic Key	An input parameter that is used in conjunction with a cryptographic algorithm and affects the output of that algorithm. Refers indifferently either to asymmetric or symmetric cryptographic keys.
LDAP	Lightweight Directory Access Protocol, a client-server protocol that supports basic use of the X.500 Directory (or other directory servers) without incurring the resource requirements of the full Directory Access Protocol (DAP).
Machine Operator	An individual acting on behalf of a SAFE Member assigned to or responsible for the registration and management of a Machine User.

TERM	SAFE Meaning
Machine Subscriber	A Machine that is the subject named or identified in a Digital Certificate issued to that Machine and that holds the Private Key that corresponds to the Public Key listed in the certificate.
Machine User	The combination of hardware and software that functions as an automated process on behalf of a SAFE Member.
Medical Practitioner	A medical professional , such as a doctor, nurse, etc. In the SAFE context there are two categories of practitioners: 1. clinical research investigators 2. all others.
Member	See “SAFE Member”.
MHLW	The Japanese Ministry of Health, Labour and Welfare.
Object Identifier (OID)	A specialized, formatted and unique alphanumeric/numeric identifier that is registered with an internationally recognized standards organization and that references a specific object or object class.
OCSP	On-Line Certificate Status Protocol protocol used to provide on-line validation of a Digital Certificate’s status.
OCSP Responder	A process that responds to Certificate Status Requests and that can issue one of three responses: “Valid”, “Invalid”, or “Unknown,” based on Certificate Revocation Lists or other mechanisms provided to it by Certification Authorities.
OID	See “Object Identifier”.
Other Participants	SAFE Stakeholder agents, third parties and Subscribers under contractual relationship with the SAFE Stakeholder to use the SAFE System as permitted by the SAFE Standards.
PAC	The SAFE Policy Authority Committee.
Pass phrase	A collection of alphanumeric characters and symbols with a specified minimum length and configuration that is used to access the user’s private key.
Person-to-Person	To identify an individual, and confirm by means of their proofs of identity that they are who they claim to be, through an in-person meeting between the individual and a trusted registration agent. In most major companies, a person-to-person meeting will be part of the employment process (e.g., performed by the human resources or security functions within the company), and is an allowable antecedent process for SAFE identity-proofing purposes - i.e., a pre-existing trust relationship.
PhRMA	The Pharmaceutical Research and Manufacturers Association.

TERM	SAFE Meaning
Private Key	A secret Key, associated with a Public Key that is used to create Digital Signatures and to decrypt confidential information.
Public Key	A publicly available Key, associated with a Private Key that is used to validate Digital Signatures and to encrypt confidential information.
Public Key Infrastructure (PKI)	A technology infrastructure that employs Digital Signatures to facilitate a verifiable association between the public components of an asymmetric Public Key with a specific Subscriber that possesses the Private Key.
Public Key Infrastructure (PKI) Domain	A PKI system of related CAs (and, optionally, RAs and other supporting servers and agents) operates under a common set of rules and/or regulations.
Record	Information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.
Registrar	A SAFE Member that performs the functions of a Registration Authority for SAFE Digital Certificates generated by a SAFE Issuer with respect to a SAFE Subscribing Member with which that Registrar has entered into a SAFE Member Agreement.
Registration Authority (RA)	An Entity to which a CA delegates responsibility for identification and authentication of Certificate subjects, but that does not sign or issue Certificates.
Registration Client	Combination of hardware and/or software used by a Registrar to communicate registration information and user life cycle data to an Issuer's Registration Service.
Registration Interface	A standard method for a SAFE Member's Registration Client and an Issuer's Registration Service to communicate registration information or User life cycle data
Registration Service	A service provided by an Issuer that allows SAFE Members to request Certificates, perform identity verification, approve Certificate requests, and suspend and revoke Certificates.
Relying Party	An Entity that has received information that includes a Certificate and a Digital Signature verifiable with reference to a Public Key listed in the Certificate and is in a position to rely on them.
Repository	A system for storing and distributing digital certificates and related information (including CRLs, CPSS, and certificate policies) to certificate users.
Revoked	With respect to a Digital Certificate, the designation by an Issuer that a previously valid certificate is invalid.
Root Certificate	A Certificate that is signed by the Root Certification Authority for itself.

TERM	SAFE Meaning
Root Certification Authority	A Certification Authority at the apex of a hierarchy of Certification Authorities that has signed its own Certificates.
SAFE	Signatures & Authentication (see "SAFE-Biopharma")
SAFE-Biopharma	The shortened version of SAFE-BioPharma, Association used in the SAFE Standard documents.
SAFE Bridge Certification Authority (SBCA)	The biopharmaceutical industry's mechanism for enabling PKI Domain interoperability.
SAFE community	The collective set of SAFE Stakeholders, supporting systems, and Subscribers.
SAFE Certificate Holder	See "SAFE Subscriber".
SAFE Credential	A Key Module that stores a cryptographic Private Key and a corresponding cryptographic Public Key contained within a Digital Certificate that is issued to a SAFE Member User.
SAFE Credential Holder	See "SAFE Subscriber".
SAFE Issuer Agreement	The Contract that binds each SAFE Issuer to SAFE-BioPharma
SAFE Issuer, SAFE Accredited Issuer	A Certification Authority that contracts with SAFE-BioPharma and that has been found by SAFE to comply with the SAFE Standard System Documentations to provide credential services to SAFE Members. Once the SAFE Bridge CA has been established, Issuers must be Cross-certified with the SAFE Bridge CA.
SAFE Machine Systems	A hardware/operating system platform that is under the control of a SAFE Machine Operator and has the ability to sign and/or verify SAFE System Transactions automatically under program or workflow direction.
SAFE Member Agreement	Contract between a SAFE Member and SAFE-BioPharma
SAFE Member, SAFE Accredited Member	An Entity that contracts with SAFE BioPharma to be bound to the SAFE Standard and that has been found by SAFE to comply with the SAFE Standards.
SAFE Participant	SAFE Stakeholders, Associate and Government Members, and Other Participants.
SAFE Roles	A definition of the expected set of functions to be performed by a SAFE Stakeholder.
SAFE Signatory	An Entity that is bound by contract with SAFE to comply with the provisions of the SAFE Standards as either a SAFE Member or a SAFE Issuer.

TERM	SAFE Meaning
SAFE Signer, Signer	A SAFE Subscriber who uses a SAFE Credential to sign a file, document, or message with a Digital Signature in accordance with the SAFE Standard.
SAFE Stakeholder	SAFE.Biopharma, SAFE Members, and SAFE Issuers.
SAFE Stakeholder Legal Entity	A Stakeholder that has its own legal existence (other than a SAFE User that is an individual).
SAFE Standards	The standards and rules (including the SAFE Technical Specifications and Requirements) issued by SAFE LLC for the use of the SAFE System.
SAFE Subscriber Agreement	The contract that binds a SAFE Subscriber to a SAFE Member in terms of affirming that the subscriber will be bound by the SAFE Standard in use of the SAFE credential.
SAFE Subscriber, Subscriber	A User that is the subject named or identified in a SAFE-compliant Digital Certificate issued to that User and that holds the Private Key that corresponds to the Public Key listed in the certificate.
SAFE System	The combination of SAFE Roles and SAFE Technology Groups, which together provide the required capabilities, features, and functions needed for SAFE implementation within the bio-pharmaceutical community.
SAFE System Transaction	A SAFE System Transaction comprises the execution of the following components and steps: <ul style="list-style-type: none">• Creation of a Digital Signature meeting all of the requirements prescribed by the SAFE Digital Signature Use & Verification Functional Process Guidelines• Verification of the authenticity of the Digital Signature and validation of the status of, and conditions contained in, the Digital Certificate and its related Certificate Chain from the SAFE Signer's Certificate up to the SAFE Signer's trust anchor using the steps defined in the SAFE Digital Signature Use & Verification Functional Process Guidelines
SAFE Technical Specifications and Requirements	Requirements that provide system development documentation upon which the SAFE System is developed and deployed.
SAFE Technology Group	A set of technology components (hardware, software, and/or networking elements) that implement a single instance of a SAFE technical solution.

TERM	SAFE Meaning
SAFE BioPharma, Association	SAFE-BioPharma, Association will be a not-for-profit organization that will maintain the SAFE Standard, and the associated Member and Issuer agreements to which affiliated entities must comply if they wish to remain part of the SAFE community. SAFE-BioPharma will provide a common trust bridge between SAFE-BioPharma and other stakeholders to facilitate the goal of achieving a legally acceptable, regulatory compliant, and biopharmaceutical Industry interoperable digital signature. Should a dispute arise amongst SAFE Stakeholders, SAFE-BioPharma will provide consistent procedures for dispute resolution.
Secure Signature Creation Device (SSCD)	Equivalent to a Token, this term is used within the European Union to refer to this type of cryptographic device.
Signature Client	A technology component (e.g., hardware or software) that presents or displays a Record to a User for signing with a Digital Signature.
Signature Container	A data object used to store a Digital Signature and relevant information such as the date/time it was created.
Signature Profile	Information that defines a consistent format for a Signature Container.
Smart Card	A card containing a computer chip that meets the SAFE Standards for Key storage and SAFE System cryptographic processing.
Sponsoring	The act by which SAFE makes an Entity an Associate Member, or, by which a SAFE Member presents an Entity as a suitable candidate for membership as an Associate Member
Suspended	Temporary ceasing by Issuers or Members to participate in the operations of the SAFE System as set forth in the document Compliance Process.
Terminated	Ceasing by Issuers or Members to participate in the operations of the SAFE System as set forth in the document Compliance Process.
Token	A piece of hardware that contains a cryptographic chip as a mechanism to create and protect a Private Key.
Trust Bridge	The collection of hardware, software, policies, procedures and agreements that allow subscribers to one Public Key Infrastructure Domain to rely on digital certificates issued by other Public Key Infrastructure Domains. Often referred to as a "trust anchor".
Trusted Agent	A person or Entity authorized to act as a representative of an Entity in confirming Subscriber identification during the registration process.
User or SAFE User	A Digital Certificate Holder within the SAFE PKI Domain (including Entities, individuals, network devices, machines and software applications) that must be authorized by a SAFE Member to use the SAFE System.
UTC	Coordinated Universal Time, the local time at the 0 meridian passing through Greenwich, England (Greenwich Mean Time), updated with leap

TERM	SAFE Meaning
	seconds.
Validate	Action whereby the status of a Certificate is checked upon request by a party.
Validation Interface	Specification for the interface between a Verifying Application and a Validation Service
Validation Service	A service that provides Certificate Status Responses.
Verifying Application	A software application that is designed to provide the authenticity of the signature for the Relying Party.