PART 1300 — DEFINITIONS

§1300.03 Definitions relating to electronic orders for controlled substances and electronic prescriptions for controlled substances.

For the purposes of this chapter, the following terms shall have the meanings specified:

Application service provider means an entity that sells electronic prescription or pharmacy applications as a hosted service, where the entity controls access to the application and maintains the software and records on its servers.

Audit trail means a record showing who has accessed an information technology application and what operations the user performed during a given period.

Authentication means verifying the identity of the user as a prerequisite to allowing access to the information application.

Authentication protocol means a well specified message exchange process that verifies possession of a token to remotely authenticate a person to an application.

Biometric authentication means authentication based on measurement of the individual's physical features or repeatable actions where those features or actions are both distinctive to the individual and measurable.

Biometric subsystem means the hardware and software used to capture, store, and compare biometric data. The biometric subsystem may be part of a larger application. The biometric subsystem is an automated system capable of:

(1) Capturing a biometric sample from an end user.

(2) Extracting and processing the biometric data from that sample.

(3) Storing the extracted information in a database.

(4) Comparing the biometric data with data contained in one or more reference databases.

(5) Determining how well the stored data matches the newly captured data and indicating whether an identification or verification of identity has been achieved.

Cache means to download and store information on a local server or hard drive.

Certificate policy means a named set of rules that sets forth the applicability of the specific digital certificate to a particular community or class of application with common security requirements.

Certificate revocation list (CRL) means a list of revoked, but unexpired certificates issued by a certification authority.

Certification authority (CA) means an organization that is responsible for verifying the identity of applicants, authorizing and issuing a digital certificate, maintaining a directory of public keys, and maintaining a Certificate Revocation List.

Certified information systems auditor (CISA) means an individual who has been certified by the Information Systems Audit and Control Association as qualified to audit information systems and who performs compliance audits as a regular ongoing business activity.

Credential means an object or data structure that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a person.

Credential service provider (CSP) means a trusted entity that issues or registers tokens and issues electronic credentials to individuals. The CSP may be an independent third party or may issue credentials for its own use.

CSOS means controlled substance ordering system.

Digital certificate means a data record that, at a minimum—

(1) Identifies the certification authority issuing it;

(2) Names or otherwise identifies the certificate holder;

(3) Contains a public key that corresponds to a private key under the sole control of the certificate holder;

(4) Identifies the operational period; and

(5) Contains a serial number and is digitally signed by the certification authority issuing it.

Digital signature means a record created when a file is algorithmically transformed into a fixed length digest that is then encrypted using an asymmetric cryptographic private key associated with a digital certificate. The combination of the encryption and algorithm transformation ensure that the signer's identity and the integrity of the file can be confirmed.

Digitally sign means to affix a digital signature to a data file.

Electronic prescription means a prescription that is generated on an electronic application and transmitted as an electronic data file.

Electronic prescription application provider means an entity that develops or markets electronic prescription software either as a stand- alone application or as a module in an electronic health record application.

Electronic signature means a method of signing an electronic message that identifies a particular person as the source of the message and indicates the person's approval of the information contained in the message.

False match rate means the rate at which an impostor's biometric is falsely accepted as being that of an authorized user. It is one of the statistics used to measure biometric performance when operating in the verification or authentication task. The false match rate is similar to the false accept (or acceptance) rate.

False non-match rate means the rate at which a genuine user's biometric is falsely rejected when the user's biometric data fail to match the enrolled data for the user. It is one of the statistics used to measure biometric performance when operating in the verification or authentication task. The false match rate is similar to the false reject (or rejection) rate, except that it does not include the rate at which a biometric system fails to acquire a biometric sample from a genuine user.

FIPS means Federal Information Processing Standards. These Federal standards, as incorporated by reference in **§ 1311.08** of this chapter, prescribe specific performance requirements, practices, formats, communications protocols, etc., for hardware, software, data, etc.

FIPS 140-2, as incorporated by reference in **§ 1311.08** of this chapter, means the National Institute of Standards and Technology publication entitled "Security Requirements for Cryptographic Modules," a Federal standard for security requirements for cryptographic modules.

FIPS 180-2, as incorporated by reference in **§ 1311.08** of this chapter, means the National Institute of Standards and Technology publication entitled "Secure Hash Standard," a Federal secure hash standard.

FIPS 180-3, as incorporated by reference in **§ 1311.08** of this chapter, means the National Institute of Standards and Technology publication entitled "Secure Hash Standard (SHS)," a Federal secure hash standard.

FIPS 186-2, as incorporated by reference in **§ 1311.08** of this chapter, means the National Institute of Standards and Technology publication entitled "Digital Signature Standard," a Federal standard for applications used to generate and rely upon digital signatures.

FIPS 186-3, as incorporated by reference in **§ 1311.08** of this chapter, means the National Institute of Standards and Technology publication entitled "Digital Signature Standard (DSS)," a Federal standard for applications used to generate and rely upon digital signatures.

Hard token means a cryptographic key stored on a special hardware device (e.g., a PDA, cell phone, smart card, USB drive, one-time password device) rather than on a general purpose computer.

Identity proofing means the process by which a credential service provider or certification authority validates sufficient information to uniquely identify a person.

Installed electronic prescription application means software that is used to create electronic prescriptions and that is installed on a practitioner's computers and servers, where access and records are controlled by the practitioner.

Installed pharmacy application means software that is used to process prescription information and that is installed on a pharmacy's computers or servers and is controlled by the pharmacy.

Intermediary means any technology system that receives and transmits an electronic prescription between the practitioner and pharmacy.

Key pair means two mathematically related keys having the properties that:

(1) One key can be used to encrypt a message that can only be decrypted using the other key; and

(2) Even knowing one key, it is computationally infeasible to discover the other key.

NIST means the National Institute of Standards and Technology.

NIST SP 800-63-1, as incorporated by reference in **§ 1311.08** of this chapter, means the National Institute of Standards and Technology publication entitled "Electronic Authentication Guideline," a Federal standard for electronic authentication.

NIST SP 800-76-1, as incorporated by reference in **§ 1311.08** of this chapter, means the National Institute of Standards and Technology publication entitled "Biometric Data Specification for Personal Identity Verification," a Federal standard for biometric data specifications for personal identity verification.

Operating point means a point chosen on a receiver operating characteristic (ROC) curve for a specific algorithm at which the biometric system is set to function. It is defined by its corresponding coordinates—a false match rate and a false non-match rate. An ROC curve shows graphically the trade-off between the principal two types of errors (false match rate and false non-match rate) of a biometric system by plotting the performance of a specific algorithm on a specific set of data.

Paper prescription means a prescription created on paper or computer generated to be printed or transmitted via facsimile that meets the requirements of **part 1306**of this chapter including a manual signature.

Password means a secret, typically a character string (letters, numbers, and other symbols), that a person memorizes and uses to authenticate his identity.

PDA means a Personal Digital Assistant, a handheld computer used to manage contacts, appointments, and tasks.

Pharmacy application provider means an entity that develops or markets software that manages the receipt and processing of electronic prescriptions.

Private key means the key of a key pair that is used to create a digital signature.

Public key means the key of a key pair that is used to verify a digital signature. The public key is made available to anyone who will receive digitally signed messages from the holder of the key pair.

Public Key Infrastructure (PKI) means a structure under which a certification authority verifies the identity of applicants; issues, renews, and revokes digital certificates; maintains a registry of public keys; and maintains an up-to-date certificate revocation list.

Readily retrievable means that certain records are kept by automatic data processing applications or other electronic or mechanized recordkeeping systems in such a manner that they can be separated out from all other records in a reasonable time and/or records are kept on which certain items are asterisked, redlined, or in some other manner visually identifiable apart from other items appearing on the records.

SAS 70 Audit means a third-party audit of a technology provider that meets the American Institute of Certified Public Accountants (AICPA) Statement of Auditing Standards (SAS) 70 criteria.

Signing function means any keystroke or other action used to indicate that the practitioner has authorized for transmission and dispensing a controlled substance prescription. The signing function may occur simultaneously with or after the completion of the two-factor authentication protocol that meets the requirements of **part 1311** of this chapter. The signing function may have different names (e.g., approve, sign, transmit), but it serves as the practitioner's final authorization that he intends to issue the prescription for a legitimate medical reason in the normal course of his professional practice.

SysTrust means a professional service performed by a qualified certified public accountant to evaluate one or more aspects of electronic systems.

Third-party audit means an independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.

Token means something a person possesses and controls (typically a key or password) used to authenticate the person's identity.

Trusted agent means an entity authorized to act as a representative of a certification authority or credential service provider in confirming practitioner identification during the enrollment process.

Valid prescription means a prescription that is issued for a legitimate medical purpose by an individual practitioner licensed by law to administer and prescribe the drugs concerned and acting in the usual course of the practitioner's professional practice.

WebTrust means a professional service performed by a qualified certified public accountant to evaluate one or more aspects of Web sites.

[75 FR 16304, Mar. 31, 2010]

Effective Date Note: At 75 FR 16304, Mar. 31, 2010, §1300.03 was added, effective June 1, 2010.