Implementation Guidance of Title 21 CFR Part 11

Version 1.1

1900 Reston Metro Plaza, Suite 303
Reston, VA 20190

www.makeidentitysafe.com

info@makeidentitysafe.com

(703) 705-2920

Version History

Version Number	Date	Revised By	Summary of Changes/Comments
1.0	March 2021	N/A	Initial Release
1.1	March 2021	Relationship Manager	The word "not" was removed from the statement, "*Implementors may elect not to use non-cryptographic signatures in lieu of superior digital signatures*." Changes were made on pages 15, 30, 33, and 34.

Terms and Conditions

SAFE Identity, LLC (SAFE) is an industry consortium comprising a number of commercial healthcare members (as further specified at http://www.makeidentitysafe.com). This Guidance Document was developed and is being released under this open-source license by SAFE.

Use of this Guidance Document is subject to the disclaimers and limitations described below. By using this Guidance Document, you (the user) agree to and accept the following terms and conditions:

1. This Guidance Document may not be modified in any way. In particular, no rights are granted to alter, transform, create derivative works from, or otherwise modify this Guidance Document. Redistribution and use of this Guidance Document, without modification, is permitted provided that the following conditions are met:

- Redistributions of this Guidance Document must retain the above copyright notice, this list of conditions, and all terms and conditions contained herein.
- Redistributions in conjunction with any product or service must reproduce the above copyright notice, this list of conditions, and all terms and conditions contained herein in the documentation and/or other materials provided with the distribution of the product or service.
- SAFE Identity's name may not be used to endorse or promote products or services derived from this Guidance Document without specific prior written permission.

2. The use of technology described in or implemented in accordance with this Guidance Document may be subject to regulatory controls under the laws and regulations of various jurisdictions. The user bears sole responsibility for the compliance of its products and/or services with any such laws and regulations and for obtaining any and all required authorizations, permits, or licenses for its products and/or services as a result of such laws or regulations.

3. THIS GUIDANCE DOCUMENT IS PROVIDED "AS IS" AND WITHOUT WARRANTY OF ANY KIND. SAFE AND EACH SAFE MEMBER DISCLAIMS ALL EXPRESS, IMPLIED AND STATUTORY WARRANTIES, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF TITLE, NONINFRINGEMENT, MERCHANTABILITY, QUIET ENJOYMENT, ACCURACY, AND FITNESS FOR A PARTICULAR PURPOSE. NEITHER SAFE NOR ANY SAFE MEMBER WARRANTS (A) THAT THIS GUIDANCE DOCUMENT IS COMPLETE OR WITHOUT ERRORS, (B) THE SUITABILITY FOR USE IN ANY JURISDICTION OF ANY PRODUCT OR SERVICE WHOSE DESIGN IS BASED IN WHOLE OR IN PART ON THIS GUIDANCE DOCUMENT, OR (C) THE SUITABILITY OF ANY PRODUCT OR A SERVICE FOR CERTIFICATION UNDER ANY CERTIFICATION PROGRAM OF SAFE OR ANY THIRD PARTY.

4. IN NO EVENT SHALL SAFE OR ANY SAFE MEMBER BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY CLAIM ARISING FROM OR RELATING TO THE USE OF THIS GUIDANCE DOCUMENT, INCLUDING, WITHIOUT LIMITATION, A CLAIM THAT SUCH USE INFRINGES A THIRD PARTY'S INTELLECTUAL PROPERTY RIGHTS OR THAT IT FAILS TO COMPLY WITH APPLICABLE LAWS OR REGULATIONS. BY USE OF THIS GUIDANCE DOCUMENT, THE USER WAIVES ANY SUCH CLAIM AGAINST SAFE OR ANY SAFE MEMBER RELATING TO THE USE OF THIS GUIDANCE DOCUMENT. IN NO EVENT SHALL SAFE OR ANY SAFE MEMBER BE LIABLE FOR ANY DIRECT OR INDIRECT DAMAGES OF ANY KIND, INCLUDING CONSEQUENTIAL, INCIDENTAL, SPECIAL, PUNITIVE, OR OTHER DAMAGES WHATSOEVER ARISING OUT OF OR RELATED TO ANY USER OF THIS GUIDANCE DOCUMENT, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

5. SAFE reserves the right to modify or amend this Guidance Document at any time, with or without notice to the user, and in its sole discretion. The user is solely responsible for determining whether this Guidance Document has been superseded by a later version or a different Guidance Document.

6. These terms and conditions will be interpreted and governed by the laws of the Commonwealth of Virginia, without regard to its conflict of laws and rules. Any party asserting any claims related to this Guidance Document irrevocably consents to the personal jurisdiction of the U.S. District Court for the Eastern District of Virginia and to any state court located in such district of the Commonwealth of Virginia and waives any objections to the venue of such court. Application to the U.N. Convention and Contracts for International Sale of Goods is expressed excluded.

Contributors

This document was developed and produced by the **SAFE Identity Document Management System Working Group**.

Special thanks to:

***Daniel McKenna**, McDougall Scientific*

***Devry Spreitzer,** Astellas Pharma US*

***Timothy Simpson,** AstraZeneca*

***Cezar Ignat,** Trans Sped*

***Patrick Patterson,** Carillon Information Security*

***Jeff Hutchison,** IdenTrust*

***Kyle Neuman,** SAFE Identity*

***Judith Spencer,** SAFE Identity*

***Eboni Akins,** SAFE Identity*

About SAFE

SAFE Identity is an industry consortium and certification body that provides an ecosystem for identity assurance in the healthcare sector to enable trust, security and user convenience. It reduces risk and assures the integrity of identities and data in virtual clinical trials, medical devices and trusted data exchange in healthcare supply chains.

Purpose

The SAFE Identity Document Management System Working Group reviewed each control in Title 21 CFR Part 11 and defined which party or parties may be responsible for satisfying each control. This guidance relies on as much of the SAFE Identity Trust Framework and certification programs as possible to help implementing organizations get the most benefit from these programs. In some cases, SAFE certification programs do not satisfy requirements in 21 CFR Part 11. In such cases, the responsibility of satisfying the control becomes the responsibility of the vendor or implementor. Implementors are ultimately responsible for 21 CFR Part 11 compliance and may use this guidance to help alleviate burden associated with FDA software validation but should always consult professional assistance in achieving an FDA validation for updated or new systems.

***Note**: The FDA does not certify or endorse any product for being independently compliant with Title 21 CFR Part 11. Any claims made by a vendor for being compliant with 21 CFR Part 11 are self-asserted. As an industry consortium and certification body supporting identity and cryptography in healthcare, the information documented in the matrix below articulates SAFE Identity's interpretation of 21 CFR Part 11 requirements. This interpretation has not been evaluated and/or endorsed by the FDA in any way.*

[Code of Federal Regulations]

[Title 21, Volume 1]

[Revised as of April 1, 2019]

[CITE: 21CFR11]

TITLE 21--FOOD AND DRUGS

CHAPTER I--FOOD AND DRUG ADMINISTRATION

DEPARTMENT OF HEALTH AND HUMAN SERVICES

SUBCHAPTER A--GENERAL

PART 11 ELECTRONIC RECORDS; ELECTRONIC SIGNATURES

https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=11&showFR=1

Table of Contents

Column Categories

Note: The matrix presents four main categories of responsibility, three of which are listed as "Responsible parties" who are responsible for satisfying certain clauses within Title 21 CFR Part 11.

Title 21 CFR Part 11:		States the clause.
SAFE Identity Interpretation:		Explains SAFE's response to the clause. SAFE's overall stance in 21 CFR Part 11 is that digital signatures are the only standards-based reliable method to adequately confirm the nonrepudiation necessary to enforce the integrity of a digitally signed document.
SAFE Identity Certification Programs		Defines the ways the SAFE Identity Certificate Policy and/or Qualified Products List program satisfies the nature of the clause.
Product Vendor:		Defines responsibilities outside of the scope of SAFE certification programs, but still potentially residing within a vendor product.
Implementor (healthcare organization):		Defines the responsibility of the implementing healthcare organization both in relation to the clause and how to best leverage SAFE certification programs and vendor products.
Informational:		Provides context for clauses. No responsibility is assessed for how the particular clause is satisfied.

Title 21 CFR Part 11	SAFE Identity Interpretation	SAFE Identity Certification Programs	Product Vendor	Implementor (healthcare organization)	Informational
Subpart A--General Provisions					
Sec. 11.1 Scope.					
(a) The regulations in this part set forth the criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.	SAFE Identity is an industry consortium and certification body supporting identity and cryptography in healthcare. SAFE operates a bridge certification authority that certifies identity providers against a common set of criteria and communicates its certification through cross-certificates, thereby cryptographically joining certified identity providers to a common identity infrastructure. The requirements for SAFE Identity certification are specified in the SAFE Identity Certificate Policy (CP). The certification process is outlined in the SAFE Identity Cross Certification Process document. SAFE Identity operates a product testing and certification capability known as the Qualified Products List (QPL). The QPL lab tests various identity and PKI-related products against industry standards and member-driven requirements as the pre-requisite for inclusion on the QPL. The combination of requirements specified in the SAFE Identity Certificate Policy and outlined in the various SAFE Identity QPL specifications is the basis of this interpretation.	None	No Responsibility	No Responsibility	Informational

Title 21 CFR Part 11	SAFE Identity Interpretation	SAFE Identity Certification Programs	Product Vendor	Implementor (healthcare organization)	Informational
(b) This part applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted, under any records requirements set forth in agency regulations. This part also applies to electronic records submitted to the agency under requirements of the Federal Food, Drug, and Cosmetic Act and the Public Health Service Act, even if such records are not specifically identified in agency regulations. However, this part does not apply to paper records that are, or have been, transmitted by electronic means.	In relation to this document, SAFE Identity is solely concerned with digital signatures applied to files using private keys associated with SAFE Certified Digital Certificates obtained from a SAFE Certified Credential Provider where the digital signature was applied using a product listed on the SAFE Identity QPL.	None	No Responsibility	No Responsibility	Informational
(c) Where electronic signatures and their associated electronic records meet the requirements of this part, the agency will consider the electronic signatures to be equivalent to full handwritten signatures, initials, and other general signings as required by agency regulations, unless specifically excepted by regulation(s) effective on or after August 20, 1997.	SAFE Certified Digital Signatures meet the criteria outlined in the Electronic Signatures in Global and National Commerce Act (E-Sign) of 2000 and the Federal CIO Council's Use of Electronic Signatures in Federal Organization Transactions v.1.0 dated January 25, 2013.	SAFE Identity Certificate Policy	No Responsibility	No Responsibility	N/A
(d) Electronic records that meet the requirements of this part may be used in lieu of paper records, in accordance with 11.2, unless paper records are specifically required.	No Response	None	No Responsibility	Implementors must identify any processes that require explicitly paper documents. In this scenario, 21 CFR Part 11 does not apply.	Informational
(e) Computer systems (including hardware and software), controls, and attendant documentation maintained under this part shall be readily available for, and subject to, FDA inspection.	No Response	None	No Responsibility	Implementors must ensure external service providers have delivered the necessary documentation to satisfy requirements in 21 CFR Part 11.	N/A

Title 21 CFR Part 11	SAFE Identity Interpretation	SAFE Identity Certification Programs	Product Vendor	Implementor (healthcare organization)	Informational
(f) This part does not apply to records required to be established or maintained by 1.326 through 1.368 of this chapter. Records that satisfy the requirements of part 1, subpart J of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.	No Response	None	No Responsibility	No Responsibility	Informational
(f) This part does not apply to records required to be established or maintained by 1.326 through 1.368 of this chapter. Records that satisfy the requirements of part 1, subpart J of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part. (g) This part does not apply to electronic signatures obtained under 101.11(d) of this chapter. (h) This part does not apply to electronic signatures obtained under 101.8(d) of this chapter.	No Response	None	No Responsibility	No Responsibility	Informational

Title 21 CFR Part 11	SAFE Identity Interpretation	SAFE Identity Certification Programs	Product Vendor	Implementor (healthcare organization)	Informational
(i) This part does not apply to records required to be established or maintained by part 117 of this chapter. Records that satisfy the requirements of part 117 of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part. (j) This part does not apply to records required to be established or maintained by part 507 of this chapter. Records that satisfy the requirements of part 507 of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part. (k) This part does not apply to records required to be established or maintained by part 112 of this chapter. Records that satisfy the requirements of part 112 of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.	No Response	None	No Responsibility	No Responsibility	Informational

Title 21 CFR Part 11	SAFE Identity Interpretation	SAFE Identity Certification Programs	Product Vendor	Implementor (healthcare organization)	Informational
(l) This part does not apply to records required to be established or maintained by subpart L of part 1 of this chapter. Records that satisfy the requirements of subpart L of part 1 of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part. (m) This part does not apply to records required to be established or maintained by subpart M of part 1 of this chapter. Records that satisfy the requirements of subpart M of part 1 of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part. (n) This part does not apply to records required to be established or maintained by subpart O of part 1 of this chapter. Records that satisfy the requirements of subpart O of part 1 of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.	No Response	None	No Responsibility	No Responsibility	Informational
(o) This part does not apply to records required to be established or maintained by part 121 of this chapter. Records that satisfy the requirements of part 121 of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part. [62 FR 13464, Mar. 20, 1997, as amended at 69 FR 71655, Dec. 9, 2004; 79 FR 71253, 71291, Dec. 1, 2014; 80 FR 71253, June 19, 2015; 80 FR 56144, 56336, Sept. 17, 2015; 80 FR 74352, 74547, 74667, Nov. 27, 2015; 81 FR 20170, Apr. 6, 2016; 81 FR 34218, May 27, 2016]	No Response	None	No Responsibility	No Responsibility	Informational

Title 21 CFR Part 11	SAFE Identity Interpretation	SAFE Identity Certification Programs	Product Vendor	Implementor (healthcare organization)	Informational
Sec. 11.2 Implementation					
(a) For records required to be maintained but not submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that the requirements of this part are met. (b) For records submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that: (1) The requirements of this part are met; and (2) The document or parts of a document to be submitted have been identified in public docket No. 92S-0251 as being the type of submission the agency accepts in electronic form. This docket will identify specifically what types of documents or parts of documents are acceptable for submission in electronic form without paper records and the agency receiving unit(s) (e.g., specific center, office, division, branch) to which such submissions may be made. Documents to agency receiving unit(s) not specified in the public docket will not be considered as official if they are submitted in electronic form; paper forms of such documents will be considered as official and must accompany any electronic records. Persons are expected to consult with the intended agency receiving unit for details on how (e.g., method of transmission, media, file formats, and technical protocols) and whether to proceed with the electronic submission.	No Response	None	No Responsibility	Implementor Requirement	To use electronic records, the implementor must ensure the requirements in 21 CFR Part 11 are met. When documents are submitted to the government in electronic form, the documents must have been identified as being a document and format that the government can accept.

Title 21 CFR Part 11	SAFE Identity Interpretation	SAFE Identity Certification Programs	Product Vendor	Implementor (healthcare organization)	Informational
Sec. 11.3 Definitions.					
(a) The definitions and interpretations of terms contained in section 201 of the act apply to those terms when used in this part. (b) The following definitions of terms also apply to this part: (1) Act means the Federal Food, Drug, and Cosmetic Act (secs. 201-903 (21 U.S.C. 321-393)). (2) Agency means the Food and Drug Administration.	No Response	None	No Responsibility	No Responsibility	Informational
(3) Biometrics means a method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable.	No Response	None	No Responsibility	No Responsibility	Informational
(4) Closed system means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.	No Response	None	No Responsibility	No Responsibility	Informational
(5) Digital signature means an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.	SAFE Certified Digital Signature requirements meet the criteria of this digital signature definition. The rules and parameters applied by SAFE Identity are conformant to industry standards (PKIX, X.509) and government requirements (NIST, FPKI, ETSI).	SAFE Identity Certificate Policy and Qualified Products List (QPL)	No Responsibility	No Responsibility	Informational

Title 21 CFR Part 11	SAFE Identity Interpretation	SAFE Identity Certification Programs	Product Vendor	Implementor (healthcare organization)	Informational
(6) Electronic record means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.	SAFE Identity recognizes that all electronic files have the capacity to be digitally signed. Currently, PDF is the only file format tested by the QPL lab. Testing for other file formats, such as the eCTD file format, are being considered.	SAFE Identity Certificate Policy and Qualified Products List (QPL)	No Responsibility	No Responsibility	Informational
(7) Electronic signature means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.	SAFE Identity does not recognize non-cryptographic electronic signatures as competent means of expressing non-repudiation of the signer, due to the risk of forgery, and therefore, advises against their use for this purpose. Later in this document, visual representations of digital signatures are contemplated.	None	No Responsibility	Implementors may elect to use non-cryptographic signatures in lieu of superior digital signatures.	Informational
(8) Handwritten signature means the scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark.	SAFE Identity does not consider the use of a non-cryptographic electronic signature (an image of a hand-written signature) a reliable means of proving non-repudiation of electronic records due to the risk of forgery.	None	No Responsibility	Implementors may elect to use non-cryptographic signatures in lieu of superior digital signatures.	Informational
(9) Open system means an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.	No Response	None	No Responsibility		Informational

Title 21 CFR Part 11	SAFE Identity Interpretation	SAFE Identity Certification Programs	Product Vendor	Implementor (healthcare organization)	Informational
Sec. 11.10 Controls for closed systems.					
Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:	Public Key Infrastructure (PKI) is specifically designed to address the questions of authenticity, integrity, non-repudiation and confidentiality. SAFE Identity certification ensures a PKI practitioner or consumer is employing suitable technology, procedures and controls to ensure this capability.	None	No Responsibility	No Responsibility	Informational
(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	The SAFE Identity QPL Lab tests digital signature validation software for its ability to detect altered records or records signed with untrustworthy digital certificates. The requirements for developing test cases originated from NIST, ISO, RFC 5280 and member driven requirements. SAFE Identity QPL lab testing satisfies some of the requirements of this control. SAFE Identity and its associated requirements do not audit or inspect the implementation of systems at deployed sites. SAFE Identity certification ensures the digital certificates being used by a system are trustworthy/authentic and that the system processes digital certificates properly. This requirement should be verified with prospective vendor products by the purchasing healthcare organization. In context of electronic records, SAFE Interprets the word: "reliability" to mean electronic records must be available and retain integrity throughout their availability period.	SAFE Identity Cross Certification Process SAFE Identity QPL Specifications *Note: the SAFE Identity QPL tests vendor products for their ability to apply and verify digital signatures in a way that is consistent with industry standards to ensure integrity by testing a product's ability to discern invalid or altered records. The QPL does not test products for availability*	All capabilities of a vendor product beyond digital signatures must be verified with the vendor	Implementors must ensure requirements are being met either by the vendor products being purchased or by some other mechanism.	N/A

Title 21 CFR Part 11	SAFE Identity Interpretation	SAFE Identity Certification Programs	Product Vendor	Implementor (healthcare organization)	Informational
(b) The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.	No Response beyond Subpart B (a)	None	All capabilities of a vendor product beyond digital signatures must be verified with the vendor.	Implementors must configure the system in a way that complies with this requirement.	N/A
(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.	SAFE Identity Certified digital signature requirements include the preservation of records to facilitate retrieval of evidence concerning the validity of digital credentials. SAFE Identity QPL lab testing satisfies some of the requirements of this control. The SAFE Identity QPL lab tests products for their ability to validate digital signatures and preserve a record of the validation. The requirements for developing test cases originated from NIST and ISO guidance, RFC 5280 and member-driven requirements. Products certified under "LTV" or "Long Term Validation" ensure products maintain accurate and valid documents throughout the lifecycle of the document.	SAFE Identity Certificate Policy SAFE Identity QPL Refer to DMSWG001 Decision Memorandum concerning the storage of a digitally signed file for archival prior to changing.	All capabilities of the vendor product beyond digital signatures must be verified with the vendor including the product's ability to retrieve the correct electronic record when necessary.	Implementors must maintain a record retention policy in compliance with this CFR. Implementors must ensure the system is configured to retrieve all applicable documents throughout the retention period.	N/A

Title 21 CFR Part 11	SAFE Identity Interpretation	SAFE Identity Certification Programs	Product Vendor	Implementor (healthcare organization)	Informational
(d) Limiting system access to authorized individuals.	No Response beyond Subpart B (a).	SAFE Identity Certificate Policy	All capabilities of a vendor product beyond digital signatures must be verified with the vendor.	Implementors must configure the system in a way that complies with this requirement. Note that digital signature credentials may not suffice for authentication in all cases. Implementors must be cognizant of system access design to meet the requirements of this control. Implementors may elect to only credential authorized individuals for signing, thus achieving authentication and authorization. Implementors may also elect to use Role-Based Certificates to ensure authorization is enforced when accessing or signing documents in a system.	N/A
(e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.	Timestamping of audit trails can be accomplished in a multitude of ways by an implementor. Audit trails may be electronic records in a database, digitally signed text entries on documents or some other mechanism. Digital signatures may or may not be used to satisfy this control. SAFE Identity QPL lab testing satisfies some of the requirements of this control. The use of the term "time-stamping" is not interpreted as meaning RFC 3161 compliant timestamping, although such technology can be used to satisfy part of the requirements in this control.	The QPL Lab tests digital signature creation software for its ability to create and apply digital signatures to files using digital certificates. The QPL does not test a product's ability to generate or retain audit logs on an implementor's system.	The vendor product may assist an implementor with compliance of this control if the vendor product records the actions of an end user in a way that the user cannot alter and associates a date/time with the actions of end users.	Implementors must configure the system in a way that complies with this control which may include configuration of a secure time source, access controls on audit data and data retention policies.	N/A

Title 21 CFR Part 11	SAFE Identity Interpretation	SAFE Identity Certification Programs	Product Vendor	Implementor (healthcare organization)	Informational
(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	SAFE Identity and its associated requirements do not audit or inspect the implementation of systems at deployed sites. SAFE Identity ensures the digital certificates being used by a system are trustworthy/authentic and that the system processes digital certificates properly. This requirement should be verified with prospective vendor products by the purchasing healthcare organization.	None	All capabilities of a vendor product beyond digital signatures must be verified with the vendor.	Implementors must configure the system in a way that complies with this requirement.	N/A
(g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	SAFE Identity and its associated requirements do not audit or inspect the implementation of systems at deployed sites. SAFE Identity ensures the digital certificates being used by a system are trustworthy/authentic and that the system processes digital certificates properly. Role-Based Certificates defined in the SAFE Identity Certificate Policy can be used to communicate authorization of system users. Vendor products must support the use of role-based certificates or implement alternative access role features. Alternatively, the implementor may elect to only credential authorized individuals for signing, thus achieving authentication and authorization. The SAFE Identity Certificate Policy can be used to satisfy this control. This requirement should be verified with prospective vendor products by the purchasing healthcare organization.	SAFE Identity Certificate Policy	All capabilities of the vendor product beyond digital signatures must be verified with the vendor.	Implementors must configure the system in a way that complies with this requirement. Note that digital signature credentials may not suffice for authentication in all cases. Implementors must be cognizant of system access design to meet the requirements of this control.	N/A

Title 21 CFR Part 11	SAFE Identity Interpretation	SAFE Identity Certification Programs	Product Vendor	Implementor (healthcare organization)	Informational
(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	Implementors must ensure custom device interfaces enforce input validation when consuming information from outside sources such as humans or other devices. Keyboards, monitors, mouses and other common hardware do not tend to fall in the scope of this control as they are generally accepted and/or tested through global technology industry processes such as common criteria. The SAFE Identity Certificate Policy can be used to satisfy part of this control. Implementors may use device certificates to prove the validity of information originating from a medical device. Code signing of firmware and code deployed to a medical device can be used to validate the inputs and instructions that a medical device uses to carry out its tasks.	SAFE Identity Certificate Policy	All capabilities of the vendor product beyond digital signatures must be verified with the vendor.	No Responsibility	N/A

Title 21 CFR Part 11	SAFE Identity Interpretation	SAFE Identity Certification Programs	Product Vendor	Implementor (healthcare organization)	Informational
(i) Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.	SAFE Identity requires that each digital signature credential holder acknowledge responsibility for the continued integrity and safeguarding of the credential via a Subscriber Agreement. There are detailed requirements for the training and experience of individuals responsible for creating and distributing digital signature credentials. The SAFE Identity Certificate Policy satisfies part of this control. SAFE Identity does not audit or inspect the education, training and experience of individuals responsible for developing, maintaining or using the deployed electronic record/electronic signature systems. Upon listing a vendor product on the SAFE Identity QPL, an approval letter is drafted and sent to the vendor as well as published online to outline the conditions and configurations used to certify a product in our lab environment. This information may be useful for implementors if they wish to replicate the configurations of the QPL to achieve the same behavior from the certified software.	SAFE Identity Certificate Policy	Vendors must provide the necessary documentation to facilitate training and successful integration within customer environment.	Implementors must train employees on the proper use of the system and organization policies.	N/A

Title 21 CFR Part 11	SAFE Identity Interpretation	SAFE Identity Certification Programs	Product Vendor	Implementor (healthcare organization)	Informational
(j) The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.	The SAFE Identity Certificate Policy places specific responsibilities on the safeguarding and use of digital signature credentials. These appear as Representations and Warranties for Subscribers (*See Section 9.6.3 in the SAFE Identity Certificate Policy*) and culminate with the signing of the Subscriber Agreement. The SAFE Identity Certificate Policy satisfies this control.	SAFE Identity Certificate Policy	No Responsibility	Implementors should establish internal policies defining responsibilities of its staff members when using digital identities within information systems. Implementors must enforce penalties for misuse of credentials. Implementors may also include legally binding acknowledgement of digital signatures equivalent of handwritten signatures in employee handbook.	N/A
(k) Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	SAFE Identity and its associated requirements do not audit or inspect the implementation of systems at deployed sites. SAFE Identity ensures the digital certificates being used by a system are trustworthy/authentic and that the system processes digital certificates properly. The SAFE Identity Certificate Policy stipulates strict change control requirements for SAFE Certified Credential Providers who are part of the federation. The SAFE Identity Certificate Policy satisfies part of this control. This requirement should be verified with prospective vendor products by the purchasing healthcare organization.	SAFE Identity Certificate Policy	All capabilities of the vendor product beyond digital signatures must be verified with the vendor. Specifically, the vendor product must ensure time sequencing of events.	Implementors must establish controls and procedures to protect system documentation and distribute system documentation to the appropriate individuals.	N/A

Title 21 CFR Part 11	SAFE Identity Interpretation	SAFE Identity Certification Programs	Product Vendor	Implementor (healthcare organization)	Informational
Sec. 11.30 Controls for open systems.					
Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.	SAFE Certified Digital Certificates are purpose-built to provide identity assurance (authenticity), digital signature (integrity) and encryption (confidentiality) capabilities for workflow process environments. The trust community of which SAFE Identity is the hub facilitates cross-organizational trust of deployed digital certificates. The SAFE Certificate Policy and QPL lab testing satisfy the requirements of this control.	SAFE Identity Certificate Policy and Qualified Products List (QPL)	No Responsibility	When confidentiality is necessary, implementors may elect to use SAFE Certified Encryption Credentials to encrypt documents. Other encryption schemes may also be used to satisfy this control, particularly when the data requiring confidentiality resides in a database rather than a file repository.	N/A

Title 21 CFR Part 11	SAFE Identity Interpretation	SAFE Identity Certification Programs	Product Vendor	Implementor (healthcare organization)	Informational
Sec. 11.50 Signature manifestations.					
(a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following: (1) The printed name of the signer; (2) The date and time when the signature was executed; and (3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.	All digital signatures include the name of the signatory and the date/time the signature was created. The meaning of the signatures is implementation-specific and should be designated in the workflow process by the deploying organization. SAFE recommends the date and time that the signature was generated should originate from an authoritative time source. SAFE QPL lab testing satisfies part of this control.	SAFE Identity Certificate Policy and Qualified Products List (QPL)	Vendors may consume the contents of a digital certificate to obtain the name of a signer. Date, time and meaning of a signature are all features that must accompany the signature.	Implementors must ensure the proper configuration of a product to meet these requirements.	N/A

Title 21 CFR Part 11	SAFE Identity Interpretation	SAFE Identity Certification Programs	Product Vendor	Implementor (healthcare organization)	Informational
(b) The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).	All digital signatures include the name of the signatory, date/time when the signature was created and, optionally, the meaning of the signature. The meaning of a signature is implementation-specific and cannot be verified through product testing or is not covered under SAFE Identity QPL product testing. The SAFE Identity QPL tests products for the visual output of digital signatures to ensure compliance to this control. SAFE Identity QPL lab testing satisfies part of this control. Note: Any time a document is printed, the electronic record does not retain cryptographic integrity. This is true across all technologies. SAFE suggests including a note that indicates the printed version is not the master version of the document. (ex. "copy-digitally signed record on file"). Implementor may include a unique identifier in the printed record to allow traceability and verification of the electronic master copy. Other processes may be used to ensure traceability back to the master copy.	SAFE Identity Certificate Policy and Qualified Products List (QPL)	Vendor products certified on the QPL meet this requirement when used with SAFE Certified Credentials. Vendor products must offer users a mechanism for entering the "meaning" or "reason" for applying a digital signature.	Implementors must ensure the proper configuration of a product to meet these requirements.	N/A

Title 21 CFR Part 11	SAFE Identity Interpretation	SAFE Identity Certification Programs	Product Vendor	Implementor (healthcare organization)	Informational
Sec. 11.70 Signature/record linking.					
Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.	SAFE Certified Digital Signatures conform to international standards and U.S. Federal requirements for providing integrity and technical non-repudiation. These standards include performing a mathematical process on the electronic record called a hash and then encrypting the hash. The resultant value becomes the document's signature. A hash value is a one-way cryptographic process. The original data involved in creating a hash cannot be derived from the resultant hash. A base document will always create the same hash and if any change is made to the base document, the hash value changes in a detectable way. A signature will only validate for the document it was created from and only if the document was not subsequently altered. The simplest and most widely supported means of satisfying this control is through the use of PKI-based digital signatures, but implementors may use other methods to satisfy this control. The SAFE Identity Certificate Policy and SAFE Identity QPL testing satisfy the requirements of this control.	SAFE Identity Certificate Policy and Qualified Products List (QPL)	Vendor products listed on the SAFE QPL meet this requirement when used with SAFE Certified Credentials.	Implementors must ensure the signature is linked to the identity of the signer. If SAFE Certified Credentials are not used, implementors must ensure the digital credentials meet the requirements of this control.	N/A

Title 21 CFR Part 11	SAFE Identity Interpretation	SAFE Identity Certification Programs	Product Vendor	Implementor (healthcare organization)	Informational
Subpart C--Electronic Signatures					
Sec. 11.100 General requirements.					
(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	SAFE Certified Digital Certificate requirements include the specification that human subscriber digital certificates must be unique to the individual named in the certificate, must be destroyed in the event the binding to that individual becomes invalid, and the private key used in the digital signature process must be in the sole possession of the subscriber. The SAFE Identity Certificate Policy satisfies this control. Note: The SAFE Identity Group Certificate assurance level is not approved for non-repudiation (signature). Role or individual certificates are required for this control.	SAFE Identity Certificate Policy and Qualified Products List (QPL)	Vendor products listed on the SAFE Identity QPL meet this requirement when used with SAFE Certified Credentials.	Implementors must ensure the signature is linked to one individual. If SAFE Certified Credentials are not used, implementors must ensure the digital credentials meet the requirements of this control.	N/A
(b) Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.	SAFE Certified Digital Certificate requirements include an identity proofing (verification) process that aligns with NIST Special Publication 800-63 Identity Assurance Level 2. Identity must be established by a Registration Authority and documentary proofs of identity must be validated prior to issuance. The SAFE Identity Certificate Policy satisfies this control.	SAFE Identity Certificate Policy and Qualified Products List (QPL)	Vendor products listed on the SAFE Identity QPL meet this requirement when used with SAFE Certified Credentials.	Implementors must ensure the signature is linked to the identity of the signer. If SAFE Certified Credentials are not used, implementors must ensure the digital credentials meet the requirements of this control.	N/A

Title 21 CFR Part 11	SAFE Identity Interpretation	SAFE Identity Certification Programs	Product Vendor	Implementor (healthcare organization)	Informational
(c) Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures. (1) The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857. (2) Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.	SAFE Certified Digital Certificate holders are required to sign a Subscriber Agreement acknowledging their responsibilities. Digital certificates specifically identify the processes for which they can be utilized. This is a 20-year-old requirement that is largely OBE (Overtaken by Events). Individual organizations may want an assurance level of this type, and if so, it would be captured in a memorandum of agreement or contracting vehicle. The SAFE Identity Certificate Policy satisfies part of this control.	SAFE Identity Certificate Policy	No Responsibility	Implementors must submit appropriate documentation to the Office of Regional Operations. Implementors may also add processes that ensure the implementor's employees attest to the legally binding equivalent of wet ink signatures.	N/A

Title 21 CFR Part 11	SAFE Identity Interpretation	SAFE Identity Certification Programs	Product Vendor	Implementor (healthcare organization)	Informational
Sec. 11.200 Electronic signature components and controls.					
(a) Electronic signatures that are not based upon biometrics shall: (1) Employ at least two distinct identification components such as an identification code and password. (i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual. (ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components. (2) Be used only by their genuine owners; and (3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.	SAFE Certified Digital Certificates require multifactor identity authentication for use: possession of the corresponding private key (something owned) and knowledge of the activation data for the private key (something known). Client software may be configured to allow multiple signings with a single key activation during a single continuous session. SAFE Identity does not monitor such activity, and this is up to the implementing organization. The private key used for a digital signature is in the sole possession of the owner and the activation data is memorized. The multifactor identity authentication process ensures the technical integrity of the signature. The Subscriber Agreement requires acknowledgment by the individual that neither the private key nor its activation data may be shared with other parties. The SAFE Identity Certificate Policy satisfies this control. Note: SAFE Identity and its associated requirements do not audit or inspect the implementation of systems at deployed sites. Some responsibility is owned by the implementing organization to ensure all requirements outlined in this control are met.	SAFE Identity Certificate Policy	Vendor products listed on the SAFE Identity QPL meet this requirement when used with SAFE Certified Credentials.	If SAFE Certified Credentials are not used, implementors must ensure the digital credentials meet the requirements of this control.	N/A

Title 21 CFR Part 11	SAFE Identity Interpretation	SAFE Identity Certification Programs	Product Vendor	Implementor (healthcare organization)	Informational
(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	SAFE Identity does not recommend the use of a biometric electronic signing process that is not combined with a cryptographic function. It does not carry the strength of integrity offered by digital certificates. SAFE Identity does support the local use of a biometric one-to-one match with a stored value (something I am) in lieu of an activation code (something I know) for activating a private key (something I have).	None	No Responsibility	Implementors may elect to use non-cryptographic signatures in lieu of superior digital signatures.	N/A

Title 21 CFR Part 11	SAFE Identity Interpretation	SAFE Identity Certification Program	Product Vendor	Implementor (healthcare organization)	Informational
Sec. 11.300 Controls for identification codes/passwords					
Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:	SAFE Identity interprets the requirements defined in the SAFE Identity Certificate Policy as satisfactory implementations of the intent of the controls laid out in this section. The use of One-Time Password (OTP) and other id code/password combinations should use cryptographic processes in order to protect them from substitution and man-in-the-middle attacks.	None	No Responsibility	No Responsibility	Informational
(a) Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.	The SAFE Identity Certificate Policy places specific responsibilities on the safeguarding and use of digital signature credentials. These include requirements for multi-factor authentication, tying a unique credential to a unique person (except for group certificates), periodic cycling, revocation, and interoperability testing among other requirements. SAFE Identity interprets the requirements defined in the SAFE Identity Certificate Policy as satisfactory implementations of the intent of the controls laid out in this section. Rather than the use of passwords, SAFE Identity applies the same controls laid out in section 11.300 to strong cryptographic PKI-based credentials. The SAFE Identity Certificate Policy satisfies this control.	SAFE Identity Certificate Policy	Vendor products listed on the SAFE Identity QPL meet this requirement when used with SAFE Certified credentials.	If SAFE Certified Credentials are not used, implementors must ensure the digital credentials meet the requirements of this control.	N/A

Title 21 CFR Part 11	SAFE Identity Interpretation	SAFE Identity Certification Program	Product Vendor	Implementor (healthcare organization)	Informational
(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	The SAFE Identity Certificate Policy places specific responsibilities on the safeguarding and use of digital signature credentials. These include requirements for multi-factor authentication, tying a unique credential to a unique person (except for group certificates), periodic cycling, revocation, and interoperability testing among other requirements. SAFE Identity interprets the requirements defined in the SAFE Identity Certificate Policy as satisfactory implementations of the intent of the controls laid out in this section. Rather than the use of passwords, SAFE Identity applies the same controls laid out in section 11.300 to strong cryptographic PKI-based credentials. The SAFE Identity Certificate Policy satisfies this control.	SAFE Identity Certificate Policy	Vendor products listed on the SAFE Identity QPL meet this requirement when used with SAFE Certified Credentials.	If SAFE Certified Credentials are not used, implementors must ensure the digital credentials meet the requirements of this control.	N/A
(c) Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.	The SAFE Identity Certificate Policy places specific responsibilities on the safeguarding and use of digital signature credentials. These include requirements for multi-factor authentication, tying a unique credential to a unique person (except for group certificates), periodic cycling, revocation, and interoperability testing among other requirements. SAFE Identity interprets the requirements defined in the SAFE Certificate Policy as satisfactory implementations of the intent of the controls laid out in this section. Rather than the use of passwords, SAFE Identity applies the same controls laid out in section 11.300 to strong cryptographic PKI-based credentials. The SAFE Identity Certificate Policy satisfies this control.	SAFE Identity Certificate Policy	Vendor products listed on the SAFE Identity QPL meet this requirement when used with SAFE Certified Credentials.	If SAFE Certified Credentials are not used, implementors must ensure the digital credentials meet the requirements of this control.	N/A

Title 21 CFR Part 11	SAFE Identity Interpretation	SAFE Identity Certification Program	Product Vendor	Implementor (healthcare organization)	Informational
(d) Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.	The SAFE Identity Certificate Policy places specific responsibilities on the safeguarding and use of digital signature credentials. These include requirements for multi-factor authentication, tying a unique credential to a unique person (except for group certificates), periodic cycling, revocation, and interoperability testing among other requirements. SAFE Identity interprets the requirements defined in the SAFE Identity Certificate Policy as satisfactory implementations of the intent of the controls laid out in this section. Rather than the use of passwords, SAFE Identity applies the same controls laid out in section 11.300 to strong cryptographic PKI-based credentials. The SAFE Identity Certificate Policy satisfies this control.	SAFE Identity Certificate Policy	Vendor products listed on the SAFE Identity QPL meet this requirement when used with SAFE Certified Credentials.	Implementors may elect to use non-cryptographic signatures in lieu of superior digital signatures.	N/A

Title 21 CFR Part 11	SAFE Identity Interpretation	SAFE Identity Certification Program	Product Vendor	Implementor (healthcare organization)	Informational
(e) Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.	The SAFE Identity Certificate Policy places specific responsibilities on the safeguarding and use of digital signature credentials. These include requirements for multi-factor authentication, tying a unique credential to a unique person (except for group certificates), periodic cycling, revocation, and interoperability testing among other requirements. SAFE Identity interprets the requirements defined in the SAFE Identity Certificate Policy as satisfactory implementations of the intent of the controls laid out in this section. Rather than the use of passwords, SAFE Identity applies the same controls laid out in section 11.300 to strong cryptographic PKI-based credentials. The SAFE Identity Certificate Policy satisfies this control.	SAFE Identity Certificate Policy	Vendor products listed on the SAFE Identity QPL meet this requirement when used with SAFE Certified Credentials.	Implementors may elect to use non-cryptographic signatures in lieu of superior digital signatures.	N/A

Glossary of Terms

Assurance Level	The level of certainty a relying party can be assured that the identity of the subject defined in a credential accurately represents the subject. Assurance levels vary by the level of identity proofing requirements, infrastructure requirements, audits and other criteria, as well as the level of private key protection in which the subscriber's private key resides.
Authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. [1]
Authorize/Authorization	To grant right(s) or permission(s) to a user to access a system resource.
Biometrics	A method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable.
Closed System	An environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.
Credential	An object that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by the entity represented by the object (person, organization or thing).
Cryptography	Refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms, to transform messages in ways that are hard to decipher.[2]

[1] fpki-x509-cert-policy-common.pdf (idmanagement.gov)
[2] https://searchsecurity.techtarget.com/definition/cryptography

Decision Memorandum DMSWG001	An output of the SAFE Identity Document Management System Working Group, which outlines a consensus reached on ways to address document flattening and usability within document management systems. The document is downloadable at makeidentitysafe.com[3]
Digital Certificate	A credential in the form of an X.509 data object used by a computer that at a minimum (1) identifies the Certification Authority vouching for the contents, (2) names or identifies a Subscriber/subject of the certificate, (3) contains the Subscriber's/subject's Public Key, (4) identifies its validity period, and (5) contains the Digital Signature from the Certification Authority this is vouching for the certificate's contents.
Digital Signature	An electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.
Electronic Record	Any combination of text, graphics, data, audio, pictorial or other information representation in digital form that is created, modified, maintained, archived, retrieved or distributed by a computer system.
Electronic Signature	A computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to represent an individual's handwritten signature. A digital signature is a secure and legally binding type of electronic signature.
Encryption	A cryptographic process that obfuscates text or other data into a cipher in such a way that the cipher can only be decrypted (or otherwise read) using a specific secret code or decryption key.
Federal Food, Drug, and Cosmetic Act	A set of laws passed by Congress in 1938 giving authority to the U.S. Food and Drug Administration to oversee the safety of food, drugs, medical devices, and cosmetics.[4]

[3] http://makeidentitysafe.com/download/decision-memorandum-dmswg001/
[4] https://www.fda.gov/regulatory-information/laws-enforced-fda/federal-food-drug-and-cosmetic-act-fdc-act

Federal PKI (FPKI)	A network of Certification Authorities (CAs) that issue: PIV credentials and person identity certificates PIV-Interoperable credentials and person identity certificates.[5]
Hash	A cryptographic process performed on the electronic data which produces a unique value for the data that was processed. The exact same data will produce that exact same hash value.
Internet Engineering Task Force (IETF)	An open standards organization, which develops and promotes voluntary Internet standards, in particular the standards that comprise the Internet protocol suite.[6]
Interoperability	In healthcare, interoperability is the ability of different information technology systems and software applications to communicate, exchange data, and use the information that has been exchanged. Data exchange schema and standards should permit data to be shared across clinician, lab, hospital, pharmacy, and patient regardless of the application or application vendor.[7]
International Standards Organization (ISO)	An international standard-setting body composed of representatives from various national standards organizations.[8]
Long-Term Validation (LTV)	LTV signatures are designed for circumstances where the validity period of the signature goes beyond the life of the credential used to sign the data. LTV signatures include fields that support embedding a full certificate chain back to a Trust Anchor and all revocation data associated with the certificate chain.
MFA (Multi-Factor Authentication)	An authentication system that requires more than one distinct authentication factor for successful authentication. Multi-factor authentication can be performed using a combination of authenticators that provide different factors. The three common authentication factors are something you know, something you have, and something you are.[9]

[5] www.fpki.idmanagement.gov/
[6] https://www.ietf.org/
[7] https://www.himss.org/previous-himss-interoperability-definitions
[8] https://www.iso.org/home.html
[9] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

NIST (National Institute of Standards and Technology)	A physical sciences laboratory and a non-regulatory agency of the United States Department of Commerce.
Non-repudiation	Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. Technical non-repudiation refers to the assurance a Relying Party has that if a public key is used to validate a digital signature, that signature had to have been made by the corresponding signing Private Key. Legal non- repudiation refers to how well possession or control of the private Signing Key can be established.
Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public/private key pairs, including the ability to issue, maintain, and revoke public key certificates.
Public Health Service Act	A United States federal law legislated in 1944.[10]
Registration Authority	A trusted entity that establishes and vouches for the identity and authorization of a certificate applicant on behalf of some authority (e.g., a CA).
Revocation	The communication process under which, a Digital Certificate signed by an Issuer that was previously valid, is no longer to be trusted and therefore considered invalid.
Role-Based Certificate	A role-based certificate identifies a specific role title on behalf of which the subscriber is authorized to act rather than the subscriber's name.
SAFE Identity Bridge Certification Authority (SIBCA)	The industry consortium's cryptographic mechanism for enabling PKI Domain interoperability.

[10] https://www.govinfo.gov/content/pkg/USCODE-2010-title42/html/USCODE-2010-title42-chap6A.htm

SAFE Identity Certificate Policy	SAFE's 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.[11]
SAFE Certified Credential Provider	A credential provider certified under the processes governed by the SAFE Identity PMA.
SAFE Certified Digital Signature	A digital signature created by a SAFE Identity certified credential.
SAFE Identity Cross Certification	The SAFE Identity Certificate Policy (CP) defines the SIBCA as an interoperability mechanism for ensuring trust across independent PKI domains. Successful cross certification with the SIBCA asserts that the Applicant PKI operates in conformance with the CP and the related standards, guidelines and practices of the SAFE Identity Policy Management Authority (PMA).
SAFE Identity Cross Certification Process	The process, steps, and criteria necessary to achieve cross certification with the SAFE Identity Bridge Certification Authority. This process is defined in the SAFE Identity Cross Certification Process Document. [12]
SAFE Identity Qualified Products List (QPL)	A public collection of applications and products that have undergone lab testing to confirm that they process identity credentials in accordance with applicable SAFE identity testing specifications.
SAFE Identity Trust Framework	SAFE's collection of policies, technical specifications, and interoperability criteria that are accepted by multi-organizational participants to satisfy a particular need.
Signatory	Any entity responsible for signing an agreement.

[11] http://makeidentitysafe.com/download/safe-certificate-policy/
[12] http://makeidentitysafe.com/download/cross-certification-process-document/

Specification	SAFE Identity's technical and functional requirements for the technology components of the participating in concert with the SAFE Identity Trust Framework, including, any requirements which may be attached or contained in any Policies, and all know-how, methodologies and processes contained and expressed in and embodied by such Specifications.
Subscriber	The entity whose name appears as the subject in an end-entity certificate, agrees to use its key and certificate in accordance with the certificate policy asserted in the certificate, and does not itself issue certificates.
Subscriber Agreement	An acknowledgement on the part of the Subscriber that identifies the responsibilities associated with the use and protection of digital credentials issued to the Subscriber.
Token	A piece of hardware that contains a cryptographic chip as a mechanism to create and protect a Private Key.