RECOMMENDED GUIDELINES FOR THE USE OF SAFE-BIOPHARMA (SBP) COMPLIANT CREDENTIALS FOR:

AUTHENTICATION FROM THE PERSPECTIVE OF STRENGH OF AUTHENTICATION VERSUS SENSITIVITY OF INFORMATION; and

DIGITAL SIGNATURES AS THE PREFERRED FORM OF ELECTRONIC SIGNATURES

October 2016

Contents

I. Introduction

The following discussion describes SAFE-BioPharma Association guidance concerning Authentication Credentials and Digital Signatures. This guidance, while primarily intended for the SAFE-BioPharma community, is considered equally applicable to the broader life sciences and healthcare areas. This guidance supports the overall life sciences and healthcare industry as they move towards expanded online business implementations.

A. Where are we now?

The online identity credentials used within industry today are based on an industrial age approach. Identities are owned by the company and begin and end at company boundaries. Most identity and access management (IAM) systems are proprietary and based on company requirements rather than on universal standards. Often companies issue and manage credentials – usually user id/password pairs (which provide weak security) – applicable for that company or application only. As applications move onto cloud services and connect to the Internet to take advantage of the freedom such services provide, management of those types of credentials becomes expensive and the access to sensitive information and assets such services provide often does not adequately protect sensitive information resources. This is especially the case in healthcare and life sciences.

The FDA requires:

> "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…."
>
> "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." (Title 21, FDA, 11.10 and 11.30)

B. Goal

Business practices in the 21st century are based upon a collaborative, online model allowing rapid access across a sphere of many partners and business locations. Identity and Access Management (IAM) systems must support and enhance the ability to conduct business electronically while protecting sensitive information and allowing users to move fluidly across the Internet.

Online identity standards provide tools for companies, vendors, regulators and others to share a common trust framework for authentication and signing. Standards allow users and vendors to develop products and applications knowing that they will be acceptable across industry and can be confidently used by industry.

Our goal as an industry is to extend standardized online identity assertions across the industry, allowing individuals to have one digital identity that can be recognized by all stakeholders. Having a common framework for trust in identity for applications access and for signing of electronic documents is especially critical in healthcare.

II. Authentication

A. Definitions

- Electronic Authentication: Electronic authentication (e-authentication) is the process of establishing confidence in user identities that have been electronically presented to an online system or application. E-authentication presents a technical challenge when this process involves the remote (i.e., not physical face-to-face) authentication of individual people over an open network (e.g., the Internet).[1]
- Levels of assurance (LoA) of identity or strength of proof that the user requesting authentication is who he or she claims to be are based upon assessments of the adequacy and strength of applicant identity proofing, the degree to which the credential technology resists threats and the comprehensiveness of the processes for issuing and managing the credential. The US government currently calls out 4 LoA of identity for authentication assertions [2] while the European Union recently adopted a 3 level scheme [3] that generally aligns with the US LOA 2-4. These LoA schemes evolve as threats and threat vectors evolve and as the eGovernment and eCommerce worlds move slowly towards a common benchmark for online trust. SAFE-BioPharma participates in this process and evolves the Standard to accommodate the changing online authentication landscape. The current US government LoA are presented here to illustrate the generic relationship between risk factors and risk mitigation implementations. Privacy protections are required of credential issuers at all levels regardless of level of assurance.

- Current LoA definitions
    - **NIST Level 1 (EU has no equivalent)** - Although there is no identity proofing requirement at this level, the authentication mechanism provides some assurance that the same Claimant who participated in previous transactions is seeking to access the current protected transaction or data.

[1] NIST SP 800-63-1 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf

[2] NIST SP 800-63-1 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf

[3] COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502 of 8 September 2015," Article 1 (1) & (2)

- **NIST Level 2 (EU Low)** –provides some assurance of identity and usually consists of single factor authentication. At Level 2, identity proofing requirements are introduced, requiring presentation of identifying materials or information.
- **NIST Level 3 (EU Substantial)** –provides substantial assurance of identity and requires multi-factor authentication methods, generally two authentication factors. At this level, identity proofing procedures require verification of identifying materials and information.
- **NIST Level 4 (EU High)**– is intended to provide the highest practical online authentication assurance. Level 4 authentication is based on multifactor cryptographic methods, often three factors. At this level, in-person identity proofing is required. Level 4 is similar to Level 3 except that only "hard" cryptographic tokens are allowed.

- Identity and access credentials must comply with standards that relate the level of trust in the asserted identity to the associated risk to the information in the online applications. The following chart relating level of assurance of identity to level of risk was developed by the US Government and is the *de facto* global standard for identity trust assurance levels of risk.

Assurance Level Impact Profiles

Potential Impact Categories for Authentication Errors	Level 1	Level 2 (EU Low)	Level 3 (EU Substantial)	Level 4 (EU High)
Inconvenience, distress or damage to standing or reputation	Low	Mod	Mod	High
Financial loss or agency liability	Low	Mod	Mod	High
Harm to agency programs or public interests	N/A	Low	Mod	High
Unauthorized release of sensitive information	N/A	Low	Mod	High
Personal Safety	N/A	N/A	Low	Mod High
Civil or criminal violations	N/A	Low	Mod	High

B. SAFE-BIOPHARMA Guidance for Authentication

The following table provides SAFE-BioPharma recommended guidance for **minimum level of assurance of a credential for each listed use case**. (NOTE: Use case definitions are provided in Section IV below.) Credentials which have been certified compliant with the SAFE-BioPharma Trust Framework Provider Program or which are credentials issued by another trust framework recognized by SAFE-BioPharma may be trusted to have the required identity proofing, credential management and credential technology to satisfy the US and EU level of assurance requirements for assertion of identity online.

Example Use Case	**Level 1**	**Level 2 (EU Low)**	**Level 3 (EU Substantial)**	**Level 4 (EU High)**
Access to web-facing applications that **do not** contain <company> sensitive information or where the user is limited to access to their own personal information	X			
<Company> public information	X			
Company Proprietary (internal) Information		X		
<Company> sensitive information			X	
<Company> most sensitive information			X	
Personally Identifiable Information		X		
Sensitive Personally Identifiable Information			X	
Personal Health Information			X	
Unrestricted Remote Access – Any individual user to enterprise network via Internet connection			X	
Remote Access to platform shared by two or more enterprises			X	
Access to any privileged network account			X	
Access to highly sensitive company information			X	
Unrestricted access of Enterprise User to enterprise information system using enterprise computing assets and account			X	
Restricted Access via an Application Gateway to a limited set of applications on the enterprise network		X		
Access to the enterprise email system via WebMail			X	
Direct Diagnostic Access			X	
Diagnostic Access		X	X	
High-value manufacturing (e.g., involving nuclear equipment, materials)				X
Sharing PII (data in motion) in EU				X
Electronic Payments Exceeding $10,000				X
Access to national security and law enforcement online systems				X
Prescribing controlled substances online			X	

III. Electronic Signatures

A. Definitions

There are two types of electronic signatures.[4] One type acknowledges the signer's intention to apply his/her electronic signature on an electronic record or other electronic object by maintaining a record of the user's actions indicating their intent to electronically sign. Generally, this is a record of the user entering their electronic signature, typically user ID and password, and the acceptance of these user credentials by the signature application. The application maintains association of the user's signature record with the object that was signed in a proprietary manner. This type is known as an **"electronic signature."**

A second type is a **"digital signature"** which uses standardized cryptographic methods and uses the record or object (actually a cryptographic digest of the object) along with the user's individual cryptographic information to form the digital signature. In so doing, digital signatures offer a number of features that make them more robust than electronic signatures. However, this is not to say that electronic signatures are not an acceptable form of signature for instances where the rigor of a digital signature is not required.

1. Electronic signatures

Generally, to create an **electronic signature** the signer invokes an electronic signature routine from within an application. This signature routine may instruct the user to add specific information into the object being signed (e.g., the physical representation of the user's name and perhaps a reason for the user's signature). Then the software will request the signer to authenticate him- or herself once more, sometimes by simply checking a box in the application but more often by having the user re-enter a user ID and password pair to the application's signing function.

Assignment and management of the user ID and password pair may be done as part of the application administration or may be done external to the application. But for either case the user authenticates him- or herself to the signing function and, if accepted, the signature routine forms a record of this

[4] NOTE: For purposes of this guidance a digitized representation of a user's wet signature is not considered an electronic signature. Such a representation of a wet signature may be added to any document as a simple (e.g., clip art) insertion without requirement for the user to authenticate the insertion. This form of digitized signature is specifically NOT recommended by SAFE-BioPharma. This should not be confused with the scan of a document which has been signed with a wet signature. Such scan results in an electronic version of the document but not an electronic signature as define here.

authentication and its acceptance. The application maintains an association of this authentication record with the object which was signed – generally in a proprietary manner. It is this record of association that actually forms the electronic signature. There should also be an audit record showing the date and time of the signature authentication. In this type of electronic signature, the "strength" of the bond between the signer and the signature application is directly linked to the strength or level of assurance of the user credential (user ID/password pair) being used for the authentication.

The required strength or level of assurance of identity of the signer's electronic signature credential (LoA) is generally determined by the value of the record or object being signed. For instance, a LoA2 credential may be acceptable for an electronic signature on a $20 expense voucher but is not likely to be acceptable on a $1M purchase order. The determination of the required LoA is a policy decision made by the enterprise or process owner.

Also, while proper system controls implemented as part of an FDA validated system can add a level of deterrence by the very nature of the electronic signature, while the signature record is associated in some manner with the object which has been signed, it is possible through malicious acts for the object to be changed while the signature record remains unchanged. The only means to assure that the electronically signed object has not been changed after it was signed is to review audit records of access (and perhaps change) to the object or file. Since it is possible for the object to be changed after it has been signed without affecting the signature record, it is also possible for the signer to repudiate his or her signature by claiming that someone else had changed the object after it was signed or that someone else had access to their user ID and password and used it to sign the object without authority to do so. The process to overturn any such claim can be laborious and expensive.

1. Digital Signatures

As noted above, a **digital signature** is a cryptographic method that combines the object with the user's private cryptographic key which is under sole control of the user. In order for a user to execute a digital signature he or she MUST: a) have a mathematically-bound, two-part digital credential *(consisting of a private cryptographic key which is under the sole control of the user that is uniquely bound to a public cryptographic key which is linked to the user's proven identity)* and, b) the signature routine called by the software must meet proven international digital

signature technical standards which ensure security and interoperability.[5] The user's digital signature is completed by cryptographically combining the user's private key with the actual object being signed.

A valid digital signature gives a recipient (relying party) assurance that the object was signed by a known user, that the user cannot deny having signed the object *(authentication and non-repudiation)* and that the object has not been altered in any way *(integrity)*. The validity of the user's signature is assured using standardized processes and the information contained in their certified digital certificate.

As part of the process to ensure the signature is valid, checks are made by the digital signature software to ascertain that the user's credential was valid at the time of signing. Since the user's private key is maintained under his or her sole control (never shared), it is very difficult for the user to claim he or she did not execute the signature. Also, while checking to see that the signature is valid, the integrity of the object is checked. If anything has been changed in the record or object since the signature was executed, the result of this process will show that the signature is not valid.

As with an electronic signature, there are levels of assurance of identity associated with the user's digital certificate. The level of assurance provided by the digital certificate has a significant impact on the strength of the non-repudiation and authentication elements of the digital signature. SAFE-BioPharma standards require that the user's digital credentials meet a minimum of NIST Level 3 requirements as described above.

B. SAFE-BIOPHARMA Guidance for Use of Electronic Signatures

The following table provides SAFE-BioPharma recommended guidance for use of electronic and digital signatures across a series of example use cases. Credentials used to execute electronic or digital signatures that are certified compliant with SAFE-BioPharma Standards (including cross-certification with the SAFE-BioPharma Bridge CA) ensure that all credentials have been issued in accordance with SAFE-BioPharma standards and that an executed digital signature also is compliant with all SAFE-BioPharma Standards.

[5] *SAFE-BioPharma digital signature standards are based on these recognized standards.*

Because regulatory requirements for expectations of electronic and digital signatures vary internationally, SAFE Biopharma recommends consulting the country or regional authority for guidance on acceptable use.

ENVIRONMENT	SCENARIO	CURRENTLY ACCEPTABLE SIGNING METHOD FOR COMPANY COLLEAGUES	RECOMMENDED SIGNING METHOD FOR EXTERNAL PARTNERS
Closed System on Company or Organization Network	Regulated R&D Documents	Electronic or Digital Signature	SAFE-Compliant Digital Signature
	Regulated Mfg. Documents	Electronic or Digital Signature	SAFE-Compliant Digital Signature
	Electronic lab notebooks	Electronic or Digital Signature	SAFE-Compliant Digital Signature
	Legally binding documents (contracts) (US)	Electronic or Digital Signature	SAFE-Compliant Digital Signature
	Legally binding documents (contracts)(EU)	Digital Signature	SAFE-Compliant Digital Signature
	Supplier/Third Party compliance attestations	Electronic or Digital Signature	SAFE-Compliant Digital Signature
	Internal business documents	Electronic or Digital Signature	SAFE-Compliant Digital Signature
External System (Hosted)	Regulated R&D Documents	SAFE-Compliant Digital Signature	SAFE-Compliant Digital Signature
	Regulated Mfg Documents	SAFE-Compliant Digital Signature	SAFE-Compliant Digital Signature
	Electronic lab notebooks	SAFE-Compliant Digital Signature	SAFE-Compliant Digital Signature
	Legally binding documents (contracts) (US)	SAFE-Compliant Digital Signature	SAFE-Compliant Digital Signature
	Legally binding documents (contracts)(EU)	SAFE-Compliant Digital Signature	SAFE-Compliant Digital Signature
	Supplier/Third Party compliance attestations	SAFE-Compliant Digital Signature	SAFE-Compliant Digital Signature
	Internal business documents	Electronic or Digital Signature	SAFE-Compliant Digital Signature
External System (Portal for Submission)	Regulatory Forms	SAFE-Compliant Digital Signature	SAFE-Compliant Digital Signature

IV. USE CASE DEFINITIONS

Access

- **Application Gateway:** a compliant application/device that terminates the user's application session and then establishes another connection to the application (e.g., a reverse proxy). Access via an Application Gateway is NOT Remote Access.

- **Application Gateway Access:** access to an application on the enterprise network from a device that is not connected to the enterprise network through any other means.

- **Business to Business (B2B) Network-to-Network connection**: a direct connection, typically via a VPN connection over the Internet that connects a business partner's network to the enterprise network. Access is typically limited to those systems that the business partner's people or system(s) need access to.
- Further restrictions may limit which portions of the business partner's network may have access to the limited set of enterprise systems.

- **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.

- **Diagnostic Access:** access to a system, typically by the vendor, for purposes of hardware or software monitoring or problem diagnosis and/or repair.

- **Direct Diagnostic Access:** diagnostic access that allows direct connection to the system, bypassing the mechanisms in place for remote access, internet application access, or a B2B connection to the enterprise network.

- **External Business Connection (EBC):** a B2B network to network connection, or a connection allowing a single External Business Partner computing device to access the enterprise network.

- **Local Access:** access to the enterprise network by directly connecting to Local Area Network (LAN) segment, within a <company> facility. Such connection could be wired or wireless and affords unrestricted access to the enterprise network.

- **Open (External) System:** 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.

- **Remote Access:** access from a single device on a non-enterprise network to the enterprise network via a public network such as the Internet or the telephone network. Access via a Business-to-Business (B2B) network-to-network connection, even if it is implemented as a VPN connection over the internet is NOT remote access.

- **Restricted Remote Access:** remote access that is controlled and limited by the network to a small subset of IP addresses, applications, or databases available on the enterprise network. Examples include access from the Internet via an Application Gateway to a limited set of applications, remote access to a restricted set of IP addresses and ports, or restricting locally-connected non-<company> computing devices access to a limited set of applications.

- **Unrestricted Access**: means Local Access or Unrestricted Remote Access.

- **Unrestricted Remote Access:** refers to broad (or unlimited) access to the enterprise network such that once connected, the user has few, if any, restrictions on which IP addresses and ports are accessible

Information

- **Personal Information**

    - **Personal Information**: Any written or electronic information that relates to an identified or identifiable person ("individual"). In practice, this means any information that can reasonably be used to identify a living person either directly or indirectly (e.g., by combining different sets of data which together form a complete record), including factual information about such person, such as name, address, telephone number, physical attributes, prescriber information, e-mail address of an individual, as well as information about his/her opinions or beliefs. Under certain local laws and regulations, even if such information is encoded (i.e., converted to a format that makes it impossible to identify an individual without access to the "key" that allows the information to be re-associated with the individual), subject to other de-identification techniques or is publicly available, it may still be treated as personal information.

- **Sensitive Personal Information**: Special category of personal information that warrants additional protection. Although the definition can vary by country, sensitive personal information is often described as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health or sex life, and data relating to offenses and/or criminal convictions. National or State issued ID number, Social Security number, driver's license number, and financial account information including credit card, debit card, and bank account information is treated as sensitive personal information.

- **Personal Health Information**
  - **Personal health information** (PHI) generally refers to demographic **information**, medical history, test and laboratory results, insurance **information** and other data that a healthcare professional collects to identify an individual and determine appropriate care. Protected health information means individually identifiable health information.
- **Regulatory Information**
  - Information which is specifically required by regulation to be controlled and/or signed.

- **Sensitivity of Company Information (classifications)**

NOTE: The specific classification labels provided below are representative only. Companies should feel free to choose their own labels depending upon what best fits the Company environment.

- Public– unrestricted information, to be released both externally and internally, as press releases, financial reports, drug leaflets, public clinical trial results,

- Internal – information for <Company> employees only, limited to internal distribution/circulation. This information must not be communicated outside of the = company without the "Need-to-know".

- Sensitive – confidential information that must have restricted access. This information must not be shared with all internal users. This includes personal and sensitive personal data as defined above.

- Highly Sensitive – confidential information for which disclosure, compromise or loss would result in a major or critical impact to <Company>, in a way that could compromise the overall business strategy.