SBA Procedural Notice

TO:	All SBA Employees	**CONTROL NO.:**	5000-1323
SUBJECT:	Acceptance of Electronic Signatures in the 7(a) and 504 Loan Program	**EFFECTIVE:**	10/21/14

The purpose of this Notice is to inform employees that, effective January 1, 2015; 7(a) and 504 lenders may utilize electronic signatures in accordance with the performance standards outlined in this Notice on SBA Forms and other documents requiring signatures.

The Electronic Signatures in Global and National Commerce (ESIGN)[i] Act, in conjunction with the Government Paperwork Elimination Act (GPEA), encourages agency acceptance of electronic signatures. Pub. L. 106-229, § 1 (June 30, 2000), 114 Stat. 464, codified at 15 U.S.C. §§ 7001-7006; and Pub. L. 105-277 (October 21, 1998). The ESIGN Act also grants agencies the ability to specify performance standards to ensure accuracy, integrity, and accessibility of records that are required to be retained.[1]

The ESIGN Act defines electronic signature as "any electronic sound, symbol, or process attached to or logically associated with a contract or record and executed or adopted by a person with the intent to sign the record."[2] Signatories should follow this definition of electronic signature with the exception that SBA will not accept an electronic signature that is solely voice or audio. Electronic signatures include digital signatures.

SBA's policy is consistent and requires lenders to comply with NIST Special Publication 800-63-2, and OMB Memorandum M-04-04 ("E-Authentication Guidance for Federal Agencies[3] and Guidance Document, Use of Electronic Signatures in Federal Organization Transactions", Version 2.0, January 25, 2013 (Specifically section D: "Requirements for Legally Binding Electronic Signatures)"[4]). For electronic signatures to be legal and binding the requirements for electronic form of signature, intent to sign, association of signature to record, identification and authentication of signer, and integrity of the signed record must comply with OMB Memorandum M-04-04.

This notice specifies key requirements that lenders must comply with, in addition to those noted above, when implementing an electronic signature technology for SBA forms and documents. Electronic signatures meeting the requirements of this Notice will now be treated as equivalent to handwritten signatures. Nothing in this Notice affects existing SBA requirements as to who is required to sign any specific document or which documents the lender is required to retain in the loan file. Based on SBA's experience with electronic signatures, it may make changes to the standards set forth in this document prior to incorporating them into the appropriate SBA Standard Operating Procedures.

[1] ESIGN § 104(a) (3).
[2] ESIGN § 106(5)
[3] http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf
[4] https://www.idmanagement.gov/sites/default/files/documents/Use_of_ESignatures_in_Federal_Agency_Transactions_v20_20130125.pdf.

A. Electronic Form of Signature

For the SBA approved forms of signature, the vendor must comply with "Use of Electronic Signatures in Federal Organization Transactions, Version 2.0, and January 25, 2013"; section D: "Requirements for Legally Binding Electronic Signatures."

The SBA will accept the following forms of signature.

- Symbols such as
    - A typed name (e.g., typed at the end of an email message by the sender, or typed into a signature block on a website form by a party);
    - A digitized image of a handwritten signature that is attached to an electronic record;
    - A shared secret (e.g., a secret code, password, or PIN) used by a person to sign the electronic record;
    - A unique biometrics based identifier, such as a fingerprint, voice print, or a retinal scan; or
    - A digital signature.
- Processes such as
    - Using a private key and applicable software to apply a "digital signature;" or
    - Scanning and applying a fingerprint.

B. Intent to Sign

The signing ceremony must (1) clearly identify the reason for signing (e.g., agreement to the contract terms; acknowledgement of receipt, etc.), and (2) clearly specify the conduct that will indicate an intent to sign for the purpose of agreeing to that reason.

Lenders are reminded that electronic signatures are only valid under the ESIGN Act if they are "executed or adopted by a person with the intent to sign the record." Therefore, lenders must establish that the signer intended to sign the record.

Establishing intent includes:

- Identifying the purpose for the borrower or other party signing the electronic record;
- Being reasonably certain that the borrower or other party knows which electronic record is being signed; and
- Providing notice to the borrower or other party that his or her electronic signature will be applied to, or associated with, the electronic record.

Lenders may establish the signatory's intent to use an electronic signature using any of the following or other similar methods:

- An online dialog box or alert advising the borrower or other party that continuing the process will result in an electronic signature;
- An online dialog box or alert indicating that an electronic signature has just been created and giving the borrower or other party an opportunity to confirm or cancel the signature; or
- A click-through agreement advising the borrower or other party that continuing the process will result in an electronic signature.

C. Association of Signature to Documents

The signing process must: 1. Ensure the document is presented to the signer before an electronic signature is obtained and 2. Be attached to, or logically associated with, the document that has been electronically signed for the life of the document.

In addition, SBA will require electronic signatures to have a record/certificate that tracks:

- Certificate of Completion Status;
- Identity of the signer or a link to the source of identifying information, such as a validated UserID, a digital certificate, a biometric database, etc.;
- Date and time of the signature;
- Method used to sign the record; and
- An indication of the reason for signing and/or events associated with signature.

D. Identification and Authentication of Signer

1. Initial Establishment/Verification

The first time a signer requests the credentials to sign a document SBA requires proofing to be performed consistent with the standards in the current NIST 800-63 for Level 3 assurance. This notice tales the level 3 standard is noted below which was taken from page 34 of http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf

Level 3	In Person	Remote
Basis for issuing credentials	Possession of verified current primary Government Picture ID that contains Applicant's picture and either address of record or nationality of record (e.g., driver's license or passport)	Possession of a valid Government ID (e.g., a driver's license or Passport) number and a financial or utility account number (e.g., checking account, savings account, utility account, loan or credit card) confirmed via records of both numbers. Note that confirmation of the financial or utility account may require supplemental information from the Applicant.
Registering Agent (RA)/Credential Service Provider (CSP) actions	***RA*** inspects photo-ID and verifies via the issuing government agency or through credit bureaus or similar databases. Confirms that: name, DoB, address and other personal information in record are consistent with the application. Compares picture to Applicant and records ID number. If ID is valid and photo matches Applicant, then: a) If personal information in records includes a telephone number, the ***CSP*** issues credentials in a manner that confirms the ability of the Applicant to receive telephone communications at a number associated with the Applicant in records, while recording the Applicant's voice or using alternative means that establish an equivalent level of non-repudiation; or b) If ID confirms address of record, ***RA*** authorizes or ***CSP*** issues credentials. Notice is sent to address of record, or; c) If ID does not confirm address of record, ***CSP*** issues credentials in a manner that confirms the claimed address.	***RA*** verifies information provided by Applicant including ID number AND account number through record checks either with the applicable agency or institution or through credit bureaus or similar databases, and confirms that: name, DoB, address and other personal information in records are consistent with the application and sufficient to identify a unique individual. At a minimum, the records check for both the ID number AND the account number should confirm the name and address of the Applicant. For utility account numbers, confirmation shall be performed by verifying knowledge of recent account activity. (This technique may also be applied to some financial accounts.) • Address confirmation: *a)* ***CSP*** issues credentials in a manner that confirms the ability of the applicant to receive mail at a physical address associated with the Applicant in records; or *b)* If personal information in records includes both an electronic address and a physical address that are linked together with the Applicant's name, and are

Level 3	In Person	Remote
		consistent with the information provided by the applicant, then the ***CSP*** may issue credentials in a manner that confirms ability of the Applicant to receive messages (SMS, voice or e-mail) sent to the electronic address. Any secret sent over an unprotected session shall be reset upon first use and shall be valid for a maximum lifetime of seven days.

NIST Special Publication 800-63-2, and OMB Memorandum M-04-04, E-Authentication Guidance for Federal Agencies detail guidance for CSPs and RAs. Page 27
NIST Special Publication 800-63-2of states the requirements to becoming a Registering Agent as noted below.

> *"In the registration process, an Applicant undergoes identity proofing by a trusted RA. If the RA is able to verify the Applicant's identity, the CSP registers or gives the Applicant a token and issues a credential as needed to bind that token to the identity or some related attribute. The Applicant is now a Subscriber of the CSP and may use the token as a Claimant in an authentication protocol. This section describes the requirements for registration and for token and credential issuance.*
>
> *The RA can be a part of the CSP, or the RA can be a separate and independent entity; however, a trusted relationship always exists between the RA and CSP. Where the RA and CSP are separate entities, the trust relationship is often contractual, but the trust relationship may also be based on laws and regulations, such as when a notary performs the RA function. The RA or CSP maintain records of the registration. The RA and CSP can provide services on behalf of an organization or may provide services to the public. The processes and mechanisms available to the RA for identity proofing may differ as a result. Where the RA operates on behalf of an organization, the identity proofing process may be able to leverage a pre-existing relationship (e.g., the Applicant is an employee or student). Where the RA provides services to the public, the identity proofing process is generally limited to confirming publicly available information and previously issued credentials."*

2. Separate Action for Each Signature/Initial

Lenders must require a separate action by the signer, evidencing intent to sign, in each location where a signature or initials are to be applied.

3. Attribution

Attribution is the process of associating the identity of an individual with his or her signature. Attribution will be performed at a level 3 as defined in the identification section above. Lenders must maintain evidence sufficient to establish that the electronic signature may be attributed to the individual purported to have signed.

The following methods are acceptable means of establishing attribution:

- Selection by or assignment to the individual of a PIN, password, or other shared secret, that the individual uses as part of the signature process;
- Delivery of a credential to the individual by a trusted third party, used either to sign electronically or to prevent undetected alteration after the electronic signature using another method;
- "Out of band/wallet" information;
- Measurement of some unique biometric attribute of the individual and creation of a computer file that represents the measurement, together with procedures;

4. Authentication

Authentication refers to the process used to confirm an individual's identity as a party in a transaction. SBA is requiring the implementation of the NIST Special Publication 800-63-2 Level 3 assurance level. Level 3 asserts the validity of the identity of the user with a high level of confidence. Level 3 provides multifactor remote network authentication.

For the first factor, the following are approved authentication mechanisms:

a. One time passwords sent to a user's email, SMS, or voice;

b. In-person authentication;

c. Electronic Notary;

d. Hard token;

e. Public key;

f. Biometrics.

The second factor will be using Knowledge Based Authentication. At this level, identity proofing procedures require verification of identifying materials and information.

SBA approved independent sources include, but are not limited to:

- National commercial credit bureaus;

- Commercially available data sources or services;
- State motor vehicle agencies; or
- Government databases.

KBA requirements are listed below.

i. SBA requires that the system use static (date of birth) information at a minimum.

ii. The lender must verify an individual's name and date of birth, and either the social security number or driver's license number.

iii. SBA prefers that the system utilize static and dynamic (verification of account balances).

iv. The system must use multiple versions of the same question to protect against scripts and hacking.

v. The system must randomly order the questions to protect against scripts and hacking.

vi. Failed attempts must be documented and reported to the lender.

vii. The system should lockout the user after 3 failed attempts.

viii. The system should delete accounts after 90 days of inactivity.

5. Credential Loss Management

If a Lender uses a PIN, password or other shared secret or delivery of a credential as the method of establishing attribution, the Lender must have a system in place to ensure the security of all issued codes or credentials. One or more of the following acceptable loss management controls must be used:

- Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password;
- Ensuring that identification code and password issuances are periodically checked, recalled, or revised;
- Following loss management procedures to electronically de-authorize lost, stolen, missing, or otherwise compromised identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls;

- Use of transaction safeguards to prevent unauthorized use of passwords or identification codes; or

- Detection and reporting of any attempts at unauthorized use of the password of identification code to the system security unit.

E. Integrity of Signed Record

Lenders must ensure that documents signed electronically cannot be altered without authorization and documented in an "audit trail." The documents must be tamper sealed to ensure their validity. Industry standard encryption must be used to protect the individual's signature and the integrity of the documents to which they are affixed.

If authorized changes to the document are made, the electronic process must be designed to provide an audit trail showing all alterations, the date and time they were made, and identify who made them.

The lender's system must be designed so that the signed document is designated as the "Authoritative Copy."

F. Electronic Signature Eligible Documents

Unless otherwise prohibited by law, 7(a) and 504 lenders may utilize electronic signatures on the documents referenced below (collectively referred to as "Eligible Documents"), provided that the signatories comply with the standards outlined in this Notice. Electronic signatures cannot be used on any document identified below if the recording office requires wet signatures.

- Application Documents: Electronic signatures may be accepted on all documents requiring signatures.

- Loan Closing Documents: Electronic signatures may be accepted on all documents requiring signatures.

- Secondary Market Sale Documents: With the exception of the Form of Detached Assignment for U.S. Small Business Administration Loan Pool or Guaranteed Interest Certificate (SBA Form 1088), electronic signatures may be accepted on all documents requiring signatures.

- Servicing Action – Pre-Disbursement Documents: Electronic signatures may be accepted on all documents requiring signatures, including but not limited to change requests and supporting documentation.

- Servicing Action – Post-Disbursement Documents: Electronic signatures may be accepted on all documents requiring signatures.

- Liquidation Documents: Electronic signatures may be accepted on all documents requiring signatures.

- Litigation Documents: Electronic signatures may be accepted on all documents requiring signatures, unless otherwise specified by a court order.

- Post Default Action Documents: Electronic signatures may be accepted on all documents requiring signatures.

- Lender On-Boarding Documents: Electronic signatures may be accepted on all documents requiring signatures, including but not limited to lender participation applications and agreements.

- Delegated Authority Documentation: Electronic Signatures may be accepted on all documents requiring signatures, including but not limited to supplemental guaranty agreements.

- Targeted and Full Lender Review Documentation: Electronic Signatures may be accepted on all documents requiring signatures.

At this time, the use of electronic signatures is voluntary; however lenders who choose to use electronic signatures must fully comply with the standards outlined in this Notice and may be held liable for failure to adhere to standards, This notice is not valid for transactions that require filing of security or other documents with a jurisdiction that does not have electronic filing capabilities. The E-Sign Act provides that section 101 of the Act (15 U.S.C. § 7001) "shall not apply to a contract or other record to the extent it is governed by … the Uniform Commercial Code, as in effect in any State, other than sections 1–107 and 1–206 and Articles 2 and 2A." 15 U.S.C. § 7003. Therefore, lenders need to comply with Uniform Commercial Code (UCC) Article 9-105 which outlines the requirements for electronic chattel paper and article 3 of the UCC which outlines the electronic equivalent of a paper promissory note, known as a "Transferrable Record".

The concept of "Authoritative Copy" comes from UCC Art. 9-105. This revision to Article 9 was intended to address the problem of electronic chattel paper. Anticipating that there may someday be a technological means for identifying or controlling an electronic "original," the drafters of 9-105 came up with the parameters, including these requirements:

> 1) a single authoritative copy of the transferable record exists which is unique, identifiable, and, except as otherwise provided in paragraphs 4), 5), and 6) below, unalterable; 2) the authoritative copy identifies the person asserting control as- a)the person to which the transferable record was issued; or b)if the authoritative copy indicates that the transferable record has been transferred, the person to which the transferable record was most recently transferred; 3) the authoritative copy is communicated to and maintained by the person asserting control or its designated custodian; 4) copies or revisions that add or change an identified assignee of the authoritative copy can be made only with the consent of the person asserting control; 5) each copy of the authoritative copy and any copy of a copy is readily identifiable as a copy that is not the authoritative copy; and 6) any revision of the authoritative copy is readily identifiable as authorized or unauthorized.

ESIGN (Title II) and UETA (Section 16) create a parallel structure for the electronic equivalent of a paper promissory note, known as a "transferable record." Since the UCC Article 3 provisions for promissory notes were not designed for use with electronic records, both laws set forth special rules for the management and retention of Transferable Records, stating that an electronic record can be treated as the equivalent of a negotiable promissory note in certain respects if:

- The electronic record contains only the same terms and conditions that are permitted in a promissory note governed by Article 3 of the UCC ;
- The electronic record is signed;
- The issuer of the record has agreed that it should be treated as a transferable record under the UETA; and
- The method used to record, register, or evidence a transfer of interests in the transferable record reliably establishes the identity of the person entitled to "control" (meaning control the transfer of) the electronic record.

The "safe harbor" for establishing control of the Transferable Record is taken directly from UCC 9-105 above.

G. Vendor/Technology Selection Requirements

A lender must ensure that any electronic signature technology vendor it uses:

- Complies with Section 101 of the ESIGN Act (http://www.gpo.gov/fdsys/pkg/PLAW-106publ229/pdf/PLAW-106publ229.pdf);
- Has the experience, capabilities, and expected longevity to meet all SBA electronic signature requirements;
- Includes vendor agreements that contain express provisions that vendors will comply with all applicable SBA requirements pertaining to this procedural notice;
- Includes vendor agreements language that would ensure that vendor representatives will be available to provide testimony to support the United States government in litigation regarding electronic signature data that will be introduced in court;
- Meets disaster recovery and archiving requirements; and
- Has adequate quality control processes.

H. Lender Liability for Failure to Adhere to Prescribed Standards

The Office of Credit Risk Management (OCRM) will review compliance with the ESIGN Act as well as standards outlined in this Notice as components of lender oversight.

As with all loan program requirements, lenders may be held accountable for not complying with the electronic signature standards and requirements set forth in this notice.

.***I. Quality Control***

Lenders must ensure their electronic signature policies and procedures meet all requirements including their own oversight of the electronic signature process.

J. Record Retention

SBA's record retention requirements are the same for both wet ink and electronic signatures. The audit trail as well as any computer systems (including hardware and software), controls, and documentation must be readily available for, and subject to, SBA inspection for the same periods as records signed in wet ink. Lenders also must adhere to the applicable record retention requirements established by their respective regulators. SBA-supervised lenders, i.e., Small Business Lending Companies, must follow the record retention requirements set out in 13 CFR 120.461 and Section 3.D of SOP 50 57 and 50 10 5 (G).

A lender's system must be able to reproduce electronic records as accurately as if they were paper when printed or viewed. These records must be made available to SBA on request.

The table below highlights SBA's retention requirements for several documents.

Loan Status	Retention Requirement
Inquiries, partial applications, and applications withdrawn, canceled or denied by the SBA.	Must be retained for 2 years after notification of incomplete application, withdrawal, cancelation or decline. After 2 years, the files may be destroyed using practices aligned with SOP 90 47 03.
General correspondence	Must be kept for one year.
Case-specific correspondence should be filed in the case file.	Must be retained for 10 years.
Paid off loan files (including the original application file, servicing file and closing file).	Must be retained for 9 years after the loan is paid in full.
Files from liquidated loans (including the original application file, closing and servicing files).	Must be kept for 10 years after the loan was charged off.

K. Notification and Questions

SBA field offices must notify Lenders about this Notice. Questions concerning this Notice should be directed to the Lender Relations Specialist in the local SBA field office. The local SBA field office may be found at www.sba.gov/about-offices-list/2.

Ann Marie Mehlum
Associate Administrator
Office of Capital Access