

Internal Revenue Service
Income Verification Express Services (IVES)
Electronic Signature Requirements

This document includes the requirements for the suggested framework which all IVES Participants must adhere to in order to participate using electronic signatures for IRS Forms 4506-T or 4506T-EZ.

Background

Due to the fact that a growing number of transactions now occur online, a legal debate has arisen in recent years over the validity of electronic contracts and the enforceability of electronic signatures. The Electronic Signature in National and Global Commerce Act, commonly referred to as E-Sign, Public Law 106-229- June 30, 2000, resolves this debate by authorizing the creation of electronic contracts, as well as the use of electronic records relating to such agreements. In the process, it provides uniform national standards for the use of electronic signatures, which have grown in use and importance over the past few years. The most promising electronic-signature technology comes in the form of “digital signatures,” which use public key cryptography. This involves two related keys: a unique “private key” for the user, which encrypts the information, and a corresponding “public key” which unlocks the information and verifies the user’s identity. Other currently popular types of electronic signatures include clickwrap signatures (e.g., an “I accept” button on a website), passwords, and biometric signatures (e.g., voice prints and fingerprints).

An electronic signature is defined as an electronic sound, symbol, or process attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record. The Electronic Signature Act as a general matter states the following:

1. Applies to all transactions if the consumer affirmatively consents to the use of electronic procedures unless the transaction is specifically excluded under the terms of the act itself.
2. Permits the use of an electronic signature in any transaction if both parties consent to the usage.

3. Dictates that any document in electronic form or executed with an electronic signature is fully enforceable.
4. Sets forth electronic record retention requirements.
5. Provides that electronic records are fully admissible in any legal proceeding.

Definition of Electronic Signature

A technologically neutral term indicating various methods of signing an electronic message that (a) identify and authenticate a particular person as source of the electronic message, and (b) indicate such person's approval of the information contained in the electronic message (definition from GPEA, Pub.L. 105-277). Examples of electronic signature technologies include PINs, user identifications and passwords, digital signatures, digitized signatures, and hardware and biometric tokens.

E-Sign Law Requirements

There are currently five requirements of the E-Sign law which we propose to implement:

1. The signature must be under the sole control of the individual. Password based signatures should be used in conjunction with PKI, signature stamps, electronic seals as well as simple click-wrap. For IVES we are requesting use of an electronic signature.
2. The signature must be verifiable. Electronic signature technology will verify in real time using complex algorithms or through forensic analysis of the signature dynamics or measurements.
3. The signature must be unique to the individual. Each signature gathered must be unique to an individual regardless of whether it is a physical measurement like a fingerprint or virtual measurement like the click of a mouse.
4. The signature must establish the individual's intent to be bound to the transaction. Signatory must be fully aware of the purpose for which the signature is being provided, regardless of underlying technology.
5. The signature must be applied in a tamper-evident manner. Industry standard encryption must be used to protect the users' signatures and the integrity of the documents to which they are affixed.

IVES Participants Must Follow the Suggested Framework for IVES Electronic Signature Requirements

1. Authentication: IVES participants must validate that the signer is who they say they are and that the document has made it into the correct hands. The most common form of authentication is “Two Factor,” referring to something the signer has (e.g. emailed successfully into their in-box) and something the signer knows (e.g. a pass code). Other common authentication options include: Knowledge based Authentication (KBA) where the signer is presented with multiple choice questions, and Single Sign-On (SSO), where “keys” or credentials are passed along from another web-site.
2. Consent: IVES participant must get consent from signer to receive and sign documents electronically prior to moving forward with the viewing and signing ceremony. This is typically done with a one page consent form presented to the signer after authentication and prior to gathering signatures. Signer must either accept or reject the consent.
3. Electronic Signature: Must be an electronic symbol logically associated with a record and executed or adopted by a person with the intent to sign the record. For the purpose of IVES, we will require an electronic signature in order to validate the name(s) against the name(s) listed on either the Form 4506-T or Form 4506T-EZ.
4. Tamper Proof Seal: After the electronic signature is collected, the document must be made tamper proof to ensure its validity.
5. Non-Repudiation: An audit log of the entire electronic signing ceremony must accompany the document for future use as needed for non-repudiation. Data in the log should include: date and time of creation, IP address of the signer, document lifecycle notifications, result of authentication, result of consent, and result of each electronic signature in the document.
6. IVES Participant Retention of Documentation: All audit log information as well as the associated Form 4506-T or Form 4506T-EZ must be retained by the IVES participant for a period of 2 years.
7. Quality Review: All IVES participants using electronic signatures must use an independent party to audit and ensure all electronic signature requests meet all requirements stated throughout this document. This audit along with its findings will be provided annually to the IVES Headquarters (HQ) Analysts. IVES participants with findings showing a failure to meet all requirements will not be allowed to continue using electronic signatures.

- (a) The audit findings should compare the audit log information against the Form 4506-T or Form 4506T-EZ to validate the name(s) and date(s).
- (b) The monthly sample size for review will be 125 from the electronically signed Form 4506-T or Form 4506T-EZ against the audit log. All IVES participants will develop their own skip interval each month by dividing their total number of requests by the sample size of 125. Each month the participant will select the first electronically signed request and apply the skip interval from there. The participant can stop the selection process once 125 requests have been selected. All participants will select a sample size of 125 requests, regardless of fluctuations in their monthly volume. The only exception is for months where fewer than 125 requests were processed. Participants should select and review all requests in the month for months where fewer than 124 requests were processed.
- (c) Although we are only asking for the audit findings to be submitted annually to the IVES HQ Analysts, these findings should include monthly results as well as the total annual computations. The annual audit findings should be submitted to the IVES HQ Analysts by January 31st of the following year. The e-mail address for the Analysts is as follows: Robert.G.Shearer@irs.gov; Mary.R.Ray@irs.gov; and Roxanne.Jones@irs.gov.
- (d) Upon request the audit logs and the Form 4506-T and Form 4506T-EZ will be made available throughout the year to the IVES HQ Analysts. They may be sent by USPS or private delivery courier to the following address:

IRS

333 W. Pershing Rd. M/S P-5 6566

Attn: Bob Shearer

Kansas City, Mo 64108