10.10.1 IRS Electronic Signature (e-Signature) Program

Manual Transmittal

December 03, 2019

Purpose

(1) This transmits new IRM 10.10.1, *Identity Assurance, IRS Electronic Signature (e-Signature) Program*.

Material Changes

(1) This new IRM provides guidance on the implementation and usage of the IRS e-Signature Program. The narrative provides form owners procedures to implement e-Signature to their respective forms, provides guidance for ensuring compliance with e-Signature policies, and outlines an appeals process.

Effect on Other Documents

None

Audience

IRS personnel involved with implementation and/or usage of the e-signature solution for external, taxpayer related forms and documents and web applications. This IRM does not address e-signature requirements for internal use IRS documents.

Effective Date

(12-03-2019)

Nanette M. Downing
Director, Identity Assurance Office

10.10.1.1 (12-03-2019)

Program Scope and Objectives

(1) This IRM covers the Service wide e-Signature policies and procedures, including:

- Service-wide Roles and Responsibilities
- Definition of e-signature terms
- IRS e-signature principles
- Determining the appropriate risk
- Adopting an e-signature signing process
- Oversight and risk assessment of an e-signature solution implementation

(2) This IRM defines the uniform guidance, policies, and procedures to be followed by internal and external stakeholders related to the implementation of an e-signature process.

(3) This IRM establishes the e-signature policy and minimum baseline requirements for all forms and documents requiring taxpayer signatures.

(4) This policy assigns roles and responsibilities for all key stakeholders to implement e-signature solutions, identify and mitigate risks, and ensure compliance with e-signature requirements.

(5) This IRM provides guidance for:

a. Adopting an e-signature signing process;

b. Ensuring all e-signatures have the appropriate risk and authentication requirements in place to ensure compliance with relevant Federal government policies;

c. Implementing and maintaining an e-signature program to provide business and form owners a resource for information regarding an e-signature solution;

d. Performing oversight functions and compliance functions within the e-signature program.

(6) The guidance in this IRM applies to all offices and divisions within the IRS.

Note:

The provisions of this IRM apply to customer-facing forms, documents, statements and tools but not employee-facing forms, documents, statements and tools.

10.10.1.1.1 (12-03-2019)

Background

(1) Section 2003(a) of the Internal Revenue Service Restructuring and Reform Act of 1998 (RRA 98) amended IRC § 6061 to direct the Secretary of the Treasury to "develop procedures for acceptance of signatures in electronic form." It further states that in the interim, "the Secretary may waive the requirement of a signature on an electronically filed tax return or provide for alternative methods of signing."

10.10.1.1.1.1 (12-03-2019)

Introduction to IRS e-Signature

(1) The IRS e-signature principles and federally mandated authentication controls describe how the IRS protects an individual's identity and assures that only authorized signers are completing the transaction.

(2) IRS e-signature requirements form the basis for implementing technology and security controls.

(3) Adherence to IRS e-signature principles and requirements is mandatory to preserve the integrity of the signed IRS record.

(4) Through this IRM, the IRS implements a framework for applying e-signature consistently across the IRS. The framework will guide how the IRS executes electronic transactions and will be an essential component of an IRS online authorization capability. The IRS e-signature Framework is based on the document *Use of Electronic Signatures in Federal Organization Transactions, Version 2.0, [UESFOT]*.

(5) Per UESFOT, the risks related to enforceability of an electronic signature analysis should include:

a. The likelihood of a successful challenge to the validity of the electronic signature, and

b. The monetary loss, or other adverse impact, that will result from such a successful challenge to the enforceability of the electronic

signature.

(6) The *National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 (Rev. 4), Appendix E*, outlines security controls designed to implement fundamental safeguards and countermeasures necessary to protect information during processing, while in storage, and during transmission based upon level of impact ranging from low impact, moderate impact, and high impact to enhanced assurance.

10.10.1.1.2 (12-03-2019)

Program Purpose

(1) Implementing general standards and guidelines for electronic signatures will encourage the use of electronic signatures in the tax industry. This IRM provides general guidelines and standards that will apply to electronic signatures on public, taxpayer-related forms and documents, and web applications requiring taxpayer signatures.

(2) The general guidelines and standards in this IRM facilitate the broader use of electronic signatures on IRS documents and increase administrative efficiency.

(3) The IRS may permit the use of an electronic signing process on a document when the IRS determines that the electronic signing process is appropriate for that document.

(4) An electronic signature executed under an electronic signing process, permitted for that specific document, may be used to sign the document. This will satisfy the requirements of Internal Revenue Code (IRC) § 6061(b), and Code of Federal Regulations (CFR) on Procedure and Administration 26 CFR § 301.6061-1.

(5) Any IRS document that is signed using the permitted electronic signing process for that document will be treated for all purposes (both civil and criminal, including penalties of perjury) in the same manner as though signed with a handwritten signature.

(6) Other than handwritten signatures, signatures shown in IRM Exhibit 10.10.1-1 are the only acceptable signatures. Form instructions must be revised to effect this provision.

10.10.1.1.3 (12-03-2019)

Authority

(1) IRS' e-signature policy implements relevant authentication laws, mandates, and compliance policies.

(2) The use of electronic signatures in transactions involving federal organizations will be primarily governed by one of the following laws ("e-Transaction Laws"):

a. ***Government Paperwork Elimination Act****(GPEA)* - a federal law enacted in 1998 that is applicable to governmental transactions and other transactions involving certain federal organizations;

b. ***Electronic Signatures in Global and National Commerce Act*** *(E-SIGN*) - a federal law enacted in 2000 that largely preempts inconsistent state law (although in certain cases state law may still control) and that is applicable to commercial, consumer, or business transactions involving federal organizations; and

c. ***Uniform Electronic Transactions Act*** *(UETA)* - a uniform state law that was finalized by the National Conference of Commissioners on Uniform State Laws (NCCUSL) in 1999 and subsequently adopted by 47 states, and which may be applicable to commercial, consumer, or governmental affairs transactions involving federal organizations in certain cases.

d. The NIST 800-63-3 includes guidance to follow subsequent updates.

Note:

Determining which e-Transaction Law will apply to any transaction will depend on the nature of the transaction. Questions regarding whether an electronic transaction is covered by GPEA, E-SIGN, and/or UETA can be directed to Identity Assurance (IA) and Chief Counsel (Procedure and Administration). Nonetheless, while there are some differences in the electronic signature requirements of each of these e-Transaction Laws, they are all generally consistent. The guidance in this IRM is designed to address electronic signature requirements in a manner that satisfies the requirements of all the e-Transaction Laws.

(3) Additional relevant Federal Government guidelines include:

a. The *NIST Special Publication (SP) 800-53 (Rev. 4), Appendix E*, outlines Security controls designed to fundamental safeguards and countermeasures necessary to protect information during processing, while in storage, and during transmission. This is

based upon level of impact ranging from low impact, moderate impact, and high impact to enhanced assurance.

b. *NIST Digital Identity Guidelines* (SP 800-63) apply to all federal agencies implementing digital identity services. NIST 800-63 guidances outlines technical ID Proofing and Authentication requirements that federal agencies are mandated to comply with within a year of the publication date.

c. On June 22, 2017, NIST published Revision 3 (NIST SP 800-63-3), which supersedes its previous publication, Revision 2 (NIST SP 800-63-2). The new guidelines separate the previous version's Level of Assurance (LOA) into Identity Assurance Levels (IAL), Authentication Assurance Levels (AAL), and Federation Assurance Levels (FAL).

d. Office of Management and Budget (OMB) Memorandum (M) 19-17 or successor documents.

e. *Use of Electronic Signatures in Federal Organizations Transactions*, Version 2.0 issued January 25, 2013.

f. Public Law No: 115-336, *21st Century Integrated Digital Experience Act*, enacted on December 20, 2018, that requires executive agencies to submit a "plan to accelerate the use of electronic signature standards established under the *Electronic Signatures in Global and National Commerce Act* (15 U.S.C. 7001 et seq)."

10.10.1.1.4 (12-03-2019)

Policy and Program Owners

(1) Identity Assurance (IA), under Privacy, Governmental Liaison and Disclosure (PGLD), is the program office responsible for oversight, policies and procedures for e-signature use by taxpayers in IRS forms, documents, and web applications.

(2) The Director of Identity Assurance reports to the Chief Privacy Officer and is responsible for IA program oversight.

10.10.1.1.5 (12-03-2019)

Terms

(1) Understanding the key term definitions in the following table is essential to support the e-Signature program:

Term	Definition
Alternative Signature	A signature other than original, handwritten signature affixed on the relevant document, including: • Electronic signatures • Personal Identification Numbers • Passwords • Signature stamps • Faxed copies of signatures • Photocopies of signatures • Signature documents such as Form 8879, *IRS e-Signature Authorization*
Authentication	The process of establishing or confirming that someone is the previously identified person they claim to be.
Digitized Signature	A digitized image of a handwritten signature.
Electronic Record	A record created, generated, sent, communicated, or stored by electronic means.
Electronic Signature Pad	An electronic device with a touch sensitive screen that allows users to acquire and register a signature, or any other physical signature capture device that captures and converts a signature into an electronic format.

Term	Definition
Electronic signing process	The overall set of actions, steps, and elements used to create a valid and enforceable electronic signature. It includes both the • application to an electronic record of a form of signature (i.e., the sound, symbol, or process) to be used as the electronic signature, and • one or more processes or security procedures to address the other signature requirements identified in IRM 10.10.1.6, *Identifying and Authenticating the Signer*.
Identifier	A unique name of an individual person (an identity) and any associated attributes; the set of properties of a person that allows the person to be distinguished from other persons.
Identify	The process of verifying and associating attributes with a person designated by an identifier.
IRS Document	Any return, statement, or other document made under any provision of the Internal Revenue Code, published guidance, publications, forms, instructions, online applications, or on the IRS.gov website.

Term	Definition
Level of Assurance	Secure Access e-Authentication adheres to the NIST 800-63-2, *e-Authentication Guidance*. It has several levels of online security and protection, following the OMB M-04-04, to address the risk of each online transaction with implemented levels of assurance on a scale from 1-4. The scale determines the type of identity proofing and authentication required: a. **Level 1:** Little or no confidence in asserted identity's validity; identity proofing not required. **Note:** Identity proofing is not required, and no taxpayer information is shared. b. **Level 2:** Provides some confidence in the asserted identity's validity; requires single-factor identity proofing and/or authentication. c. **Level 3:** Provides high confidence in the asserted identity's validity; requires multi-factor identity proofing and/or authentication requesting "Something you know" input and "Something you have" input. d. **Level 4:** Provides very high confidence in the asserted identity's validity; requires in-person identity proofing or multi-factor authentication requesting "Something you know" input and "Something you have" input. **Note:** With the NIST SP 800-63-3 issuance, the OMB M-19-17 guidelines will become obsolete at some date in the future. This IRM will be updated to reflect the IRS implementation of the NIST SP 800-63-3 assurance levels when effective.

Term	Definition
Linkable Information	Information about or related to an individual for which there is a possibility of logical association with other information about the individual. Refer to IRM 11.3.1, Introduction to Disclosure.
Password	A secret word or string of characters that is used for authentication, to prove identity, or gain access to a resource.
PIN	An acronym for personal identification number and means a numeric password used to help authenticate a person.
PII	Personally identifiable information means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual [OMB A-130].
Stylus Device	A device used on a display screen to input commands or handwritten text.

10.10.1.1.6 (12-03-2019)

Acronyms

(1) The following table contains definitions for the acronyms used in this IRM:

Acronym	Definition
AAL	**Authentication Assurance Levels**
CFR	Code of Federal Regulations
DIRA	Digital Identity Risk Assessment
E-SIGN	Electronic Signatures in Global and National Commerce Act
FIPS	Federal Information Processing Standards
GPEA	Government Paperwork Elimination Act
IA	Identity Assurance

Acronym	Definition
AAL	**Authentication Assurance Levels**
IAL	Identity Assurance Levels
IRC	Internal Revenue Code
LOA	Level of Assurance
NCCUSL	National Conference of Commissioners on Uniform State Laws
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PGLD	Privacy, Governmental Liaison and Disclosure
PIN	Personal identification number
UESFOT	Use of Electronic Signatures in Federal Organization Transactions
UETA	Uniform Electronic Transactions Act
XML	Extensible Markup Language

10.10.1.1.7 (12-03-2019)

Related Resources

(1) IRC § 6061(b)

(2) 26 CFR § 301.6061-1

(3) IRM 10.5.1, *Privacy Policy*

10.10.1.2 (12-03-2019)

Identity Assurance

(1) IA's role is to strengthen the IRS authentication posture by enhancing visibility and coordination for:

- identity proofing;
- authentication;
- authorization; and

- access strategies, processes and capabilities.

(2) One component of the IA mission is to establish and maintain a Servicewide strategy that provides a framework for assessing risk and developing proposed mitigations that strive for a consistent approach for accepting alternative signatures.

(3) IA provides e-signature policy guidance and subject matter expertise on both procedural issues and involved legal issues that have already been addressed by the Office of Associate Chief Counsel, Procedure and Administration (P&A).

(4) IA is responsible for the e-signature policy. To meet this responsibility, IA personnel must be kept informed of the problems and questions that the IRS functions encounter regarding e-signature.

10.10.1.3 (12-03-2019)

Electronic Signatures

(1) An electronic signature may be used to sign an IRS document and will satisfy the requirements of IRC § 6061(b) and CFR § 301.6061-1 if the signature is made using the permitted electronic signing process for that specific IRS document.

(2) Any IRS document that is signed using the permitted electronic signing process will be treated for all purposes (both civil and criminal, including penalties for perjury) in the same manner as though signed with a handwritten signature.

10.10.1.3.1 (12-03-2019)

Requirements for Legally Binding Electronic Signatures

(1) Each permitted electronic signing process must satisfy each of the following five requirements:

a. The signer(s) must use an acceptable form of electronic signature(s) described in IRM 10.10.1.3.2, *Acceptable Forms of Electronic Signatures*;

b. The electronic signature(s) must be executed or adopted by a person(s) in a manner that meets IRM 10.10.1.4, *Intent to Sign the Electronic Record*, that demonstrates the intent of the person(s) to sign the electronic record;

c. The electronic signature(s) must be attached to or associated with the electronic record being signed in accordance with IRM 10.10.1.5, *Attachment or Association of the Electronic Signature with the Electronic Record*;

d. There is a means to identify and authenticate a person(s) as the signer(s) in accordance with IRM 10.10.1.6, *Identifying and Authenticating the Signer*; and the signer must be authorized to execute the document.

e. There is a means to preserve the integrity of the signed electronic record in accordance with IRM 10.10.1.7, *Preserving the Integrity of the Signed Electronic Record.*

10.10.1.3.2 (12-03-2019)

Acceptable Forms of Electronic Signatures

(1) Any electronic sound, symbol, or process can be used as the form of electronic signature provided the form of electronic signature is permitted for use on the specific IRS document by IRS guidance.

(2) If permitted by IRS guidance on the specific IRS document, the following forms of electronic signature are currently permissible for use:

a. A typed name that is typed within or at the end of an electronic record, such as typed into a signature block;

b. A scanned or digitized image of a handwritten signature that is attached to an electronic record;

c. A shared secret, such as a code, password, or PIN;

d. A unique biometric-based identifier, such as a fingerprint, voice print, or a retinal scan;

e. A handwritten signature input onto an electronic signature pad;

f. A handwritten signature, mark, or command input on a display screen by means of a stylus device; or

g. Other electronic sounds, symbols, or processes identified in IRS guidance.

Note:

See IRM Exhibit 10.10.1-1, *Current Approved Methods,* for a complete listing of approved signature methods and their related forms.

10.10.1.4 (12-03-2019)

Intent to Sign the Electronic Record

(1) An electronic signature must be executed or adopted by the signer with the intent to sign the electronic record.

(2) Intent to sign can be inferred from a signer's approval of the reason for signing the electronic record as stated in the text of the record being signed or elsewhere in the signing process.

10.10.1.4.1 (12-03-2019)

Confirming Intent to Sign the Electronic Record

(1) Each permitted electronic signing process will require that the context in which an electronic signature is applied or the process by which a person applies an electronic signature to the record includes a step where the signer confirms his or her intent to sign the record.

(2) The signer must establish the intent to sign through a clear and conspicuous notice that a document is being signed with an electronic signature. The notice must include a:

- description of the signing process;
- clear statement of the purpose for the electronic signature; and
- statement that the completed signing process will constitute the signer's legally binding signature.

(3) The purpose for signing with an electronic signature must be set forth in the text of the document being signed. Examples are:

a. Requesting confirmation of the signer's electronic signature whereby the signer must acknowledge the signer's electronic signature and then providing the option to cancel, or

b. Continue, or adding a submission step following the signature step whereby the signed records are not effective until submitted.

(4) Each permitted electronic signing process must include requirements that minimize the risk that signers could:

- Disavow their electronic signature; or
- Claim they did not understand the legal significance of the electronic signature; or
- Did not understand the reason for signing; or
- Did not intend to sign.

10.10.1.5 (12-03-2019)

Attachment or Association of the Electronic Signature with the Electronic Record

(1) The electronic signature must be attached to or associated with the electronic record in a manner that establishes that an electronic signature was applied to a specific electronic record. The signing process must:

a. Apply the electronic signature to a document that the signer can perceive and review in a manner that makes clear to the signer exactly what is being signed; and

b. Attach or associate the electronic signature to the electronic record by linking the electronic signature and making it a part of the electronic record being signed.

(2) The permitted electronic signing process will make clear to the signer exactly what IRS document is being signed.

10.10.1.5.1 (12-03-2019)

Embedding or Associating the Integrity of the Signature

(1) Each permitted electronic signing process will require that the electronic signature be associated with the electronic record being signed. After the electronic record has been signed, the electronic record must be tamper-proof to ensure that the signature(s) applied to or associated with one document is not applied to or associated with another document and to prevent the contents of the document to which the signature(s) applied from being altered.

(2) Alternatively, the permitted electronic signing process will require the data representing the electronic signature to be stored separately from the electronic record being signed, provided a demonstrably reliable and provable process is in place which will include a relational

database or a digital signature algorithm to associate the electronic signature with the electronic record.

10.10.1.5.2 (12-03-2019)

Storing the Electronic Signing Process

(1) Each electronic signing process permitted for use on a specific IRS document by IRS guidance will require that the data constituting the electronic signature be stored in a manner that permanently attaches or associates the electronic signature with the electronic record that was signed.

(2) An electronic signature created using a set of actions, steps, and elements, requires the generation of a specific data element that indicates completion of the electronic signing process. The data element or procedure must be permanently attached to or associated with the electronic record that was signed.

10.10.1.6 (12-03-2019)

Identifying and Authenticating the Signer

(1) The electronic signing process must identify and authenticate a person as the signer and source of the electronic document or message.

(2) The electronic signing process must be able to generate evidence of the person to whom the electronic signature belongs and generate evidence that the identified person is associated with the electronic record.

(3) Signers may be identified and authenticated through multifactor authentication, or other methods designed to ensure that the IRS or other recipient of the IRS document knows the identity of the signer.

(4) Specifically, this requirement must include measures to ensure that a person with the signer's claimed attributes exists, those attributes are sufficient to uniquely identify a single person, and if an authenticator is issued, that the signer whose authenticator is registered is in fact the person who is entitled to the identity. See NIST Special Publication 800-63-3, *Digital Identity Guidelines* (June 2017), or successor document.

(5) If there is more than one signer required for the electronic record, the electronic signing process must be designed to separately identify and authenticate each signer.

10.10.1.6.1 (12-03-2019)

Methods of Identity Proofing the Signer

(1) Each permitted electronic signing process will require that the signer be identity proofed to confirm the signer's identity.

(2) The initial identification will be required only once through one or more permitted methods. A method is permitted only if specifically provided for in IRS guidance. Examples of permitted initial identification methods may include the following:

- previous business transactions with the signer
- Presenting one document bearing a photograph (such as a passport or identification badge)
- Presenting two items of identification which do not bear a photograph but do bear both a name and address (such as a driver's license, voter's registration card, or a credit card)
- Verifying an ID number or account number is valid through record checks either through internal records or through credit bureaus or similar databases (this technique may also be applied to some financial accounts)
- Leveraging an available IRS application (e.g., Secure Access e-Authentication application, successor IRS application, or IRS common infrastructure framework) that proves identity, registers individuals, or provides credentials for electronic access to IRS systems and applications

10.10.1.7 (12-03-2019)

Preserving the Integrity of the Signed Electronic Record

(1) Electronic signatures must be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record.

(2) After the electronic record has been signed, the electronic record must be tamper-proof to ensure that the signature(s) applied to or associated with one document is not applied to or associated with another document and to prevent the contents of the document to which the signature(s) applied from being altered.

10.10.1.8 (12-03-2019)

Secure Storage

(1) Each permitted electronic signing process requires techniques to lock the electronic record and prevent it from being modified.

(2) Storage systems require secure access control to ensure that the electronic records cannot be modified.

Note:

See IRM 1.15.6 for guidance on ensuring electronic information systems that produce, use, or store data have disposition instructions incorporated into the system design. The National Archives and Records Administration (NARA) is responsible for issuing standards for management of federal records created or received on electronic systems.

(3) Storage systems require an indexed retrieval system and the ability to reproduce legible and readable hardcopies of electronic records, including for inspection by an authorized IRS employee.

Note:

All IRS employees and contractors are responsible for ensuring IRS records (hard copy and electronic) are appropriately managed, retained, and archived in accordance with IRMs 1.15, *Records and Information Management* series on records retention and disposition requirements before documents can be destroyed. The electronic records retention period includes the period by which the record may be material for tax administration purposes. Refer to Document 12990, *IRS Records Control Schedules (RCS)*, for the NARA-approved IRS records disposition to prevent unauthorized/unlawful destruction of records. Refer to Document 12829, *General Records Schedules (GRS)*, for the NARA-issued disposal authorizations for temporary administrative records common to all Federal agencies.

(4) All IRS employees and contractors have responsibility for ensuring IRS records (hard copy and electronic) are appropriately managed, retained, and archived in accordance with IRMs 1.15, *Records and Information Management*, series on records retention and disposition requirements before documents can be destroyed. The electronic records retention period includes the period by which the record may be material for tax administration purposes. Refer to Document 12990, *IRS Records Control Schedules* (RCS) for the NARA-approved IRS records disposition to prevent unauthorized/unlawful destruction of records. Refer to Document 12829, *General Records Schedules* (GRS) for the NARA-issued disposal authorizations for temporary

administrative records common to all Federal agencies. The IRS has issued guidance to taxpayers that maintain books and records using an electronic storage system. See Rev. Proc. 97-22, 1997-1 C.B. 652(guidelines for electronic storage of documents by taxpayers).

10.10.1.9 (12-03-2019)

Requesting the Implementation of an e-Signature

(1) IA provides consultation, best practices and subject matter expertise. Business operating division and functional operating division (BOD/FOD) owners and form owners are responsible for driving the process to implement an e-signature.

(2) IA facilitates conversations between parties, (e.g., BOD/FOD owners and IT) providing Authentication, Authorization, and Access (A3) compliance knowledge an ensuring all appropriate stakeholders participate to identify and implement the e-signature based on the form owners requirements. BOD/FOD owners/form owners interested in adopting an e-signature process should contact IA to request assistance in submitting the request to implement an e-signature.

10.10.1.10 (12-03-2019)

Oversight Procedure

(1) The IRS requires all electronic customer facing applications that require authentication to go through a risk assessment process. The Service uses the Digital Identity Risk Assessment (DIRA) framework to assess risks associated with electronic transactions.

(2) e-Signatures are electronic transactions by definition and are subject to a risk assessment. The e-signature risk assessment process is used to assess risks associated with the likelihood of a successful challenge to the validity of an electronic signature.

(3) The business owner will use DIRA to determine the appropriate identity proofing and authentication protocol in addition to completing e-signature risk assessment to determine the appropriate signing process.

Exhibit 10.10.1-1

Current Approved Methods

The following signature methods have been approved in earlier IRS regulations, publications, or other documents and continue to be accepted by the IRS under current IRS guidance:

Signature Method	**Applicable IRS Form**
Selecting a checkbox on an electronic device such as a computer or tablet	• Form 8655, *Reporting Agent Authorization*
Inputting a Personal Identification Number	• Form 720, *Quarterly Federal Excise Tax Return* • Form 940, *Employer's Annual Federal Unemployment (FUTA) Tax Return* • Form 941, *Employer's Quarterly Federal Tax Return* • Form 990, *Return of Organization Exempt From Income Tax* • Form 1040, *U.S. Individual Income Tax Return* • Form 1065, *U.S. Return of Partnership Income* • Form 1120, *U.S. Corporation Income Tax Return* • Form 2290, *Heavy Highway Vehicle Use Tax Return* • Form 4506-T, *Request for Transcript of Tax Return* • Form 8849, *Claim for Refund of Excise Taxes* • Form 8878, *IRS e-file Signature Authorization for Form 4868 and Form*

Signature Method	Applicable IRS Form
	2350; and those forms in the Form 8878 family • Form 8879, *IRS e-file Signature Authorization*; and those forms in the Form 8879 family
Inputting a Security Code and an Authorization Code	• Form 720-CS, *Carrier Summary Report* • Form 720-TO, *Terminal Operator Report*
Using an electronic signature pad	• Form 8878, *IRS e-file Signature Authorization for Form 4868 and Form 2350*, and those forms in the Form 8878 family • Form 8879, *IRS e-file Signature Authorization*; and those forms in the Form 8879 family.
Using a stylus device	• Form 4506-T, *Request for Transcript of Tax Return* • Form 8655, *Reporting Agent Authorization* • ACH Direct Pay
Using voice signature technologies	• Form 8850, *Pre-Screening Notice and Certification Request for the Work Opportunity and Welfare-to-Work Credits*
Using a scanned or digitized image of a handwritten signature	• Form 8879-F, *IRS e-file Signature Authorization for Form 1041*

More Internal Revenue Manual

Page Last Reviewed or Updated: 10-Dec-2019