Electronic Signature Guidance for Forms 8878 and 8879

Electronic signatures appear in many forms, and may be created by many different technologies. No specific technology is required. Examples of currently acceptable electronic signature methods include:

- A handwritten signature input onto an electronic signature pad;
- A handwritten signature, mark or command input on a display screen by means of a stylus device;
- A digitized image of a handwritten signature that is attached to an electronic record;
- A typed name (e.g., typed at the end of an electronic record or typed into a signature block on a website form by a signer);
- A shared secret (e.g., a secret code, password or PIN) used by a person to sign the electronic record;
- A digital signature; or
- A mark captured as a scalable graphic.

The software must record the following data:

- Digital image of the signed form;
- Date and time of the signature;
- Taxpayer's computer IP address (Remote transaction only);
- Taxpayer's login identification - user name (Remote transaction only);
- Identity verification: taxpayer's knowledge based authentication passed results and for in person transactions, confirmation that government picture identification has been verified; and
- Method used to sign the record,(e.g., typed name); or a system log; or other audit trail that reflects the completion of the electronic signature process by the signer.

Note: The ERO must provide this information upon request.

Identity Verification Requirements

The electronic signing process must be associated with a person, and accordingly, ensuring the validity of any electronically signed record begins with identification and authentication of the taxpayer. The electronic signature process must be able to generate evidence of the person the electronic form of signature belongs to, as well as generate evidence that the identified person is actually associated with the electronic record. If there is more than one taxpayer for the electronic record, the electronic signature process must be designed to separately identify and authenticate each taxpayer.

The identity verification requirements must be in accordance with National Institute of Standards and Technology, Special Publication 800-63, Electronic Authentication Guideline, Level 2 assurance level and knowledge based authentication or higher assurance level.

In-Person Transaction

The ERO must inspect a valid government picture identification; compare picture to applicant; and record the name, social security number, address and date of birth. Verify that the name, social security number, address, date of birth and other personal information on record are

consistent with the information provided through record checks with the applicable agency or institution or through credit bureaus or similar databases. For in-person transactions, the record checks with the applicable agency or institution or through credit bureaus or similar databases are optional.
Examples of government picture identification (ID) include a driver's license, employer ID, school ID, state ID, military ID, national ID, voter ID, visa or passport.
If there is a multi-year business relationship, you should identify and authenticate the taxpayer.

Remote Transaction
The ERO must record the name, social security number, address and date of birth. Verify that the name, social security number, address, date of birth and other personal information on record are consistent with the information provided through record checks with the applicable agency or institution or through credit bureaus or similar databases.

Identity Verification Failure
If an ERO is unable to complete identity verification after three attempts, the ERO must obtain a handwritten signature.

Electronic Records
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. After the electronic record has been signed, it must be tamper-proof. Therefore, techniques must be employed that lock a document and prevent it from being modified. Storage systems must have secure access control to ensure that the electronic records cannot be modified. Additionally, storage systems must also contain a retrieval system that includes an indexing system, and the ability to reproduce legible and readable hard copies of electronically stored records.

Page Last Reviewed or Updated: 11-Mar-2014