Verifyle

Electronic Signing for Forms 8878 and 8879

Verifyle can be used to capture electronic signatures in a manner that is compliant with IRS electronic signature guidance for forms 8878 and 8879. According to the IRS Publication 1345:

Taxpayers have the option of using electronic signatures for Forms 8878 and 8879 if the software provides the electronic signature capability. If taxpayers use an electronic signature, the software and the Electronic Return Originator (ERO) must meet certain requirements for verifying the taxpayer's identity.

Electronic signatures appear in many forms and may be created by many different technologies. No specific technology is required.

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 (KBA) passed results and for in-person transactions, confirmation that government picture identification has been verified.
- 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.

Verifyle *automatically* records all of these *except* the results of an identity verification check. In order for Verifyle to record these results, the user must either (1) conduct an identity verification check in Verifyle and record the passed result also in Verifyle, or (2) record their own identity verification check method and passed result in Verifyle.

To conduct an identity verification check of a Verifyle guest (your client) in Verifyle, you can ask them to confirm a piece of information that only they would know. This is known as knowledge-based authentication, or KBA.

IRS requirements do not mandate a specific method for identity verification, but below is a simple, compliant method for conducting and recording the results of your own identity verification check using a Verifyle Thread:

1) Outside of Verifyle (for example, by phone call or text message to a verified phone number), share a unique 7-digit code with your client.

2) Inside a Verifyle Thread shared with this client, paste the following request: "In order to verify your identity, please confirm the 7-digit code I shared with you over the phone (or sent to you via text message)."

3) Confirm and record in Verifyle that your client entered the correct code. If they did not enter the correct code, then the KBA has failed and any subsequent

electronic signatures are invalid until a successful KBA has been recorded (maximum of three attempts).

Further Information on Identity Verification for Forms 8878 and 8879

Verifyle automatically records all of the data required for an electronic signature to be considered valid by the IRS *except* for the passed results of an identity verification. Verifyle can be used to record this data by entering it in a Thread, but *it is the electronic return originator's (ERO's) responsibility to perform this verification*.

As far as how the identity verification should be performed. The same IRS Publication 1345 states the following with regard to 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.

It goes on to describe a process for KBA that *may* (not "must," "shall," or "should") be used. We consult the above referenced National Institute of Standards and Technology (NIST), Special Publication 800-63 for more explicit guidance.

There are two basic requirements: authentication and identity verification. The details of those requirement are discussed further in Internal Revenue Manuals, Part 10, which also references NIST. In particular, we look to NIST SP 800-63B, Digital Identity Guidelines: Authentication & Lifecycle Management for normative requirements for the requirements that define "Electronic Authentication Guideline, Level 2 assurance level and knowledge-based authentication."

NIST SP 800-63B section 4.2 addresses Authenticator Assurance Level 2 (AAL2). It states:

> At AAL2, authentication shall occur by the use of either a multi-factor authenticator or a combination of two single-factor authenticators.

Verifyle supports the use of multi-factor authentication in a variety of ways, including via Multi-Factor OTP Device, Memorized Secret authenticator, Out-of-Band Device, and Single-Factor Cryptographic Software.
As referenced above, IRS Publication 1345 prescribes the use of KBA (also known as knowledge-based verification, or KBV within the NIST publications), the requirements of which are given in NIST SP 800-63A, Digital Identity Guidelines: Enrollment & Identity Proofing, Section 5.3.2 for Identity Assurance Level 2 (IAL2).

In this section we will need the following definition from NIST SP 800-63-3 Appendix A —Definitions and Abbreviations:

> Credential Service Provider (CSP): A trusted entity that issues or registers subscriber authenticators and issues electronic credentials to subscribers. A CSP may be an independent third party or issue credentials for its own use.

There are five requirements on KBA stated in section 5.3.2.

> 1. The CSP SHALL NOT use KBA to verify an applicant's identity against more than one piece of validated identity evidence.

Verifyle neither does nor advocates this.

> 2. The CSP SHALL only use information that is expected to be known only to the applicant and the authoritative source, to include any information needed to begin the KBA process. Information accessible freely, for a fee in the public domain, or via the black market shall not be used.

Verifyle shares the view of the Government Accountability Office[1] that the use of data from data brokers and consumer reporting agencies (e.g. Equifax, Experian, LexisNexis, Kroll Background America, Corelogic, etc.) for KBA is insecure. This information is accessible, often freely via resources like whitepages.com; for a fee in the public domain; and certainly on the black market, given several cybersecurity breaches, including those of Experian in 2015[2] and Equifax in 2017[3].

> 3. The CSP SHALL allow a resolved and validated identity to opt out of KBA and leverage another process for verification.

That remains the tax professional's choice. If the tax professional has validated the identity of the taxpayer through some other means, they may choose to record the method of validation and the results in Verifyle in order to comply with IRS guidelines and NIST, Special Publication 800-63, Electronic Authentication Guideline, Level 2.

> 4. The CSP **SHOULD** perform KBA by verifying knowledge of recent transactional history in which the CSP is a participant. The CSP SHALL ensure that transaction information has at least 20 bits of entropy. For example, to reach minimum entropy requirements, the CSP could ask the applicant for verification of the amount(s) and transaction numbers(s) of a micro-deposit(s) to a valid bank account, so long as the total number of digits is seven or greater.

This is the nature of the KBA that we advocate; the way that that NIST says KBA "SHOULD" be performed. The "transaction" we suggest is via the tax professional (who serves as the CSP for this purpose) providing the client with a unique 7-digit integer known only to the CSP until it is provided, and then known only to the CSP and client. This is clearly in accord with the requirement from 2, which states that "The CSP SHALL only use information that is expected to be known only to the applicant

and the authoritative source." And it satisfies the requirements for the "recommended as particularly suitable" or "preferred" method in 4 of recency and with CSP participation.

Finally, part 5 describes a method that "MAY" be used in performing KBA. This is the method most commonly known, but it is not the preferred method, it is only "permissible." Verifyle neither does nor advocates the method described below.

> 5. The CSP MAY perform KBA by asking the applicant questions to demonstrate they are the owner of the claimed information. However, the following requirements apply:
>
> a. KBA SHOULD be based on multiple authoritative sources.
>
> b. The CSP SHALL require a minimum of four KBA questions with each requiring a correct answer to successfully complete the KBA step.
>
> c. The CSP SHOULD require free-form response KBA questions. The CSP MAY allow multiple choice questions, however, if multiple choice questions are provided, the CSP SHALL require a minimum of four answer options per question.
>
> d. The CSP SHOULD allow two attempts for an applicant to complete the KBA. A CSP SHALL NOT allow more than three attempts to complete the KBA.
>
> e. The CSP SHALL time out KBA sessions after two minutes of inactivity per question. In cases of session timeout, the CSP SHALL restart the entire KBA process and consider this a failed attempt.
>
> f. The CSP SHALL NOT present a majority of diversionary KBA questions (i.e., those where "none of the above" is the correct answer).
>
> g. The CSP SHOULD NOT ask the same KBA questions in subsequent attempts.
>
> h. The CSP SHALL NOT ask a KBA question that provides information that could assist in answering any future KBA question in a single session or a subsequent session after a failed attempt.
>
> i. The CSP SHALL NOT use KBA questions for which the answers do not change (e.g., "What was your first car?").
>
> j. The CSP SHALL ensure that any KBA question does not reveal personally identifiable information that the applicant has not already provided, nor personal information that, when combined with other information in a KBA session, could result in unique identification.

[1] https://www.gao.gov/assets/700/699195.pdf

[2] https://www.theguardian.com/business/2015/oct/01/experian-hack-t-mobile-credit-checks-personal-information

[2] https://www.washingtonpost.com/business/technology/equifax-hack-hits-credit-histories-of-up-to-143-million-americans/2017/09/07/a4ae6f82-941a-11e7-b9bc-b2f7903bab0d_story.html