



STATE BOARD OF EQUALIZATION
PROPERTY TAX DEPARTMENT
PO BOX 942879, SACRAMENTO, CALIFORNIA 94279-0064
1-916-274-3350 • FAX 1-916-285-0134
www.boe.ca.gov

TED GAINES
First District, Sacramento

SALLY J. LIEBER
Second District, San Francisco

ANTONIO VAZQUEZ
Third District, Santa Monica

MIKE SCHAEFER
Fourth District, San Diego

MALIA M. COHEN
State Controller

YVETTE M. STOWERS
Executive Director
No. 2026/006

February 17, 2026

TO CLERKS OF COUNTY BOARDS AND
COUNTY ASSESSORS:

CLARIFICATION ON E-FILING OF ASSESSMENT APPEAL APPLICATIONS

On December 20, 2007, the State Board of Equalization (BOE) issued guidance regarding the acceptance of an electronically filed *Application for Changed Assessment* (now called the BOE-305-AH, *Assessment Appeal Application*) in Letter to Assessors (LTA) [No. 2007/059](#). Since that time, the BOE has received several requests for clarification to address potential administrative confusion and to promote uniform practices amongst clerks of county boards of equalization or county assessment appeals boards. This letter is issued in response to those requests.

Effective January 1, 2008, Assembly Bill [\(AB\) 1042](#) (Statutes of 2007, Chapter 195) added subdivision (g) to [section 1603](#) of the Revenue and Taxation Code¹ (RTC). This provision authorizes the clerk of a county board of equalization or county assessment appeals board to accept an electronically filed application for changed assessment that contains an electronic signature if all of the following statutory requirements are met:

- The application complies with all other requirements for filing the application.
- The electronic signature is accompanied by the certification described in section 1603, subdivision (f), related to affirming under the penalty of perjury that the information is true, correct, and complete.
- The electronic signature is authenticated in a manner that is approved by the county board of supervisors, which manner may include, but is not limited to, the use of personal identification numbers the clerk of the board has assigned to applicants.

Electronic signatures are defined by Civil Code [section 1633.2\(h\)](#) as:

"...an electronic sound, symbol, or process attached to or logically associated with an electronic record and executed or adopted by a person with the intent to sign the electronic record..."

The following authentication methods are examples of electronic signature approaches that can be used individually or in combination (single-factor or multi-factor authentication), depending on

¹ All statutory references are to the Revenue and Taxation Code, unless otherwise provided.

the risk level of the process and the preference of the county board of supervisors. These examples are not exhaustive.

1. **Email authentication:** The signer is sent an email, inviting them to access the e-sign document by clicking a link. Authentication occurs when the signer successfully logs in to the email account.
2. **Login credentials:** The signer is authenticated by the sending party's system prior to accessing the transaction. Authentication requires a valid user ID and password.
3. **SMS authentication:** The signer's identity is verified through a secure, one-time SMS code sent to the signer's phone. The signer enters the code on the login page to access documents requiring a signature.²
4. **Government ID verification:** The signer's identity is verified remotely using a government-issued identification document (e.g., driver's license or passport). The process may involve uploading a photo of the ID or using a mobile application to capture and verify the ID before accessing and signing documents.³
5. **Biometric comparison:** Biometric comparison is typically used for higher-risk or higher-value transactions involving unknown signers. The signer may be required to capture a photograph (e.g., a selfie), which is then compared to the photograph on the signer's government-issued identification to verify their identity. Biometric authentication offers a higher level of security and is particularly well-suited for transactions where strong authentication is crucial, such as those involving legal documents, financial transactions, and government applications.⁴
6. **Knowledge-based authentication (KBA):** Knowledge-based authentication, used in conjunction with electronic signatures, verifies identity by posing questions based on publicly available information, enhancing security, and meeting e-signature requirements like those of the Internal Revenue Service. KBA is a method of verifying a user's identity by asking them questions about their personal information that are based on publicly available records. Examples of questions might include: "What is your current home address?" "What are the last four digits of your SSN?", or "What was the name of your

² While SMS authentication offers improved protection compared to passwords alone, it is not without vulnerabilities. Security concerns include SIM swapping, where attackers can obtain access to a user's phone number and intercept SMS codes. Other risks include SMS outages and phishing attacks that can intercept verification codes.

³ Utilize the service of companies such as OneSpan or DocuSign.

⁴ Biometric signature capture requires specialized hardware, such as a tablet and stylus. Biometric data must be stored securely to prevent unauthorized access. The signing process may be slightly more complex than traditional electronic signatures. Biometric signature solutions can be more expensive than traditional electronic signature solutions.

high school?" KBA is often used in conjunction with electronic signatures to ensure that the person signing the document is who they claim to be.⁵

Additionally, government entities are also authorized under Government Code [section 16.5](#) to accept digital signatures, provided the signatures meet specified statutory and regulatory requirements⁶. *Digital signatures* are a form of electronic signature that relies on digital certificates to verify the authenticity and integrity of a document. While digital signatures provide a higher level of security and remain permissible, their implementation can be administratively burdensome and costly.

The addition of section 1603(g) was intended to provide counties with flexibility by allowing the acceptance of electronic signatures for applications for changed assessment, thereby reducing administrative burdens and costs, keeping pace with evolving technology, and improving the efficiency of the assessment appeals process. As such, county boards of supervisors have the authority and discretion to determine whether to accept applications for changed assessments that include electronic or digital signatures, based on their respective organizational, operational, and fiscal needs.

Sincerely,

/s/ David Yeung

David Yeung
Deputy Director
Property Tax Department

DY:mo

⁵ KBA is only valid for vetting the identity of US-based recipients. Signers must have public records to generate questions and answers. The KBA process may not be able to generate questions for a client for various reasons, such as an incorrect name, TIN, date of birth, or address, or if the client doesn't have enough public records.

⁶ As adopted by the Secretary of State. See <https://www.sos.ca.gov/administration/regulations/current-regulations/technology/digital-signatures>.