JUDICIAL COUNCIL OF CALIFORNIA

455 Golden Gate Avenue • San Francisco, California 94102-3688
Telephone 415-865-4200 • Fax 415-865-4205 • TDD 415-865-4272

MEMORANDUM

Date
August 7, 2015

To
Court Technology Advisory Committee

From
Rules and Policy Subcommittee
Hon. Peter J. Siggins, Chair

Subject
Update to the *Trial Court Records Manual*: Electronic Signature Standards and Guidelines

Action Requested
Please review for August 18 meeting

Deadline
August 18, 2015

Contact
Tara Lundstrom
415-865-7650 phone
tara.lundstrom@jud.ca.gov

Background

Both the Court Technology Advisory Committee (CTAC) and the Court Executives Advisory Committee (CEAC) have been tasked with proposing standards and guidelines governing electronic signatures by courts and judicial officers. These standards are intended to implement Government Code section 68150(g), which authorizes the use of electronic signatures by courts and judicial officers "in accordance with procedures, standards, and guidelines established by the Judicial Council pursuant to this section." The CEAC Records Management Subcommittee developed proposed standards and guidelines for inclusion in the *Trial Court Records Manual*. During their August 5 and 7 meetings, CTAC's Rules and Policy Subcommittee (RPS) and CEAC reviewed the proposed standards and guidelines and recommended that they be circulated for comment to the presiding judges and court executive officers of the superior courts.

Recommendation

RPS proposes that CTAC recommend circulating the proposed electronic signature standards and guidelines to the presiding judges and court executive officers of the superior courts for comment.

Discussion

Electronic signatures by courts and judicial officers are authorized under Government Code section 68150(g), which provides as follows:

> Any notice, order, judgment, decree, decision, ruling, opinion, memorandum, warrant, certificate of service, writ, subpoena, or other legal process or similar document issued by a trial court or by a judicial officer of a trial court may be signed, subscribed, or verified using a computer or other technology *in accordance with procedures, standards, and guidelines established by the Judicial Council pursuant to this section*. Notwithstanding any other provision of law, all notices, orders, judgments, decrees, decisions, rulings, opinions, memoranda, warrants, certificates of service, writs, subpoenas, or other legal process or similar documents that are signed, subscribed, or verified by computer or other technological means pursuant to this subdivision shall have the same validity, and the same legal force and effect, as paper documents signed, subscribed, or verified by a trial court or a judicial officer of the court.

(Italics added). Subdivision (g) was added to the Government Code, effective January 1, 2011, by Assembly Bill 1926.[1] (Stats. 2010; ch. 167.) The Judicial Council has not yet developed implementing procedures, standards, and guidelines. The proposed standards and guidelines are loosely modeled on the Uniform Electronic Transactions Act and New York State's Electronic Signatures and Records Act Guidelines.

The proposed standards and guidelines include sections (1) describing their purpose and the underlying principles motivating the drafters; (2) providing definitions; (3) establishing the format for electronic signatures; (4) stating guidelines for ensuring that electronic signatures are executed or adopted with intent to sign, attributable to an authorized person, and capable of verification; (5) establishing how to execute electronic signatures under penalty of perjury; (6) establishing the legal effect of electronic signatures; (7) providing a list of acceptable security procedures; (8) stating the effect of the digitized signatures created by scanning the original

[1] This amendment was part of a broader reform of Government Code section 68150 in AB 1926 to authorize the creation and maintenance of electronic trial court records.

signatures of judicial officers and courts; and (9) providing examples of court-created documents that may be electronically signed by a court or judicial officer.

In addition to these standards implementing Government Code section 68150(g), the proposed update to the *Trial Court Records Manual* includes a section outlining the various provisions in the Code of Civil Procedure, Penal Code, and California Rules of Court that authorize electronic signatures submitted to the courts by attorneys, parties, and law enforcement officers. Lastly, there is a section stating the effect of digitized signatures created by scanning paper documents submitted to the courts.

Coordination with the Court Executives Advisory Committee

Both CTAC and CEAC are responsible for developing the electronic signature standards and guidelines implementing Government Code section 6150(g). During its meeting on August 7, 2015, CEAC reviewed the proposed standards and guidelines and decided to recommend circulating them for comment to the presiding judges and court executive officers of the superior courts.

Attachments and Links

- Memorandum to the Presiding Judges and Court Executive Officers of the Superior Courts with attachment (proposed update to the *Trial Court Records Manual)*
- *Trial Court Records Manual* (rev. January 1, 2014), available at *http://www.courts.ca.gov/documents/trial-court-records-manual.pdf*

JUDICIAL COUNCIL OF CALIFORNIA

455 Golden Gate Avenue • San Francisco, California 94102-3688
Telephone 415-865-4200 • Fax 415-865-4205 • TDD 415-865-4272

MEMORANDUM

Date
August 6, 2015

To
Presiding Judges of the Superior Courts
Court Executive Officers of the Superior Courts

From
Court Executives Advisory Committee
Ms. Mary Beth Todd, Chair
Mr. Richard D. Feldstein, Vice-chair

Court Technology Advisory Committee
Hon. Terence L. Bruiniers

Subject
Trial Court Records Manual: Proposed Electronic Signature Standards and Guidelines to Implement Government Code Section 68150(g)

Action Requested
Please review and submit any comments by e-mail to josely.yangco-fronda@jud.ca.gov

Deadline
[To be determined]

Contact
Josely Yangco-Fronda
(415) 865-7626
josely.yangco-fronda@jud.ca.gov

Executive Summary

The Court Executives Advisory Committee (CEAC) and the Court Technology Advisory Committee (CTAC) propose updating the *Trial Court Records Manual* to include new standards and guidelines that would govern the use of electronic signatures by trial courts and judicial officers. These standards and guidelines would implement Government Code section 68150(g), which authorizes electronic signatures by a court or judicial officer "in accordance with procedures, standards, and guidelines established by the Judicial Council." The update would also include new sections in the *Trial Court Records Manual* that would (1) outline the various

provisions in the Code of Civil Procedure, Penal Code, and California Rules of Court that authorize electronic signatures submitted to the courts by attorneys, parties, and law enforcement officers; and (2) state the effect of digitized signatures created by scanning paper court records.

Background

For over twenty years, Government Code section 68150(a) has authorized the preservation of trial court records in electronic form. (Stats. 1994; ch. 1030.) With the enactment of Assembly Bill 1926 in 2010, this provision was expanded to allow superior courts to create and maintain court records in electronic form. (Stats. 2010; ch. 167.) Electronic court records were to be subject to rules adopted by the Judicial Council establishing standards and guidelines for their creation, maintenance, reproduction, and preservation. (See Gov. Code, §§ 68150(a) and (c).) The Judicial Council sponsored AB 1926 to facilitate the transition by courts to paperless case environments.

Trial Court Records Manual

Effective January 1, 2011, the Judicial Council adopted rule 10.854 to implement AB 1926. This rule tasked Judicial Council staff—in collaboration with the trial court presiding judges and court executives—with preparing, maintaining, and distributing a manual providing standards and guidelines for the creation, maintenance, and retention of trial court records, consistent with the Government Code and the rules of court and policies adopted by the council. The first version of this manual, known as the *Trial Court Records Manual*, was approved by the council at the same time that it adopted rule 10.854.

Judicial Council staff—in collaboration with the trial court presiding judges and court executives—is also responsible for periodically updating the *Trial Court Records Manual* to reflect changes in technology that affect the creation, maintenance, and retention of court records. (Cal. Rules of Court, rule 10.854(c).) Proposed changes must be made available for comment from the trial courts before the manual is updated or changed. (*Ibid.*) Since it was first issued, the council has twice updated the *Trial Court Records Manual.*

Electronic signatures by courts and judicial officers

As part of the effort to modernize the management of trial court records, AB 1926 also authorized the use of electronic signatures by courts and judicial officers. The bill added subdivision (g) to Government Code section 68150, which provides as follows:

> Any notice, order, judgment, decree, decision, ruling, opinion, memorandum, warrant, certificate of service, writ, subpoena, or other legal process or similar document issued by a trial court or by a judicial officer of a trial court may be signed, subscribed, or verified using a computer or other technology *in*

> *accordance with procedures, standards, and guidelines established by the Judicial Council pursuant to this section*. Notwithstanding any other provision of law, all notices, orders, judgments, decrees, decisions, rulings, opinions, memoranda, warrants, certificates of service, writs, subpoenas, or other legal process or similar documents that are signed, subscribed, or verified by computer or other technological means pursuant to this subdivision shall have the same validity, and the same legal force and effect, as paper documents signed, subscribed, or verified by a trial court or a judicial officer of the court.

(Gov. Code, § 68150(g).) This proposal would implement Government Code section 68150(g) by updating the *Trial Court Records Manual* to include standards and guidelines for the use of electronic signatures by courts and judicial officers.

This year, the Legislature enacted AB 432, which will introduce new section 34 to the Code of Civil Procedure. Similar to Government Code section 68150(g), new Code of Civil Procedure section 34 will provide that electronic signatures by courts and judicial officers are as effective as original signatures. AB 432 also defines the term "electronic signature" in Code of Civil Procedure section 17(a)(3) 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 Proposal

This proposal would update the *Trial Court Records Manual* to implement Government Code section 68150(g) by adding a new section to the manual that would establish standards and guidelines governing the use of electronic signatures on court-created records. In addition, new sections would be added to (1) outline the various provisions in the Code of Civil Procedure, Penal Code, and California Rules of Court that authorize electronic signatures submitted to the courts by attorneys, parties, and law enforcement officers and (2) state the effect of digitized signatures created by scanning paper court records.

Electronic signatures on court-created documents

A new section 6.2.1 would be added to the manual to establish standards and guidelines governing electronic signatures by the court and judicial officers. The proposed standards and guidelines are loosely modeled on the Uniform Electronic Transactions Act and New York State's Electronic Signatures and Records Act Guidelines.

Purpose, drafting principles, and definitions. A new section 6.2.1.A would state the purpose of the standards and guidelines and list the principles that motivated the drafters. These principles include that the standards should not be more restrictive than those for traditional "wet"

signatures; that they should consider how the signature is being applied when setting the level of authentication required; that they should allow for flexibility in the method of applying and the appearance of the signature; and that they should, wherever possible, avoid requiring specific proprietary tools. A new section 6.2.1.B would provide definitions applicable to the standards and guidelines, including a definition for "electronic signature" that mirrors the definition that will be added by AB 432 to Civil Code of Procedure section 17.

Format of electronic signatures. The format of electronic signatures would be stated in new section 6.2.1.C. Electronic signatures could be in the form of (1) a digitalized image of the person's signature, (2) an "/s/" followed by the person's name, or (3) any other electronically created method of indicating with clarity the name of the person whose signature is being affixed to the document.

Guidelines governing intent, attribution, and verification. A new section 6.2.1.D would provide guidelines to ensure (1) that the signer intended to sign the document, (2) that the electronic signature is attributable to an authorized person, and (3) that the electronic signature can be verified. To demonstrate intent, it must be clear to a person, when presented with the opportunity to sign a document, that the person is being asked to sign the document electronically. To ensure that the signer is authorized to sign, the document must be presented for an electronic signature only to an authorized person or someone authorized to execute the signature on that person's behalf. An electronic signature may be attributed to a person if it was the act of the person (or the act of someone authorized to sign on that person's behalf), which may be shown in any manner, including the efficacy of the security procedure applied when the signature is executed or adopted. And lastly, the identity of the signer must be capable of verification. Courts would be instructed to retain any data relevant to verifying electronic signatures, such as the signer's identity and the date and time that the signature is executed or adopted.

This section would also provide a "practice tip" to recommend that courts consider designing their business practices and technology systems—such as workflows, pop-up screens, and access and security procedures—to facilitate compliance with these guidelines.

Signatures under penalty of perjury. A new section 6.2.1.E would govern signatures required by law to be made under penalty of perjury. Electronic signatures would be made under penalty of perjury if the electronic record includes the electronic signature, all of the information as to which the declaration pertains, and a declaration under penalty of perjury by the person who submits the electronic signature that the information is true and correct.

Legal effect of electronic signatures. As provided by Government Code section 68150(g) and Code of Civil Procedure section 34, a new section 6.2.1.F would state that electronic signatures by courts and judicial officers have the same effect as original signatures on paper documents.

Acceptable security procedures. Acceptable security procedures for identity verification would be addressed in a new section 6.2.1.G. This section would provide that all systems used in the capture, application, and storage of electronic signatures and documents are subject to the data and information security guidelines recommend in *How to Use the Information Systems Controls Framework: A Guide to California Superior Courts (Draft-May 27, 2015)*. This requirement would ensure that access is limited to authorized individuals and that original files and documents have not been altered or modified since they were created.

In addition, this section would recognize both real-time digitized signatures and system-applied signatures as acceptable procedures for verifying identity. Real-time digitized signatures would be defined as graphical images of a handwritten signature, where the signature is captured by means of a digital pen, pad, or other device that converts the physical act of signing into a digital representation of the signature and applies that digital representation to a document, transaction, or database entry. User authentication for real-time digitized signatures would be similar to the authentication of traditional "wet" signatures.

System-applied signatures would be defined as electronic signatures applied to documents, transactions, or databases through the use of a computer, software, or application following an affirmative action (e.g., clicking on a check box) by the signer or someone authorized to act on his or her behalf. Four methods of user identification would be recognized for system-applied electronic signatures: (1) password or PIN, where the user is authenticated through a password or PIN either tied directly to the application of the signature or used to gain access to the computer application, database, or network; (2) symmetric cryptography, where the user is authenticated using a cryptographic key that is known to the system and the signer; (3) asymmetric cryptography (digital certificates), where the user is authenticated using both public and private keys; and (4) biometrics, where the user is authenticated using biometrics such as voice, fingerprint, or retina.

Scanned signatures. A new section 6.2.1.H would be added to address digitized signatures that are created when courts convert their paper records into electronic records by scanning. This section would provide that the digitized signatures of judicial officers and courts created by scanning have the same validity and the same legal force and effect, as their original signatures.

Examples of court-created documents that may be electronically signed. A new section 6.2.1.I would provide a list of various court documents that may be signed electronically by a court or judicial officer. The list would be provided for illustrative purposes only and would not be intended to suggest that a signature is required on any of the identified documents, unless a signature is otherwise mandated by statute or rule. Examples provided would include judgments, orders after hearings, minute orders, notices, abstracts of judgment, arrest and search warrants, and certificates of service, among others.

Electronic signatures on documents submitted to the courts
A new section 6.2.2 would be added to the *Trial Court Records Manual* to address the statutes and rules that authorize electronic signatures on documents submitted to the courts by attorneys, parties, and law enforcement officers. This legal authority would include (1) Code of Civil Procedure section 1010.6 and rule 2.257, which govern the use of electronic signatures on electronically filed documents in civil cases; (2) Penal Code sections 817 and 1526, which provide the procedures required to authorize the electronic signatures of law enforcement officers on probable cause declarations for arrest and search warrants; and (3) Penal Code section 959.1, which authorizes the digitized facsimile of a defendant's signature on Notices to Appear issued in traffic and criminal cases for infraction and misdemeanor violations.

Signatures on scanned documents
This proposal would also add a new section 6.2.3 to address digitized signatures that are created when courts convert their paper records into electronic records by scanning. This section would provide that these digitized signatures have the same validity and the same legal force and effect, as the original signatures. It would largely duplicate the language proposed for section 6.2.1.H that is specific to the scanned signatures of judicial officers and courts. This language is duplicated here to clarify that it also applies to electronic signatures on documents submitted to the courts.

Alternatives Considered

Because Government Code section 68150(g) requires that the Judicial Council establish implementing standards and guidelines, CEAC and CTAC did not consider alternatives to this proposal to adopt these standards and guidelines as part of the *Trial Court Records Manual.*

Implementation Requirements, Costs, and Operational Impacts

Potentially significant costs could be incurred by individual courts in implementing this proposal as they might be required to procure new technology systems and equipment for capturing the electronic signatures of judicial officers and court officials. These initial costs, however, may be outweighed by the cost savings and efficiency gains that would be realized by allowing judicial officers and courts to use electronic signatures. Because implementation is voluntary, each court would determine if the benefits outweigh the costs in deciding whether to use electronic signatures on court-generated documents. Updating the manual, which is in electronic format and posted online, would result in only minimal costs to the branch.

Request for Specific Comments

In addition to comments on the proposal as a whole, the advisory committee is interested in comments from the courts on the following:

- Does the proposal appropriately address the stated purpose?

The advisory committee also seeks comments from courts on the following cost and implementation matters:

- Would the proposal provide cost savings? If so please quantify.
- What would the implementation requirements be for courts? For example, training staff (please identify position and expected hours of training), revising processes and procedures (please describe), changing docket codes in case management systems, or modifying case management systems.
- Do any of the proposed standards need further clarification? If so, please describe how they should be revised.
- Are there any effective practices related to electronic signatures that are currently in use by the courts that are not covered by the proposed standards? If so, please describe these practices.

Attachments and Links

1. Proposed update to the *Trial Court Records Manual* at pages 8–19
2. *Trial Court Records Manual* (rev. January 1, 2014), available at *http://www.courts.ca.gov/documents/trial-court-records-manual.pdf*

This proposal would revise the *Trial Court Records Manual*, section 2.11, and add sections 6.2.1, 6.22, and 6.23, as follows:

2. Statutes and Rules of Court Governing Trial Court Records Management

* * *

2.1.1 Signatures on Electronically Created Court Documents

Government Code section 68150(g) provides that any notice, order, judgment, decree, decision, ruling, opinion, memorandum, warrant, certificate of service, or similar document issued by a trial court or judicial officer of a trial court may be signed, subscribed, or verified using a computer or other technology. ~~Future versions of this manual will contain procedures, standards, or guidelines for signing, subscribing, and verifying court documents by electronic means.~~ Section 6.2.1 of this manual provides standards and guidelines for signing, subscribing, and verifying court documents by electronic means.

* * *

6. Creation, Storage, Maintenance, and Security of Records

* * *

6.2 Electronic Signatures: Standards and Guidelines

6.2.1. Electronic Signatures on Court-Created Records

A. Purpose

This section provides standards and guidelines for the creation of electronic signatures by judicial officers and the superior courts. These standards and guidelines implement Government Code section 68150(g), which provides that any notice, order, judgment, decree, decision, ruling opinion, memorandum, warrant, certificate of service, or similar document issued by a court or a judicial officer may be signed, subscribed, or verified using computer or other technology in accordance with procedures, standards, and guidelines established by the Judicial Council.

The following principles guided the drafters in preparing these standards and guidelines:

- Electronic signature standards should provide appropriate requirements and should generally not be more restrictive than standards for traditional 'wet' signatures.
- Electronic signature standards should consider how the signature is being applied when setting the level of authentication required.
- Electronic signature standards should allow for flexibility in the method of applying and the appearance of the signature.

- Electronic signature standards, wherever possible, should avoid requiring specific proprietary tools. Instead the standards should present attributes of acceptable authentication tools and encourage leveraging security within other business critical systems.

B. Definitions

As used in these standards and guidelines, the following definitions apply:

- ***Electronic*** means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.
- ***Electronic court record*** means a court record created, generated, sent, communicated, received, or stored by electronic means.
- ***Electronic signature*** means an electronic sound, symbol, or process attached to or logically associated with an electronic court record and executed or adopted by a person with the intent to sign the electronic court record. (Code of Civ. Proc., § 17.)
- ***Person*** includes judicial officers, court clerks, deputy court clerks, and others authorized to sign documents issued by a judicial officer or a court.
- ***Record*** means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.
- ***Security procedure*** means a procedure employed for the purpose of verifying that an electronic signature, record, or performance is that of a specific person or for detecting changes or errors in the information in an electronic record. The term includes a procedure that requires the use of algorithms or other codes, identifying words or numbers, encryption, or callback or other acknowledgment procedures.

C. Format of Signatures

Unless otherwise prescribed in a statute or rule, an electronic signature may be in the form of:

- A digitalized image of the person's signature;
- An /s/ followed by the person's name; or
- Any other electronically created method of indicating with clarity the name of the person whose signature is being affixed to the document.

All such signatures, to be legally effective, must satisfy the requirements stated in this section.

D. Electronic Signatures Must Be Executed or Adopted with an Intent to Sign, Attributable to an Authorized Person, and Capable of Verification

The following guidelines apply to electronic signatures executed or adopted by a judicial officer or the court:

- When a person is presented with the opportunity to sign a document electronically, it must be clear to the person that he or she is being asked to sign the document electronically. This demonstrates that the person in fact intended to sign the document. (See Code of Civ. Proc., § 17 [electronic signatures must be "executed or adopted with the intent to sign"].)
- When a document is to be signed electronically, it must be presented only to an authorized person or to someone authorized to execute the signature on the person's behalf.
- An electronic signature is attributed to a person if it was the act of that person (or the act of someone authorized to execute or adopt the signature on that person's behalf), which may be shown in any manner, including by showing the efficacy of any security procedure applied when the signature was executed or adopted.
- The identity of the person who executed or adopted the electronic signature must be capable of verification. If a document is signed electronically, the court should retain any data relevant to verifying the signature, such as the identity of the person who executed or adopted the signature and the date and time that the signature was executed or adopted.

Practice Tip: Courts should consider designing business practices and technology systems—such as workflows, pop-up screens, and access and security procedures—to facilitate compliance with these guidelines.

E. Signatures Under Penalty of Perjury

If a law requires that a statement be signed under penalty of perjury, the requirement is satisfied with respect to an electronic signature, if an electronic record includes:

- The electronic signature;
- All of the information as to which the declaration pertains; and
- A declaration under penalty of perjury by the person who submits the electronic signature that the information is true and correct.

F. Legal Effect

Unless otherwise specifically provided by law, all notices, orders, judgments, decrees, decisions, rulings, opinions, memoranda, warrants, certificates of service, or similar documents that are signed, subscribed, or verified by using a computer or other technological means shall have the same validity, and the same legal force and effect, as paper documents signed, subscribed, or verified by a court official or judicial officer. (Gov. Code, § 68150(g); see also Code of Civ. Proc., § 34 ["An electronic signature . . . by a court or judicial officer shall be as effective as an original signature"].)

A signature may not be denied legal effect or enforceability solely because it is in electronic form. The legal effect of an electronic signature is determined from the context and circumstances surrounding its creation, execution, or adoption, and otherwise as provided by law.

G. Acceptable Security Procedures for Verification of Identity When Applying Electronic Signature

The acceptable procedures for verifying the identity of persons executing electronic signatures are varied and are subject to change as the technology in this area is developing quickly. Certain guidelines can be applied at this time to determine whether electronic signatures are verifiable.

First, all systems used in the capture, application, and storage of electronic media, including any electronic signatures or electronic documents, are subject to data and information security guidelines as recommended in *How to Use the Information Systems Controls Framework: A Guide to California Superior Courts (Draft-May 27, 2015)*. This requirement ensures that access to any electronic signature, electronically signed document, or the tools and mechanisms for applying an electronic signature is limited to authorized individuals and that original files and documents have not been altered or modified since they were created.

Second, currently acceptable procedures for verification of electronic signatures include the following:

1. Real-time digitized electronic signatures

A digitized signature is a graphical image of a handwritten signature. The signature is captured by means of a digital pen, pad, or other device that converts the physical act of signing into a digital representation of the signature and applies that digital representation to the document, transaction, or database entry.

User authentication before the application of the digitized signature should be similar to authentication methods used when a physical handwritten signature is applied to a hard copy or traditional paper document.

2. System-applied electronic signatures

A system-applied electronic signature is an electronic signature that is applied to a document, transaction or database through use of a computer, software, or application following affirmative action by the individual or a person authorized to act on the person's behalf. The affirmative action could include, for example, the requirement that the signer click on an "OK" box or similar act.

User authentication for applying a system-applied electronic signature may be obtained through one of the following methods:

- ***Password or PIN*** - The user is authenticated through a password or PIN to gain access to the computer application, database, or network. Alternatively or in addition, the user is authenticated through a password or PIN tied directly to the application of the signature.
- ***Symmetric Cryptography*** – The user is authenticated using a cryptographic key that is known to the system and the individual signing the document. This is often done via a single use password that is randomly generated.
- ***Asymmetric Cryptography (Digital Certificates)*** – The user is authenticated using both private and public keys. This is the most secure method of user authentication and should be considered when applying signatures made under penalty of perjury.
- ***Biometrics*** – The user is authenticated using biometrics, including but not limited to voice, fingerprint, or retina.

The method selected should take into consideration business requirements, cost, and relative risk and consequence of a breach. Courts should document and adopt security procedures for authentication before the implementation of a system-applied electronic signature.

H. Judicial Signatures on Scanned Documents

Government Code section 68150(a) authorizes the preservation and maintenance of trial court records in electronic form. Under this provision, trial courts may convert their paper records to electronic form by scanning. The act of scanning an original signature results in a digitized signature. The digitized signature of a court or judicial officer created by scanning shall have the same validity, and the same legal force and effect, as the original signature.

I. Examples of Court-Created Documents that May Be Electronically Signed by a Judicial Officer or Clerk

The following is a list of various court-created documents that may be signed electronically by a judge or clerk under Government Code 68150(g). This list is provided for illustrative purposes only. It is not intended to suggest that a signature is required on these documents, unless a signature is otherwise mandated by statute or rule.

- Judgments
- Deferred entry of judgment
- Orders after hearings
- Minute orders
- Exemplification of records
- Probable cause determinations
- Arrest warrants
- Abstracts of judgment
- Summons
- Notices
- Fee waivers granted by statute
- Certificate of mailing
- Clerk's declarations
- Entry of judgment

- Search warrants
- Bench warrants
- Protective orders
- Letters for probate
- Writs of attachment
- Writs of possession
- Writs of execution
- Lis pendens
- Notices of intent to dispose of exhibits
- Certification of records
- Clerk's certificate of service
- Felony abstract of judgment
- Notice of cost of electronic recording
- Letters for probate
- Elisors

6.2.2. Electronic Signatures on Documents Submitted to the Courts

A. Purpose

The purpose of this section is to provide guidance on the signatures that appear on documents that are submitted electronically to the courts. For such signatures, there is currently no equivalent to the comprehensive authorization for the use of electronic signatures that exists for the signatures of judicial officers and court clerks under Government Code section 68150(g) and Code of Civil Procedure section 34. There are, however, various statutes and rules on signatures on electronically submitted documents that apply to particular types of proceedings.

B. Signatures on Documents Filed Electronically in Civil Cases

The statutes and rules on e-filing in civil cases include specific provisions on signatures. Code of Civil Procedure section 1010.6(b)(2) provides:

> (A) When a document to be filed requires the signature, not under penalty of perjury, of an attorney or a self-represented party, the document shall be deemed to have been signed by that attorney or self-represented party if filed electronically.
>
> (B) When a document to be filed requires the signature, under penalty of perjury, of any person, the document shall be deemed to have been signed by that person if filed electronically and if a printed form of the document has been signed by that person prior to, or on the same day as, the date of filing. The attorney or person filing the document represents, by the act of filing, that the declarant has complied with this section. The attorney or person filing the document shall maintain the printed form of the document bearing the original signature and make it available for review and copying upon the request of the court or any party to the action or proceeding in which it is filed.

Similarly, the California Rules of Court have a specific rule on the requirement for signatures on documents filed electronically with the court. Rule 2.257 provides:

(a) Documents signed under penalty of perjury

When a document to be filed electronically provides for a signature under penalty of perjury, the following applies:

(1) The document is deemed signed by the declarant if, before filing, the declarant has signed a printed form of the document.

(2) By electronically filing the document, the electronic filer certifies that (1) has been complied with and that the original, signed document is available for inspection and copying at the request of the court or any other party.

(3) At any time after the document is filed, any other party may serve a demand for production of the original signed document. The demand must be served on all other parties but need not be filed with the court.

(4) Within five days of service of the demand under (3), the party on whom the demand is made must make the original signed document available for inspection and copying by all other parties.

(5) At any time after the document is filed, the court may order the filing party to produce the original signed document in court for inspection and copying by the court. The order must specify the date, time, and place for the production and must be served on all parties.

(b) Documents not signed under penalty of perjury

If a document does not require a signature under penalty of perjury, the document is deemed signed by the party if the document is filed electronically.

(c) Documents requiring signatures of opposing parties

When a document to be filed electronically, such as a stipulation, requires the signatures of opposing parties, the following procedure applies:

(1) The party filing the document must obtain the signatures of all parties on a printed form of the document.

(2) The party filing the document must maintain the original, signed document and must make it available for inspection and copying as provided in (a)(2). The court and any other party may demand production of the original signed document in the manner provided in (a)(3)-(5).

(3) By electronically filing the document, the electronic filer indicates that all parties have signed the document and that the filer has the signed original in his or her possession.

(d) Digital signature

A party is not required to use a digital signature on an electronically filed document.

(e) Judicial signatures

If a document requires a signature by a court or a judicial officer, the document may be electronically signed in any manner permitted by law.

C. Signatures on Documents in Criminal and Traffic Cases

In criminal and traffic proceedings, the Legislature has authorized the use of electronic or digital signatures in particular types of matters.

1. Probable Cause Declarations for Warrants for Arrest

Penal Code section 817 addresses the procedures to be used when a peace officer submits a declaration of probable cause to obtain a warrant of arrest before criminal charges are filed.[1] These warrants are sometimes called *Ramey* warrants, referring to *People v. Ramey* (1976) 16 Cal.3d 263. (*Goodwin v. Superior Court* (2001) 90 Cal.App.4th 215, 218.) Penal Code section 817 requires the peace officer to submit a sworn statement made in writing in support of the warrant of probable cause. (Pen. Code, § 817(b).) As an alternative under Penal Code section 817(c)(2), the magistrate may take an oral statement under oath if the oral oath is made using telephone and facsimile transmission equipment, or made using telephone and electronic mail, and the following conditions are met:

(A) The oath is made during a telephone conversation with the magistrate, after which the declarant shall sign his or her declaration in support of the warrant of probable cause for arrest. The declarant's signature shall be in the form of a digital signature or electronic signature if electronic mail or computer server is used for transmission to the magistrate. The proposed warrant and all supporting declarations and attachments shall then be transmitted to the magistrate utilizing facsimile transmission equipment, electronic mail, or computer server.

[1] Penal Code section 817 does not apply to bench warrants or warrants for arrest that are sought via a criminal complaint. (Pen. Code, § 817(b); see also *id.*, §§ 740, 813.)

(B) The magistrate shall confirm with the declarant the receipt of the warrant and the supporting declarations and attachments. The magistrate shall verify that all the pages sent have been received, that all pages are legible, and that the declarant's signature, digital signature, or electronic signature is acknowledged as genuine.

(C) If the magistrate decides to issue the warrant,[2] he or she shall:

(i) Cause the warrant, supporting declarations, and attachments to be subsequently printed if those documents are received by electronic mail or computer server.

(ii) Sign the warrant. The magistrate's signature may be in the form of a digital signature or electronic signature if electronic mail or computer server is used for transmission to the magistrate.

(iii) Note on the warrant the exact date and time of the issuance of the warrant.

(iv) Indicate on the warrant that the oath of the declarant was administered orally over the telephone.

The completed warrant, as signed by the magistrate, shall be deemed to be the original warrant.

(D) The magistrate shall transmit via facsimile transmission equipment, electronic mail, or computer server, the signed warrant to the declarant who shall telephonically acknowledge its receipt. The magistrate shall then telephonically authorize the declarant to write the words "duplicate original" on the copy of the completed warrant transmitted to the declarant and this document shall be deemed to be a duplicate original warrant.

2. Probable Cause Declarations for Search Warrants: Penal Code Section 1526(b)

[The text below will need to be modified if AB 39 is enacted.]

Before issuing a search warrant, the magistrate must take the officer's affidavit in writing and cause the affidavit to be subscribed by the affiant. (Pen. Code, § 1526(a); see *Powelson v. Superior Court* (1970) 9 Cal.App.3d 357, 360–361.) As an alternative to this written affidavit, Penal Code section 1526(b)(2) authorizes the magistrate to take an oral statement under oath if the oral oath is made using telephone and facsimile transmission equipment, telephone and electronic mail, or telephone and computer server, and if the following conditions are met:

[2] The magistrate may issue the warrant, if and only if, he or she is satisfied from the declaration that there exists probable cause that the offense described in the declaration has been committed and that the defendant described in the declaration has committed the offense. (Pen. Code, § 817(a)(1).)

(A) The oath is made during a telephone conversation with the magistrate, whereafter the affiant shall sign his or her affidavit in support of the application for the search warrant. The affiant's signature shall be in the form of a digital signature or electronic signature if electronic mail or computer server is used for transmission to the magistrate. The proposed search warrant and all supporting affidavits and attachments shall then be transmitted to the magistrate utilizing facsimile transmission equipment, electronic mail, or computer server.

(B) The magistrate shall confirm with the affiant the receipt of the search warrant and the supporting affidavits and attachments. The magistrate shall verify that all the pages sent have been received, that all pages are legible, and that the affiant's signature, digital signature, or electronic signature is acknowledged as genuine.

(C) If the magistrate decides to issue the search warrant, he or she shall:

(i) Sign the warrant. The magistrate's signature may be in the form of a digital signature or electronic signature if electronic mail or computer server is used for transmission to the magistrate.

(ii) Note on the warrant the exact date and time of the issuance of the warrant.

(iii) Indicate on the warrant that the oath of the affiant was administered orally over the telephone.

The completed search warrant, as signed by the magistrate, shall be deemed to be the original warrant.

(D) The magistrate shall transmit via facsimile transmission equipment, electronic mail, or computer server, the signed search warrant to the affiant who shall telephonically acknowledge its receipt. The magistrate shall then telephonically authorize the affiant to write the words “duplicate original” on the copy of the completed search warrant transmitted to the affiant and this document shall be deemed to be a duplicate original search warrant. The duplicate original warrant and any affidavits or attachments in support thereof shall be returned as provided in Penal Code section 1534.

3. Electronic Signatures on Notices to Appear

Vehicle Code section 40500 addresses Notice to Appear for traffic violations and requires that the arresting officer prepare in triplicate a written notice to appear in court. (Veh. Code, § 40500(a); *id.* § 40600(a) [similar provisions].) The arresting officer must deliver a copy to the arrested person, a copy to the court, and a copy to the commissioner, chief of police, sheriff or other superior officer of the arresting officer. (*Id.*, §§ 40500(d), 40506.) A Notice to Appear may also be issued for non-traffic infraction and misdemeanor offenses. (Pen. Code, §§ 853.5, 853.6.)

Penal Code section 959.1(d) authorizes a court to receive and file an electronically transmitted Notice to Appear issued on a form approved by the Judicial Council if the following conditions are met:

> (1) The notice to appear is issued and transmitted by a law enforcement agency pursuant to specified Penal Code or Vehicle Code sections;
>
> (2) The court has all of the following:
>
> > (A) The ability to receive the notice to appear in electronic format.
> >
> > (B) The facility to electronically store an electronic copy and the data elements of the notice to appear for the statutory period of record retention.
> >
> > (C) The ability to reproduce the electronic copy of the notice to appear and those data elements in printed form upon demand and payment of any costs involved.
>
> (3) The issuing agency has the ability to reproduce the notice to appear in physical form upon demand and payment of any costs involved.
>
> (4) The notice to appear that is received under subdivision (d) is deemed to have been filed when it has been accepted by the court and is in the form approved by the Judicial Council.
>
> (5) If transmitted in electronic form, the notice to appear is deemed to have been signed by the defendant if it includes a digitized facsimile of the defendant's signature on the notice to appear. A notice to appear filed electronically under subdivision (d) need not be subscribed by the citing officer. An electronically submitted notice to appear need not be verified by the citing officer with a declaration under penalty of perjury if the electronic form indicates which parts of the notice are verified by that declaration and the name of the officer making the declaration.
> 853.9

A Judicial Council Notice to Appear form that is issued when a person is arrested for misdemeanor or infraction violations of the Vehicle Code or for nontraffic misdemeanors or infractions serves as a complaint. (Veh. Code § 40500(b); Pen. Code, § 853.9(b).) Under rule 4.103 of the California Rules of Court, the Judicial Council has approved the following types of Notice to Appear forms:

Form TR-115	Automated Traffic Enforcement System Notice to Appear
Form TR-130	Traffic/Nontraffic Notice to Appear
Form TR-120	Nontraffic Notice to Appear

Form TR-106	Continuation of Notice to Appear
Form TR-108	Continuation of Citation

Form TR-130 is used for both electronic and handwritten citations. (See www.courts.ca.gov/documents/trinst.pdf; Cal. Rules of Court, rule 4.103.)

6.2.3. Signatures on Scanned Documents

Government Code section 68150(a) authorizes the preservation and maintenance of trial court records in electronic form. Under this provision, trial courts may convert their paper records to electronic form by scanning. The act of scanning an original signature results in a digitized signature. This digitized signature shall have the same validity, and the same legal force and effect, as the original signature. This section applies generally to electronic signatures by parties and others on documents submitted to the courts, in addition to electronic signatures by judicial officers and courts (which are also addressed above in the standards and guidelines implementing Government Code section 68150(g).)