Recommend not using

POLICY TITLE: Digital Signature Policy
POLICY NUMBER: 1060

1060.1 Policy. It is the policy of the [DISTRICT] to accept electronic signatures affixed to documents in which a signature is required or used, provided that: (1) the electronic signatures are "digital" signatures that comply with the requirements of California Government Code Section 16.5 and applicable state regulations[1], (2) the signatories are willing and wanting to utilize digital signatures, and (3) the digital signatures are created by technologies authorized by the California Secretary of State and made available by the District. Signatories may digitally sign the following types of documents:

-
-
-
-
-
-
-
-
-
-

The use, or the District's acceptance, of a digital signature is at the option of the District and the signer(s). Nothing in this Policy requires the District to use or permit the use of a digital signature or accept the submission of a document containing a digital signature.

1060.2 Definitions.

a) "Digital Signature" means an electronic identifier, created by computer, intended by the party using it to have the same force and effect as the use of a manual signature.[2]
b) "Digital Signature Certification Authority" means an entity authorized by the Secretary of State to issue digital certificates that are required for a digital signature under California law and that is listed on the Secretary of State's "Approved List of Digital Signature Certification Authorities."
c) "Digital Signature Provider" means an entity that provides document signing services using digital technology.
d) "Electronic Signature" means 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, including a digital signature.[3]

[1] Cal. Code Regs., tit. 2, § 22000 *et seq.*
[2] Cal. Gov. Code, § 16.5(d).
[3] Cal. Civ. Code, § 1633.2(h).

1060.3 Electronic Signatures. The use of electronic signatures is authorized by two California statutes, the Uniform Electronic Transactions Act ("UETA"), codified at Civil Code Section 1633.1 *et seq.*, and Government Code Section 16.5.

The UETA provides that a signature may not be denied legal effect or enforceability solely because it is in electronic form.[4] The UETA applies a transaction only when the parties have agreed to conduct the transaction by electronic means, and whether they have agreed to do so "is determined from the context and surrounding circumstances, including the parties' conduct."[5]

Government Code Section 16.5 applies to public entities[6] such as the District, and authorizes any party to a written communication with a public entity, in which a signature is required or used, to affix a signature by use of a digital signature that complies with the requirements of Section 16.5.[7] Digital signature transactions involving public entities that are subject to the UETA are also subject to the more particular requirements of Government Code Section 16.5.[8] The use of a digital signature will have the same force and effect as the use of a manual signature if, and only if, the digital signature embodies the five attributes[9] discussed in Section 1060.4 below.

1060.4 Digital Signatures.

Government Code Section 16.5 and State regulations require that a digital signature (i) be created by a technology that is acceptable for use by the State of California and (ii) embody the following five attributes:

1) It is unique to the person using it;
2) It is capable of verification;
3) It is under the sole control of the person using it;
4) It is linked to data in such a manner that if the data are changed, the digital signature is invalidated; and
5) It conforms to regulations adopted by the Secretary of State, codified at Chapter 10 of Division 7 of Title 2 (commencing at Section 22000) of the California Code of Regulations.[10]

1060.5 Digital Signature Technologies

The Secretary of State allows public entities to utilize digital signatures that are created by one of two different technologies – "public key cryptography" and "signature dynamics" – provided that the digital signatures are also created consistent with the provisions of Section 22003 of the California Code of Regulations.

[4] Cal. Civ. Code, § 1633.7.
[5] Cal. Civ. Code, § 1633.5(b)
[6] "'Public entity' includes the state, the Regents of the University of California, the Trustees of the California State University and the California State University, a county, city, district, public authority, public agency, and any other political subdivision or public corporation in the State." Cal. Gov. Code, §§ 16.5(a) & 811.2 (emphasis added).
[7] Cal. Gov. Code, § 16.5(a).
[8] See Civ. Code, § 1633.3(e).
[9] Gov. Code, § 16.5(a).
[10] Cal. Gov. Code, § 16.5; 2 C.C.R. § 22002.

~~Public key cryptography ("PKC") is a form of cryptography that generally allows users to communicate securely. PKC signatures are affixed to documents using software enhancements to existing applications and web browsers and are capable of immediate third-party verification.~~

~~Signature dynamics uses the individual's handwritten signature. Unlike PKC signatures, signature dynamics signatures require additional hardware to create the signatures. An electronic drawing tablet and stylus are used to record the direction, speed, and coordinates of a handwritten signature – essentially, taking a snapshot of a person's signature. This type of digital signature does not offer encryption, confidentiality, or the level of security that is inherent in PKC signatures. PKC allows for third party verification of the signature by certification authorities approved by the State, while signature dynamics signatures require additional steps (including handwriting analysis) to verify the signer of a document (similar to a non-notarized, paper based signature). A formal handwriting analysis of a signature dynamics signature may be lengthy. However, some degree of certainty can be obtained by a lay comparison of manual handwritten signatures that may already be on file with the District.~~

~~The District shall only contract with digital signature providers that offer their digital signature services with a certificate issued by a digital signature certification authority. District staff shall only accept digital signatures created by PKC or signature dynamics technologies. As advised by the Secretary of State, District staff shall consider the following issues and other issues when identifying the appropriate technology to use for each document that includes a digital signature component:~~

- ~~Are the documents containing signatures going to be transmitted over an "open" or a "closed" network?~~
- ~~Does the signature on the document need to be verified?~~
- ~~How much time and resources can be allocated to verification?~~
- ~~Does the signature need to be compared to a manual signature on paper or can a digital certificate adequately provide one-stop verification?~~
- ~~Will immediate verifiability reduce the potential of fraud?~~
- ~~Will the documents containing digital signatures need to be reproduced for public access to the records?~~
- ~~Will the documents containing digital signatures need to be utilized by another local, state or federal agency? If so, is the technology compatible with the other agency's needs?~~

~~However, whenever a document requires immediate absolute verification of a signature, District staff shall only use and accept digital signatures created by the PKC technology.~~