Frequently Asked Questions

Table of Contents

What a digital signature?

Under California law, a digital signature is defined as "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."

Government Code section 16.5 states a digital signature shall have the same force and effect as a manual signature if and only if:

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.

Government Code section 16.5 also states that the use or acceptance of a digital signature is at the option of the parties to the transaction and nothing in the law requires a public entity to use or accept the submission of a document containing a digital signature.

The **regulations** adopted by the Secretary of State define the types of technologies that are acceptable for creating digital signatures for use by public entities in California. They also provide guidance to public entities that want to use digital signatures for certain transactions.

Top

What are some potential applications of the technology?

Digital signatures can be used for many transactions that currently require a hand written signature. Potential uses include on-line college applications, filing state income tax forms, and submitting applications for business permits at the local level.

Top

Who is affected by California's digital signature regulations?

Government Code section 16.5 and the **regulations** adopted by the Secretary of State affect public entities in California, which are defined by the Government Code as the State, the Regents of the University of California, a county, city, district, public authority, public agency, and any other political subdivision or public corporation in the State.

Top

We want to use digital signatures to help us computerize our employees' filing of time-cards. Where do we start?

Government Code section 16.5 specifies that the use of digital signatures shall be at the option of the parties involved in the transaction. Before beginning a transition from paper documents to

electronic ones, public entities must ensure that all the parties to the transaction are willing to use digital signatures.

These **regulations** allow public entities to utilize digital signatures that are created by one of two different technologies—"public key cryptography (PKC)" and "signature dynamics."

For a public entity to get started, the first step is to determine the amount of security necessary to conduct the transaction. Some issues to consider are:

- 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?

Answering these and countless other questions can help public entities identify the appropriate technology to use for each application that includes a digital signature component.

Top

How should we choose between a public key cryptography (PKC) system and a signature dynamics system?

PKC signatures have a greater degree of verifiability than signature dynamics signatures. PKC allows for a third party verification of the signature, while signature dynamics signatures require additional steps (including handwriting analysis) to verify the signer of a document.

PKC signatures are designed to be immediately verifiable. Signatures using signature dynamics technology are designed to allow future verification of the signature (similar to a non-notarized, paper-based signature).

PKC signatures are affixed to documents using software enhancements to existing applications and web browsers. Signature dynamics signatures require additional hardware to create the signatures.

Signature dynamics signatures are easier for the average user to understand, but they do not provide the level of security that is inherent in PKC signatures, which are immediately verifiable with a third-party issued certificate.

Public entities should conduct an extensive review of their needs and match them to the appropriate technology approved for use in the Secretary of State's approved **regulations**.

Top

Why does California permit signatures created by signature dynamics to be used?

Although signature dynamics signatures require the lengthy process of handwriting analysis to achieve certain verification of a signature, they are still "capable of verification" as required by Government Code section 16.5. Additionally, some degree of certainty can also be obtained by a lay-comparison of manual handwritten signatures, which may already be on file within a particular agency.

If a public entity needs immediate absolute verification of a signature, then this technology may not be the best option for those transactions.

Top