



ORDINANCE ADDING CHAPTER 1-06 TO THE SANTA ROSA CITY CODE AUTHORIZING THE USE OF ELECTRONIC RECORDS, ELECTRONIC SIGNATURES AND DIGITAL SIGNATURES

City Council Meeting
May 28, 2019

Eric McHenry
Chief Information Technology Officer

BACKGROUND

- In 1995, the California legislature passed a statute authorizing public entities to accept “digital signatures” with stringent verification procedures established by the Secretary of State (Gov. Code Section 16.5.).
- In 1999, California adopted a version of the Uniform Electronic Transactions Act (UETA), guaranteeing that electronic signatures would have the same legal effect as “wet” or manual signature (Civ. Code Section 1633.1-1633.17.).
- In 2016, AB 2296 was signed by Governor Brown to clarify how state government agencies can accept signatures electronically.

BACKGROUND

- AB 2296 resolved issues around perceived discrepancies in the 1990's legislation, making it easier for agencies to use electronic signature technology.
- Due to AB 2296, California government agencies can transition to the use of electronic records with clear understanding of the law.

ANALYSIS

- The use of digital signatures will enable efficiencies in citywide department processes and will reduce paper document creation.
- California's UETA provides, "if a law requires a signature, an electronic signature satisfies the law."
- "Electronic signature" is defined in the UETA 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."

ANALYSIS

- The California Government Code defines “digital signature” as “an electronic identifier, created by a computer, intended by the party using it to have the same force and effect as the use of a manual signature.
- A valid digital signature must embody the following attributes:
 - It is unique to the person using it
 - It is capable of verification
 - It is under the sole control of the person using it
 - It is linked to data in such a manner that if the data are changed, the digital signature is invalidated.
 - It conforms to regulations adopted by the Secretary of State

ANALYSIS

- If the City elects to use digital signatures, the technology that creates the signature must be acceptable to use by the State of California. At this time, there are two acceptable technologies:
 1. Public Key Cryptography
 2. Signature Dynamics
- If public key cryptography is used the signer must be capable of being issued a certificate to certify the signer controls the key pair used to create the signature.
- Public entities may only accept certificates from Certification Authorities that appear on the Secretary of State's Approved List of Certification Authorities.

ANALYSIS

- If digital signatures are used, the City must follow the following procedures:
 - Prior to accepting a digital signature, the City must ensure that the level of security used to identify the signer of a document and to transmit the signature, are sufficient for the transaction being conducted.
 - If a certificate is a required component of a digital signature transaction, the City must also ensure that the certificate format used by the signer is sufficient for the security and interoperability needs of the City.

RECOMMENDATION

It is recommended by the Information Technology Department and the City Manager's Office that the Council, by ordinance, add Chapter 1-06 to the Santa Rosa City Code authorizing the use of Electronic Records, and Electronic and Digital Signatures.