DGS **MEMORANDUM**

CONFIDENTIAL WORK PRODUCT PROTECTED BY ATTORNEY-CLIENT PRIVILEGE

Date: August 7, 2008

To: Melodie Cato
Procurement Division/E-Procurement Strategies Section
Department of General Services
Office of Legal Services

From: Shari Miura, Staff Counsel SM
Department of General Services
Office of Legal Services

Subject: **Digital Signatures Relative to E-Procurement**

Questions

You have requested an opinion as to the following questions:

(1) Are digital signatures legally binding in the context of a State web-based Electronic Procurement (E-Procurement) system?

(2) Does a user name and password method create a legally binding document?

(3) Is a signed document legally defensible if transmitted in "pdf" format?

Answers

(1) Yes. Two specific technologies are approved by the Secretary of State for accepting digital signatures: Public Key Cryptography and "Signature Dynamics." Both of these methods are appropriate for an E-Procurement system.

(2) No. A system which utilizes a user name and password is not legally equivalent to a system which utilizes digital signatures. It is our opinion that a user name and password system alone would not be sufficient to withstand legal challenge and does not meet the minimum standards for digital signature technology acceptable for use by the State.

(3) Yes. A system utilizing scanned "pdf" versions of documents may be acceptable, provided the security of the system can be verified with regard to creating and transmitting electronic documents.

Analysis

I. The Validity and Authenticity of Digital Signatures

Prior to accepting a digital signature, public entities are responsible for ensuring the level of security for identifying and transmitting the signature is sufficient, as well as ensuring the certificate format used by the signer is secure and sufficient for the transaction being conducted. (2 CCR section 22005.) A digital signature may be used with the same force and effect as the use of a manual signature only if the following elements are shown:

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;
5. It conforms to Title 2, Division 7, Chapter 10 of the California Code of Regulations, which defines the specific technologies acceptable to the State of California.

(Gov. Code section 16.5 and 2 CCR section 22002.)

A. Public Key Cryptography

A "public-key-based" cryptographic method can assure the authenticity and message integrity within the digital signature and therefore is an acceptable method for use by the State. (2 CCR section 22003.) Public Key Cryptography utilizes two different but mathematically related "keys" employing an algorithm. The "private key" is used for creating a digital signature (transforming data into a seemingly unintelligible form), while the "public key" is used to verify the digital signature (returning the message to its original form). The "private key" is known only to the signer, while the "public key" must be available to whomever the signer wishes to verify its signature.

Authentication of a signer's public key and assurance that it corresponds to the signer's public key can be problematic when the parties are corporations or entities which act through agents communicating via the Internet. A third party which can associate a signer with a specific public key can be a solution to this issue. This third party is referred to as a "Certification Authority." If a certificate of authentication is required by the public entity utilizing Public Key Cryptography, the Certification Authority must be on an approved list monitored by the Secretary of State. (2 CCR section 22003 (a) (3) (B), 2 CCR section 22003 (a) (6).)

The Certification Authority issues a certificate – an electronic record which lists a public key as the "subject" of the certificate – and confirms that the prospective signer identified in the certificate holds the corresponding private key. The Certification

Authority digitally signs the certificate, which then may start the public/private key cycle again to authenticate the Certification Authority's digital signature. The certificate may be stored in a repository to make it readily available for use in verification.

However, a certificate may prove unreliable after issuance. If the signer's private key becomes compromised, the certificate becomes unreliable, and the Certification Authority may suspend or revoke the certificate. The Certification Authority must then publish notice of the new status of the certificate.

To utilize digital signatures for e-commerce, a high degree of information security must be in place and consistently enforced to prevent compromise of private keys. Computer equipment and software utilizing private and public keys are collectively termed an "asymmetric cryptosystem." Costs are incurred for the procurement and maintenance for an asymmetric cryptosystem. In addition, establishing, utilizing, and assuring quality of performance of Certification Authorities and repositories are costs to consider, additional to the software costs for the issuance of a certificate, along with hardware to secure the private key.

B. Signature Dynamics

"Signature Dynamics" is an acceptable technology for use by public entities in California if it meets the following elements set out in 2 CCR section 22003 (b) (1)-(5): be unique to the person using it, be capable of verification, remain under the sole control of the person using it, and the signature must be linked to the message in such a way that if the data in the message is changed, the "signature digest" is invalidated. The "signature digest" is a bit-string which is produced when a handwritten signature is tied to a document using Signature Dynamics, such as by signing an electronic notepad.

The signature digest is the component of Signature Dynamics which provides verification; therefore, it must withstand the following specific elements to prove its authenticity.

1. The signature digest is unique to the person using it if it contains the following elements:

    a. it is a record of the handwriting measurements of the person signing the document;
    b. it is cryptographically bound to the handwriting measurements; and
    c. it is computationally infeasible to separate the handwriting measurements and bind them to a different signature digest.

(2 CCR section 22003 (b) (2).)

2. A signature digest is capable of verification when the following elements are present:

   a. the acceptor of the digitally-signed message can obtain the handwriting measurements for purposes of comparison, and
   b. the handwriting measurements can allow a handwriting expert to assess the authenticity of a signature.

(2 CCR section 22003 (b) (3).)

3. The signature digest must be under the sole control of the person using it. Sole control is proven if

   a. the signature digest captures the handwriting measurements and cryptographically binds them to the message directed by the signer and to no other message, and
   b. the signature digest makes it computationally infeasible for the handwriting measurements to be bound to any other message.

(2 CCR section 22003 (b) (4).)

4. The signature digest must be linked to the message in such a way that if the data is changed, the signature digest is invalidated.

(2 CCR section 22003 (b) (5).)

C. User-Name-and-Password Systems

As discussed above, only two technologies for digital signatures are accepted by the State: Public Key Cryptography and Signature Dynamics. Therefore, a system which utilizes a user name and password does not create a legally binding document for procurement and contract purposes because there is no adequate manner by which to verify and authenticate the user except through the password, which is not the legal equivalent to a signature for purposes of electronic commerce with the State.

II. Scanned "pdf" Versions of Documents

A system which utilizes "pdf" versions of signed bids or contracts may be acceptable as an electronic means of transacting business. However, as this is not a "digital signature" technology, this system is not on the list of acceptable technologies in the California Code of Regulations, section 22003. The validity of electronic records and electronic signatures is specified pursuant to Civil Code sections 1633.1 et seq. and includes specific exceptions. (Civ. Code section 1633.3.)

In a system which utilizes a "pdf" format of documents, the document is executed in hardcopy, scanned, and transmitted electronically as a "pdf" file. A record or signature may not be denied legal effect or enforceability solely because it is in electronic form. (Civ. Code section 1633.7 (a).) If a law requires a signature, an electronic signature satisfies the law. (Civ. Code section 1633.7 (d).) Assuming a "pdf" version of a document cannot be altered, an electronic record or electronic signature is acceptable if it is attributable to that person – that is, if it was the act of the person, and the act may be shown "in any manner, including a showing of the efficacy of any security procedure applied to determine the person to which the electronic record or electronic signature was attributable." (Civ. Code section 1633.9, subd. (a).)

Therefore, if the "pdf" version of a bid or contract is challenged, the security of the system used to scan and transmit the document must be able to withstand legal scrutiny. The "pdf" version of the signature of the person, like a photocopy or facsimile, should be verifiable through a handwriting expert, and the hardcopy of the document should be available for examination as well.

An *automated* system utilizing "pdf" versions of documents would not be advisable. In an automated transaction, a contract may be formed by the interaction of the electronic agents of the parties, even if no individual was aware of or reviewed the agents' actions or the resulting terms and agreements. (Civ. Code section 1633.14.) Therefore sufficient procedures should be in place for verifying and accepting "pdf" forms of documents such that the mere transmittal of the document will not form a contract without the knowledge of the State.

III. Other Options

We are not aware of any other options for the State to conduct electronic commerce or procurements aside from utilizing Public Key Cryptography or Signature Dynamics for digital signatures, or electronic transmittals by using "pdf" formats. If another technology is developed, the DGS could request a review by the Secretary of State for approval of any new technology. The Secretary of State may review any petition filed to add new technologies to the list of technologies acceptable to the State relative to digital signatures. If the Secretary of State determines the technology to be acceptable, the Secretary of State shall adopt regulations which add the proposed technology to the list of acceptable technologies in section 22003. (2 CCR section 22004.)

Conclusion

The following are three viable options to accepting signatures in digital or electronic form:

Option 1. Public Key Cryptography may be utilized wherein the bidder pays for the third-party certification verification with the Secretary of State.

Option 2. A system utilizing Signature Dynamics may be utilized if the State provides the means for bidders to sign their bid or contract document on an electronic signature pad when the document is accepted into the State's procurement or contract system, thereby verifying that document is associated with the signature and completing the document acceptance.

Option 3. A system which utilizes "pdf" versions of documents may be acceptable for bid and contract transactions if the system is not automated (thereby contracts cannot be created without requiring the State's knowledge) and if sufficient security procedures are in place to show the transmittal of the documents can be verified and authenticated. The documents must be scanned versions of hardcopies and not subject to conversion into another format where they can be altered and converted back into "pdf" form.

cc: José Aguirre, Deputy Director, OLS