SB

232

FISCAL NOTE

STATE OF ALASKA **BILL NO. CSSB232 (JUD)**

1998 LEGISLATIVE SESSION

Revision Date:

Title: Electronic Records, Record Requirements

Department: Commerce and Economic Development

BRU: Banking, Securities and Corporations

Component: Banking, Securities and Corporations

Sponsor: Sen. Parnell

Requestor: House Judiciary

COMPONENT SERIAL NO.

Expenditures/Revenues (Thousands of Dollars)

OPERATING EXPENDITURES	FY 99	FY 00	FY 01	FY02	FY 03	FY 04
PERSONAL SERVICES						
TRAVEL						
CONTRACTUAL						
SUPPLIES						
EQUIPMENT						
LAND & STRUCTURES						
GRANTS, CLAIMS						
MISCELLANEOUS						
TOTAL OPERATING	0.0	0.0	0.0	0.0	0.0	0.0
CAPITAL EXPENDITURES	0.0	0.0	0.0	0.0	0.0	0.0
CHANGE IN REVENUES	0.0	0.0	0.0	0.0	0.0	0.0

FUND SOURCE (Thousands of Dollars)

1002 Federal Receipts						
1003 GF Match						
1004 General Fund						
1005 GF/Program Receipts						
1006 GF/Mental Health						
Other						
TOTAL	0.0	0.0	0.0	0.0	0.0	0.0

Estimate of any current year (FY 98) cost: $ 0.0

POSITIONS

FULL-TIME						
PART-TIME						
TEMPORARY						

ANALYSIS: (Attach a separate page if necessary)

Prepared by: Willis F. Kirkpatrick, Director Phone: 465-2521

Division: Banking, Securities and Corporations Date:

Approved by Commissioner: Deborah B. Sedwick Date: 5/5/98

Agency: Commerce and Economic Development

PREPARER TO PROVIDE ALL DISTRIBUTION COPIES TO GOVERNOR'S LEGISLATIVE OFFICE

For further distribution information, call the Governor's Legislative Office

FISCAL NOTE

STATE OF ALASKA **BILL NO. CSSB232 (JUD)**

1998 LEGISLATIVE SESSION

Revision Date:

Department: Commerce and Economic Development

Title: Electronic Records, Record Requirements

BRU: Banking, Securities and Corporations

Component: Banking, Securities and Corporations

Sponsor: Sen. Parnell

Requestor: House Judiciary

COMPONENT SERIAL NO.

Expenditures/Revenues (Thousands of Dollars)

OPERATING EXPENDITURES	FY 99	FY 00	FY 01	FY02	FY 03	FY 04
PERSONAL SERVICES						
TRAVEL						
CONTRACTUAL						
SUPPLIES						
EQUIPMENT						
LAND & STRUCTURES						
GRANTS, CLAIMS						
MISCELLANEOUS						
TOTAL OPERATING	0.0	0.0	0.0	0.0	0.0	0.0
CAPITAL EXPENDITURES	0.0	0.0	0.0	0.0	0.0	0.0
CHANGE IN REVENUES	0.0	0.0	0.0	0.0	0.0	0.0

FUND SOURCE (Thousands of Dollars)

1002 Federal Receipts						
1003 GF Match						
1004 General Fund						
1005 GF/Program Receipts						
1006 GF/Mental Health						
Other						
TOTAL	0.0	0.0	0.0	0.0	0.0	0.0

Estimate of any current year (FY 98) cost: $ 0.0

POSITIONS

FULL-TIME						
PART-TIME						
TEMPORARY						

ANALYSIS: (Attach a separate page if necessary)

Prepared by: Willis F. Kirkpatrick, Director Phone: 465-2521

Division: Banking, Securities and Corporations Date:

Approved by Commissioner: Deborah B. Sedwick Date: 5/5/98

Agency: Commerce and Economic Development

PREPARER TO PROVIDE ALL DISTRIBUTION COPIES TO GOVERNOR'S LEGISLATIVE OFFICE

For further distribution information, call the Governor's Legislative Office

SB 232
Bill Summary/Sectional Analysis

Bill Summary:

This bill makes electronic signatures legal in our state. It will help bring the state of Alaska and the businesses that operate here into the electronic age - allowing business and government to conduct business electronically with counterparts in Alaska, other states and other countries.

The various sections accomplish the following:

1. Declare that the use of electronic signatures in Alaska between consenting parties is legal. Electronic signatures would have the same legal standing as a standard signature from an individual.
2. Allow state agencies to promulgate regulations for using electronic signatures in their interactions with the public.
3. Define various terms relating to electronic signatures.
4. Repeals for some state agencies selected notarization requirements that could hinder an agency's ability to implement the use of electronic signatures.

By making electronic signatures legal, the bill provides an opportunity for state agencies to better serve the public "online." State government will be able to serve citizens participating in the new world of electronic commerce.

This bill has the support of the Telecommunications Information Council. It is modeled on the Georgia State Act, which is considered one of the foremost electronic signature laws in the United States.

Sectional Analysis

Section 1: Removes the requirement that reports filed by banks with the Department of Commerce and Economic Development be verified by a notary and replaces it with a requirement for signature under penalty of unsworn falsification.

Section 2: Specifies that information in state records that would compromise the security of an electronic signature is an "exception" from the state public records statute.

Section 3: Accomplishes the following:

1. Articulates the purposes of electronic signatures, such as facilitating government business and private commerce and promoting electronic government and commerce.

Digital Signature Tutorial

The authentication of computer-based business information interrelates both technology and the law, and calls for cooperation between people of different professional backgrounds and areas of expertise. Each field of expertise brings to the topic of authentication a different repertoire of concepts. Often the concepts from the information security field correspond only loosely to concepts from the legal field, even though both fields apply the same term to their differing concepts.

This interdisciplinary contrast exists even for basic, central concepts such as "authentication" or "digital signature". From a technical point of view, "digital signature" means the result of applying to specific information the technical processes described below. From a legal point of view, handwriting one's name on paper has been the principal means of signature for centuries. In addition, the legal concept of signature recognizes, in many cases, not only a handwritten name but any mark made with the intention of authenticating the marked document.fn.1 In an electronic setting, today's broad legal concept of "signature" may well include markings such as digitized images of paper signatures, typed notations such as "s/John Smith", or even addressing notations such as letterheads, electronic mail origination headers, and the like. From an information security viewpoint, these simple electronic signatures are entirely different from the "digital signatures" described in this tutorial and in technical documents, although "digital signature" is sometimes used colloquially or in some legal writing to mean another or any form of computer-based signature. To avoid confusion, this publication uses "digital signature" only in the sense in which the term is used in information security terminology, as meaning the result of applying the technical processes described in this tutorial.

The differences between digital signatures and other electronic signatures are significant, not only in terms of process and result, but also because those differences make digital signatures more serviceable for legal purposes. However, some electronic signatures, though perhaps legally recognizable as signatures, may not be as secure as digital signatures, and may lead to uncertainty and disputes.

To understand why digital signatures serve well in legal applications, this tutorial begins with an overview of the significance of signatures in legal transactions. It then explains digital signature technology in simple terms, and examines how, with some legal and institutional infrastructure, digital signature technology can be applied as a computer-based alternative to traditional signatures.

Signatures and the Law

A signature is not part of the substance of a transaction, but rather of its representation or form. Parties often represent their transactions in signed writings. Signing writings and other formalistic legal processes or customs serve the following general purposes: fn.2

- **Evidence**: A signature identifies the signer with the signed document; by signing, the signer marks the text in her own unique way and makes it attributable to her. fn.3
- **Ceremony**: Signing calls to the signer's attention the legal significance of his act, and thereby helps prevent "inconsiderate engagements". fn.4 The act of signing may satisfy a human desire to mark an event. fn.5
- **Approval**: In certain contexts defined by law or custom, a signature expresses the signer's approval or authorization of the writing, or the signer's intention that it have legal effect. fn.6
- **Efficiency and logistics**: A signature on a written memorandum often imparts a sense of clarity and finality to the transaction, especially if the signature is used to indicate approval or authorization. Because of this apparent clarity and finality, signatures may lessen the need to inquire beyond the face of a document, fn.7 and, at face value, a document may be processed more efficiently and with less risk than a document beneath which traps for the unwary may lie. Negotiable instruments, for example, attain their ability to change hands with ease, rapidity, and minimal interruption through legal rules triggered by compliance with certain formal requirements including a signature. fn.8 Furthermore, the finality of signing makes it useful as a decisive point

in staging how a transaction takes effect.

Although achieving these purposes is salutary, legal systems vary, both among themselves and over time, in the degree to which a particular form, including one or more signatures, is required for a legal transaction. If a particular form is required, legal systems also vary in prescribing consequences for failure to cast the transaction in the required form. The statute of frauds of the common law tradition, for example, requires a signature, but does not render a transaction invalid for lack of one. Rather, it makes it unenforceable in court, fn.9 and the persistent notion that the underlying transaction remained valid led case law to greatly limit the practical application of the statute.

In general, the trend in most legal systems for at least this century has been toward reducing formal requirements in law, fn.10 or toward minimizing the consequences of failure to satisfy formal requirements. Nevertheless, sound practice remains to formalize a transaction in a manner that best assures the parties of its validity and enforceability. fn.11 In current practice, that formalization usually entails documenting the transaction and signing or authenticating the documentation.

However, the centuries-old means of documenting transactions and creating signatures are changing fundamentally. Documents continue to be written on paper, but sometimes merely to satisfy the need for a legally recognized form. In many instances, the information exchanged to effect a transaction never takes paper form. It also no longer moves as paper does; it is not physically carried from place to place but rather streams along digital conduits at a speed impossible for paper. The computer-based information is also utilized differently than its paper counterpart. Paper documents can be read efficiently only by human eyes, but computers can also read digital information and take programmable actions based on the information.

The law has only begun to adapt to the new technological forms. The basic nature of the transaction has not changed; however, the transaction's form, the means by which it is represented and effected, is changing. Formal requirements in law need to be updated accordingly. The legal and business communities need to develop and adopt rules and practices which recognize in the new, computer-based technology the effects achieved or desired from the paper forms.

To achieve the basic purposes of signatures outlined above, the following effects are needed: fn.12

- **Signer authentication**: To provide good evidence of who participated in a transaction, a signature should indicate by whom a document or message is signed and be difficult for any other person to produce without authorization.
- **Document authentication**: To provide good evidence of the substance of the transaction, a signature should identify what is signed, fn.13 and make it impracticable to falsify or alter, without detection, either the signed matter or the signature. fn.14
- **Affirmative act**: To serve the ceremonial and approval functions of a signature, a person should be able to create a signature to mark an event, indicate approval and authorization, and establish the sense of having legally consummated a transaction.
- **Efficiency**: Optimally, a signature and its creation and verification processes should provide the greatest possible assurance of authenticity and validity with the least possible expenditure of resources.

The concepts of signer authentication and document authentication comprise what is often called "nonrepudiation service" in technical documents. The nonrepudiation service of information security "provides proof of the origin or delivery of data in order to protect the sender against false denial by the recipient that the data has been received, or to protect the recipient against false denial by the sender that the data has been sent." fn.15 In other words, a nonrepudiation service provides evidence fn.16 to prevent a person from unilaterally modifying or terminating her legal obligations arising out of a transaction effected by computer-based means.

Digital signature technology generally surpasses paper technology in yielding these desired effects. fn.17 To understand why, one must first understand how digital signature technology works.

How Digital Signature Technology Works

Digital signatures are created and verified by means of cryptography, the branch of applied mathematics that concerns itself with transforming messages into seemingly unintelligible forms and back again. For digital signatures, two different keys are generally used, one for creating a digital signature or transforming data into a seemingly unintelligible form, and another key for verifying a digital signature or returning the message to its original form. fn.18 Computer equipment and software utilizing two such keys is often termed an "**asymmetric cryptosystem**".

The keys of an asymmetric cryptosystem for digital signatures are termed the **private key**, which is known only to the signer fn.19 and used to create the digital signature, and the **public key**, which is ordinarily more widely known and is used to verify the digital signature. A recipient must have the corresponding public key in order to verify that a digital signature is the signer's. If many people need to verify the signer's digital signatures, the public key must be distributed to all of them, perhaps by publication in an on-line repository or directory where they can easily obtain it.

Although the keys fn.20 of the pair are mathematically related, it is XE "Computational infeasibility:deriving private key from public"computationally infeasible fn.21 to derive one key from the other, if the asymmetric cryptosystem has been designed and implemented securely for digital signatures. fn.22 Although many people will know the public key of a given signer and use it to verify that signer's signatures, they cannot discover that signer's private key and use it to forge digital signatures.

Use of digital signatures is comprised of two processes, one performed by the signer and the other by the receiver of the digital signature:

- **Digital signature creation** is the process of the computing a code derived from and unique to both the signed message and a given private key. For that code or digital signature to be secure, there must be at most only a negligible chance that the same digital signature could be created by any other message or private key. fn.23
- **Digital signature verification** is the process of checking the digital signature by reference to the original message and a public key, and thereby determining whether the digital signature was created for that same message using the private key that corresponds to the referenced public key.

A more fundamental process, termed a "**hash function**" fn.24 in computer jargon, is used in both creating and verifying a digital signature. A hash function creates in effect a digital freeze frame of the message, a code usually much smaller than the message but nevertheless unique to it. fn.25 If the message changes, the hash result of the message will invariably fn.26 be different. Hash functions enable the software for creating digital signatures to operate on smaller and predictable amounts of data, while still providing a strong evidentiary correlation to the original message content.

As illustrated in figure 1, to sign a document or any other item of information, the signer first delimits precisely what is to be signed. The delimited information to be signed is termed the "**message**" in the ABA Guidelines and Utah Act. Then a hash function in the signer's software computes a hash result, a code unique to the message. The signer's software then transforms the hash result into a digital signature by reference to the signer's private key. This transformation is sometimes described as "encryption". The resulting digital signature is thus unique to both the message and the private key used to create it.

Typically, a digital signature is attached to its message and stored or transmitted with its message. However, it may also be sent or stored as a separate data element, so long as it maintains a reliable association with its message. Since a digital signature is unique to its message, it is useless if wholly dissociated from its message.

Verification of a digital signature, as illustrated in Figure 2, is accomplished by computing a new hash result of the original message by means of the same hash function used in creating the digital signature.

Then, using the public key, the verifier checks whether the digital signature was created using the corresponding private key, and whether the newly computed hash result matches the hash result derived from the digital signature. If the signer's private key was used and the hash results are identical, then the digital signature is verified. Verification thus indicates (1) that the digital signature was created using the signer's private key, because only the signer's public key will verify a digital signature created with the signer's private key, fn.27 and (2) that the message was not altered since it was signed, because the hash result computed in verification matches the hash result from the digital signature, which was computed when the message was digitally signed.

Various asymmetric cryptosystems create and verify digital signatures using different mathematical formulas and procedures, but all share this overall operational pattern.

The processes of creating a digital signature and verifying it accomplish the essential effects desired of a signature:

- **Signer authentication**: If a public and private key pair is associated with an identified signer as described below, a digital signature by the private key effectively identifies the signer with the message. The digital signature cannot be forged by a person other than the proper signer, unless the proper signer loses control of the private key, such as by divulging it or losing a computer-readable card and its associated personal identification number (PIN) or pass phrase.fn.28
- **Message authentication**: The process of digitally signing also identifies the matter to be signed, typically with far greater certainty and precision than paper signatures. Verification also reveals any tampering with the message, since processing the hash results (one made at signing and the other made at verifying) discloses whether the message is the same as when signed.
- **Affirmative act**: Creating a digital signature requires the signer to provide her private key and invoke a software function to create a digital signature. This act can be the basis of a ceremony and can be used in staging the completion of a transaction. fn.29
- **Efficiency**: The processes of creating and verifying a digital signature provide a high level of assurance that the digital signature is genuinely the signer's and are almost entirely automated or capable of automation. They can be set up to run with great speed and accuracy, with human interaction only for non-routine processing decisions. Compared to paper methods such as checking bank signature cards, methods so impracticable that they are rarely actually used, digital signatures yield a high degree of assurance without adding greatly to the resources required for processing.

The core of the programs used for digital signatures have undergone thorough peer review, and an extensive scientific and technical literature underlies them. Digital signatures have been accepted in several national and international standards developed in cooperation with and accepted by many corporations, banks, and government agencies. The likelihood of malfunction or a security problem in a digital signature cryptosystem designed and implemented as prescribed in the industry standards is extremely remote, and far less than the risk of undetected forgery or alteration on paper or of using other less secure electronic signature techniques.

Public Key Certificates

To verify a digital signature, the verifier must obtain a public key and have assurance that that public key corresponds to the signer's private key. However, a public and private key pair has no intrinsic association with any person; it is simply a pair of numbers. The association between a particular person and key pair must be made by people using the fact-finding capabilities of their senses.

In a transaction involving two parties, for example, the parties could bilaterally identify each other with the key pair each party will use, but making such an identification is no small task, especially when the parties are geographically distant from each other, communicate over an open, insecure information

network, are not natural persons but rather corporations or similar artificial entities, and act through agents whose authority must be ascertained. Since reliably identifying a remote party involves considerable effort, establishing a remote party's digital signature capability specially for each of many transactions is inefficient. Instead, a prospective digital signer will often wish to identify itself with a key pair and reuse that identification in multiple transactions over a period of time.

To that end, a prospective signer could issue a statement such as: "Signatures verifiable by the following public key are mine". However, others doing business with the signer may well be unwilling to take the signer's own purported word for its identification with the key pair. Especially for electronic transactions made over worldwide information networks rather than face to face, a party would run a great risk of dealing with a phantom or an impostor, or of facing a disavowal of a digital signature by claiming it to be the work of an impostor, particularly if a transaction proves disadvantageous for the purported signer. To assure that each party is indeed identified with a particular key pair, one or more third parties trusted by both of the others must associate an identified person on one end of the transaction with the key pair creating the digital signature received at the other end, and vice versa. That trusted third party is termed a "**certification authority**" in the ABA Guidelines, the Utah Act, and most technical standards.

To associate a key pair with a prospective signer, a certification authority issues a certificate, an electronic record that sets forth a public key and represents that the prospective signer identified in the certificate holds the corresponding private key. That prospective signer is termed the "subscriber". Thus, a certificate's principal function is to identify a key pair with a subscriber, so that a person verifying a digital signature by the public key listed in the certificate can have assurance that the corresponding private key is held by the subscriber also listed in the certificate.

To assure the authenticity and inviolability of the certificate, the certification authority digitally signs it. The issuing certification authority's digital signature on the certificate can be verified using the public key listed in another certificate, and that other certificate can be verified by the public key listed in yet another certificate, and so on, until the person relying on the digital signature is adequately assured of its genuineness.

To make a public key and its identification with a specific subscriber readily available for use in verification, the certificate may be published in a repository. Repositories are on-line databases of certificates available for retrieval and use in verifying digital signatures. Often, retrieval is accomplished automatically by having the verification program inquire of the repository to obtain certificates as needed.

Once issued, a certificate may prove to be unreliable, such as in situations where the subscriber misrepresents his identity to the certification authority. In other situations, a certificate may be reliable enough when issued but come to be unreliable sometime thereafter. For example, if the subscriber loses control of the private key, the certificate becomes unreliable, since digital signatures created by the lost private key would appear to be the subscriber's according to the certificate. In such situations where the certificate has become unreliable, the certification authority, perhaps at the subscriber's request, may suspend (temporarily invalidate) or revoke (permanently invalidate) the certificate. Immediately upon suspending or revoking a certificate, the certification authority must publish notice of the revocation or suspension, or at least notify persons who inquire or who are known to have received a digital signature verifiable by reference to the unreliable certificate.

Challenges and Opportunities

The prospect of fully implementing digital signatures in general commerce presents both advantages and disadvantages, or benefits and costs. The costs or disadvantages consist mainly of:

- **Institutional overhead**: The cost of establishing and utilizing certification authorities, repositories, and other important services, as well as assuring quality in the performance of their

functions through means such as professional accreditation, oversight by another, superior certification authority, fn.30 licensing and governmental regulation, periodic auditing, or legal and financial responsibility for errors and omissions.

- **Product cost**: A digital signer will require software that may well be more expensive than a simple pen, and may probably also have to pay a certification authority to issue a certificate. Equipment to secure one's private key may also be advisable. Recipients of digital signatures will incur expenses for verification software and perhaps for access to certificates in a repository.

On the plus side, the principal advantage to be gained is more reliable authentication of messages. Digital signatures, if properly implemented and utilized:

- **Impostors**: Minimize the risk of dealing with impostors or persons who can escape responsibility by claiming to have been impersonated.
- **Message corruption**: Minimize the risk of tampering with messages, altering the terms of a transaction and covering up the traces of the alteration, or false claims that a message was altered after it was sent.
- **Formal legal requirements**: Strengthen the support for concluding that legal requirements of form, such as writing, signature, and an original document, are satisfied, since digital signatures are functionally on a par with or superior to paper forms.
- **Open systems**: Retain a high degree of information security, even for information sent over open, insecure, but inexpensive and widely used communication channels.

Considering the alternatives, such as paper signatures, computerized images of handwritten signatures, or typed signatures such as "s/John Smith", the benefits of digital signatures outweigh their burdens. The ABA Guidelines and Utah Act are intended to advance legal recognition of digital signatures and establish an institutional infrastructure to support digital authentication.

Notes

Note 1

See, e.g., Uniform Commercial Code § 1-201(39) (1992).

Note 2

This list is not exhaustive. For example, Restatement (Second) of Contracts notes another function, termed the "deterrent function", which seeks to "discourage transactions of doubtful utility. Restatement (Second) of Contracts § 72 comment c (1981). Professor Perillo also notes, in an especially comprehensive list, earmarking of intent, clarification, managerial efficiency, publicity, education, as well as taxation and regulation as functions as served by the statute of frauds. Joseph M. Perillo, The Statute of Frauds in the Light of the Functions and Dysfunctions of Form, 43 Fordham L. Rev. 39, 48-64 (1974) (hereinafter "Perillo").

Note 3

Restatement (Second) of Contracts, statutory note preceding § 110 (1982) (purpose of the statute of frauds, which includes a signature requirement); Lon L. Fuller, Consideration and Form, 41 Colum. L. Rev. 799, 800 (1941) (hereinafter "Fuller"); Jeremy Bentham, The Works of Jeremy Bentham 508-85 (Bowring ed. 1839) (Bentham called forms serving evidentiary functions "preappointed [i.e., made in advance] evidence"). A handwritten signature creates probative evidence in part because of the chemical properties of ink that make it adhere to paper, and because handwriting style is quite unique to the signer; Perillo at 64-69.

Note 4

2 John Austin, Lectures on Jurisprudence 939-44 (4th ed. 1873); Restatement (Second) of Contracts § 72 comment c (1982) and statutory note preceding § 110 (1982) (what is here termed a "ceremonial" function is termed a "cautionary" function in the Restatement); Perillo at 53-56; Fuller at 800; Rudolf von Jhering, Geist des römischen Rechts § 45 at 494-98 (8th ed. 1883) (hereinafter "Jhering").

Note 5

Frequently Asked Questions Regarding Digital Signatures

What are Digital Signatures?

A reliable electronic means of signing electronic documents that provides sender authentication, message integrity and non-repudiation. A digital signature is a convenient, time-saving, and secure way of signing electronic documents.

What is an electronic document?

An electronic document is any document that is generated or stored on a computer, such as a letter, a contract, or a will. In addition, an electronic document can be an image, such as a blueprint, a survey plat, a drawing, or even a photograph. A digital signature can be used to sign all these documents

What does a digital signature look like?

A signature looks like a random series of numbers, letters and symbols. Each signature is unique and by using the appropriate public key, each signsature can be linked back to the sender of the message.

----------BEGIN SIGNATURE----------

ivb1aWubmvsIa5qycUmFGnyJAQFAKgL/ZkBfbeNEsbthba4BlrcnjaqbckgNv+a5kr4537y8
Rcd+RDv56yYh5ttieufljlk4kjlj3ojljkjljlkj67NSjliujoj6AAcjawuJLKdk21Vkm+qymC2hRbh+Rb2h5WI

----------END SIGNATURE---------

How do they work?

In simplest terms, the digital signature software does all the work for you. The software will prompt you to follow the commands and will automatically generate a key pair for you. Once your key pair is generated you simply identify the electronic document you want digitally signed and you simply hit the sign prompt. The new file that is created is the digitally signed electronic document that you can then send to anyone. The receiver of the electronic document then can verify your signature using interoperable digital signature software. If the electronic document was altered in any manner in transmission, it will not verify.

How are they used?

Digital signatures are used for any electronic document that requires sender authenticity, message integrity, and non-repudiation (can't say you never sent the document or its contents). It is a secure form of transacting. Contracts, images, letters, etc., may be digitally signed and sent electronically in seconds. Examples of specific applications in Utah: Court Filings, Corporate Filings, UCC Filings, Procurement, Grant Applications, Motor Vehicle Titling, Real Estate Transactions, and etc.

Where do I get one? How do I register with a Certifying Authority?

You can purchase digital signature software at your local computer and software retailer. Once you have generated your key pairs via your digital signature software, you need to link your corresponding key pairs with your identity. To do this you need to contact a licensed certification authority who will verify your corresponding key pairs and your identity. Thereafter, certification authority will issue you a certificate certifying that you are who you say you are and that the correspond key pairs belong to you. This certificate will then be publish at the certification authorities on-line repository for relying parties to verify your digital signature.

The approved Certifying Authorities are:

Utah Digital Signature Trust, One So. Main, Salt Lake City, Utah 84111 (801) 524-8671

How am I identified as the signer?

When you use your digital signature software, you create a matched pair of keys. One is the private key, which is used only by you and is required during the signing process.

The second key is the public key, which is available for use by anyone wanting to authenticate the electronic documents you sign. The public key will read the digital signature created by the private key and verify the authenticity of the electronic documents created with it.

What will this cost me?

Depending on what type of digital signature software you decide to purchase, it will cost approximately $150. However, if an individual chooses not to purchase the digital signature software to generate their own key pairs, then your local licensed certification authority can provide that service at a nominal fee ranging anywhere from $10-$30. To obtain a certificate from a certification authority will also be a nominal fee ranging anywhere from $20-$50. Normally, the certificate will be valid for a period of one year. Thereafter, an individual could use their digitally signature to sign an infinite number of electronic documents during the validity period of the certificate.

Do I have to register with a CA?

No. However, it is recommended. In Utah, in order for your digital signature to be self-authenticating and obtain the benefits of the Utah Digital Signature Act, a digital signature must be verified through a valid certificate issued by a Utah licensed certification authority. However, this does not preclude a digital signature that has not been verified through a valid certificate issued by a Utah licensed certification authority, from satisfying the signature requirement. In those circumstances, the burden of proof in a court of law is very similar to that required for a handwritten signature. Consequently, a digital signature verified through a valid certificate issued by a Utah licensed certification authority will be self-authenticating and much easier to prove in a court of law.

SENATE COMMITTEE REPORT

DATE: 4/1/98

FURTHER:

DATE TURNED IN TO OFFICE: 4-21-98

Judiciary Committee considered SENATE BILL NO. 232

"An Act relating to electronic signatures, electronic records, requirements for records, and the reproduction of public records."

and recommends:

[X] be **replaced** with ____ CS FOR SENATE BILL (JUD)

[ ] adopt **previous** ____ CS ____( )

[ ] attached amendment(s)

[ ] adopt Letter of Intent by ____ Committee

[ ] further referral to the ____ Committee

Senate Bill:
[ ] same title
[ ] new title

House Bill:
[ ] same title
[ ] technical title
[ ] new: SCR#____

SIGNING DO PASS	DP	OTHER RECOMMENDATIONS	NR	DNP	AM
Jean Ramell	✓				
Mike Miller	✓				
Pearce	✓				
CHAIR: Adrian L. Taylor	✓	CHAIR:			

NEW FISCAL NOTE(S):

Department	Date	Zero	Fiscal

PREVIOUS FISCAL NOTE(S):*

Department	Date	Zero	Fiscal
ALL STATE AGENCIES	4-1-98	✓	

[ ] **APPROPRIATION -- no fiscal note**

***include fiscal notes accompanying Governor's bill**

STATE OF ALASKA

DEPARTMENT OF COMMERCE AND ECONOMIC DEVELOPMENT

DIVISION OF BANKING, SECURITIES AND CORPORATIONS

TONY KNOWLES, GOVERNOR

P.O. BOX 110807
JUNEAU, ALASKA 99811-0807
Banking & Securities (907) 465-2521
Corporation Section (907) 465-2530
E-Mail: DBSC@commerce.state.ak.us
Web Site: http://www.state.ak.us/bsc/bsc.htm

ANCHORAGE
Corporation Information (907) 269-8140
TDD: (907) 465-5437

April 20, 1998

The Honorable Robin L. Taylor
Alaska State Senate
State Capitol, Room 30
Juneau, AK 99801-1182

Dear Senator Taylor:

The division supports SB 232. There are 33 states that have adopted some form of legislation relating to electronic or digital signatures. They are Arizona, California, Connecticut, Delaware, Florida, Georgia, Hawaii, Illinois, Indiana, Iowa, Kansas, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Montana, Nebraska, Nevada, New Hampshire, New Mexico, New York, Oklahoma, Oregon, Rhode Island, Texas, Utah, Vermont, Virginia, Washington, and Wyoming. We believe that this legislation is necessary to allow Alaska businesses and government agencies to take advantage of technological advances in electronic commerce.

SB 232 removes statutory barriers to electronic commerce, provides legal recognition to electronic or digital signatures used in commerce, provides legal recognition for retention and retrieval of information in electronic media, and allows state agencies to adopt regulations necessary to verify authenticity of electronic signatures.

Sincerely,

Willis F. Kirkpatrick
Director

WFK/mme618wfk.doc
042098a

08-H14LH

FISCAL NOTE

STATE OF ALASKA **BILL NO. SB232**

1998 LEGISLATIVE SESSION

Revision Date:

Department: Commerce and Economic Development

Title: Electronic Records; Record Requirements

BRU: Banking, Securities and Corporations

Component: Banking, Securities and Corporations

Sponsor: Sen. Parnell

Requestor: Senate Judiciary

COMPONENT SERIAL NO.

Expenditures/Revenues (Thousands of Dollars)

OPERATING EXPENDITURES	FY 99	FY 00	FY 01	FY02	FY 03	FY 04
PERSONAL SERVICES						
TRAVEL						
CONTRACTUAL						
SUPPLIES						
EQUIPMENT						
LAND & STRUCTURES						
GRANTS, CLAIMS						
MISCELLANEOUS						
TOTAL OPERATING	0.0	0.0	0.0	0.0	0.0	0.0
CAPITAL EXPENDITURES	0.0	0.0	0.0	0.0	0.0	0.0
CHANGE IN REVENUES	0.0	0.0	0.0	0.0	0.0	0.0

FUND SOURCE (Thousands of Dollars)

1002 Federal Receipts						
1003 GF Match						
1004 General Fund						
1005 GF/Program Receipts						
1006 GF/Mental Health						
Other						
TOTAL	0.0	0.0	0.0	0.0	0.0	0.0

Estimate of any current year (FY 98) cost: $ 0.0

POSITIONS

FULL-TIME						
PART-TIME						
TEMPORARY						

ANALYSIS: (Attach a separate page if necessary)

Prepared by: Willis F. Kirkpatrick, Director Phone: 465-2521

Division: Banking, Securities and Corporations Date: 4-20-98

Approved by Commissioner: Deborah B. Sedwick Date:

Agency: Commerce and Economic Development

PREPARER TO PROVIDE ALL DISTRIBUTION COPIES TO GOVERNOR'S LEGISLATIVE OFFICE

For further distribution information, call the Governor's Legislative Office