Approved: 3/6/97
Date

MINUTES OF THE HOUSE COMMITTEE ON JUDICIARY.

The meeting was called to order by Chairperson Tim Carmody at 3:30 p.m.. on February 5, 1997 in Room 313--S of the Capitol.

All members were present except: Representative Kline (excused)

Committee staff present: Jerry Ann Donaldson, Legislative Research Department
Mike Heim, Legislative Research Department
Jill Wolters, Revisor of Statutes
Jan Brasher, Committee Secretary

Conferees appearing before the committee: Kyle Smith, KBI
Representative Morrison
Fred Boesch, Chief Information Architect for the State of Kansas
Janet Chubb, Assistant Secretary of State
Joe Barron, General Counsel for the Board of Regents
Matthew Goddard, Heartland Communtiy Bankers Association
Don Houlihan, Information Network of Kansas

Others attending: See attached list

The Chair called the meeting to order at 3:40 p.m.

HB 2058: **Revision of statutes relating to computer crime and making false information.**

Kyle Smith, KBI testified in support of **HB 2058**. The conferee stated that during a meeting of various state agencies concerns were raised about the adequacy of the existing statute concerning computer crimes. The conferee offered some amendments. One change proposed by the conferee was to drop the sentencing structure based on dollar amount and treat computer crime much like making a false writing (K.S.A. 21-3711) and cover actions besides mere theft. The conferee requested striking all references to the dollar amounts and make a violation a non-person felony. The conferee suggested striking "or attempting to access" because that phrase is more properly covered under a new computer trespass crime . The conferee cited a case, *State v. Rios*, and suggested that the phrase "impair the detection of a theft or felony offense" be included after the word "defraud" in line 2, page 1, to cover those situations where a person alters written instructions or electronic data to either cover up a prior theft or obscure or prevent the detection of some other serious criminal activity. The conferee proposed adding computer crime to the Standard Asset Seizure and Forfeiture Act. (Attachment 1)

The Chair stated that there were no opponents listed to testify on **HB 2058** and opened the hearings on **HB 2059**.

HB 2059: **Kansas Digital Signature Act.**

Representative Morrison testified in favor of **HB 2059**. The conferee pointed out to the Committee members that an increasing amount of private communications are being routed through electronic channels. The conferee stated that using envelopes when sending private paper documents is similar to sending encrypted e-mail messages. The conferee explained the need for encryption as electronic mail is replacing conventional paper. The conferee discussed the use of "private" and "public" keys in that medium. Representative Morrison explained some elements of public key cryptosystems. The conferee discussed the application of encryption for historical documents. The conferee stated that this technology is used in foreign trade. (Attachment 2 and Attachment 3) The conferee referred to a balloon containing amendments. One of the amendments would make the use of this technology optional.

Fred Boesch, Chief Information Architect for the State of Kansas, testified in support of **HB 2059**. The conferee stated that the concept and use of digital signatures to authenticate electronic transactions and documents are relatively new and commercial practices are still evolving. The conferee pointed out that

Unless specifically noted, the individual remarks recorded herein have not been transcribed verbatim. Individual remarks as reported herein have not been submitted to the individuals appearing before the committee for editing or corrections.

businesses have been using electronic commerce for a number of years. The conferee stated that the state of Kansas needs to establish legislation which enables the use of digital signatures. This technology is in direct support of electronic commerce, a capability which will allow Kansas individuals and businesses to participate in the global economy. The conferee outlined the authority the Secretary of State's Office will have under this bill. The conferee stated that **HB 2059** will provide legal protection for Kansas clients of digital signature services. (Attachment 4)

The Committee members and conferee discussed laws enacted in other states.

Janet Chubb, Assistant Secretary of State, testified in support of **HB 2059.** Ms Chubb stated that **HB 2059** grants broad administrative and regulatory powers to the Secretary of State. (Attachment5)

The conferee stated that her office has several simple amendments which appear on the balloon. (Attachment 6)

The Committee members discussed with the conferee the regulatory authority granted by this bill for the Secretary of States Office. The conferee stated that this legislation was purposely made broad to allow for flexibility. The conferee and Committee members discussed the possibility of bonding digital signature repositories established in Kansas.

In response to the Chair's question regarding the creation of authority in the Secretary of State's office, the conferee stated that the scope of this legislation will create regulatory powers not currently held by that office. Ms Chubb stated that the Secretary of State's office acts as a service agency for corporations in Kansas. In response to a Committee member's question, Ms Chubb related that the experience of the Secretary of State's office with licensing has been with the Kansas Athletic Agent Act.

The Committee members and the conferee discussed the use of a private verification agencies and the qualifications of the Secretary of State's office in verification of authenticity of the electronic key(s) used as a digital signature. The conferee stated that this bill still allows non-licensed certification authorities to provide keys to Kansas residents. The conferee discussed the system for repository providers to be licensed The Committee members discussed with Ms Chubb recovery of costs of implementing this function. Issues concerning the state's liability exposure were discussed. Issues concerning consumer protection were discussed.

Joe Barron, General Counsel for the Board of Regents testified in support of **HB 2059**. The conferee stated that the Regents universities had some questions concerning whether this bill was broad enough to cover the use of digital signatures applicable to universities' needs. (Attachment 7)

Matthew Goddard, Heartland Community Bankers Association, testified to request that an amendment to **HB 2059** be added concerning the bill's provision in New Section 1(i). The amendment would make the use of digital signatures an option (non-mandatory) (Attachment 8)

Dan Houlihan, Information Network of Kansas, stated that 14 states have such legislation, 9 states are currently enacting such legislation. Mr. Houlihan stated that the movement of industry is that they are setting a repository, and the key is in existence for only two years for security reasons. The conferee told of a meeting among state agencies to discuss commonalities across states. The conferee stated that the validation Visa or Mastercard transactions works on organizational agreements/safeguards.

Representative Morrison addressed Mr. Barrons questions. Representative Morrison stated that by changing the word, "commerce" to "communication" the concerns raised by the Board of Regents should be resolved. Representative Morrison stated that the bill is broad enough to include everyone else who uses encrypted technology.

Representative Morrison stated that **HB 2058** is the crime bill concerning electronic communication. The conferee addresses issues concerning child pornography through the electronic medium. The conferee stated that currently two encryption technologies are used, one private and other public. The conferee stated that **HB 2059** is model legislation on communication and information policy.

Representative Morrison requested an amendment to address terminology problems. The amendment will resolve the conflict in terms on page one, line 25 "shall" and on line 39, "if". The Chair requested that the amendment be presented when the bill is worked.

The Chair adjourned the meeting at 5:10 p.m.
The next meeting is scheduled for February 6, 1997.

HOUSE JUDICIARY COMMITTEE COMMITTEE GUEST LIST

DATE: 2-5-97

NAME	REPRESENTING
Kyle G. Smith	KBI
Teresa Dean	Sec. of State
Matt Goddard	Heartland Community Bankers Assoc.
Michl G Rumell	AG's OFFICE
Marvin Burris	Ks Bd of Regents
Judith Penrod Simmons	"
Joe Barron	KBOR
J. Chubb	SOS
Fred Bauer	Chief Information Architect
Paul Shelby	OJA
Steven E Johnson	CIA OFFICE
Jon McKenzie	KCC
Jason Oldham	OJA
Amy Waddle	OJA
Charlene Satzler	KDHE
Mark Barcellina	KDOC&H
Michelle Gay	NSNA
Mary Kay Freed	NSNA
Angela Brainard	BUTLER CCC

Denise C. Apt KPMA

Oran Burnett KPMA

HOUSE JUDICIARY COMMITTEE COMMITTEE GUEST LIST

DATE: 2-5-97

NAME	REPRESENTING
Margaret Fry	KSNA (Butler CCC)
Wendy Simms	KSNA (Bethel College)
Tonya Berry	KSNA (Bethel College)
Pat Johnson	KSBN
Mark Braun Asst AG	KSBN
Diane Glynn	KSBN
Anne Rumin	KSNA (Bethel College)
[illegible]	Ks. Pod. Med. Assn
Doug Smith	KSSA
SHELBY Smith	KPMA
R L Bradbury DPM	KPMA
Verda Deckert	KSNA - NSS
Karen Gilpin	KSNA
K. Harrison	KSNA
Michael Gapon	KSNA
Carrie Taylor Jones	KSNA (Southwestern College)

Kansas Bureau of Investigation

Larry Welch
Director

Carla J. Stovall
Attorney General

TESTIMONY
KYLE G. SMITH
SPECIAL AGENT AND ASSISTANT ATTORNEY GENERAL
KANSAS BUREAU OF INVESTIGATION
BEFORE THE HOUSE JUDICIARY COMMITTEE
IN SUPPORT OF HOUSE BILL 2058
FEBRUARY 5, 1997

Mr. Chairman and Members of the Committee:

I appear today on behalf of the Kansas Bureau of Investigation (KBI) in support of House Bill 2058, but with some proposed amendments, which I believe will both simplify and improve this legislation.

Fred Boesch, Chief Information Architect, State of Kansas, called a meeting back in October of various state agencies to discuss the adequacy of current Kansas computer crime statutes and review other approaches that have been tried in various jurisdictions.

I attended that meeting, and several concerns were raised with the adequacy of the existing statute. In particular, there was concern with persons accessing governmental data which may be confidential, but has no commercial value. Examples would include: the database in the KBI which includes the identity of confidential informants; the Department of Revenue would have income tax records and SRS would have various records concerning investigations of neglected and abused children. Accessing and copying this kind of information would have little or no economic value, but could have devastating results nonetheless.

House Judiciary
Attachment 1
2/5/97

Further, the KBI provides special agents trained in the investigation of computer crime and through discussions with these agents and prosecutors in Kansas, I believe these changes should be added.

The current statute makes accessing, copying and damaging such information a crime based on its loss of value. It simply doesn't fit the type of computer crime that occurs outside the commercial realm.

HB 2058 as introduced is an improvement over our existing law, but I was unable to work with Ms. Torrence on the final draft and I do believe the amendments contained in my balloons would improve this statute and make it more useful as well as easier to understand.

As noted above, the current computer crime statute is drafted along traditional theft lines of thinking, where the value of the property can be readily calculated. Computer crime is much broader than that as the examples above illustrate.

In *State v. Allen*, 260 Kan. 17 (1996) the Supreme Court wrestled with another problem in that approach. Attempted access was spotted and extra security added which thwarted actual damage or theft. Since no theft occurred and the thousands of dollars were spent to prevent the theft, not the value of what was taken, the Supreme Court held no crime had occurred.

HB 2058 approaches the *Allen* problem by providing an expanded definition of loss to specifically include the type of expenses suffered by the victim in the *Allen* case. What we would like the committee to consider is a different, simpler approach of dropping the sentencing structure based on dollar amount and treat computer crime much like making a false writing. K.S.A. 21-3711. That statute makes both frauds and efforts to induce official action simply a level 8 non-person felony. Like making false information, the activities prohibited by the computer crime statute covers actions besides mere thefts. Since commercial value can't be calculated in either case, an approach which has worked well in K.S.A. 21-3711 seems to make good sense.

We would propose in HB 2058 striking all references to the dollar amounts and make a violation of the crime a severity level 8 non-person felony, just as making false information is under current law.

Also, on page 2, line 25, I would suggest striking "or attempting to access" as the phrase is more properly covered under a new computer trespass crime found in subsection (d) on page 3, line 9; or simply as an attempted crime using K.S.A. 21-3301. Since the phrase "or attempting to access" is followed by the conjunctive "and" a mere attempt would not be prohibited by this section because by definition the attempt was unsuccessful and so there would not be the required proof of damage, modification, altering, etc. If it could be proven a person attempted to access with the intent to do one of the required acts under subsection (b)(1), then the person could be charged under the current attempt, K.S.A. 21-3301.

We also have a balloon affecting section 1, which is the making a false information statute. As it stands now with HB 2058, these changes are primarily cleanup; however, a case came to my attention, *State v. Rios*, 246 Kan. 517 (1990), where the Kansas Supreme Court held that the provisions of this statute did not apply to a person who made a false writing to cover up a prior theft. Given the pervasive use of computerized records, I am confident that occasions will arise where persons have altered computer records and have created false information with intent to impair the detection of either a theft or some other version of computer crime.

Therefore, we have suggested that the phrase "impair the detection of a theft or felony offense" be included after the word "defraud" in line 2, page 1, to cover those situations where a person alters written instruments or electronic data to either cover up a prior theft or obscure or prevent the detection of some other serious criminal activity.

Finally, there is a proposal to add computer crime to the Standard Asset Seizure and Forfeiture Act. Computer crime would be added to the list under K.S.A. 60-4104, as being one of the criminal acts that can give rise to forfeiture of the property used to facilitate the crime, i.e. the defendant's computer and modem. Forfeiture is a separate civil cause of action which is designed to remove the means of committing the crime from the defendant as well as providing a financial disincentive to commit the crime. As done in other states, computer crime would seem an appropriate predicate offense for a forfeiture. This last amendment would provide for such forfeiture after the safeguards and procedures within the asset forfeiture act are followed.

With the caveat that I am an investigator and prosecutor, not a computer expert, I would be happy to try to answer any questions. Thank you for your consideration.

Session of 1997

HOUSE BILL No. 2058

By Joint Committee on Computers and Telecommunications

1-22

AN ACT concerning crimes, punishment and criminal procedure; relating to certain crimes involving information and computers; amending K.S.A. 21-3755 and K.S.A. 1996 Supp. 21-3711 and repealing the existing sections.

Be it enacted by the Legislature of the State of Kansas:

Section 1. K.S.A. 1996 Supp. 21-3711 is hereby amended to read as follows: 21-3711. Making~~,~~ ~~generating,~~ ~~distributing~~ ~~a~~ false information is making, *generating, distributing* or drawing, or causing to be made, generated, distributed or drawn, any written instrument, electronic data or entry in a book of account with knowledge that such information falsely states or represents some material matter or is not what it purports to be, and with intent to defraud, impair the detection of a theft or felony offense or induce official action.

Making ~~a~~ false information is a severity level 8, nonperson felony.

Sec. 2. K.S.A. 21-3755 is hereby amended to read as follows: 21-3755. (a) As used in this section~~,~~ ~~the following words and phrases shall have the meanings respectively ascribed thereto~~:

(1) "Access" means to ~~approach,~~ instruct, communicate with, store data in, retrieve data from~~,~~ or otherwise make use of any resources of a computer, computer system or computer network.

(2) "Computer" means an electronic device which performs work using programmed instruction and which has one or more of the capabilities of storage, logic, arithmetic or communication and includes all input, output, processing, storage, software or communication facilities which are connected or related to such a device in a system or network.

(3) "Computer network" means the interconnection of communication lines, including microwave or other means of electronic communication, with a computer through remote terminals, or a complex consisting of two or more interconnected computers.

(4) "Computer program" means a series of instructions or statements in a form acceptable to a computer which permits the functioning of a computer system in a manner designed to provide appropriate products from such computer system.

(5) "Computer software" means computer programs, procedures and associated documentation concerned with the operation of a computer

1-9

system.

(6) "Computer system" means a set of related computer equipment or devices and computer software which may be connected or unconnected.

(7) "Financial instrument" means any check, draft, money order, certificate of deposit, letter of credit, bill of exchange, credit card, debit card or marketable security.

~~*(8) "Loss" includes the fair market value of any services used and any expenditure reasonably and necessarily incurred to verify that a computer, computer network, computer program or data was or was not altered, deleted, damaged or destroyed by unauthorized use.*~~

~~(8)~~ ~~*(9)*~~ "Property" includes, but is not limited to, financial instruments, information, electronically produced or stored data, supporting documentation and computer software in either machine or human readable form. (8)

~~(9)~~ ~~*(10)*~~ "Services" includes, but is not limited to, computer time, data processing and storage functions and other uses of a computer, computer system or computer network to perform useful work. (9)

~~(10)~~ ~~*(11)*~~ "Supporting documentation" includes, but is not limited to, all documentation used in the construction, classification, implementation, use or modification of computer software, computer programs or data. (10)

(b) *(1)* Computer crime is:

~~(1)~~ *(A)* Intentionally and without authorization ~~gaining or attempting to gain access to~~ *accessing* ~~*or attempting to access*~~ and damaging, modifying, altering, destroying, copying, disclosing or taking possession of a computer, computer system, computer network or any other property;

~~(2)~~ *(B)* using a computer, computer system, computer network or any other property for the purpose of devising or executing a scheme or artifice with the intent to defraud or for the purpose of obtaining money, property, services or any other thing of value by means of false or fraudulent pretense or representation; or

~~(3)~~ *(C)* intentionally exceeding the limits of authorization and damaging, modifying, altering, destroying, copying, disclosing or taking possession of a computer, computer system, computer network or any other property.

~~(c)~~ ~~(1)~~ *(2)* ~~*(A)*~~ Computer crime ~~*which causes a loss of the value of less than $500 is a class A nonperson misdemeanor*~~ is a severity level 8, nonperson felony.

~~(2)~~ *(B)* ~~*Computer crime which causes a loss of the value of at least $500 but less than $25,000 is a severity level 9, nonperson felony*~~

~~(3)~~ *(C)* ~~*Computer crime which causes a loss of the value of $25,000 or more is a severity level 7, nonperson felony*~~

~~(d)~~ *(3)* In any prosecution for computer crime, it is a defense that the property or services were appropriated openly and avowedly under a claim of title made in good faith.

(c) (1) Computer password disclosure is the unauthorized and intentional *disclosure of a number, code, password or other means of access to a computer or computer network, ~~knowing that the disclosure is without authority, when the disclosure causes a loss of the value of at least $500~~*

(2) Computer password disclosure is a class A nonperson misdemeanor.

~~(c)~~ ~~Criminal~~ ~~computer~~ ~~access~~ *(d) Computer trespass* is intentionally, ~~fraudulently~~ and without authorization ~~gaining~~ ~~or~~ ~~attempting~~ ~~to~~ ~~gain~~ ~~access~~ ~~to~~ *accessing or attempting to access* any computer, computer system, computer network or ~~to~~ ~~any~~ computer software, program, documentation, data or property contained in any computer, computer system or computer network. ~~Criminal~~ ~~computer~~ ~~access~~ *Computer trespass* is a class A nonperson misdemeanor.

~~(f)~~ *(e)* This section shall be part of and supplemental to the Kansas criminal code.

Sec. 3. K.S.A. 21-3755 and K.S.A. 1996 Supp. 21-3711 are hereby repealed.

Sec. 4. This act shall take effect and be in force from and after its publication in the statute book.

60-4104. Covered offenses and conduct giving rise to forfeiture. Conduct and offenses giving rise to forfeiture under this act, whether or not there is a prosecution or conviction related to the offense, are:

(a) All offenses which statutorily and specifically authorize forfeiture;

(b) violations of the uniform controlled substances act, K.S.A. 65-4101 et seq., and amendments thereto;

(c) theft which is classified as a felony violation pursuant to K.S.A. 21-3701, and amendments thereto, in which the property taken was livestock;

(d) unlawful discharge of a firearm, K.S.A. 21-4219, and amendments thereto;

(e) money laundering, K.S.A. 65-4142, and amendments thereto;

(f) gambling, K.S.A. 21-4303, and amendments thereto, and commercial gambling, K.S.A. 21-4304, and amendments thereto;

(g) computer crime, K.S.A. 21-3755, and amendments thereto;

(~~g~~) (h) an act or omission occurring outside this state, which would be a violation in the place of occurrence and would be described in this section if the act occurred in this state, whether or not it is prosecuted in any state;

(~~h~~) (i) an act or omission committed in furtherance of any act or omission described in this section including any inchoate or preparatory offense, whether or not there is a prosecution or conviction related to the act or omission;

(~~i~~) (j) any solicitation or conspiracy to commit any act or omission described in this section, whether or not there is a prosecution or conviction related to the act or omission.

History: L. 1994, ch. 339, § 4; July 1.

#2

STATE OF KANSAS

JIM MORRISON
REPRESENTATIVE, 121ST DISTRICT
3 COTTONWOOD DRIVE
COLBY, KANSAS 67701
(913) 462-3264
CAPITOL OFFICE 174-W
(913) 296-7676
email: jmorriso@ink.org
URL: http://www.idir.net/~jmorriso

TOPEKA

HOUSE OF REPRESENTATIVES

STATE CAPITOL
TOPEKA, KANSAS 66612-1504
COMMITTEE ASSIGNMENTS
Vice Chairman:
JOINT COMMITTEE ON COMPUTERS
AND TELECOMMUNICATIONS
Vice-Chairman:
HEALTH & HUMAN SERVICES
Member:
EDUCATION
Member:
FISCAL OVERSIGHT

What is Encryption (PGP)==========

It's personal. It's private. And it's no one's business but yours. You may be planning a political campaign, discussing your taxes, or having an illicit affair. Or you may be doing something that you feel shouldn't be illegal, but is. Whatever it is, you don't want your private electronic mail (E-mail) or confidential documents read by anyone else. There's nothing wrong with asserting your privacy. Privacy is as apple-pie as the Constitution.

Perhaps you think your E-mail is legitimate enough that encryption is unwarranted. If you really are a law-abiding citizen with nothing to hide, then why don't you always send your paper mail on postcards? Why not submit to drug testing on demand? Why require a warrant for police searches of your house? Are you trying to hide something? You must be a subversive or a drug dealer if you hide your mail inside envelopes. Or maybe a paranoid nut. Do law-abiding citizens have any need to encrypt their E-mail?

What if everyone believed that law-abiding citizens should use postcards for their mail? If some brave soul tried to assert his privacy by using an envelope for his mail, it would draw suspicion. Perhaps the authorities would open his mail to see what he's hiding. Fortunately, we don't live in that kind of world, because everyone protects most of his or her mail with envelopes. So no one draws suspicion by asserting his or her privacy with an envelope. There's safety in numbers. Analogously, it would be nice if everyone routinely used encryption for all their E-mail, innocent or not, so that no one drew suspicion by asserting their E-mail privacy with encryption. Think of it as a form of solidarity.

Today, if the Government wants to violate the privacy of ordinary citizens, it has to expend a certain amount of expense and labor to intercept and steam open and read paper mail, and listen to and possibly transcribe spoken telephone conversation. This kind of labor-intensive monitoring is not practical on a large scale. This is only done in important cases when it seems worthwhile.

More and more of our private communications are being routed through electronic channels. Electronic mail is gradually replacing conventional paper

House Judiciary
Attachment 2
2/5/97

mail. E-mail messages are just too easy to intercept and scan for interesting keywords. This can be done easily, routinely, automatically, and undetectably on a grand scale. The NSA (National Security Agency) already scans international cablegrams.

If privacy is outlawed, only outlaws will have privacy. Intelligence agencies have access to good cryptographic technology. So do the big arms and drug traffickers. So do defense contractors, oil companies, and other corporate giants. But ordinary people and grassroots political organizations mostly have not had access to affordable "military grade" public-key cryptographic technology.

PGP empowers people to take their privacy into their own hands. There's a growing social need for it. We are moving toward a future when the nation will be crisscrossed with high capacity fiber optic data networks linking together all our increasingly ubiquitous personal computers. E-mail will be the norm for everyone, not the novelty it is today. The Government will protect our E-mail with Government-designed encryption protocols. Probably most people will acquiesce to that. But perhaps some people will prefer their own protective measures.

How it Works ============

It would help if you were already familiar with the concept of cryptography in general and public key cryptography in particular. Nonetheless, here are a few introductory remarks about public key cryptography.

First, some elementary terminology. Suppose I want to send you a message, but I don't want anyone but you to be able to read it. I can "encrypt", or "encipher" the message, which means I scramble it up in a hopelessly complicated way, rendering it unreadable to anyone except you, the intended recipient of the message. I supply a cryptographic "key" to encrypt the message, and you have to use the same key to decipher or "decrypt" it. At least that's how it works in conventional "single-key" cryptosystems.

In conventional cryptosystems, such as the US Federal Data Encryption Standard (DES), a single key is used for both encryption and decryption. This means that a key must be initially transmitted via secure channels so that both parties can know it before encrypted messages can be sent over insecure channels. This may be inconvenient. If you have a secure channel for exchanging keys, then why do you need cryptography in the first place?

In public key cryptosystems, everyone has two related complementary keys, a publicly revealed key and a secret key (also frequently called a private key). Each key unlocks the code that the other key makes. Knowing the public key does not help you deduce the corresponding secret key. The public key can be published and widely disseminated across a communications network. This protocol provides privacy without the need for the same kind of secure channels that a conventional cryptosystem requires.

Anyone can use a recipient's public key to encrypt a message to that person, and that recipient uses her own corresponding secret key to decrypt that message. No one but the recipient can decrypt it, because no one else has access to that secret key. Not even the person who encrypted the message can decrypt it.

Message authentication is also provided. The sender's own secret key can be used to encrypt a message, thereby "signing" it. This creates a digital signature of a message, which the recipient (or anyone else) can check by using the sender's public key to decrypt it. This proves that the sender was the true originator of the message, and that the message has not been subsequently altered by anyone else, because the sender alone possesses the secret key that made that signature. Forgery of a signed message is infeasible, and the sender cannot later disavow his signature.

These two processes can be combined to provide both privacy and authentication by first signing a message with your own secret key, then encrypting the signed message with the recipient's public key. The recipient reverses these steps by first decrypting the message with her own secret key, then checking the enclosed signature with your public key. These steps are done automatically by the recipient's software.

Because the public key encryption algorithm is much slower than conventional single-key encryption, encryption is better accomplished by using a high-quality fast conventional single-key encryption algorithm to encipher the message. This original unenciphered message is called "plaintext". In a process invisible to the user, a temporary random key, created just for this one "session", is used to conventionally encipher the plaintext file. Then the recipient's public key is used to encipher this temporary random conventional key. This public-key-enciphered conventional "session" key is sent along with the enciphered text (called "ciphertext") to the recipient. The recipient uses her own secret key to recover this temporary session key, and then uses that key to run the fast conventional single-key algorithm to decipher the large ciphertext message.

Public keys are kept in individual "key certificates" that include the key owner's user ID (which is that person's name), a timestamp of when the key pair was generated, and the actual key material. Public key certificates contain the public key material, while secret key certificates contain the secret key material. Each secret key is also encrypted with its own password, in case it gets stolen. A key file or "key ring" contains one or more of these key certificates. Public key rings contain public key certificates, and secret key rings contain secret key certificates.

The keys are also internally referenced by a "key ID", which is an "abbreviation" of the public key (the least significant 64 bits of the large public key). When this key ID is displayed, only the lower 32 bits are shown for further brevity. While many keys may share the same user ID, for all practical purposes no two keys share the same key ID.

PGP uses "message digests" to form signatures. A message digest is a 128-bit cryptographically strong one-way hash function of the message. It is somewhat analogous to a "checksum" or CRC error checking code, in that it compactly "represents" the message and is used to detect changes in the message. Unlike a CRC, however, it is computationally infeasible for an attacker to devise a substitute message that would produce an identical message digest. The message digest gets encrypted by the secret key to form a signature.

Documents are signed by prefixing them with signature certificates, which contain the key ID of the key that was used to sign it, a secret-key-signed message digest of the document, and a timestamp of when the signature was made. The key ID is used by the receiver to look up the sender's public key to check the signature. The receiver's software automatically looks up the sender's public key and user ID in the receiver's public key ring.

Encrypted files are prefixed by the key ID of the public key used to encrypt them. The receiver uses this key ID message prefix to look up the secret key needed to decrypt the message. The receiver's software automatically looks up the necessary secret decryption key in the receiver's secret key ring.

These two types of key rings are the principal method of storing and managing public and secret keys. Rather than keep individual keys in separate key files, they are collected in key rings to facilitate the automatic lookup of keys either by key ID or by user ID. Each user keeps his own pair of key rings. An individual public key is temporarily kept in a separate file long enough to send to your friend who will then add it to her key ring.

Encryption Use for Historical Documents========

The files mentioned could easily be anything "scanned" or "converted" to electronic readable form. Most county offices in the state of Kansas are beginning to feel the "crunch" of space problems. The legislature may soon act to allow mandated storage of records to include the conversion of paper documents to electronic readable form. Many documents contained at the Kansas Museum of History are deteriorating and need to be converted to electronically readable form as soon as possible.

What happens if the *historical document* archived by the conversion process is changed by someone illegally gaining access to the original electronic file and altering it? What can we do to ***guarantee*** that document is unchanged from the original? Today even a notarized copy is subject to the forgers pen and can easily be altered. Our passage of and encouragement of use of specialized encryption technology and *digital signatures* avoids all that problem.

The encryption of a special file or document by a self-destructive sercret/public key is very easy to do. The private or secret key is used to encrypt the document and to produce a *public* key to read that document. Immediately upon encryption the secret key can be made to "expire" or "self-destruct." With the secret key now gone it is virtually impossible to alter the original "signed" and encrypted document as the write authority permission is permanently lost. The public key is used to read or display the encrypted document but cannot be used to alter it.

Please recommend passage of HB 2059. It will place Kansas in the forefront of states and should serve as a model piece of legislation for others to use throughout the country.

A3

Summary

Electronic mail is gradually replacing conventional paper mail. In public key cryptosystems, everyone has two related complementary keys, a publicly revealed key and a secret key (also frequently called a private key). Each key unlocks the code that the other key makes. Knowing the public key does not help you deduce the corresponding secret key. Anyone can use a recipient's public key to encrypt a message to that person, and that recipient uses her own corresponding secret key to decrypt that message. The sender's own secret key can be used to encrypt a message, thereby "signing" it. The recipient reverses these steps by first decrypting the message with her own secret key, then checking the enclosed signature with your public key. Because the public key encryption algorithm is much slower than conventional single-key encryption, encryption is better accomplished by using a high-quality fast conventional single-key encryption algorithm to encipher the message. Then the recipient's public key is used to encipher this temporary random conventional key. This public-key-enciphered conventional "session" key is sent along with the enciphered text (called "ciphertext") to the recipient. The recipient uses her own secret key to recover this temporary session key, and then uses that key to run the fast conventional single-key algorithm to decipher the large ciphertext message.

Public keys are kept in individual "key certificates" that include the key owner's user ID (which is that person's name), a timestamp of when the key pair was generated, and the actual key material. Public key certificates contain the public key material, while secret key certificates contain the secret key material. A key file or "key ring" contains one or more of these key certificates. Public key rings contain public key certificates, and secret key rings contain secret key certificates.

The keys are also internally referenced by a "key ID", which is an "abbreviation" of the public key (the least significant 64 bits of the large public key). While many keys may share the same user ID, for all practical purposes no two keys share the same key ID.

PGP uses "message digests" to form signatures. The message digest gets encrypted by the secret key to form a signature.

The receiver's software automatically looks up the sender's public key and user ID in the receiver's public key ring.

Encrypted files are prefixed by the key ID of the public key used to encrypt them. The receiver uses this key ID message prefix to look up the secret key needed to decrypt the message. The receiver's software automatically looks up the necessary secret decryption key in the receiver's secret key ring.

Rather than keep individual keys in separate key files, they are collected in key rings to facilitate the automatic lookup of keys either by key ID or by user ID. The private or secret key is used to encrypt the document and to produce a *public* key to read that document.

House Judiciary
Attachment 3
2/5/97

Message and Document Privacy,
And Why You Need It and how to obtain it

Your files and messages. They may be personal. They certainly are private. And no one's business but yours. You may be planning corporate strategy, preparing your taxes, or negotiating a contract. Whatever it is, you don't want your private electronic mail (email) or confidential documents read by anyone without your permission.

Email messages are just too easy to intercept and scan for interesting keywords. This can be done easily, routinely, automatically, and undetectably on a grand scale. International cablegrams are already scanned this way on a large scale by the National Security Agency.

The threat is not just from the outside. Our Local Area Network (LAN) is "viewable" by any technician with a garden-variety LAN analyzer. Our TCP/IP network allows anyone who desires the ability to see and read everything on the LAN.

A cartoon in a recent trade magazine showed several night shift employees entertaining themselves by reading the confidential files on their manager's PC. In many businesses, this very opportunity is all too real.

The list goes on-and-on: your laptop computer is stolen; a competitor reads your email; your computer is seized because of your son's BBS activities. To be sure, I am not trying to generate discomfort, but as you begin to think about the possibilities you may find that you are far more exposed than you should be.

You would never consider writing highly confidential correspondence on a postcard. If you did, the entire world could read it. Instead, you mail your letter in an envelope, preventing unauthorized, curious, or prying eyes from reading it. Shouldn't your electronic mail and electronic files have the same protection routinely given to their paper counterparts?

Digital Signatures

For any written correspondence involving business, legal, or monetary issues, the mark of authenticity provided by your signature is required. For example, the Internal Revenue Service is practically begging people to file their tax returns electronically, but the IRS still must receive a signed paper copy of your return before issuing your refund check. The reason is that your paper return contains your signature, but the electronic version currently does not.

The electronic analogy to a written signature is the digital signature. It can be a unique to you as is your fingerprint, retina scan or DNA. Digital signatures provide two things:

•Assurance that the message is from the purported sender, and:

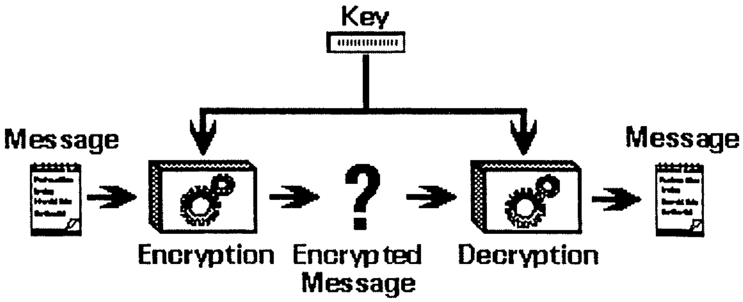
•The message has not been altered since it was signed.

The technical details of how this is achieved are covered in the next section, but it is important to realize that the ability to attach your digital signature to any electronic message or file opens up possibilities that never before existed. Digital signatures are the key to widespread use of electronic commerce.

How It Works

First, some basic terminology. Suppose you want to send a message to a colleague, whom we'll call Alice, and you don't want anyone but Alice to be able to read it. As shown in Figure 1, you can encrypt, or encipher the message, which means scrambling it up in a hopelessly complicated way, rendering it unreadable to anyone except you and Alice. You supply a cryptographic key to encrypt the message, and Alice must use the same key to decipher or decrypt it. At least that's how it works in conventional "single-key" cryptosystems.

Figure 1
Conventional "Single-Key" Cryptosystem



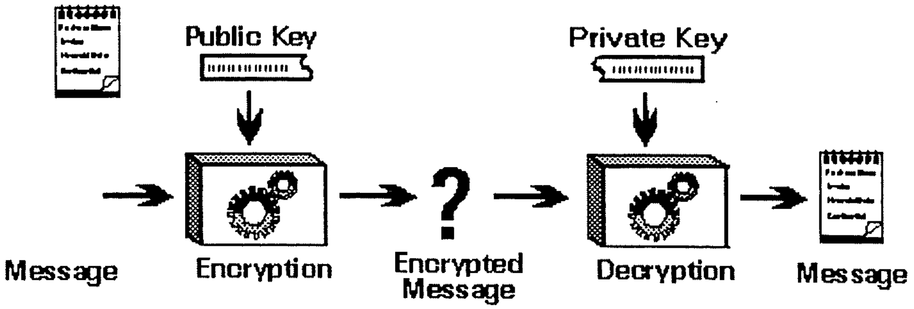
In conventional cryptosystems, such as the International Data Encryption Algorithm (IDEA), a single key is used for both encryption and decryption. This means that this key must be initially transmitted via secure channels so that both parties can know it before encrypted messages can be sent over insecure channels. This may be inconvenient. If you have a secure channel for exchanging keys, then why do you need cryptography in the first place?

Public Key Cryptosystems

In public key cryptosystems, as shown in Figure 2, everyone has two related complementary keys, a publicly revealed key and a secret key. Each key unlocks the code that the other key makes. Knowing the public key does not help you deduce the corresponding secret key. The public key can be published and widely disseminated across a communications network.

This protocol provides privacy without the need for the same kind of secure channels that a conventional cryptosystem requires.

Figure 2
Public Key Cryptosystem



Anyone can use a recipient's public key to encrypt a message to that person, and that recipient uses her own corresponding secret key to decrypt that message. No one but the recipient can decrypt it, because no one else has access to that secret key. Not even the person who encrypted the message can decrypt it.

Because the public key encryption algorithm is much slower than conventional single-key encryption, encryption is better accomplished by using the process shown in Figure 3.

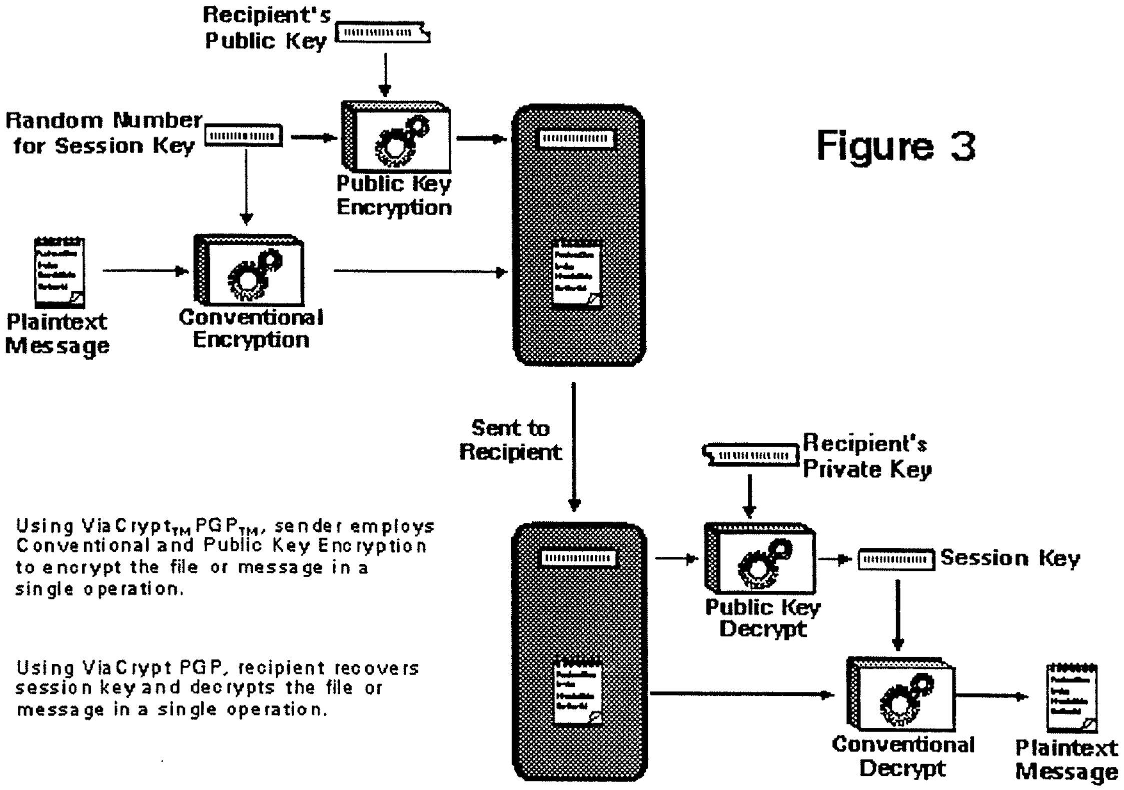


Figure 3

Using ViaCrypt$_{TM}$ PGP$_{TM}$, sender employs Conventional and Public Key Encryption to encrypt the file or message in a single operation.

Using ViaCrypt PGP, recipient recovers session key and decrypts the file or message in a single operation.

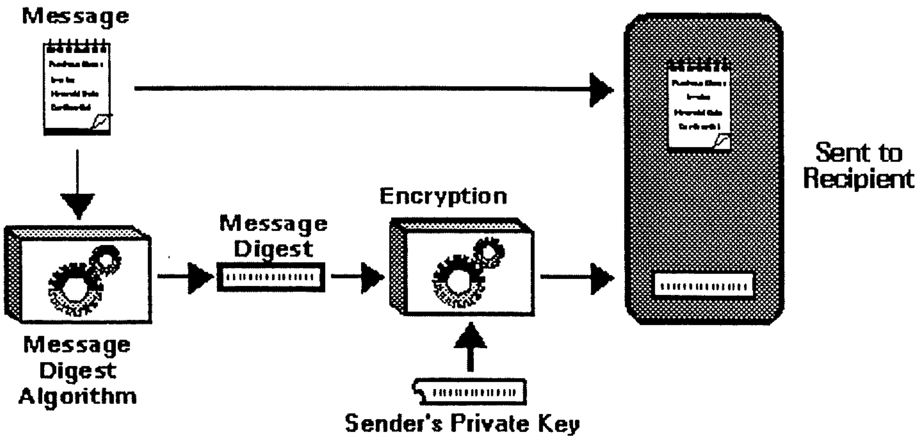
A high-quality fast conventional single-key encryption algorithm is used to encipher the message. This original unenciphered message is called "plaintext". In a process invisible to the user, a temporary random key, created just for this one "session", is used to conventionally encipher the plaintext file. Then the recipient's public key is used to encipher this temporary random conventional key. This public-key-enciphered conventional "session" key is sent along with the enciphered text (called "ciphertext") to the recipient. The recipient uses her own secret key to recover this temporary session key, and then uses that key to run the fast conventional single-key algorithm to decipher the large ciphertext message.

How Digital Signatures Work

PGP uses digital signatures to provide message authentication. The sender's own secret key can be used to encrypt a message digest, thereby 'signing' the message. A message digest is a 128-bit cryptographically-strong one-way hash function. It is somewhat analogous to a "checksum" or CRC error checking code, in that it compactly represents the message and is used to detect changes in the message. Unlike a CRC, however, it is computationally infeasible for an attacker to devise a substitute message that would produce an identical message digest. The message digest gets encrypted by the sender's secret key, creating a digital signature of the message.

Figure 4

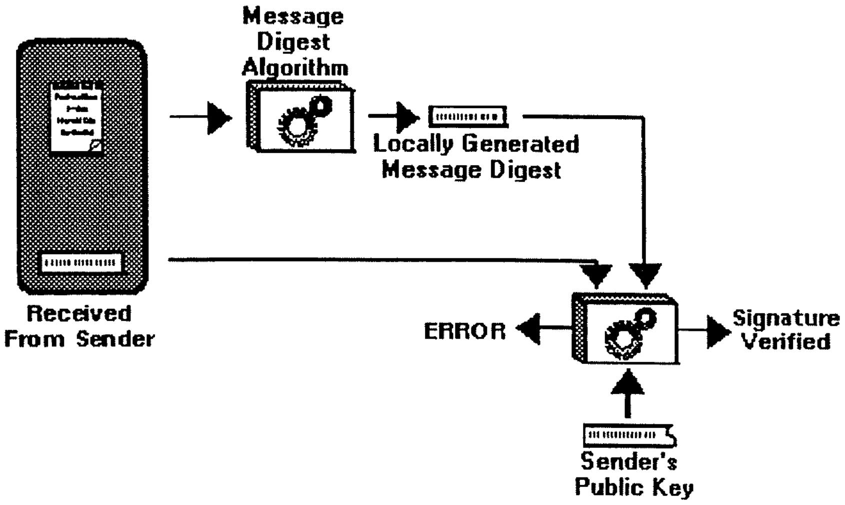
Digital Signature Generation



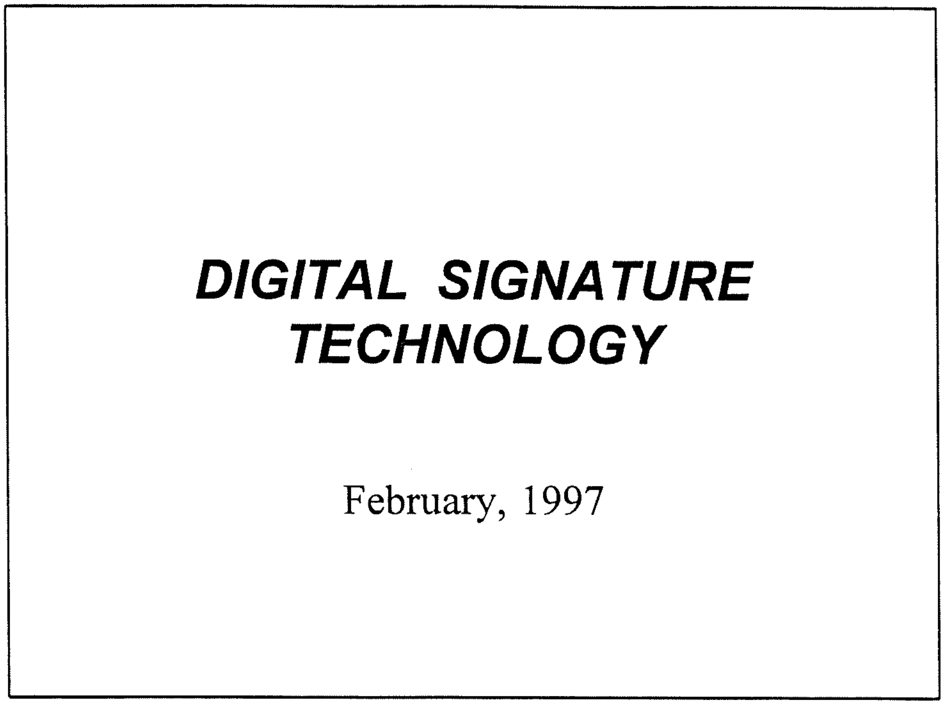
The recipient (or anyone else) can verify the digital signature by using the sender's public key to decrypt it. This proves that the sender was the true originator of the message, and that the message has not been subsequently altered by anyone else, because the sender alone possesses the secret key that made that signature. Forgery of a signed message is infeasible, and the sender cannot later disavow his signature.

Figure 5

Digital Signature Verification

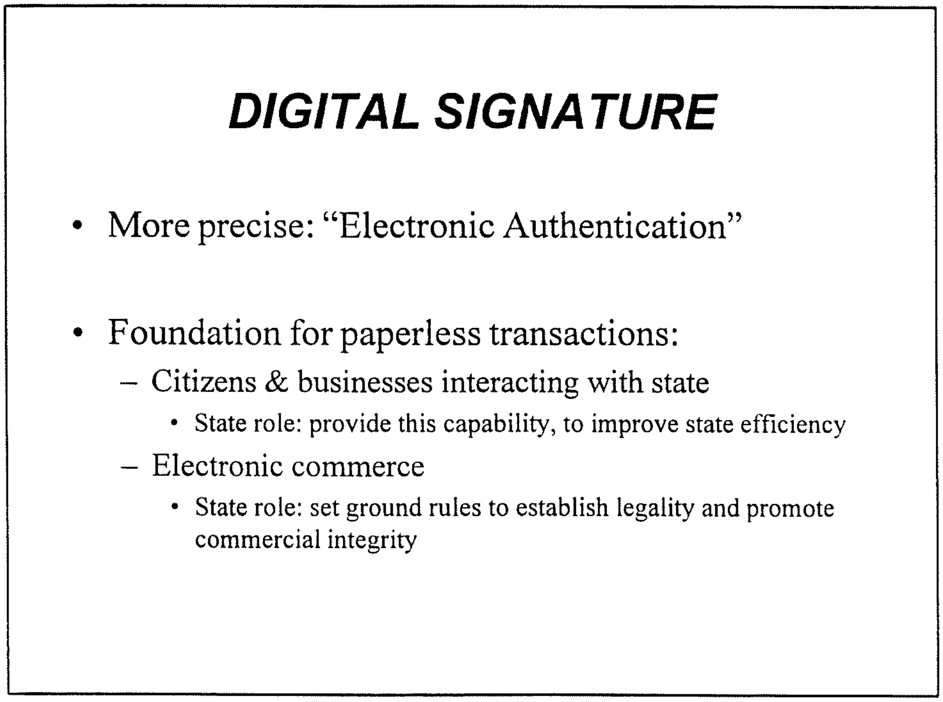


These two processes (encryption and digital signatures) can be combined to provide both privacy and authentication by first signing a message with your own secret key, then encrypting the signed message with the recipient's public key. The recipient reverses these steps by first decrypting the message with her own secret key, then checking the enclosed signature with your public key. These steps are done automatically by ViaCrypt PGP.



DIGITAL SIGNATURE TECHNOLOGY

February, 1997



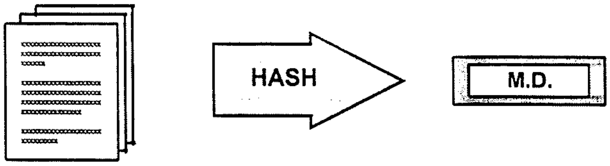
DIGITAL SIGNATURE

- More precise: "Electronic Authentication"
- Foundation for paperless transactions:
  - Citizens & businesses interacting with state
    - State role: provide this capability, to improve state efficiency
  - Electronic commerce
    - State role: set ground rules to establish legality and promote commercial integrity

SIGNING A DOCUMENT

To send a "signed" file (message) to Bob, Alice uses special software to:

1.

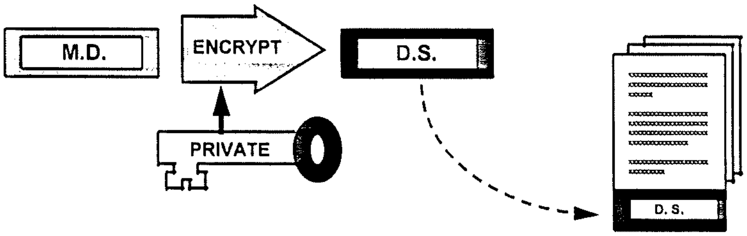


Compute ("hash") a small Message Digest from the source file, which is not affected.

- Any change to source file results in different Message Digest
- Not possible to recreate source file from Message Digest
- Can be used with any file type - text, image, sound, ...

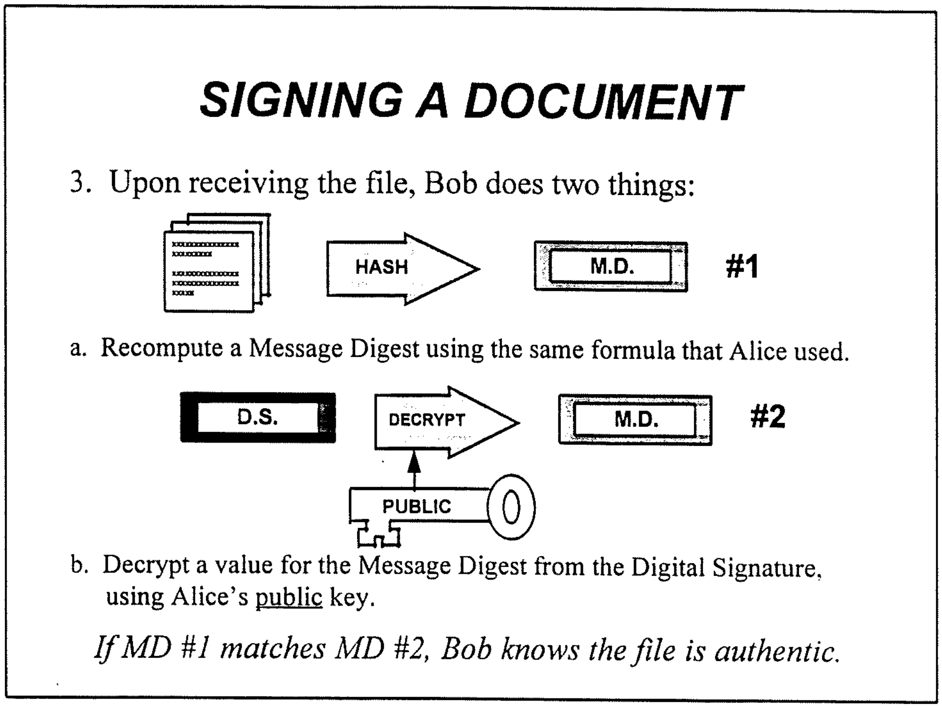
SIGNING A DOCUMENT

2.



Alice's private (secret) key is used to encrypt the Message Digest. The result is a Digital Signature, which is added to the source file (message) sent to Bob.

The source file itself is not encrypted.



SIGNING A DOCUMENT

3. Upon receiving the file, Bob does two things:

HASH

M.D.

#1

a. Recompute a Message Digest using the same formula that Alice used.

D.S.

DECRYPT

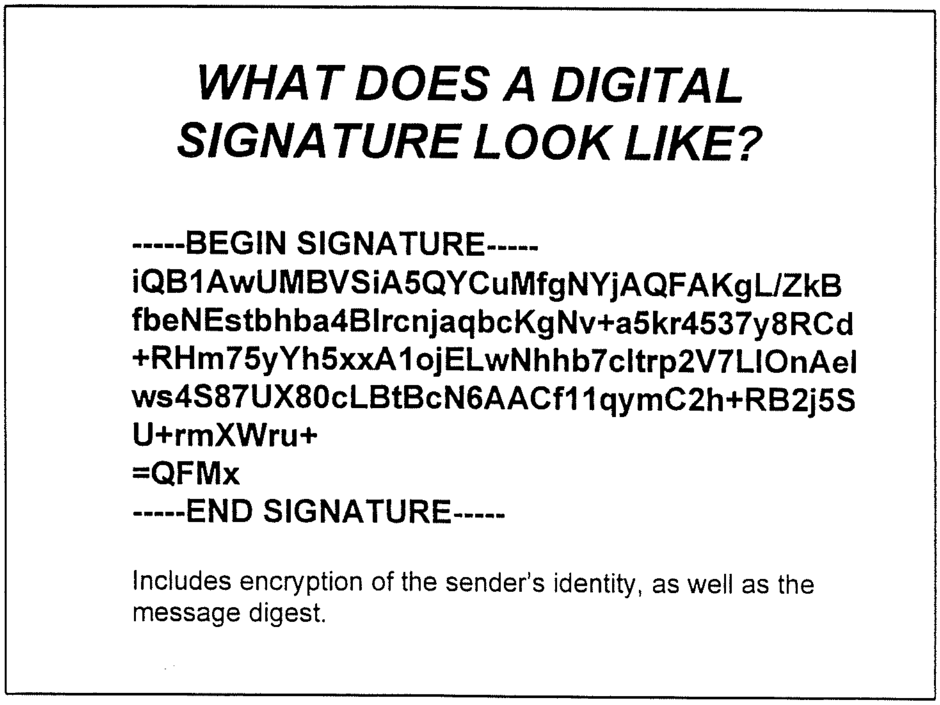
M.D.

#2

PUBLIC

b. Decrypt a value for the Message Digest from the Digital Signature, using Alice's <u>public</u> key.

If MD #1 matches MD #2, Bob knows the file is authentic.



WHAT DOES A DIGITAL SIGNATURE LOOK LIKE?

```
-----BEGIN SIGNATURE-----
iQB1AwUMBVSiA5QYCuMfgNYjAQFAKgL/ZkB
fbeNEstbhba4BlrcnjaqbcKgNv+a5kr4537y8RCd
+RHm75yYh5xxA1ojELwNhhb7cltrp2V7LlOnAel
ws4S87UX80cLBtBcN6AACf11qymC2h+RB2j5S
U+rmXWru+
=QFMx
-----END SIGNATURE-----
```

Includes encryption of the sender's identity, as well as the message digest.

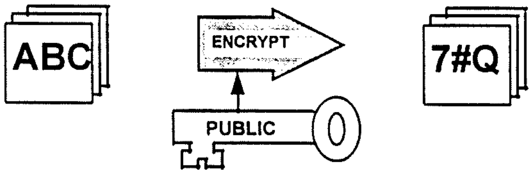
WHAT DOES "AUTHENTIC" MEAN?

- **KNOWN IDENTITY OF SENDER**
  - Only someone with access to the private key could have signed the file (message)
- **INTEGRITY OF CONTENTS**
  - Contents of the file are complete and unchanged since being signed
- **NON-REPUDIATION**
  - It will not be possible for the sender to later deny having signed the file

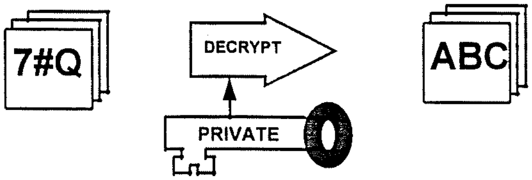
Better protection than manual signatures on paper

SECOND USE: CONFIDENTIALITY

Digital Signature alone does not conceal contents. Use public and private keys in the opposite direction to encrypt:



1. Alice uses <u>Bob's</u> public key to encrypt the entire file.



2. Only Bob's private (secret) key will be able to decrypt the file contents.

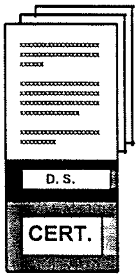
CERTIFICATION AUTHORITY

COMMERCIAL OR GOVERNMENT ENTITY TO:

- Register public keys
  - Establish identity of applicant
  - Issue a certificate
- Publish public keys -- accessible database
- Purge expired or revoked public keys
  - Preserve historical record of keys by either:
    - Maintaining an archive file, or
    - Establishing procedures to date/time stamp signatures
- Meet liability requirements as defined by state

WHAT IS A "CERTIFICATE"?

- Identifying text, in plain language (not encrypted), added to a signed, transmitted file
- Need not be used if receiver already knows the public key
- Typical contents:
  - Sender's ID (name, organization, address)
  - Sender's public key
  - Public key validity dates (start, expire)
  - Certificate number
  - Certification Authority ID
  - Certification Authority's digital signature (establishes authenticity of the Certificate)



HOW MUCH DOES KEY REGISTRATION COST?

As an example,VeriSign, Inc., a commercial Certification Authority in California, charges the following:

- Commercial sites and Web servers:
  - $290 for the first certificate (public key)
  - $95 for each additional certificate (different public key)
  - $75 for annual renewal of each certificate
- Individuals:
  - $15 per year for each certificate (public key)

STANDARDS

- RSA - De facto commercial standard for public key cryptography; used in many software products
- DSS - Digital Signature Standard in federal government (FIPS 186); similar concept, different implementation than RSA - not compatible
- CCITT X.509 - international standard for contents & format of public-key Certificates; related to e-mail directory standard (X.500); can be used with RSA or DSS
- Digital Signature Guidelines - American Bar Association; released in August, 1996; tutorial & legal ramifications

RELATED AREAS OF "ELECTRONIC COMMERCE"

- Digital signature / certification
  - Firms offering: VeriSign, CivicLink
- Notary / timestamp
  - Identifies *when* file was signed, rather than *who* signed
  - Firms offering: Stamper, Surety
- Digital cash
  - Paying party can be anonymous to payee
  - Firms offering: DigiCash, First Virtual, CyberCash
- Digital pen
  - Manually sign on digitizer pad; biometric measurements
  - Firms offering: PenOp

#4

[illegible]

TESTIMONY BEFORE THE
HOUSE JUDICIARY COMMITTEE
REGARDING HOUSE BILL 2059

Presented by Fred Boesch
Chief Information Architect
February 5, 1997

Good afternoon, Mister Chairman. I appreciate the opportunity to discuss House Bill 2059, concerning digital signatures in Kansas. The concept and use of digital signatures to authenticate electronic transactions and documents are relatively new, and commercial practices are still evolving. However, businesses have been using electronic commerce for a number of years. The scope of electronic commerce is changing from structured business to business agreed upon arrangements for limited transactions to more general use of a broad range of services with other businesses and customers. Thus, we see expanded demands being placed upon technology to enable this expanded use of electronic commerce.

Digital signatures, a technology to authenticate an electronic document and the identity of the sender, is important to electronic commerce. But let me be clear about one point, I am not advocating that the state take a position on the use of a specific technology or set of products. The marketplace will determine that. What I am advocating is for the state to enable business in Kansas to use this technology to be competitive in world commerce. We can do this by establishing that electronic documents using this technology will be as valid as manually signed documents and will have the force of law in our courts.

I must also add at this point that I believe we in state government have much to gain by employing this technology. Citizens will expect to do business with the state as they do with businesses, meaning that they have the same ease and speed of executing a transaction and where appropriate, they use the same tools such as smart cards, electronic services, and one stop services. We have many uses to verify authenticity of documents and originators such as electronic filing for courts, electronic submission of contracts, and internal workflow processing of electronic documents with approval signatures. Thus, I have a second motive for advocating establishing the legal basis for electronic documents and advocating recognition of digital signature technology.

As you may recall from the demonstration hosted yesterday by Representative Morrison, it is possible for anyone, right now, to use digital signatures and encryption technology to safeguard their electronic business transactions. However, these transactions are enforceable by law only when both parties have a pre-existing agreement or contract to recognize each other's signatures. In the case of transactions between parties without such trade agreements, as when a new customer purchases an item from an electronic catalog, each party takes a risk in offering or accepting a digital signature. Few states offer the legal framework to enforce such transactions.

House Judiciary
Attachment 4
2/5/97

And in the absence of case law, commercial service providers alone cannot guarantee this enforceability. The primary role of the state, then, is to ensure that a trusted environment exists for digital-signature transactions, an environment which meets certain minimum criteria to satisfy the rules of evidence.

For example, one popular method of electronic authentication is the public/private key pair approach licensed by RSA Data Security, Inc. This appears to be a de facto commercial standard today. Digital signatures have only recently seen widespread use. With this technology, there must be assurances that:

- The computational process, or algorithm, for matching the public and private keys is secure from tampering;
- A trusted third party, or Certification Authority, must ensure that the public key is authentic (that is, attributable to a known party), accessible (or available for use by anyone), and current (that is, not have expired or been revoked);
- Key pairs must be generated and maintained in a secure fashion, so that a signer's private key will not be accidentally divulged.

I must also point out there are conflicting standards and technologies in play. For example, the RSA standard mentioned above is different from, and not interoperable with, the Digital Signature Standard created by the federal government. Both of these public/private key pair approaches differ from a pen-based technique which records biometric characteristics of a person's written signature.

There are also questions of liability and consumer protection. Where does the liability stemming from fraud or misuse of a digital signature reside -- with the Certification Authority which incorrectly confirmed a signature to be authentic, or with the digital signature customer who selected the vendor? Should there be limits to liability?

States, in establishing their digital signature statutes, have addressed electronic documents and digital signature legislation in different ways. Utah and Washington attempted to ensure the integrity of digital signatures by putting into law some very specific requirements that must be met for public/private key pair validity. In addition to formally establishing the legality of digital signatures and identifying responsibilities for the Secretary of State in carrying out a licensing program, their statutes place requirements on subscribers to public key Certificates, and spell out extensive requirements for Certification Authorities:

- Rules for conducting business and prohibited activities;
- Minimum qualifications for Certification Authorities and the public-key repositories they manage;
- State-initiated performance audits and license investigations;

- Warranties and obligations of the Certification Authorities; and
- Processes for issuing, suspending, revoking or handling expiration of public key Certificates.

California and Wyoming drafted much simpler statutes. These laws authorize use of digital signatures with any public entity, provided both parties agree; define functional attributes of any digital signature technique, without specifying a particular one (such as public/private key pairs and Certificates); and require the Secretary of State to establish implementing regulations.

Massachusetts, Oklahoma and Georgia are drafting statutes which are between the "regulatory" and "minimalist" extremes. They also avoid formal sanction for one particular technology by listing functional requirements for digital signatures, and provide the force of law to any technique which meets the criteria. However, they provide more detailed guidance to the rules of evidence by elaborating on definitions of "electronic records" and "electronic signing."

Since the commercial vendors now offering digital signature services, including third-party authentication, are all outside of Kansas, it may appear that they are beyond the jurisdiction of Kansas legislative action. However, the important issue to be addressed is whether individuals and businesses can seek protection in Kansas courts for transactions executed using these vendors' products and services. Through reciprocity agreements, this court protection could be extended to any other state with whom Kansas has established mutual recognition of licensure. This protection must rest on legislation which formally provides a legal foundation for digital signatures.

In my view, House Bill 2059 provides this foundation in law. The bill is technology-neutral, so the state will be able to recognize and adapt to new technologies for authentication without changing the law. The bill does not assume responsibility for nor impose solutions on complex issues which are currently being worked out among vendors, standards organizations, state governments and businesses. And the bill recognizes the role to be played by the Secretary of State as a natural adjunct to responsibilities already assigned to that office. It is important that this legislation provide the legal authority the Secretary of State will need to implement regulations. This authority includes the ability to request criminal background checks from law enforcement entities throughout the state; to negotiate and establish reciprocity agreements with other states; and to establish guidelines for digital signature repositories which may be established within Kansas.

In summary, the state of Kansas needs to establish legislation which enables use of digital signatures. This technology is in direct support of electronic commerce, a capability which will allow Kansas individuals and businesses to participate in the global economy into the next century. I highly encourage the Legislature to take action in this session. Other states are now passing laws and negotiating with vendors. Without enabling legislation in Kansas, we will have no basis on which to enter a dialogue with these states, much less to provide legal protection for Kansas clients of digital signature services. The industry is setting patterns which may last for quite some time. This is the best chance we will have to influence that direction, in concert with other states.

Thank you for the opportunity to bring these matters to your attention.

#5

TESTIMONY TO THE HOUSE JUDICIARY COMMITTEE
BY THE SECRETARY OF STATE
ON HB 2059, DIGITAL SIGNATURES

February 5, 1997

Mr. Chairman, members of the committee. I am Assistant Secretary of State Janet Chubb, and I appreciate the opportunity to present Mr. Thornburgh's testimony concerning the proposed digital signature act.

HB 2059 grants broad administrative and regulatory powers to the secretary of state, charging him not only with developing the digital signature model for Kansas but also with regulating it. These powers include developing rules and regulations; acting as a certification authority; investigating, licensing and regulating certification authorities; and recovering costs of enforcement.

Unlike the digital signature acts adopted by the states of Utah and Washington, which are techologically and legally detailed bills leaving little flexibility for the administrator, this bill follows the minimalist approach taken by the states of California and Wyoming. HB 2059 grants broad authority to the secretary of state to adopt rules and regulations as he determines necessary.

Simply put, the bill provides that, unless otherwise specifically provided by law, a digital signature shall have the same force and effect as a manual signature or, if a simple amendment we propose is adopted, other signature that under law may be used to authenticate a writing.

Legislation authorizing digital signatures is consistent with the electronic mission we have implemented in the secretary of state's office the past two years: e.g. electronic filing in our UCC division, integrated optical imaging systems for our UCC and corporations divisions, and electronic filing and transmission of election data. We are on the road to electronic and paper less commerce. HB 2059 is the best vehicle to protect the integrity of the electronic communications involved, and it is flexible enough to incorporate the latest developments in technology, commercial transactions and business law.

We do suggest several simple amendments which are the result of a meeting attended by representatives of INK, the chief information architect, the secretary of state, the judiciary and the revisor. They appear on the ballon we copied for the committee and handed out today. I am happy to review those for the committee if that is appropriate.

Thank you for the opportunity to present this testimony.

House Judiciary
Attachment 5
2/5/97

Session of 1997

HOUSE BILL No. 2059

By Joint Committee on Computers and Telecommunications

1-22

AN ACT concerning digital signatures; relating to the effect of digital signatures; providing for authentication and regulation of digital signatures and licensure of certain entities to perform authentication; amending K.S.A. 1996 Supp. 12-4516 and 21-4619 and repealing the existing sections; also repealing K.S.A. 1996 Supp. 21-4619b.

Be it enacted by the Legislature of the State of Kansas:

New Section 1. (a) This act may be cited as the Kansas digital signature act.

(b) As used in this act, "digital signature" means a computer-created electronic identifier that is: (1) Intended by the party using it to have the same force and effect as the use of a manual signature; (2) unique to the party using it; (3) capable of verification; (4) under the sole control of the party using it; (5) linked to data in such a manner that it is invalidated if the data are changed; and (6) in conformity with any applicable rules and regulations adopted by the secretary of state under this act.

(c) The secretary of state shall adopt such rules and regulations as the secretary of state determines necessary to provide for authentication and reliability of digital signatures and to minimize incidence of forged digital signatures and fraud in electronic commerce. Such rules and regulations shall include but not be limited to:

(1) Provisions for authentication of digital signatures by the secretary of state or entities licensed by the secretary of state, or both;

(2) procedures and standards for licensure and renewal of licensure of entities to authenticate digital signatures;

(3) fees for application for licensure and license renewal in an amount equal to the costs of processing the application, including costs of any background investigation required; ~~and~~

(4) fees for licensure and license renewal in an amount equal to the costs of such licensure or license renewal; ¶ (5) provisions for reciprocal recognition of digital signatures authenticated in accordance with the law of another jurisdiction having standards for authentication that are comparable to those of this state; and ¶ (6) limitations on liability incurred by a party authorized to use a digital signature for wrongful use of such digital signature by a party other than a party authorized use such signature

If the rules and regulations adopted by the secretary of state provide for licensure of entities to authenticate digital signatures, such license may be suspended or revoked in accordance with the Kansas administrative procedure act for failure to maintain the required standards or pay the required fees.

House Judiciary Attachment 6 2/5/97

#6

(d) The secretary of state may recover any costs, including costs of investigation, staff time and attorney fees, incurred by the secretary of state in any administrative or judicial proceeding to enforce the provisions of this act or rules and regulations adopted under this act if the secretary of state prevails under the final order entered in the proceeding.

(e) No temporary or permanent rules and regulations adopted under this act shall take effect earlier than 30 days after such rules and regulations are submitted by the secretary of state to the joint committee on computers and telecommunications for review and comment by the committee.

(f) The secretary of state may investigate the activities of an entity licensed under this act material to the entity's compliance with this act and rules and regulations adopted under this act. The secretary of state shall require fingerprinting of all persons necessary to verify qualification for a license to authenticate digital signatures. The secretary of state shall submit such fingerprints to the Kansas bureau of investigation and to the federal bureau of investigation for the purposes of verifying the identity of such persons and obtaining records of criminal arrests and convictions.

(g) The secretary of state may receive from the Kansas bureau of investigation or other criminal justice agencies, including but not limited to the federal bureau of investigation and the federal internal revenue service, such criminal history record information (including arrest and nonconviction data), criminal intelligence information and information relating to criminal and background investigations as necessary for the purpose of determining qualifications of an entity applying for or holding a license to authenticate digital signatures. ~~Upon the written request of the secretary of state, the secretary of state may receive from the district courts such information relating to juvenile proceedings as necessary for the purpose of determining qualifications of an entity applying for or holding a license to authenticate digital signatures.~~ Such information, other than conviction data, shall be confidential and shall not be disclosed except to employees of the secretary of state as necessary to determine qualifications of such applicants and license holders. Any other disclosure of such confidential information is a class A misdemeanor and shall constitute grounds for removal from office or termination of employment.

,

and juvenile offender information

(h) The secretary of state may enter into agreements with the federal bureau of investigation, the federal internal revenue service, the Kansas attorney general or any state, federal or local agency as necessary to carry out the duties of the secretary of state under this act.

(i) Unless otherwise specifically provided by law, when law requires a signature or provides for certain consequences in the absence of a signature, a digital signature shall have the same force and effect as a manual ~~signature.~~

or other signature that under law may be used to authenticate a writing.

(j) The use or acceptance of a digital signature shall be at the op[illegible] of the parties. Nothing in this act shall require a public entity to use or permit the use of a digital signature.

2-2

by the secretary of state pursuant to section 1;

or qualifications for employment with the secretary of state in connection with authentication of digital signatures by the secretary of state pursuant to section 1

(3) the court, in the order of expungement, may specify other circumstances under which the conviction is to be disclosed; and

(4) the conviction may be disclosed in a subsequent prosecution for an offense which requires as an element of such offense a prior conviction of the type expunged.

(f) Whenever a person is convicted of an ordinance violation, pleads guilty and pays a fine for such a violation, is placed on parole or probation or is granted a suspended sentence for such a violation, the person shall be informed of the ability to expunge the conviction.

(g) Subject to the disclosures required pursuant to subsection (e), in any application for employment, license or other civil right or privilege, or any appearance as a witness, a person whose conviction of an offense has been expunged under this statute may state that such person has never been convicted of such offense.

(h) Whenever the record of any conviction has been expunged under the provisions of this section or under the provisions of any other existing or former statute, the custodian of the records of arrest, conviction and incarceration relating to that crime shall not disclose the existence of such records, except when requested by:

(1) The person whose record was expunged;

(2) a criminal justice agency, private detective agency or a private patrol operator, and the request is accompanied by a statement that the request is being made in conjunction with an application for employment with such agency or operator by the person whose record has been expunged;

(3) a court, upon a showing of a subsequent conviction of the person whose record has been expunged;

(4) the secretary of social and rehabilitation services, or a designee of the secretary, for the purpose of obtaining information relating to employment in an institution, as defined in K.S.A. 76-12a01, and amendments thereto, of the department of social and rehabilitation services of any person whose record has been expunged;

(5) a person entitled to such information pursuant to the terms of the expungement order;

(6) a prosecuting attorney, and such request is accompanied by a statement that the request is being made in conjunction with a prosecution of an offense that requires a prior conviction as one of the elements of such offense;

(7) the supreme court, the clerk or disciplinary administrator thereof, the state board for admission of attorneys or the state board for discipline of attorneys, and the request is accompanied by a statement that the request is being made in conjunction with an application for admission,

6-3

or for an order of reinstatement, to the practice of law in this state by the person whose record has been expunged;

(8) the Kansas lottery, and the request is accompanied by a statement that the request is being made to aid in determining qualifications for employment with the Kansas lottery or for work in sensitive areas within the Kansas lottery as deemed appropriate by the executive director of the Kansas lottery;

(9) the governor or the Kansas racing commission, or a designee of the commission, and the request is accompanied by a statement that the request is being made to aid in determining qualifications for executive director of the commission, for employment with the commission, for work in sensitive areas in parimutuel racing as deemed appropriate by the executive director of the commission or for licensure, renewal of licensure or continued licensure by the commission; ~~or~~

(10) the state gaming agency, and the request is accompanied by a statement that the request is being made to aid in determining qualifications: (A) To be an employee of the state gaming agency; or (B) to be an employee of a tribal gaming commission or to hold a license issued pursuant to a tribal-state gaming compact; *or*

(11) the secretary of state, and the request is accompanied by a statement that the request is being made to aid in determining qualifications for licensure pursuant to section 1.

or qualifications for employment with the secretary of state in connection with authentication of digital signatures by the secretary of state pursuant to section 1

Sec. 3. K.S.A. 1996 Supp. 21-4619 is hereby amended to read as follows: 21-4619. (a) Except as provided in subsections (b) and (c), any person convicted in this state of a traffic infraction, cigarette or tobacco infraction, misdemeanor or a class D or E felony, or for crimes committed on or after July 1, 1993, nondrug crimes ranked in severity levels 6 through 10 or any felony ranked in severity level 4 of the drug grid, may petition the convicting court for the expungement of such conviction if three or more years have elapsed since the person: (1) Satisfied the sentence imposed; or (2) was discharged from probation, a community correctional services program, parole, postrelease supervision, conditional release or a suspended sentence.

(b) Except as provided in subsection (c), no person may petition for expungement until five or more years have elapsed since the person satisfied the sentence imposed or was discharged from probation, a community correctional services program, parole, postrelease supervision, conditional release or a suspended sentence, if such person was convicted of a class A, B or C felony, or for crimes committed on or after July 1, 1993, if convicted of an off-grid felony or any nondrug crime ranked in severity levels 1 through 5 or any felony ranked in severity levels 1 through 3 of the drug grid, or:

(1) Vehicular homicide, as defined by K.S.A. 21-3405 and amend-

6-4

qualifications for employment with the Kansas lottery or for work in sensitive areas within the Kansas lottery as deemed appropriate by the executive director of the Kansas lottery; (D) to aid in determining the petitioner's qualifications for executive director of the Kansas racing commission, for employment with the commission or for work in sensitive areas in parimutuel racing as deemed appropriate by the executive director of the commission, or to aid in determining qualifications for licensure or renewal of licensure by the commission; ~~or~~ (E) upon application for a commercial driver's license under K.S.A. 8-2,125 through 8-2,142, and amendments thereto; *(F) to aid in determining the petitioner's qualifications to be an employee of the state gaming agency; (G) to aid in determining the petitioner's qualifications to be an employee of a tribal gaming commission or to hold a license issued pursuant to a tribal-state gaming compact; or (H) to aid in determining qualifications for licensure by the secretary of state pursuant to section 1;*

or qualifications for employment with the secretary of state in connection with authentication of digital signatures by the secretary of state pursuant to section 1

(3) the court, in the order of expungement, may specify other circumstances under which the conviction is to be disclosed;

(4) the conviction may be disclosed in a subsequent prosecution for an offense which requires as an element of such offense a prior conviction of the type expunged; and

(5) upon commitment to the custody of the secretary of corrections, any previously expunged record in the possession of the secretary of corrections may be reinstated and the expungement disregarded, and the record continued for the purpose of the new commitment.

(g) Whenever a person is convicted of a crime, pleads guilty and pays a fine for a crime, is placed on parole, postrelease supervision or probation, is assigned to a community correctional services program, is granted a suspended sentence or is released on conditional release, the person shall be informed of the ability to expunge the conviction.

(h) Subject to the disclosures required pursuant to subsection (f), in any application for employment, license or other civil right or privilege, or any appearance as a witness, a person whose conviction of a crime has been expunged under this statute may state that such person has never been convicted of such crime, but the expungement of a felony conviction does not relieve an individual of complying with any state or federal law relating to the use or possession of firearms by persons convicted of a felony.

(i) Whenever the record of any conviction has been expunged under the provisions of this section or under the provisions of any other existing or former statute, the custodian of the records of arrest, conviction and incarceration relating to that crime shall not disclose the existence of such records, except when requested by:

(1) The person whose record was expunged;

2-5

(2) a criminal justice agency, private detective agency or a private patrol operator, and the request is accompanied by a statement that the request is being made in conjunction with an application for employment with such agency or operator by the person whose record has been expunged;

(3) a court, upon a showing of a subsequent conviction of the person whose record has been expunged;

(4) the secretary of social and rehabilitation services, or a designee of the secretary, for the purpose of obtaining information relating to employment in an institution, as defined in K.S.A. 76-12a01 and amendments thereto, of the department of social and rehabilitation services of any person whose record has been expunged;

(5) a person entitled to such information pursuant to the terms of the expungement order;

(6) a prosecuting attorney, and such request is accompanied by a statement that the request is being made in conjunction with a prosecution of an offense that requires a prior conviction as one of the elements of such offense;

(7) the supreme court, the clerk or disciplinary administrator thereof, the state board for admission of attorneys or the state board for discipline of attorneys, and the request is accompanied by a statement that the request is being made in conjunction with an application for admission, or for an order of reinstatement, to the practice of law in this state by the person whose record has been expunged;

(8) the Kansas lottery, and the request is accompanied by a statement that the request is being made to aid in determining qualifications for employment with the Kansas lottery or for work in sensitive areas within the Kansas lottery as deemed appropriate by the executive director of the Kansas lottery;

(9) the governor or the Kansas racing commission, or a designee of the commission, and the request is accompanied by a statement that the request is being made to aid in determining qualifications for executive director of the commission, for employment with the commission, for work in sensitive areas in parimutuel racing as deemed appropriate by the executive director of the commission or for licensure, renewal of licensure or continued licensure by the commission; ~~or~~

(10) the Kansas sentencing commission;

(11) the state gaming agency, and the request is accompanied by a statement that the request is being made to aid in determining qualifications: (A) To be an employee of the state gaming agency; or (B) to be an employee of a tribal gaming commission or to hold a license issued pursuant to a tribal-state gaming compact; or

(12) the secretary of state, and the request is accompanied by a state-

ment that the request is being made to aid in determining qualifications for licensure pursuant to section 1. or qualifications for employment with the secretary of state in connection with authentication of digital signatures by the secretary of state pursuant to section 1

Sec. 4. K.S.A. 1996 Supp. 12-4516 and 21-4619 and 21-4619b are hereby repealed.

Sec. 5. This act shall take effect and be in force from and after its publication in the statute book.

6-7

#7

KANSAS BOARD OF REGENTS

700 SW HARRISON • SUITE 1410 • TOPEKA, KS 66603-3760

GENERAL ADMINISTRATION - 913 296-3421 • STUDENT ASSISTANCE - 913 296-3517 • FAX 913 296-0983

TESTIMONY ON HOUSE BILL 2059

Joseph T. Barron, Jr.

February 5, 1997 - 3:30 p.m.

I am Joseph T. Barron, Jr. I am the General Counsel to the Kansas Board of Regents. I wish to speak in support of House Bill 2059. Digital signature technology is an important part of the ever-growing use of electronic media in communications and business. However, I have some questions about the application of the bill to the Regents universities.

House Bill 2059, as it relates to digital signatures, raises some questions concerning its use by the Regents universities when dealing with applications for admission to a university, financial aid application, and interactions with other state agencies such as submitting payment vouchers for vendors to the Department of Administration or obtaining the signatures required for capital improvement related documents such as architectural services on bond approvals.

In section 1(c) of the bill, the rules and regulations shall minimize forgery and fraud in "electronic commerce." Is this term broad enough to cover the use of digital signatures in applications to a university, for example?

Since the technology to create digital signatures is widely available, would applicants to a university be able to submit their own encrypted application with a digital signature to a university that could then authenticate it?

Would the university require a license from the Secretary of State in order to authenticate digital signatures or is authentication only done by outside entities?

How would the authentication of digital signatures work between agencies of the state, i.e., submitting payment vouchers to the Department of Administration?

Would the Department of Administration require a license from the Secretary of State to authenticate the university's digital signature?

How do out-of-state students or businesses use digital signatures; i.e., a student from Maine submitting an electronic application with a digital signature?

I am sure that there are more possible applications and the concern is that the bill be broad enough to permit flexibility in the use of digital signature technology so that transitions can be smooth and the state educational institutions more efficient.

House Judiciary
Attachment 7
2/5/97

#8

HEARTLAND
COMMUNITY
BANKERS
ASSOCIATION

Matthew S. Goddard, Vice President

700 S. Kansas Ave., Suite 512
Topeka, Kansas 66603
(913) 232-8215

To: House Judiciary Committee

From: Matthew Goddard
Heartland Community Bankers Association

Date: February 5, 1997

Re: HB 2059

The Heartland Community Bankers Association appreciates the opportunity to appear before the House Committee on Judiciary to request adoption of the attached amendment to HB 2059.

As more financial institutions begin to operate in cyberspace, it is important that safeguards exist to protect both the consumer and the institution. The acceptance of digital signatures is an important step in creating public confidence in the security and safety of electronic commerce and "on-line banking." Digital signatures are a significant advancement over the basic encryption methods currently utilized by most on-line institutions.

We are concerned, however, that HB 2059 is ambiguous concerning the bill's provision in New Section 1(i) that "a digital signature shall have the same force and effect as a manual signature." The attached amendment would add to New Section 1 language which clarifies it is not mandatory that a person or entity use or accept a digital signature in lieu of a manual signature.

Many businesses, including some of our membership, are not equipped to accept digital signatures. In addition, business relationships may exist with entities outside of Kansas that do not recognize them as legally binding. For example, many FHA/VA loan programs require specific copies of certain forms to be signed. A digital signature could not meet the requirements.

We respectfully request that the House Committee on Judiciary recommend HB 2059 for passage, as amended.

Thank you.

House Judiciary
Attachment 8
2/5/97

HOUSE BILL No. 2059

By Joint Committee on Computers and Telecommunications

New Section 1.

...

(j) The use or acceptance of a digital signature shall be at the option of the parties to the communication. Nothing in this act shall require a person or entity to use or permit the use of a digital signature.