# SCOMM 106:3

No: 1

# FISCAL NOTE

Bill version: HB 345
(H) Publish Date: 1/23/98

**STATE OF ALASKA**
**1998 LEGISLATIVE SESSION**

Revision Date (Note if correction) _____ Dept. Affected All state agencies
Title An Act relating to electronic records and signatures. BRU _____
Component _____
Sponsor Rules Committee
Requester Governor Component Serial No. _____

**Expenditures/Revenues** (Thousands of Dollars)

| OPERATING EXPENDITURES | FY 99 | FY 00 | FY 01 | FY 02 | 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 | | | | | | |
| CHANGE IN REVENUES ( ) | | | | | | |

**FUND SOURCE** (Thousands of Dollars)

| | | | | | | |
|---|---|---|---|---|---|---|
| 1002 Federal Receipts | | | | | | |
| 1003 GF Match | | | | | | |
| 1004 GF | | | | | | |
| 1005 GF/Program Receipts | | | | | | |
| 1037 GF/Mental Health | | | | | | |
| Other (Specify Type) | | | | | | |
| TOTAL | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 |

**Estimate of any current year (FY98) cost:** _____

**POSITIONS**

| | | | | | | |
|---|---|---|---|---|---|---|
| Full-time | | | | | | |
| Part-time | | | | | | |
| Temporary | | | | | | |

**ANALYSIS:** *(Attach a separate page if necessary)*

This bill would not have a significant fiscal impact on any state agency.

Prepared by Jack Kreinheder Jack Kreinheder Phone 465-4676
Division Office of Management and Budget Date 1/6/98
Approved by Commissioner Jim Ayers, Chief of Staff Date _____
Agency Office of the Governor

**PREPARER TO PROVIDE ALL DISTRIBUTION COPIES TO GOVERNOR'S LEGISLATIVE OFFICE**
For further distribution information, call the Governor's Legislative Office

**COMMITTEE COPY**

HOUSE SPECIAL COMMITTEE ON TELECOMMUNICATIONS
February 11, 1998
4:05 p.m.

MEMBERS PRESENT

Representative Brian Porter, Chairman
Representative Ivan Ivan
Representative Fred Dyson
Representative Ethan Berkowitz

MEMBERS ABSENT

Representative Jeannette James

OTHER HOUSE MEMBERS PRESENT

Representative J. Allen Kemplen

COMMITTEE CALENDAR

* HOUSE BILL NO. 345
"An Act relating to electronic records and signatures, revising certain requirements that signatures be notarized or verified, and providing for electronic records in the state archives; relating to the permanency of records in the state archives; and providing for an effective date."

- MOVED HB 345 OUT OF COMMITTEE

(* First public hearing)

PREVIOUS ACTION

BILL: HB 345
SHORT TITLE: STATE ARCHIVES RECORDS
SPONSOR(S): RULES BY REQUEST OF THE GOVERNOR

| Jrn-Date | Jrn-Page | | Action |
|---|---|---|---|
| 01/23/98 | 2116 | (H) | READ THE FIRST TIME - REFERRAL(S) |
| 01/23/98 | 2116 | (H) | TEL, LABOR AND COMMERCE |
| 01/23/98 | 2117 | (H) | ZERO FISCAL NOTE (GOV/ALL DEPTS) |
| 01/23/98 | 2117 | (H) | GOVERNOR'S TRANSMITTAL LETTER |
| 02/11/98 | | (H) | TEL AT 4:00 PM CAPITOL 120 |

WITNESS REGISTER

ANDY KLINE, Special Staff Assistant
Office of the Lieutenant Governor
P.O. Box 110015
Juneau, Alaska 99811-0015
Telephone: (907) 465-3520
POSITION STATEMENT: Presented HB 345 and answered questions.

ACTION NARRATIVE

TAPE 98-1, SIDE A
Number 0001

CHAIRMAN BRIAN PORTER called the House Special Committee on Telecommunications meeting to order at 4:05 p.m. Members present at the call to order were Representatives Porter, Ivan and Dyson. Representative Berkowitz arrived at 4:13 p.m.

CHAIRMAN PORTER advised listeners that the committee had been established the previous year by resolution to look at telecommunications issues for the House, and had met during the interim.

HB 345 - STATE ARCHIVES RECORDS

CHAIRMAN PORTER announced the committee would hear HB 345, "An Act relating to electronic records and signatures, revising certain requirements that signatures be notarized or verified, and providing for electronic records in the state archives; relating to the permanency of records in the state archives; and providing for an effective date." He called on Andy Kline to present the bill.

Number 0063

ANDY KLINE, Special Staff Assistant, Office of the Lieutenant Governor, advised members he is a special assistant for telecommunications to Lieutenant Governor Fran Ulmer, who chairs the Telecommunications Information Council (TIC), the main policy-making body in state government for telecommunications and information technology. Mr. Kline added that he staffs that council and had therefore been chosen to testify on this bill.

MR. KLINE said through their telecommunications planning effort, the TIC had identified electronic signatures as an important issue to resolve in state government, and in December of 1996 they had released a state plan on telecommunications and information technology. In that plan, recommendation number 56 is that the

state should address the use of electronic signatures, which will streamline many internal processes and will position the state for a method of authentication and verification of electronic communications with the public.

MR. KLINE advised members that 28 other states have enacted electronic signature and digital signature legislation. Alaska is not on the leading edge but is trying to stay in the pack, ready and open for business on the Information Highway.

Number 0216

MR. KLINE told members that a number of internal state government functions and other types of functions that electronic signatures will help have been identified nationwide, and even internationally. Utah is probably the leading state in electronic signatures, and many other states lean on Utah's progress and mistakes in developing statutes and regulations regarding electronic signatures.

MR. KLINE stated, "I can tell you from Utah's point of view, they have a short list in that packet that I gave you of the things that they see as specific applications, including court filings and corporation filings, procurement, grant applications, motor vehicle titling, real estate transactions. I mean, the list kind of is endless, with the way that business interacts with state government, ... with the way that business interacts with other business in a state, and in the way the public interacts, in a transactional way, with state government." Mr. Kline said this allows a person, with a click of a mouse button, to encrypt a document and make it verifiable who sent it.

Number 0303

MR. KLINE pointed out that someone receiving an E-mail message today has no way of really knowing whom it came from without verification, because there are simple ways to electronically modify addresses and so forth to indicate that a message came from another source. Verification can be done through a number of methods.

MR. KLINE informed members that three kinds of legislation have been passed nationally dealing with electronic signatures, as described by the Internet Law and Policy Forum, a think-tank organization. The three types of legislation are: prescriptive, the most detailed; criteria-based, which is in the middle; and signature-enabling, which reduces barriers existing in law today that say things like "must be signed," which in legal terms means

a piece of paper signed.

MR. KLINE cited Utah's as the best example of prescriptive legislation. In Utah, they had set out detailed implementation in statute. Although on-target at the time, it became problematic because of rapidly changing technology, resulting in one revising piece of legislation already. Therefore, Utah's legislation is a good example of going too far.

Number 0430

MR. KLINE said Massachusetts has the best example of signature-enabling legislation. It doesn't get into any technical standards or criteria upon which a signature is determined to be verifiable. Instead, it says electronic signatures are as good as written signatures.

MR. KLINE advised members that California and Georgia have criteria-based legislation, which is middle ground. "And that's the model that we chose to go with," Mr. Kline explained. "We felt that there needed to be some language that talked about what the state would accept ... as a verifiable signature. So, that's in the law itself."

MR. KLINE referred to page 2, beginning on line 29, which sets out criteria: "'electronic signature' means an electronic or digital method, executed or adopted by a person with the intent to be bound by or to authenticate a record, that is unique to the person using it, is capable of verification, is under the sole control of the person using it, and is linked to data in such a manner that if the data are changed the electronic signature is invalidated ...." Mr. Kline noted that Massachusetts' legislation hadn't gone that far.

Number 0548

MR. KLINE said the main things they want to address in HB 345 are removing those legal barriers and setting these simple criteria for potential technologies. He pointed out that different methods exist to obtain digital signatures, such as using public and private keys; for example, a person may hold a private diskette that uses encryption technology, to put together with a public "key" for verification. Mr. Kline explained that they had not been specific with the criteria in the framework because of foreseeable technological changes. In addition, few citizens or industries in Alaska today are really ready to start using these complicated and sometimes costly methods of getting public and private keys. Mr. Kline said they want to allow industry to come in and answer those questions, with technology that fits into the law.

Number 0669

CHAIRMAN PORTER recognized Representative Kemplen, who had joined members at the table. Noting that signatures are essential to some documents, he asked Mr. Kline what the thought is on litigation relating to lack of specific criteria for verification.

MR. KLINE explained that the specifics of the technology that will be used to make verifiable signatures will be handled through a regulation process. The state will speak to what technologies are acceptable, but they believe it is best handled not through statute but through regulation, in order to adapt more easily to changing technologies. Mr. Kline said they are not leaving it wide-open. However, following the problems that Utah, especially, has had, they didn't believe it was appropriate to address that in the original legislation.

Number 0781

CHAIRMAN PORTER advised members that present to answer questions were Sarah Felix from the Office of the Attorney General; John Stewart and George Smith from the Division of Libraries, Archives and Museums; and Mike Monagle from the Division of Banking, Securities and Corporations.

Number 0795

REPRESENTATIVE J. ALLEN KEMPLEN asked which industries Mr. Kline envisions as most likely to take advantage of this change in the law.

MR. KLINE said he believes banks will be the first to do so. From there, economies of scale come in. Large industries will find a small savings per transaction by using electronic signatures, and an entity with numerous transactions, or with transactions involving large dollar amounts, will benefit most. Mr. Kline said they see this as a wave of the future, noting that four years ago, many people wouldn't have predicted how much electronic mail has changed the business process. "And we feel that this is the next logical step," he concluded.

Number 0879

REPRESENTATIVE KEMPLEN asked whether Mr. Kline has information from other states about the volume and rate of growth of the demand for electronic signatures.

MR. KLINE answered that except in Utah, this really isn't happening

much in practice. Utah, he explained, is forward-thinking when it comes to technology, and they are attracting technology businesses and industry through this type of legislation. There is some information on the Utah Website concerning demand, mostly around high technology industries that want to use electronic signatures as part of a paperless way of doing business.

MR. KLINE noted that electronic signatures, inasmuch as they allow for paperless government and business transactions, can be a part of incredible efficiencies. As an example he cited Cisco Systems, a large company whose chief information officer had said that by going completely paperless - and by using other, purely electronic, ways of dealing with employees, including training, travel reimbursements and payroll - that company saves $360 million yearly. Mr. Kline suggested that high-technology industries with numerous transactions see this as something friendly to their businesses.

Number 0998

REPRESENTATIVE KEMPLEN asked whether this is mostly interstate or intrastate.

MR. KLINE replied, "It's both, and also internationally. And that's a difficult part of the law: How do you mesh what different states and different countries are doing, and are saying are verifiable signatures?" He indicated that isn't really addressed in HB 345, then added that it can be problematic to specify which types of technology will be accepted. Mr. Kline stated, "What we're saying is that ... if there's two parties and they're both agreeing, and the signature is verifiable through a mutually agreed verification process that the state has approved through regulations, then that's an acceptable signature."

MR. KLINE pointed out that firms in Washington State and Pacific Rim countries are conducting business with electronic signatures. He said in Washington State, digital signature legislation was recently passed, largely because Microsoft wanted to see it passed because they want to conduct business this way.

Number 1083

REPRESENTATIVE KEMPLEN asked whether if this legislation is passed, it would it be a significant incentive for some industry to locate here in Alaska because of the state's providing this flexibility.

MR. KLINE replied that it is a signal to high-technology firms, especially, that Alaska is a technologically aware state. He

hadn't seen anything that says industries are some quantifiable percent more likely to locate in an area that has electronic signature legislation. However, high-technology firms look for states that are forward-thinking in technology legislation when they are locating.

Number 1149

REPRESENTATIVE ETHAN BERKOWITZ asked whether there is any provision for facsimile signatures.

MR. KLINE replied that it doesn't address faxes specifically, and faxes are problematic. Most digital signature legislation assumes use of a computer and that a person can encrypt something using a logarithmic encryption device; that is not really possible on a fax. Mr. Kline pointed out that faxes are some of the most easily forged types of documents, because everything is already fuzzy and it is easy to make something look authentic.

Number 1207

REPRESENTATIVE BERKOWITZ explained that part of the reason he'd asked is that on page 21, it says, "'electronic record' means any information that is recorded in machine-readable form." He suggested that signatures could be read into machines.

MR. KLINE said that is a good point, for which he didn't have a specific answer.

Number 1240

REPRESENTATIVE IVAN IVAN referred to the zero fiscal note and asked about any technological requirements to use this.

MR. KLINE responded that it is difficult to answer only because they haven't specified a technology associated with this bill. However, most encryption programs are software, which work on existing mainframe computers or existing personal computers (PCs). Although he couldn't say that there wouldn't be a penny spent on software or a scanner, for example, there certainly are no widespread, large costs associated with passing legislation about using verifiable electronic signatures on legal documents.

Number 1321

CHAIRMAN PORTER noted that to be consistent with this law, if data on the document were altered, the electronic signature would be invalidated. He suggested it would require software.

MR. KLINE agreed, saying it requires software on both ends. He suggested that if the state is concerned about costs, they could say, "The state recognizes a certain type of signature as a verifiable electronic signature, but we're not going to be the certifying agency; we're not going to be the certification authority. Key Bank, National Bank of Alaska, will be the certification authority. They will buy a license from us to become that certification authority. They'll own the software, own the hardware, ... and people will have to take a document to them to verify it." Mr. Kline pointed out that there are different ways of doing it. It could be set up in-house, with the Department of Administration, for example, having a certification authority within it that verifies electronic signature documents. "And we've left that up to regulation, as well," Mr. Kline added.

Number 1387

CHAIRMAN PORTER asked about the evolution in other states, and whether this might become a nationally recognized system, for example.

MR. KLINE referred to a 133-page document from the American Bar Association, which he said was an attempt to make a nationwide model legislation. "They couldn't do it," he explained. "They came up with digital signature guidelines, which ... actually shaped what Utah ended up doing. But the short answer is no, different states have tended to want to do different types of things. As I said, Washington's very concerned about dealing with Japan, for instance. Other states are concerned with other types of activities. ... And then ... there are different philosophies on how detailed ... the initial statute should be. And for that reason, there isn't a nationwide standard yet."

MR. KLINE continued, "And that's one reason why we're holding back on specifying a standard, because ... we're recognizing here that this is technology that is not fully and widespread developed to this point. The technology is there, and people understand how to use it. There's not a huge, widespread demand at this point. There may be by next January. Next February, there may be a huge demand, and we all know how fast technology moves. And that's why ... we don't want to have unnecessary legal barriers in the way of that happening, if it becomes a widespread-type of thing, or something that industry ... is demanding."

Number 1475

REPRESENTATIVE BERKOWITZ said, "The reason why we're addressing this sort of legislation, it seems to me, is the banks, or whatever

group decides to use electronic signatures, is going to do so at its own peril. But we need to put some kind of enabling legislation down in order that they can venture out into that minefield?"

MR. KLINE replied, "That's right. That's one part of it. And the other part of it is we want state government to be able to interact with business and citizens, and do it in a way that's consistent with our laws. ... And in large part, it's recognizing something brand new, that wasn't envisioned when laws were passed about having a signature on a piece of paper, to verify that."

Number 1520

CHAIRMAN PORTER asked whether there were further questions. He expressed his understanding that the bill is not trying to answer all questions available to be asked on this type of technology. Chairman Porter added, "And I think if there was ever an area that was conducive to regulation, as opposed to statute, it would be telecommunications." He asked the wish of the committee.

Number 1545

REPRESENTATIVE FRED DYSON responded, "Move it."

CHAIRMAN PORTER noted the motion to move the bill with individual recommendations and fiscal notes as attached. He asked whether there was any objection. There being none, HB 345 was moved from the House Special Committee on Telecommunications.

Number 1591

CHAIRMAN PORTER called an at-ease at 4:28 p.m. in order to prepare for the joint work session with the Telecommunications Information Council policy committee. [See cover sheet relating to that portion of the meeting.]

## TIC Policy Committee/House Special Committee on Telecommunications

Feb. 11, 1998

***Discussion Items***

1. Year 2000 - Annalee McConnell
2. Using Technology to Deliver Services (DMV, Etc.) -- Mark Boyer
3. E-Rate Subcommittee -- Subsidy for schools and Rural Health Care Providers - Lt. Governor Ulmer
4. FCC Advisory Committee -- Lt. Governor Ulmer
5. Standards for Government Systems -- Email and Office Products -- Andy Kline
6. Other TIC Committees --
   - Emergency Services
   - Webmaster
   - Technical Advisory Committee
7. Progress on TIC Plan -- (70 of 90 recommendations in progress or met) -- Andy Kline

TONY KNOWLES
GOVERNOR

P.O. Box 110001
Juneau, Alaska 99811-0001
(907) 465-3500
Fax (907) 465-3532

STATE OF ALASKA
OFFICE OF THE GOVERNOR
JUNEAU

February 5, 1998

The Honorable Mike Miller
President of the Senate
Alaska State Legislature
State Capitol, Room 107
Juneau, AK 99801-1182

The Honorable Gail Phillips
Speaker of the House
Alaska State Legislature
State Capitol, Room 208
Juneau, AK 99801-1182

Jerome Komisar, President
University of Alaska
P.O. Box 755000
Anchorage, AK 99508-4675

Chief Justice Warren Matthews
Alaska Supreme Court
303 K Street
Anchorage, AK 99501-2084

Dear Speaker Phillips and Gentlemen:

As you are undoubtedly aware, the Year 2000 computer problem has virtually every business, organization, and government in the world working to ensure continuity of services as we head into the next century. An astonishing variety of things we take for granted are potentially impacted if computer codes are not rewritten to expand date fields from two digits to four. For governments, everything from check writing to elevator controls and prison release dates could be affected.

We have been analyzing the situation for the executive branch. We established a Year 2000 Task Force under the Telecommunications Information Council which has assessed executive agency progress and provided some technical assistance. Our next step is the selection of a full-time Year 2000 project manager who will work under the Director of Management and Budget.

We are confident from our assessment work that the executive branch is positioned to correct the Year 2000 problem in a timely fashion. Many states are finding it can be a costly and time-intensive effort to make the changeover in all their computer systems. To ensure the necessary resources will be directed in the most coordinated, cost effective way possible, we believe it would be appropriate to undertake a cooperative effort among

all branches of state government. Together, we have an obligation to ensure services to Alaskans are not compromised by the Year 2000 problem.

We propose a task force consisting of top-level representatives of the executive, legislative, and judicial branches and the University of Alaska. We also think it would be extremely beneficial to include representatives of two or three large Alaska businesses that can give us the benefit of their private sector advice. This group will help guide our efforts and oversee the massive amount of work that must occur in all state entities.

I am asking Commissioner Mark Boyer and OMB Director Annalee McConnell to represent the executive branch in this important work group. I urge you each to appoint a legislator—or for the courts and university, a senior policy-level manager—to represent you in this critical effort.

Since this work is time critical, we propose an initial meeting next week on Tuesday, February 10, at 3:30 p.m. in the Governor's Conference Room. Please contact Kari Spencer at (907) 465-3986 with the name of your representatives so we can confirm the meeting time directly with them. Video conference facilities will be available if everyone cannot be in Juneau.

Thank you in advance for being willing to face this challenge together. I believe our joint effort will serve Alaskans well.

Sincerely,

Tony Knowles
Governor

# Personalized License Plates Online
# Alaska Division of Motor Vehicles

**1.** Enter a personalized plate that is 2 to 6 characters: TICK


**2.** Select a plate and press "Check it out!" to view each plate with your personalized message.

Check it out! Reset

**NOTE!** If you use less than 6 letters or numbers on your plate, use the space bar to position the letters or numbers where you want them to be placed.

**What you CAN USE on a personalized license plate:**

Letters A to Z
Numbers 0 to 9
Spaces

**What you CANNOT USE on a personalized license plate:**

Ham radio call signs
Three letters followed by three numbers
Four numbers followed by two letters
Special symbols such as -, #, %, &, etc.
Duplicates of active personalized plates
Ethnic, racial, vulgar, or indecent connotations

**Registration Renewal by Phone:**
IVR Registration Renewal: (907) 269-5590, (888) DMV-KWIK

- Additional Vehicle License Plate Information
- DMV home page
- Vehicle Registration Renewal

# TICK

Yes! I want this plate.

**Congratulations! Your plate is available. To order this plate please fill out the form below and click on NEXT.** (You can find the necessary information on your vehicle registration card).

| | |
|---|---|
| Registration Renewal Number (RRN): | |
| **OR** | |
| License Plate Number: **and** Last 2 of VIN/Serial Number: | |

| | |
|---|---|
| First Name | |
| Last Name | |

Next

# Universal Service Fund (E-Rate)

## What's at stake for Alaska's schools, libraries, and rural health care facilities?

Hundreds of thousand of dollars in phone charges and other telecommunication savings! These discounts will reduce monthly charges and the costs of interior connections, making it possible to reallocate those dollars and acquire more services.



**For Alaskans**

**Keeping Current**

**Mailing Lists**

- Here are three email listservs which pertain the Universal Service Fund:
  **FCCsend** is a one-way listserv that provides the latest FCC updates and suggestions for preparing your school or library to get the most out of communications technology.
  To subscribe, send e-mail to: subscribe@info.fcc.gov. In the message, write: sub FCCsend yourname
  **FCCshare** is an interactive listserv for communicating with teachers, parents and others using education technology.
  To sign up, send e-mail to: subscribe@info.fcc.gov. In the message, write: sub FCCshare yourname
  **AK-Telecom-L** is an interactive listserv for Alaskans to talk about telecommunication issues in Alaska.
  To subscribe, send e-mail to: listserv@galileo.uafadm.alaska.edu. In the message, write: sub AK-Telecom-L yourname

**Additional Resources**

- Alaska Public Utilities Commission (APUC) APUC will play a major role in interpreting and implementing the Universal Service provisions of the Telecommunications Act in Alaska.
- American Library Association-Universal Service The American Library Association's Office of Information Technology Policies reports on developments as they affect libraries.
- ATU Telecommunications ATU gives their interpretation of the new program and offers limited technical advice to schools and libraries statewide.
- Education and Library Networks Coalition (EdLINC) This news formatted site is put up by a coalition of education and library networks. Rulings and issues that impact library and educational networks are highlighted here.
- FCC-Telecommunications Act of 1996 The Federal Communication Commission's page which details the Commissions actions and communications on the Telecommunications Act.
- National Exchange Carrier Association The organization who will "administer" the Universal Service Fund.
- NetDay Alaska 2000 NetDay Alaska is a grass roots volunteer effort to get all of Alaska's schools wired for Internet Access by the year 2000. It is sponsored by the Alaska Science & Technology Foundation.
- Northwest Educational Technology Consortium (NETC) An organizational page which will link you to many sites concerned with FCC Universal Service decisions, implementation, etc.

Posted by: T. Swaim, February 4, 1998, Alaska State Library

For Alaskans

ALASKA STATE LIBRARY

# Letter from the Lt. Governor and the Commissioner of Education

July 17, 1997

Dear Alaska Superintendents, Library Directors and Private Schools:

The Federal Communications Commission (FCC) Report and Order regarding the Universal Service Fund issued on May 8, offers tremendous potential for Alaska's schools and public libraries. The fund established an Educational Rate (E-Rate) which will give schools and libraries across the country access to more than 2.25 billion dollars in discounts for telecommunications services.

As this is a new program, details are still being worked out at both the state and federal levels. The U.S. Department of Education (USDOE) and a coalition of education groups are working on the design of the application and the review and approval process at the federal level. Once applications are approved, the Alaska Department of Education will distribute those forms to all schools districts, private schools, and public libraries. We expect the forms to be available sometime in August.

The First step in allowing our schools and libraries to participate in the universal service fund was taken on July 9, when the Alaska Public Utilities Commission adopted R-97-4, Intrastate Discounts for Schools and Libraries, which match the federal discount matrix. Eligible schools and libraries can receive discounts of 20 to 90 percent on telecommunication services, Internet access and internal connections necessary for bringing technology into the library or classroom. Information on where to find the amount of your discount is found in the attachment.

In addition to completing an application, all schools or school districts and public libraries must complete a technology assessment/inventory and a technology plan in order to be eligible for the discounts. Those inventories and plans must be certified by a state agency as determined by each state. In Alaska, the State's Telecommunications Information Council (TIC) and the Department of Education have formed a committee to certify plans for both schools and libraries. Karen Crane, Director of Libraries, Archives and Museums will chair the Technology Certification Committee (TCC) composed of state members from the Department of Education, the University of Alaska, the Alaska Society for Technology in Education, and public members.

In order to expedite the process and to allow Alaskan participants to submit timely requests, we have determined the state will set no additional requirements for technology plans beyond those outlined by the FCC. The FCC guidelines are listed in the information sheets enclosed with this letter. The state will begin reviewing and certifying plans in mid-August.

There are a number of resources available to answer your questions. We have posted information on the Department of Education's web page (http://www.educ.state.ak.us). This web site will keep you advised on the state time lines and actions. It also points to related sites of interest such as the FCC, USDOE, EdLinc and others. The State Library's school library media coordinator, Della Mathis, is also

knowledgeable about the process. She can be reached in Anchorage at 269-6568 or by email at dmathis@educ.state.ak.us.

The department will begin accepting plans for review on August 11, 1997. [Nine (9) copies]* of the plan should be sent to:

Karen Crane, Director
Libraries, Archives and Museums
P.O. Box 110571
Juneau, AK 99811-0571

These discounts represent a great potential for all of Alaska's teachers, students and for the general public through their public libraries, to have greater access to a wide range of educational resources. We urge you to participate and we look forward to working with you during the process.

Sincerely,

Fran Ulmer,
Lieutenant Governor
Chair, TIC

Shirley Holloway
Commissioner
Department of Education

*[Nine (9) copies] This has been modified; the original was Seven (7) copies.

---

Key Dates | Preparation Steps | Main Page | Alaska State Library Home Page
If your question was not completely answered here, please send an e-mail to dellam@muskox.alaska.edu and we will try to find an answer for you.

Posted by: T. Swaim, Alaska State Library, August 1, 1997

## Local and State Government Advisory Committee Meeting
## Expected Participants

**LSGAC**

**Kenneth S. Fellman**
City Council Member
Arvada, CO

**Mayor Michael Guido**
Dearborn, MI

**Rep. Myra Jones**
Little Rock, AR

**Timothy M. Kaine***
Council Member
Richmond, VA

**Senator Douglas Kristensen**
Lincoln, NE

**Commissioner Darryl T. Owens**
Jefferson County, KY

**Mary Poss**
City Council Member
Dallas, TX

**Marilyn J. Praisner**
President
Montgomery County Council

**Louise H. Renne**
City Attorney
San Francisco, CA

**Commissioner David A. Svanda**
MI Public Service Commission

**Lt. Governor Fran Ulmer**
Juneau, AK

***Unable to Attend:***
***Mayor Victor Ashe, Knoxville, TN***
***Mayor Bill Campbell, Atlanta, GA***
***Commissioner Randy Johnson, Minneapolis, MN***
***Pat Spears, ICOUP***

* *To be confirmed*

**State and Local Government Reps**

**Bob Fogel**
NACO

**Jane Lawton**
Montgomery County

**Tim Masanz**
NGA

**Nick Miller**
Miller & Van Eaton

**Barrie Tabin**
NLOC

**Neil Osten**
NCSL

**J. Bradford Ramsey**
NARUC

**Marideth Sandler**
Office of Lt. Gov. Fran Ulmer

**David Thorpe**
NCSL

**FCC Staff**

**Susan Fox**
Office of General Counsel

**Blair Levin**
Chief of Staff

**Commissioner Susan Ness**
FCC

**Sheryl J. Wilkerson**
Office of General Counsel

[ text version ]

**DA 97-460**
**February 28, 1997**

# Chairman Hundt Appoints Members to the Local and State Government Advisory Committee

Today, Chairman Reed E. Hundt announced the appointment of 13 members to the Commission's newly formed Local and State Government Advisory Committee. Chairman Hundt announced the formation of the Advisory Committee at the Commission's public forum on the use and management of public rights-of-way in the provision of telecommunications services.

The members of the Local and State Government Advisory Committee are: The Honorable Victor Ashe, Mayor of Knoxville, TN; The Honorable Bill Campbell, Mayor of Atlanta, GA; Ken Fellman, City Council Member, Arvada, CO; The Honorable Michael Guido, Mayor of Dearborn, MI; The Honorable Randy Johnson, Commissioner, Hennepin County, Minneapolis, MN; Representative Myra Jones, Little Rock, AR; Timothy M. Kaine, Council Member, Richmond, VA; Senator Douglas Kristensen, Minden, NE; The Honorable Darryl T. Owens, Commissioner, Jefferson County, Louisville, KY; Mary Poss, City Council Member, Dallas, TX; The Honorable Marilyn J. Praisner, President, Montgomery County Council, Rockville, MD; David A. Svanda, Commissioner, Michigan Public Service Commission; and Lieutenant Governor Fran Ulmer, Juneau, AK. Chairman Hundt will also appoint a Tribal government representative to the Advisory Committee.

The Committee will facilitate intergovernmental communication between local and state governments and the Commission. The Committee will also provide advice and information to the Commission on key issues that concern local and state governments and communicate state and local government policy concerns regarding proposed Commission actions pursuant to the Telecommunications Act of 1996. The Local and State Government Advisory Committee was established pursuant to Section 204(b) of the Unfunded Mandates Reform Act of 1995, Pub. L. No. 104-4, 109 Stat. 66, the Committee is not subject to, and will not follow, the procedures set forth in the Federal Advisory Committee Act 5 U.S.C., App. 2 (1988).

"I am pleased to announce the appointment of this impressive group of public servants to the Local and State Advisory Committee," said Chairman Hundt. "Their combined experience in local and state government and telecommunications policy and development will be of immense value to the Commission. Since implementation of the 1996 Act, it has been increasingly important for the Commission to understand how our rules impact local and state governments. Congress established a framework in which we all must work together to promote, not impede competition. We at the Commission know that to bring real competition to the communications marketplace is going to take hard work from federal, state and local governments alike. I look forward to hearing the perspectives of the local and state governments and to working with the members of the Committee."

For further information on the Local and State Government Advisory Committee contact Sheryl J. Wilkerson in the Office of General Counsel at (202) 418-1700, 1919 M Street, N.W., Room 614, Washington, D.C. 20554.

Action by the Office of General Counsel.

- FCC -

# MEMORANDUM

# STATE OF ALASKA
**Office of the Lieutenant Governor**

**TO:** Telecommunications Information Council (TIC) **DATE:** Nov. 20, 1997

**FROM:** Fran Ulmer
Lieutenant Governor

**TELEPHONE:** 907-465-3520
**FAX:** 907-465-5400

**E-MAIL:** fran_ulmer@gov.state.ak.us

**SUBJECT:** Enterprise-wide Email System; TIC Appropriation

The TIC Policy Committee met on Nov. 18, 1997 and considered recommendations for an enterprise-wide email system and proposals for spending a portion of the $433,000 appropriation for enterprise-wide needs related to information technology. This is a brief report on our recommendations.

**Email system:**

Earlier this year the TIC endorsed the concept of moving forward to establish an enterprise-wide Email system. The TIC Policy Committee has accepted the recommendations of the Email Design Team in their report dated September 5, 1997. The proposed design will provide for a central system that will be of immediate benefit to agencies that do not have special messaging needs. This design will also allow for the state to alleviate much of the pressure being put on an aging and increasingly fragile Email backbone maintained by the Department of Administration. The design will also allow for Departments that are in need of this service to transfer first, and Departments with more specialized needs to work with a new Electronic Messaging Committee on gradual implementation of the new system.

The Electronic Messaging Committee will periodically review the design and adapt it to a changing technological environment. Committee members include: Brian Duncan, Administration; Larry Talley, Fish and Game; Leo Lutchansky, Transportation and Public Facilities; Richard McMahon, Natural Resources; David Simons, Health and Social Services; Mike Pusich, Governor's Office; Chair - Rick Cross, Education.

**Technology appropriation**

The TIC Policy Committee received many excellent suggestions on how to use these funds. The two which are the most time-sensitive and which will benefit the entire cabinet are:

1. Use $175,000 as a match to University of Alaska funds for a **technology training program**. The TIC Telecommunications and Information Technology Plan identified lack of adequate training opportunities as one of the biggest internal problems for state agencies. This program establishes a TIC, Gartner Group, and University information technology knowledge growth program. The program will deliver to State employees, Alaska students, and University faculty easy access to online courses, and multimedia and computer assisted courses at no cost to State employees. The Gartner Group learning resources are state of the art. In partnership coupled with University of Alaska campuses, many needs can be addressed.

2. Use $50,000 towards the **Year 2000** compliance effort. A Year 2000 committee chaired by Don Wanie of the Department of Administration is developing methodologies, project timelines and goals for the Year 2000 conversion effort the state must undertake. This money will help pay for some of the initial project administrative costs so that we can organize an effective response program, assisting all agencies.

If you have objections to using the money for these two purposes, please let me know soon. We can call a full meeting of the TIC to discuss it if necessary. The remainder of the funds will be considered for other appropriate technology expenditures in the near future.

**TONY KNOWLES**
Governor

P.O. Box 110001
Juneau, Alaska 99811-0001
(907) 465-3500

**STATE OF ALASKA**

**JUNEAU**
**MEMORANDUM**



**TO:** Fran Ulmer
Lieutenant Governor
Chair, Telecommunications Information Council

**DATE:** September 5, 1997

**FROM:** Rick Cross
Deputy Commissioner, Dept. Of Education
Chair, Email Design Team

**TELEPHONE:** 465-2800

**SUBJECT:** Enterprise Email Design

Enclosed please find a proposal for a new enterprise Email system for the State of Alaska. This is a report put together by the Email Design Team which was assigned with the task of designing a new, more functional and more efficient electronic messaging system for the State.

The Team met for two full days and two half days over the past two months. Team members were assigned with researching various aspects of the existing system and the proposed design. The report is based on what the team believes is the best data we could find, and a good faith effort on all members to put the needs of the state as a whole before the needs of their individual agencies. I think the proposed design answers the needs of the State, agencies and individual users.

I would like to thank the design team members for their hard work and their determination to produce the best design possible. The team members are:
Bill Bohlman, Department of Transportation and Public Facilities
Brian Duncan, Department of Administration
Richard McMahon, Department of Natural Resources
David Riccio, Alaska Permanent Fund Corporation
Joe Spears, Department of Community and Regional Affairs
Larry Talley, Department of Fish and Game

The Design Team feels that this proposal should be considered by both the TIC Policy Committee and the TAC before implementation. But this process should take place as quickly as possible. The proposal calls for a January 1, 1998 start-up date for the new system. To achieve this goal, the TIC process must move quickly on a number of recommendations.

Enclosure

# An Enterprise Email System for the State of Alaska

**A Proposal to the Telecommunications Information Council**

**Submitted by the TAC Email Design Team**

CONTENTS

# Introduction

## *Background*

### Existing Conditions

As of July 1997 the State of Alaska has no single enterprise Email system. Email to, from and within state government is handled by a variety of agency Email systems interconnected by an Email backbone (Appendix 4). This complex system does deliver mail, but it is expensive, there is no reliable directory service and address formats are not consistent between departments, and the exchange of attachments between departments is problematic. In addition a significant number of State agencies are experiencing constraints and limitations of their LAN based Email systems and are in the early stages of planning for their replacements.

Meanwhile the last two years have seen significant increases in the use of and dependency on electronic messaging among agencies and with the public, primarily through Internet and Intranet/WAN based messaging services. Open messaging standards have evolved, matured, and been adopted by a significant segment of the State's customers and the world in general. Internet services (and Internet messaging services in particular) are becoming significant and mission critical in the State's daily business.

### Design Team Created and given their Initial Charge

The TIC Policy Committee appointed seven TAC members to an Email Design Team on July 14, 1997 to develop a proposal for an enterprise Email system. Instructions to the Email Design Team were verbal and emphasized the TIC's desire for a less expensive but more seamless, consistent and reliable enterprise Email system. The Email Design Team was instructed to aim for an eighty-percent solution (i.e., satisfy eighty-percent of the functionality required), rather than try to design a system that would do everything for everyone. The TIC Policy Committee specified more explicit goals in a memorandum from John Lindback dated July 17, 1997 (appendix 6).

The design team was charged with the task of "thinking out of the box" and to be technologically aggressive in their designs.

The design team broke the work down into component parts. First, to define an architecture for statewide messaging services that would be as universal and extensible as possible. Second, to propose a specific implementation of that architecture which would provide for the immediate replacement of the State's aging Email backbone and provide basic functionality for those agencies currently facing the obsolescence of their LAN based Email systems.

## *Vision*

As a long term goal the Email Design Team adopted the electronic messaging vision propounded by the federal Government-wide Email Program Management Office, to wit:

> ***A service that appears to the user to be a single, unified electronic postal system that offers robust and trustworthy capabilities with legally sufficient controls for moving all forms of electronic information among employees at all levels of government, and with the public we serve; and, like the Nation's telephone network, is affordable, ubiquitous, efficient, accessible, easy-to-use, reliable, cost effective, and supported by an effective directory service.***
> ***[URL http://www.fed.gov/arch/final/intro.html]***

It should be noted that this design proposal does not address the vision of "*robust and trustworthy capabilities with legally sufficient controls*" at a level that will meet all the requirements of state agencies.

However, our design does consider these issues and our intent is to establish a baseline capability that can be enhanced in future phases to fully implement this vision.

## *Design Goals*

The overall goal for the new messaging services for the State of Alaska is to put in place the needed organizational infrastructure and adopt a design architecture which will:

1. Be as cost efficient as is practical,
2. Foster sharing and cooperative use of IT resources across State agencies,
3. Support the existing State electronic messaging needs,
4. Allow for easy and convenient use by State employees,
5. Be easily extensible for future needs,
6. Allow for flexible implementations to support the variety of agency needs,
7. Allow for the ability to address specific or unique agency needs,
8. Allow for the future adoption of a State Groupware standard,
9. Meet the criteria of "open standards" (as defined by the Internet RFCs),
10. Allow the easily exchange messages with the Internet,
11. Promote a common message exchange format and method within the State,
12. Be scalable in function and capacity,
13. Take advantage of the impending telecommunications changes,
14. Support a broad class of messaging services (Email, FAX, pagers, etc.)
15. Provide a uniform directory service for the State,
16. Allow the exchange of directory services with non-State entities,
17. Foster the use of messaging services between the State and It's citizenry,
18. Support the future messaging needs of the State for the next 5 to 10 years.

(Note: items above not listed in any particular order.)

## *Scope*

The design team was charged with producing a conceptual design for a new State of Alaska electronic message service based upon open (and currently evolving) standards. After considerable debate and discussion, the design team interpreted this charge as a two-fold assignment:

- Adoption of a proposed set of statewide standards and guidelines and development of a plan for an architecture and infrastructure to support those standards and guidelines that allows for future change and successful implementation.

- Development of a proposed plan for the replacement for the DOA's current Email backbone. Consideration was given to the integration of any existing State systems that adhere to the proposed standards and guidelines. Consideration was also given to the natural extensions of messaging services such as groupware, fax services, pagers, etc.

The group further defined the scope to include all forms of digital messaging and related server and client software issues. However, the group excluded from consideration all forms of messaging that were not traditionally considered elements of Information Systems. This discussion resulted in excluding telephony/voice, TV, and other digitally encoded analog signals. (However, some consideration of such crossover technologies such as video and voice over the Internet/Intranet were briefly considered and intentionally deferred to future design teams.) Please see "Future Considerations" below for more discussion.

# System Requirements

## *Usability: Seamless, consistent and predictable*

The enterprise Email system must present a simple and uniform interface to the public as well as state staff. It should be ubiquitous – Email should be able to reach every state desktop.
Directory Services should provide for:

- A distributed directory
- Automated replication / updating of other directories
- Public and private entries
- State verses non-state staff distinctions
- Authentication services
- Organizational structures
- Additional groupings (such as all state IS staff)
- List services integration

## *Reliability*

### Timely Delivery

Messages must be delivered from desktop to desktop within one hour in typical use. A guaranteed delivery time will initially be set to 24 hours. If the transport facilities cannot deliver the message because of delivery problems (e.g., destination host unavailable), it must return it to the sender within the guaranteed delivery time, indicating the reason for failure. Any change to the guaranteed delivery time will be posted.

### Message Integrity

The enterprise Email infrastructure must deliver messages intact. It must not corrupt the message content or truncate it. If the transport facilities cannot deliver the message because of content problems (e.g., excessively large message), it must return it to the sender within the guaranteed delivery time, indicating the reason for failure.

### Ability to Trace Failures

In the event of failure, the sender must be notified within the guaranteed delivery time. Where appropriate, operations staff will also be notified. Information about the circumstances of the failure will be maintained in a log for corrective action.

## *Scalable Architecture*

Messaging servers need to be very scalable and compliant with the open standards. Currently, it is the group's consensus that UNIX based hosts are the best choice for messaging servers. As industry standards and products evolve this consensus should be reexamined.

## *Security*

The enterprise Email system will be capable of carrying encrypted messages and messages with digital signatures. Providing the encryption and digital signature services may be outside the scope of the Email system. When and if the Internet Engineering Task Force adopts open published standards for electronic messaging security the state should adopt those standards.

## Attachment Support

This section addresses the requirements for supporting the transmission and reception of files and other data attached to E-mail messages. Much of the text in this section has been quoted verbatim or paraphrased (with permission) from a NASA document [URL http://it-www.hq.nasa.gov/OLD/EmailWhitePaper.html].

Because the issues of Email attachments are complex and may not be commonly understood, we want to discuss those issues before specifying the attachment requirements. Between the transmission and receipt of an E-mail attachment, there are numerous places where the metaphor of traditional mail is insufficient to explain potential problems. For our purposes, we will look at five areas where electronic attachments have special potential for problems.

Incompatible E-mail message architecture (e.g., SMTP vs. Lotus cc:Mail)
Incompatible attachment encoding standard (e.g., Base64 vs. UUencode)
Incompatible hardware and or operating system (e.g., IBM PC vs. Macintosh)
Incompatible application program (e.g., Microsoft Word vs. WordPerfect)
Incompatible application program version (e.g., Microsoft Word 97 vs. Word 95)

1. Incompatible E-mail message architecture (e.g., SMTP vs. Lotus cc:Mail).

State agencies currently use several messaging architectures that are fundamentally different from one another. These different systems are interconnected through Email gateways that translate between the different messaging formats. Inadequacies in the translation programs can result in damaged or lost attachments. This is clearly an area that can be improved by this proposal.

2. Incompatible attachment encoding standard (e.g., Base64 vs. UUencode).

Many older Email protocols were designed to transmit text encoded in the ASCII character set. The ASCII character set uses seven bits to represent 128 different characters. More modern text representation schemes use eight bits or more to represent c' .acters and generally any computerized information can be naturally broken into 8-bit "bytes". However .ere is not a single consistent way to encode 8-bit or larger chunks into 7-bit chunks; instead there are many incompatible schemes, known by names such as UUencode, base64, and BinHex. Additionally, encodings have been developed to represent the hierarchical Macintosh file structure as a flat file for transmission, and to insert checksums to verify the quality of the transmitted data. If a recipient's E-mail system does not recognize the encoding used by the sender, then the encoded data is presented directly to the recipient as unintelligible text. This proliferation of encoding methods is a clear impediment to ease of use, and while our enterprise Email proposal does address attachment encoding among state agencies, this issue will still arise in Email to and from the public or outside agencies.

3. Incompatible hardware and or operating system (e.g., IBM PC vs. Macintosh)

Some operating systems such as Macintosh have a unique hierarchical file structure that does not map well to other systems. All operating systems have different and incompatible executable file structures (e.g., a UNIX program will not run on a Microsoft Windows platform). Some systems may use different character sets. This is a reality that an Email system cannot address.

4. Incompatible application program (e.g., Microsoft Word vs. WordPerfect)

Application data files from specific applications will not be useful unless the recipient has a compatible application. Many commercial products can read the data file of competing products, but this is not always the case and these translations are frequently imperfect. This has been addressed within state agencies by the TIC's office products standard, but this issue will still arise in Email to and from outside sources.

5. Incompatible application program version (e.g., Microsoft Word 97 vs. Word 95)

Even though two users may have the same software package, an application data file exchanged between them may still be useless if they are not running compatible versions. Often, data files of later program versions will not be usable by an earlier version. This document recommends that the TIC address this issue with a document exchange format policy, but this issue will still arise.

The attachment requirements that follow address items 1 and 2 above. Items 3, 4 and 5 are outside of the scope of an Email system.

Following are specific requirements for messaging attachment support:

## File Content Integrity

The contents and structure of the received file should be identical to those of the transmitted file. Data and file structure should not be lost or altered by the transmission process. If altered during transmission (as with binary encoding schemes), the file should be restored to its original state before presentation to the recipient. In cases where system-dependent information is not relevant to or usable by the receiving system, the receiving system may discard the unusable portion(s) and keep the usable portion(s) (for example, a UNIX recipient has no use for Macintosh resource data).

## File Name Integrity

The original name of the file should be retained. If the file name violates system restrictions on the receiving system, the recipient should have the opportunity to see the original file name and specify a replacement name. If this is not possible (e.g., because of architectural restrictions), as much of the original file name as possible should be used in the new file name.

## File Type/Context Information

The type of a file is just as important as the name of the file. The receiving system or user will be unable to easily use the file unless this can be determined. On MS/DOS- and MS Windows-based systems, the three-character file name extension often identifies the type of data file (e.g., ".DOC" or ".XLS). However, this is not the case with Macintosh and UNIX systems. A unilaterally understood (i.e. statewide) specification of file type information makes it possible for the receiving system to recognize file types and present them to the recipient system appropriately (e.g., "double-click-able" in a Macintosh or MS Windows environment). This document recommends that the TIC adopt a document exchange format policy (Appendix 5).

## Support for Multiple Attachments

Multiple attachments should be supported in the same way as a single attachment. This support should extend to an arbitrarily large number of attachments without being restricted by the architecture.

## Education of the User Community

What is and is not possible with binary attachments is not well understood by the user community. For example, it will never be possible to view application data files without a compatible application or to execute programs on an incompatible computing platform. There are also security concerns related to receiving and executing programs whose source cannot be verified, and attachment size and number restrictions. A comprehensive education program on the correct and incorrect use of binary attachments is required.

## Attachment Size Limits

The Electronic Messaging Committee will establish size limits for attachments. Initially those limits will probably be identical to the current limits applied by the Email backbone, to wit: users should not exceed 2.5meg of attached files per Email message to a single or multiple destination during normal working hours or 5.0meg after normal working hours. Users are required to 'zip' multiple files into a single compressed file

where possible. If a user needs to send larger file(s), they should coordinate with their DP/IS staff to utilize more appropriate technology such as shared folders, FTP, etc.

## *Administration*

There must be the ability to separate the administration of system components from the administration of users. The core system components will be administered by a central group of systems staff, while the routine user administration operations such as add, delete, reset password, etc., will be delegated to human resources personnel at an agency and/or sub-agency level.

## *Miscellaneous Features*

### FTP Services

The new statewide messaging servers will provide shared FTP services for the exchange / dissemination of large files and attachments.

### Internet Connectivity

The new statewide messaging service will be connected to the Internet. As communications infrastructure, funding, and time allow the Internet connection shall be made as redundant as possible. Access routers in Juneau, Anchorage, and Fairbanks should be considered. Backup access in the lower-48 should also be implemented as funding allows.

### Message Filtering

Mail Clients will be responsible for all message filtering.

### Group and Bulk Messaging

Any electronic message will be addressable to an individual, to a selection of individuals, to named groups, or to groups sharing common attribute values (i.e., "Job Class" = "Accounting Technician"). However the ability to address Email to groups will be controlled to reduce the amount of junk mail.

Messages between groups of geographically dispersed individuals (Email needing to travel over the WAN) must comply with the statewide standards for messaging. Any groupware messages that must travel over the WAN will need to be pre-approved by the proposed Electronic Messaging Committee. If possible all groupware messaging traffic traveling on the WAN should be converted to statewide standards (preferably at the messaging clients).

List services will be provided on the new statewide messaging servers.

### Shared Folders

It is highly desirable that the new statewide messaging servers provide shared file folders for messages and attachments.

## *Future Considerations*

### Groupware

The design group believes that at this point in time all groupware is experimental and the selection of a standard is premature by at least 12 to 18 months. The design group feels that agencies with a business need for groupware should restrict their experimentation to those products that have a good chance of survival in the market place and those products that are "open" and standards oriented. We suggest that agencies limit their groupware experiments to the following products Netscape Suitespot, Lotus Notes, Microsoft Exchange, and Groupwise.

### Other

- Authentication Services
- Web / Messaging Services Interactions
- Gateways
- Certificate Management, Public Keys, etc
- EDI Messaging Services
- Firewalls
- Agents
- Chat Services
- Voice over the Internet
- Point to Point Video over the Internet
- Audio Broadcast Services
- "Net Casting" Services
- Public Records Issues
- Conversion from Existing Email Formats and Systems
- Message Encryption
- Message (Network) Transport Encryption
- Attachment Encryption
- Directory Services for non-state organizations
- Non-state use of messaging services
- Return Receipt / Notification of Delivery Services
- Mail generating programs / bots
- FAX Support
- Pager Support
- Non-Traditional Uses of Messaging Services
- SPAM Management
- Virus Protection
- Historical Email / Archives
- WAN file services
- Calendar Services
- Push Technology

## Proposed System

### *Governance*

It is recognized that messaging services are a vital function of all state agencies. We propose that the enterprise messaging system be managed by a committee under the authority of the TIC. This committee, hereafter called the Electronic Messaging Committee, will oversee the establishment, enforcement, and management of all State wide electronic messaging related issues (See appendix 1).

### *Standards Adopted*

### Open Standards

As a State wide standard for all new and replacement messaging systems the following open standards are adopted:

- SMTP as the State Email transfer protocol
- LDAP as the State directory services protocol
- MIME as the State attachment encoding protocol

- POP and IMAP as the State Email client-to-server protocols
- It is intended that all POP clients will transition to IMAP as software upgrades and funding allow

The proposed enterprise electronic messaging system will be based on these open standards. Open standards offer numerous advantages over proprietary standards, including:

- Continual incremental improvements while maintaining backward compatibility
- Maximum interoperability on a global scale
- Wide choice of implementations features and costs

Clearly a system based on open standards is in the best long term interests of the state. However, implementation and maintenance of a large geographically distributed system will be considerably easier if we minimize the number of different vendors and products involved and the platforms on which they run. For this reason we will conduct a competitive procurement process to select specific products for each of the server components, and a limited selection of "certified" products for the client components.

Also for this reason, we are specifying that server software must run under the Unix operating system. The state's current distributed enterprise systems are hosted on Unix platforms and the state has considerable resources invested in Unix systems. Unix is an open architecture and provides the option of maintaining hardware and software vendor independence. Unix is a proven performer in enterprise scale systems and meets all our requirements for an electronic messaging platform. There is no clear and compelling reason to move away from this platform and this investment.

## Directory Services

The most critical component of an effective messaging architecture is the directory services. The team proposes the following features for a directory service:

- LDAP standard as the basis for directory services
- A distributed and replicated enterprise directory service
- Web browser interface for query and update
- A bottom up, agency operated network of directory servers, which will replicate/refer their entries up to the Electronic Messaging Committee operated state-wide servers

## Naming Conventions

It is critical that a set of naming conventions be developed and approved by the Electronic Messaging Committee. The design team proposes the following elements:

- Common employee names in the form that they are entered in AKPAY
- Department names will be acronyms where those acronyms are commonly understood and are unique
- Department is defined in liberal sense in that State entities that are not official departmental entities but that are generally perceived by the public as being independent entities shall be for purposes of messaging addressing be considered as "departments." For example, AHFC, CFEC, etc.
- The directory server shall maintain a list of State of Alaska entities
- Aliases will be supported for different forms of names (for example, William may list an alias Bill)
- Email addresses will generally be in the form first_last@dept.state.ak.us
- Where name collisions occur they may be resolved by middle initials or suffixed digits

## *Existing System Investments Preserved*

Any existing systems being operated in compliance with the new architecture shall continued to be operated (at the agencies discretion) provided that they can meet all exchange standard with the new enterprise system.

Any existing agency systems not in compliance with the new standards and architecture shall be converted as funding and time consideration will allow. The enterprise system will be available for initial agency conversions beginning January 1, 1998. A target date of January 1, 2000 is set as the date for complete conversion to the new system.

Any existing agency systems that can't exchange Email with the new backbone system must be replaced and/or a new gateway installed to allow message exchange until they can be brought into compliance.

Groupware considerations which effect the choice of message exchange and message formats are deferred to the "Electronic Messaging Committee" for future consideration. (See Groupware discussion above.)

## *Conceptual Design*

The vision promises "*a service that appears to the user to be a single, unified electronic postal system....*" The proposed design delivers this capability through a system of directory/message delivery servers and client Email programs that provide the user interface to these servers. This system will include distributed shared servers operated by the Electronic Messaging Committee with the option for additional agency owned and operated servers where justified.

## Components

### Directory

A distributed and replicated enterprise directory service with LDAP and Web browser interfaces:

- common names will be in the form that they are entered in AKPAY
- aliases will be supported for different forms of names (for example, William may list an alias Bill)
- Email addresses will generally be in the form first_last@dept.state.ak.us
- where name collisions occur they may be resolved by middle initials or suffixed digits
- department names will be acronyms where those acronyms are commonly understood and are unique
- agencies could operate any number of their own LDAP servers, which could replicate/refer their entries up to the Electronic Messaging Committee operated LDAP servers

### Delivery

A distributed message delivery service based on SMTP. Directory services and message delivery services will normally be provided on the same server platform. The design proposes

- distributed, shared directory/delivery servers in regional hubs (Juneau, Anchorage & Fairbanks)
- additional distributed, shared directory/delivery servers in remote locations where the Electronic Messaging Committee determines they are necessary
- additional exclusive (not shared) agency owned and operated directory/delivery servers where the Electronic Messaging Committee determines that such servers are justified

It may be appropriate to have several directory/delivery servers in the large metropolitan areas; for example, Juneau would probably have at least 3 (the existing DOTPF server; the existing Permanent Fund server; and the Electronic Messaging Committee operated shared server). However, it probably would not be appropriate for smaller communities (for example Kodiak) to have more than 1 directory/delivery server.

### Servers

All servers in the messaging system will be Unix based (see discussion in standards section). The selection of server products will be by competitive procurement with oversight by the Electronic Messaging Committee.

## Client Email Program

Customers must select enterprise Email clients from a certified list. The Electronic Messaging Committee will certify clients for the list.

### Certification criteria

- Address resolution via LDAP
- Client-to-server protocol either POP or IMAP
- (eventually only IMAP will be supported)
- Attachments handled via MIME
- Attachments will be handled in manner consistent with the other clients and the TIC Policy Committee's specifications (no secret handshake)
- Initial list of clients to be considered for certification
  Netscape Communicator
  Microsoft Outlook

## *Cost Analysis*

Instructions to the Email Design Team included the TIC's desire for a less expensive Email system. While there has been no rigorous analysis of the costs of the current system, it is clear that there are significant inefficiencies. For example, the current system includes at least four Email post offices in Kodiak (ADF&G, H&SS (2), and Public Safety). There may be legitimate reasons for implementing multiple post offices in a large metropolitan area, but any enterprise Email design that includes more than one post office in Kodiak is probably not optimal.

The current system also includes a very complex network of message stores, message transfer agents and gateways. A quick census of just the Microsoft and Lotus Email installations found over 264 postoffices; we estimate that there are over one hundred message transfer agents associated with these postoffices, leading to an estimate of at least 364 server-side components. Clearly there are significant costs involved in maintaining and managing this complex infrastructure.

The current system does not make efficient use of WAN bandwidth. For example, consider the WAN travels of a message from a Fish and Game user in Ketchikan to a Public Safety user in Ketchikan. The message travels from Ketchikan's Fish and Game postoffice to Douglas Fish and Game to Juneau Fish and Game to the Juneau Email backbone to Anchorage Public Safety HQ to Juneau Public Safety to Ketchikan Public Safety. Also note that each of these WAN hops is processed by a message transfer agent running a polling process, so besides being an inefficient use of WAN bandwidth this process is likely to take from fifteen to thirty minutes.

In addition to these obvious inefficiencies, we do have data from the Compass study from which we can develop a quantitative estimate of one component of the costs of the current system. Using the Compass data collection item for the number of FTE's administering Mail applications, and removing one response, which appears to be an outlier, we get $450,000 per year in administrative costs alone. (Six departments responded to this data collection item; responses in seats/FTE are 1700, 920, 16450, 3775, 3423, and 3614. If we consider the response of 16450 to be an outlier and remove that data point, responses from the five remaining departments total 2.29 FTEs. These five departments account for thirty-nine percent of state employees. Expanding from the five departments in our sample to a total for all departments gives approximately six FTEs (2.29(1/.39)=5.9). Adding to this the 1.5 FTEs administering the Email backbone gives 7.5 FTEs. Multiply 7.5 by the COMPASS cost per FTE ($60,000) for a total of $450,000/year.)

There are other categories of costs for which we have no data, including the costs of acquisition and support of Email hardware and software, the cost of bandwidth on local and wide area networks, and the costs of training and support (some support costs are doubtless included under administration). A commercial Internet Service Provider (ISP) would charge from $480,000 to $960,000/year to provide messaging services for 10,000 mailboxes [PTI Communications; personal communication with Dave Riccio]. Given

that we have a known cost of $450,000 per year, and additional unknown costs, it is likely that we are spending more for our current system than we would pay to buy basic messaging services from the private sector.

We have made no attempt to conduct a more rigorous estimate of the costs of the current system or to improve or verify these estimates. The Email design team concluded that our limited resources would be better spent in analyzing where we want to go than in documenting where we are. Therefore our evidence that the proposed system is less expensive than the current system is based on addressing the obvious inefficiencies documented above and predicting lower support personnel costs than the current system.

Examples of how the proposed design will streamline the state's messaging capability include: the Kodiak offices of ADF&G, H&SS, and Public Safety would share one postoffice; Email gateways will be eliminated, and the number of message store and message transfer components will be reduced significantly by hosting multiple agencies on shared systems; the elimination of gateways will reduce the consumption of WAN bandwidth described in the example above -- if Ketchikan was one of the locations with a local server WAN travel would be eliminated; if Ketchikan didn't have a local server, then the example message would still travel across the WAN, but the message would simply go from Ketchikan to Juneau, and then back to Ketchikan, reducing WAN hops from six to two.

## *Implementation Plan*

### Delivery

1. Deploy Messaging server services on Unix hosts in regional hub locations (Juneau, Anchorage, & Fairbanks) and additional locations deemed appropriate by the Electronic Messaging Committee.
2. Develop semi-automated or fully-automated method of Email account creation to allow each agency to create Email accounts.
3. Develop and document account management procedures.

### Directory

1. Deploy LDAP directory services on each shared Email server.
2. Configure administration so that each agency can self administrate their branch of the LDAP directory to the appropriate level.
3. Determine and document how to manage directory information to insure appropriate access to personnel and other object information.
4. Deploy LDAP/Web directory access to allow internal and external directory access as a replacement to the current WhitePages Directory.

### Schedule

### Electronic Messaging Committee Appointed

The TIC should appoint the Electronic Messaging Committee by October 1, 1997.

### Procurement

DIS will conduct procurement under the oversight of the Electronic Messaging Committee. Procurement should be complete by December 1, 1997.

### Delivery and Setup

DIS will have the initial hardware and software for the regional systems in Juneau and Anchorage available within 30 days of completion of procurement. These systems should suffice for the Initial, Second Pilot steps, and possible the First Agency Conversion. Should the Electronic Messaging Committee specify

additional locations, hardware and software should be able to ordered, delivered, and setup within 60 days of the committee decision.

## Initial Pilot

The Initial Pilot would consist of a small group of users (<100) that would actively use the Email system and provide feedback on functionality and capability. As this is the initial implementation, the time spent here exploring and resolving issues will result in easier completion of the following steps. The Initial Pilot should not exceed 45 days unless there is considerable problems/issues. During the Initial Pilot, baseline performance measurements, deployment notes, and recommendations for smooth agency transition should be started and maintained.

## Second Pilot

The Second Pilot would consist of a larger number of users (<1000) that continue the testing of the Email system. This step should not exceed 30 days unless there are considerable problems/issues. During the Second Pilot, baseline performance, deployment notes, and recommendations for smooth agency translation should be continued and maintained.

## First Agency Conversion

The First Agency Conversion will convert an agency with a minimal number of sites. All agency users will be converted. It is anticipated that the best method of doing this conversion would be to do this quickly and completely over as short of time frame as possible. A long multiple week process of conversion would only be considered if absolutely necessary. Should the location of remote sites require additional Email host(s), more time might be required for their procurement, delivery, and setup. The agency would be responsible for the deployment of any new Email clients and/or any configuration changes on the desktops. This step should not exceed 30 days unless there are considerable problems/issues. During the First Agency Conversion, baseline performance, deployment notes, and recommendations for smooth agency translation should be continued and maintained.

## Second Agency Conversion

The Second Agency Conversion will mirror the first conversion.

## General Availability

At the conclusion of the Second Agency Conversion, the system would become generally available for agencies. It is anticipated that agencies would schedule a time slot for migration so that a minimum number of agencies where concurrently converting.

# Appendix 1: Electronic Messaging Committee Charter

## *Mission*

A Statewide policy and oversight group, hereafter called the Electronic Messaging Committee, will be established under the TIC authority for the ongoing establishment, enforcement, and management of all State wide electronic messaging related issues.

## *Duties of the Electronic Messaging Committee Delineated*

The Electronic Messaging Committee will meet on a regular basis to set direction, approve changes, and provide overall management of the enterprise electronic messaging system.

The committee will also operate as an arbitrator and will hear appeals for all state electronic messaging related issues.

The committee will review and approve designs and implementation plans, monitor implementation and operation of centralized systems, and recommend chargeback mechanisms for TIC approval.

The committee will adopt criteria for certification for messaging software (clients and server). The committee will oversee the certification process. The principle criteria for certification will be that the software adheres to the adopted standards and guidelines.

## *Membership in the Electronic Messaging Committee Defined*

Membership in the Electronic Messaging Committee shall be representative of the major "stake holders" for messaging services with at least two members representative of small and/or rural State messaging users. The membership will be recommended by sponsorship of a TIC member and confirmed by a vote of the TIC Executive Committee. The Director of the Division of Information Services, DOA shall appoint a non-voting member to sit on the Electronic Messaging Committee. Division of Information Services, DOA shall provide any needed administrative support required to conduct the Electronic Messaging Committee's functions, and shall act as advisor to Electronic Messaging Committee as required.

## *Relationship to State Agencies / Rights to Appeal*

Any State agency may bring an electronic messaging issue or requests before the Electronic Messaging Committee for consideration and appeal. The Electronic Messaging Committee shall consider the agency request and rule accordingly. Implementation of Electronic Messaging Committee approved projects or systems shall be in conformance with standards and guidelines and shall be executed by DOA Division of Information Service under RSA agreements with the requesting Agency, or by the Agency should the Electronic Messaging Committee consider that in the State's best interests.

## *Relationship to Department of Administration Defined*

The Department of Administration, Division of Information Services will provide operational support and implementation services under the direction of the Electronic Messaging Committee for a new state electronic messaging system. This new system would replace the existing state Email backbone operated by DIS.

# Appendix 2: Electronic Messaging Committee Guidelines

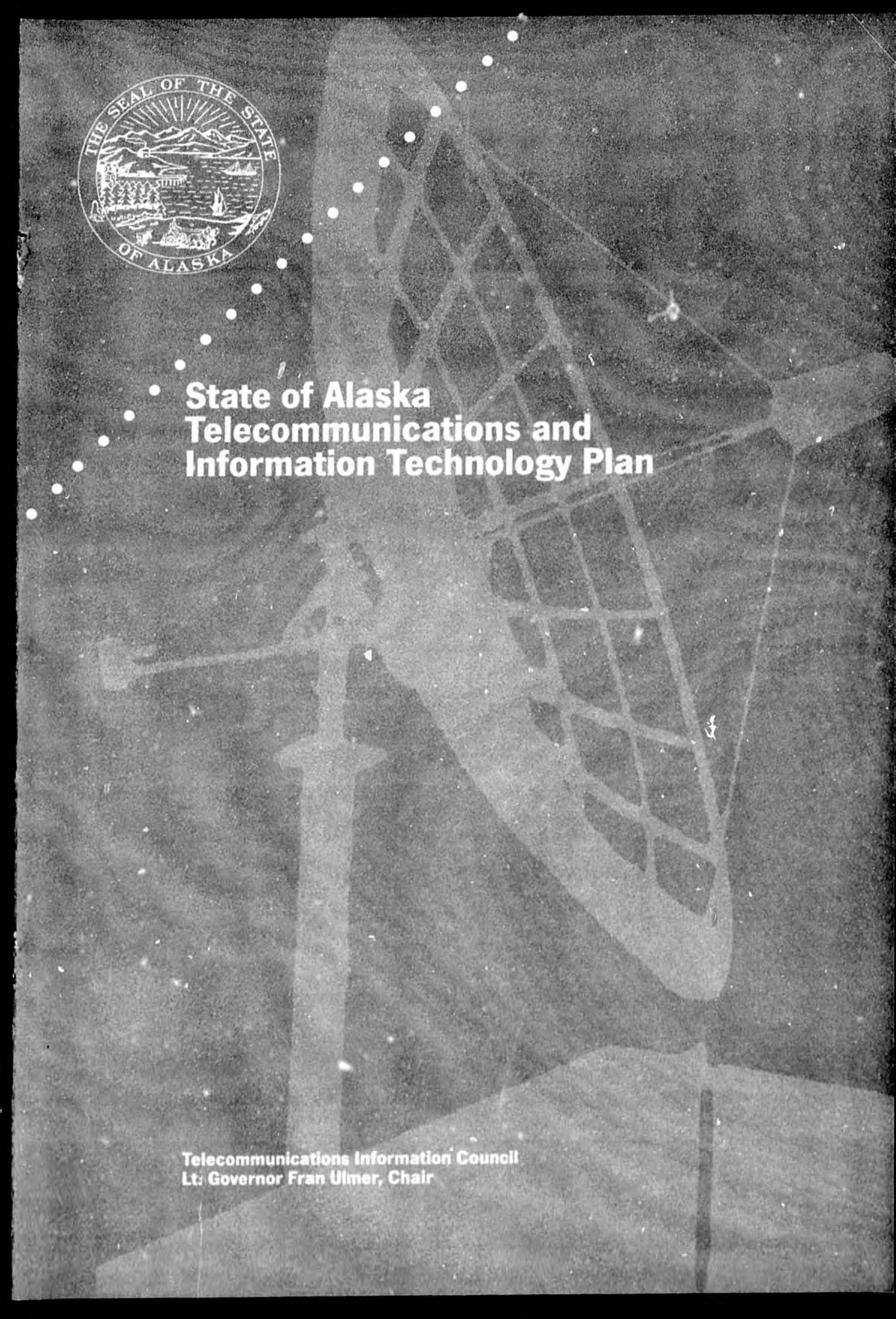
## *Considering an agency request to run its own electronic messaging server(s)*

The Electronic messaging committee should consider the following issues before granting an agency permission to run their own electronic messaging server(s).

1. Can the agency provide comparable services at less cost than the cost of participating in the shared system?
2. Will granting the agency request result in a reduced load on shared resources? Will it in any way compromise shared resources?
3. Is there a clear potential for significant innovation or improved level of service that could eventually benefit the shared system?
4. Does the agency have truly unique requirements that cannot be met by the shared system?
5. Will granting the agency request impact the rate base and therefore raise costs for users of the shared system?
6. Will granting the agency request optimize service for all parties? That is, is there a net gain for the state as a whole?

## *Chargeback*

1. Chargeback for the DOA operated Email backbone and servers will accurately reflect the costs of the services to be provided.
2. Costs will be consistent and predictable to facilitate budgeting.
3. Services and costs will be tiered to allow for a minimum service (the basic transport of message traffic) and other add-on services such as large volume Email storage, pager services, broadcast services, etc.
4. Costs will be competitive with (or be cheaper) than the same service from an external service provider.
5. Implementations that require budget adjustments should be done in a timeframe that the budget process can accommodate.



# State of Alaska Telecommunications and Information Technology Plan

Telecommunications Information Council
Lt. Governor Fran Ulmer, Chair

## Contents



# Dear Alaska Citizen:

The plan you are about to read is the product of a lot of labor by citizens and public officials in our state. But it is not an end product - it is the beginning of a long road. That road will eventually lead to a future where all Alaskans can use the telecommunications and information technology they need to be effective at home, at school and at work.

The development of this plan was indeed labor-intensive. Within State government, about a hundred people formed eight task forces that met for two months. The task forces considered telemedicine, education, information systems, economic development, emergency communications, and public broadcasting - among many other topics. Each task force generated a report on the discussions they held during spring. Those reports formed the basis of a draft plan which was released for public comment in September and October. The plan was also put on my homepage on the Internet, and many public comments came in through e-mail in what amounted to a statewide virtual town meeting.

I held six public hearings in October - two were videoconferenced in Juneau, Anchorage and Fairbanks, and two more were teleconferenced statewide. Hundreds of public comments came in through this process and were considered by the Telecommunications Information Council (TIC) for inclusion into the final draft of the plan. That final draft was presented to the council and approved on December 18.

The vision behind the plan is based on the principle of universal and equitable access to telecommunications in Alaska. Simply put, everyone should be able to get access at a reasonable cost. Without this principle, new technology could create another class of "haves and have nots" in our state, instead of fulfilling the promise of erasing distance and equalizing opportunity. The plan strives to eliminate the need for citizens to know the intricate structure of state government in order to get information. People should be able to ask a simple question and get an answer - and technology makes this possible.

The plan also recommends pursuing a cooperative partnership with telecommunications providers in the state. Developing good relations with providers is the key to getting Alaskans the service they deserve in the most cost-effective manner.

Read this plan - and let me know what you think. Contact my office with any questions or comments you have. Our web address is www.gov.state.ak.us/ltgov/home2.html and you can contact Andy Kline in my office at andy_kline@gov.state.ak.us. Your input is a vital part of the planning process that needs to continue in order for us to take full advantage of the opportunities technology promises.

Sincerely,

Fran Ulmer

Lieutenant Governor

# Introduction to the Planning Process

## SCOPE

This document attempts to identify the telecommunications and information technology needs and goals of Alaska's state government. "The State" is referred to throughout this document. Within this document, "The State" is defined as all functions and agencies funded in whole or in part by the Alaska state government. Some entities, such as the University of Alaska, have had and will continue to have a larger role to play in the State's telecommunications system than others.

Other interests, such as telemedicine, are not as directly controlled by the state, but government still has a vital role to play. All of these interests are represented in this plan.

## GOAL

Alaska has as much or more to gain from advances in telecommunications than any other area of our country. Our vast distances, disparate and sparse population, and severe climate make the challenges and potential gains greater here than anywhere.

But in order to take advantage of that potential, we as a state must have a well-considered plan that maps out the state's goals and ways that we can achieve those goals. That is the purpose of this document.

This plan is the starting point of a continuing process that will identify and hopefully help us achieve our high expectations in telecommunications. This document will change over the years, but the underlying goals are likely to stay the same.

The Knowles/Ulmer Administration has set the following goals in telecommunications:

- Improve public access to government information
- Maximize service to the public through voice, video and data systems
- Optimize government efficiencies
- Explore innovative and cost-effective services that meet Alaska's challenges
- Stimulate the development of private and public services

The Telecommunications Information Council (TIC) is responsible for formulating the State's plan for taking advantage of information technology. This year, there was a recognition that in order to follow the Knowles/Ulmer goals, a comprehensive look at the State's telecommunications and information technology needs was required. Paramount in this examination of goals is the need to facilitate a fundamental change in how state citizens, the customers of state government, interact with government. This "paradigm shift" in customer service, illustrated in Figure 1 shows how customers now must know the structure of state government in order to get needed information. Under the new scenario, agency divisions will become invisible to the customer.

## PROCESS

The TIC decided on an intense internal look at where the state is now, and where the State should go in the short, mid and long term. To bring clarity to these questions, eight internal task forces were formed which looked at the following areas:

- Economic Development
- Public Telecommunications
- Emergency Communications
- Telemedicine
- Telecommunications Act of 1996
- Public Transactions
- Education
- Management of Information Systems and Data Processing

After two months of meetings, these groups gave recommendations which formed the building blocks of this plan. This plan is the State government's portion of the Alaska 2001 plan which was approved by the Alaska Public Utilities Commission (APUC) in March. That document attempted to articulate the needs of Alaska's citizens, this plan attempts to articulate the needs of State government.

# Public and Private Responsibilities

## SUMMARY

One of the major issues the state must grapple with as it works in the telecommunications arena is when the state should own and operate private networks versus when the state should rely on public telecommunications providers to answer its needs. The answer to this question must include an analysis of the costs and benefits to the citizens of the state, the state's responsibility to provide for emergency and public safety communications needs, the availability of public networks in remote areas of the state, and the federal laws which govern access to telecommunications facilities in emergencies. The consensus is that a balance must be developed through partnership between the state and public telecommunications providers. The following recommendations reflect this philosophy.

## GUIDING PRINCIPLES

1. The Telecommunications Information Council acknowledges that State's government has an important leadership role to play in helping to assure an equitable provision of basic telecommunications services to all Alaskans. The State should be a stimulator of public telecommunications by serving as an anchor tenant in order to encourage the development of advanced telecommunications technologies.
2. Market economics will guide the provision of telecommunications services throughout the State unless there is a compelling public interest served by direct State action to insure the safety and well being of its citizens. However, the State should not subsidize any one private, commercial interest at the expense of the state citizenry and competition.
3. The state should be a stimulator as well as a facilitator of private-sector efforts to expand, improve, and modernize the existing telecommunications infrastructure.
4. The State should be pro-active and pro-competition throughout these efforts.
5. The State should encourage partnership development for the purposes of information sharing, coordination, needs assessment, demonstration, and evaluation of statewide projects. (particularly telemedicine, education)
6. The state should use the stimulus of its competitive procurement of services to encourage providers to develop cost effective enhancements, expansions of existing services, and provision of new ones.
7. In instances where the private sector by itself may not be able to adequately meet the basic telecommunications needs of Alaskans, the State should actively and cooperatively seek to ensure that those needs are met.

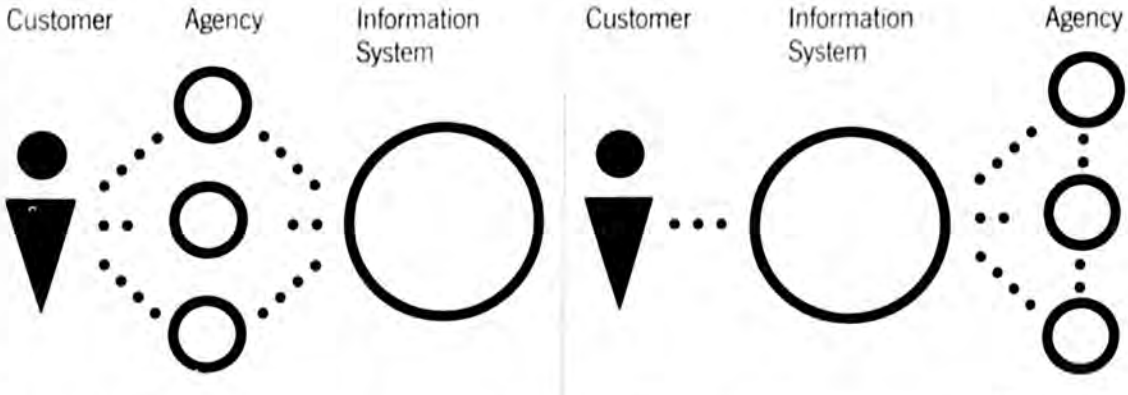
## RECOMMENDATIONS

### By January 1998:

8. The Telecommunications Information Council (TIC) should pursue discussions

**Figure 1**

Program Shift in Customer Service



and explore the possibility of allowing the private sector to collocate at State-owned telecommunications sites. Legal issues must be explored and adequate restrictions and safeguards must be in place. There is also a potential use of State-owned rights of way along Alaska's intertie, railroad and road system and pipeline corridors.

9. The state should work to minimize legal barriers to insure that public and private health care providers and their patients will be able to take advantage of the benefits of telemedicine. The State should also examine its reimbursement mechanisms to minimize barriers to utilization of emerging technologies in health care delivery.
10. The State should create a statewide advisory group consisting of the local governmental entities that have E-911 systems, consumers, federal public safety groups, telephone companies, the state and other private sector companies with some involvement in E-911. This group would be charged with organizing disaster recovery/rerouting plans to be adopted by localities to ensure backup for inter-operability and coordination.
11. The State should pursue the provision of highway emergency communication systems. A highway emergency communication system is an important part of a statewide emergency communications network. Communities impacted by the placement of communications systems should be consulted prior to any equipment being installed.
12. The State should provision its public safety communication system so that State control of the system is not compromised in a time of emergency. The State should take the lead role in evaluating the feasibility and in the implementation of a statewide trunked radio system working with all public safety and emergency response entities as well as providers.
13. The TIC should appoint a task force to draft policy affecting state operation on the Alaska Rural Communications Service system and the question of in-kind subsidy of commercial broadcasting.

**By 2000:**

14. The State should consider a contracting with providers that offer a Value Added Network (VAN) - those networks that provide service beyond basic transport - in order to provide the needed communication links between it and its various business partners. The State should take advantage of the commercial infrastructure and associated standards and protocols whenever possible.
15. The State should explore a range of strategies for meeting statewide broadband capacity needs, but among these should be the option of joining with private sector and federal parties in the development or financing of a second fiber optic cable linking Alaska to the Seattle telecommunications grid.
16. The State should work with the private sector, including oil companies, banks, telecommunications providers and other major businesses, to adopt a set of minimal technical standards to allow interoperability of local, regional and statewide systems.

# Bandwidth

## SUMMARY

Bandwidth refers to the speed at which electronic information can be transmitted. Sometimes this is defined as a "size" of pipe. Bandwidth is a consistent issue that permeates all telecommunications discussions in Alaska. With enough of it, all things are possible - without it, many of these points are moot. The crux of the problem is how to get adequate bandwidth across the state and to the state at a reasonable cost.

## GUIDING PRINCIPLES

17. The state should encourage the telecommunications service providers to expedite the deployment of new technology and additional capacity in order to meet the needs of the expanding Alaska market. Key pieces of this infrastructure should be focused on: the special requirements and challenges of rural Alaska including elimination of multiple satellite routing the potential use of State-owned rights of way along Alaska's intertie, railroad and road system corridors the adequacy of the fiber-optic telecommunications link between Alaska and Seattle.
18. The State should support a mix of narrow to wideband technologies to facilitate the continuing development of Internet, satellite, wireless, cable and other solutions to our communications needs.

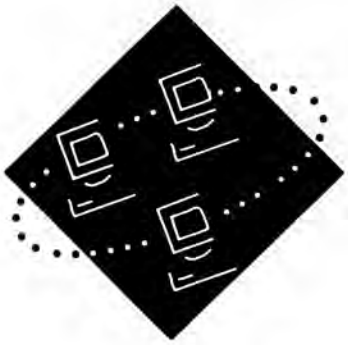
## RECOMMENDATIONS

### By January 1998:

19. The State should evaluate the ability of its network infrastructure to accommodate various forms of electronic commerce, and the abilities of its contractors and suppliers to engage in it.
20. The State should assess its bandwidth needs and explore a range of strategies for meeting statewide broadband capacity needs, such as a second fiber optic cable linking Alaska to the Seattle telecommunications grid and expanded connectivity to the Arctic Region Supercomputer.
21. Efforts shall be made to encourage network providers to make available additional bandwidth to support the rapidly expanding use of private networks and the Internet for business and educational purposes. Connections between Alaska regional centers and the lower 48 states are nearing the maximum carrying capacity. If the growth is to continue, more capacity is needed.
22. The State should adopt Federal and industry standards in multiple uses of bandwidth, including but not limited to voice, video, data, audio and interactive applications. These standards should allow for interoperability with existing state equipment. These standards should be reviewed as wider society and industry standards develop.
23. The State should investigate the use of wireless technology as a way of filling future bandwidth needs.
24. The State should conduct a comprehensive study to determine the anticipated needs and the satellite and fiber-optic-delivered bandwidth and services that will be available in the year 2000 and beyond. Because of the State's continuing need for satellite-delivered bandwidth statewide, the number and types of circuits available now and their costs should be determined in order for adequate planning to take place.
25. The State should complete the transition from analog to digital system delivery of UA distance education.
26. The State should continue planning for replacement of the two-way radio system used by law enforcement, public safety, and emergency services. Recent policy decisions put out by the FCC will result in the State needing to replace this system over the next ten years.
27. The State should update its network study conducted in Fiscal Year 1993 to include the advancements in Internet use for State business.

### By 2000:

28. Following the recommended study in #24, the state should explore how it can leverage these new and as yet undefined technologies as part of an overall plan.



# Access

## SUMMARY

While urban Alaska has better telecommunications access than rural Alaska does, demand in even the urban areas for reliable, high-speed access is expected to grow exponentially as more users, more kinds of communications, thousands of official transactions and totally new ways of conducting commerce and other business go "on line." Urban areas are the hub for expanding access to the very needy rural areas, and high use in any area can dry up access for other areas. Therefore, planning for expanded access must address inter-related needs in all areas, and ensure that telecommunications technology does not create "have and have-not" communities in Alaska. It is not enough for the State to provide information and the ability to transact business online unless there is a good-faith attempt to make sure citizens have access from all over Alaska.

## GUIDING PRINCIPLES

29. The State's telecommunications policy is to support universal and equitable access in order to better provide state services and information to all citizens.

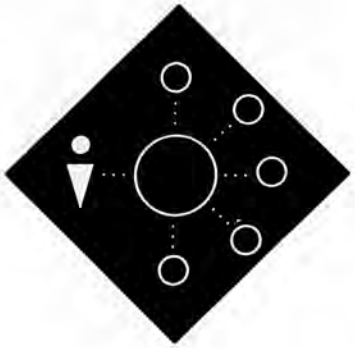
## RECOMMENDATIONS

### By January 1998:

30. The State should review and if necessary revise its management policies and procurement policies, to encourage competition among telecommunications services providers on service standards, prices, and the development and offering of broader band services.
31. The State should have the APUC examine its regulations to ensure that service providers can compete regarding the delivery of telecommunications services to rural Alaska where appropriate.
32. The APUC should adopt regulations regarding the universal service needs of public schools, libraries and rural health care providers.
33. The State should encourage community and regional consortia in developing networks which provide access to and ensure growth for the communities; linking schools, University of Alaska campuses and remote sites, public libraries, local government entities and other agencies.
34. The State should explore ways to provide access in remote areas of the state by sharing costs for bandwidth coming into a community. In many communities, public dollars are funding separate high-speed lines for the University, the state's WAN, school districts, libraries, and federal agencies. If the state partners for public access dial-ups to a shared point of presence in these communities, money savings and improved access to the public are possible.
35. The State should establish a continuing working group (e.g., as part of TIC, or as an interdepartmental working group) to identify issues regarding rural telecommunications needs and capabilities, and develop conceptual frameworks for addressing them. Part of this working group's mandate should be to look at how other states and countries with similar rural-area concerns have addressed the special issues surrounding development and implementation of telecommunications systems and networks in rural areas.
36. The State should negotiate for lower audioconferencing rates for student phone-ins to teleclasses. The State should also encourage the upgrading of its audio conferencing networks acknowledging its importance and appropriate support of education and State affairs.
37. The State should develop mechanisms for the use of the existing state communication system infrastructure by local educational and governmental entities.
38. The State should work toward Internet access to student, faculty and staff at all education sites, at reduced cost.
39. Alaska should work towards high speed, switched, broadband telecommunications capability in every school, library and educational facility in the state.

**By 2000:**

40. The State should work with the private sector towards: Connectivity to all educational facilities with existing viable infrastructure Internet access to rural campuses where infrastructure is in place or upgradable Internet access to all K-16 sites with viable infrastructure.
41. The State should explore interagency partnering (between the three branches of state government branches, local and federal agencies), sharing personnel, operations and equipment to provide telecommunications and information technology service to the public. For example, the State could make better use of the 21 non-partisan Legislative Information Offices statewide.
42. The State should take a leadership role and should foster leadership in communities to increase rural access to telecommunications and information technology. The State should encourage agencies, publicly funded programs, schools, the university, etc., to develop, at the local level, multi-year plans for the expected use of telecommunications. The State should facilitate community and/or regional consortia to make regional/community WANs affordable.



# Services

## SUMMARY

There are several core state government functions, including public safety, public health and welfare, education, resource and environmental management, economic development, and transportation. These primary services should be mirrored in our telecommunications priorities. Government services in telecommunications are widespread and far-reaching. The definition of these services will have much to do with the way citizens perceive state government, and the way they participate in the political process. As referred to in this document's introduction (Fig. 1), State government is undergoing a "paradigm shift" in customer relations. Telecommunications and Information Technology are at the heart of this redefinition of State service to citizens.

## GUIDING PRINCIPLES

43. Telecommunications and Information Technology development in the State should reflect the "paradigm shift"(fig. 1) in customer service which allows for Alaska citizens to receive information without detailed knowledge of the structure of state government.
44. The State should identify ways to use telecommunications to share of sharing information resources with local governments, and to provide local governments with more effective and efficient means of participating in state programs.
45. To maximize the value information technologies can bring State government there must be good alignment of the business objectives and information technology. This calls on government to clearly reaffirm what its primary goals are and to reengineer its business processes with information technology used as an enabler.
46. Information technology planning and evaluation of business goals are a continuing process. To keep this process alive a strategy for information technology governance and deployment must be instituted. While strategic planning sets the general course, tactical planning addresses specific areas for agencies to proceed with daily operations while adhering to the State's desire to improve government's delivery of services.

## RECOMMENDATIONS

### By January 1998:

47. Everyone in State government should be reachable through electronic mail.
48. The State should complete an assessment of its current use of mainframe and distributed, or networked, computer systems. This "benchmarking" study should compare the state profile with private industry and other states or large government organizations and analyze whether the state is positioned well to make the most best use of its computing resources and to serve the public. The study should lead to a more detailed recommendation for a statewide information technology strategy that will best facilitate state government's business goals.
49. The State should develop a directory of existing State telecommunications and information technologies services. The State should also develop a directory of electronic State addresses.
50. The TIC should oversee developing a strategy for providing Basic 911 in all areas not now covered. Statutes should be reviewed and, if appropriate, revised so that areas where there is no formal local government entity, the State could request (at the request of the community) that surcharges be collected by telephone companies.
51. The State should assess existing videoconference sites and create new ones or improve existing ones where appropriate to reduce conflicts on room time. The State also needs to better assess cost-benefit of departmental use of video conferencing.
52. The State should focus on infrastructure necessary to preserve and extend public broadcasting services for all Alaskans.
53. The State should develop an equitable

assessment and schedule of costs for use of the state satellite transponder.

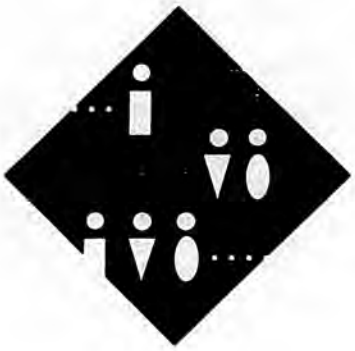
54. The State should follow the recommendation of "Marketing Alaska" to streamline the reporting requirements placed on the seafood industry by state and local governments, by establishing the capability for private industry to report required information to the state and to local governments electronically. One electronic form could be designed which would be transmitted electronically and shared by the state agencies, cities and boroughs that used the data. Department of Revenue and Fish and Game, and municipalities are the primary users of this data. Such a system would reduce the need for industry to file duplicative data with many entities, eliminate paperwork, and generally improve the speed and accuracy of data collection. This concept could also be applied to reports in the fields of hazardous materials, court scheduling, data mining, the Alaska Public Offices Commission and geographical information systems.
55. The State should interconnect with federal agencies via the Internet and encourage federal agencies to do the same. The State should take full advantage of the communications potential of the Internet in its dealings with the Federal government.
56. The State should address the use of electronic signatures. Electronic signatures will streamline many internal processes and will position the State for a method of authentication/verification of electronic communications with the public.
57. The State should increase efforts to reduce paperwork by storing our records electronically. Copies of these electronic records are admissible in an administrative or court proceeding.
58. The State should conduct a legal review of all relevant Alaska statutes, regulations, codes, and procedures requiring legal advertising with respect to the advent of Internet publishing.
59. The State should restrict purchases of two-way radios until technical standards are adopted.
60. In order to encourage electronic transactions, the State must resolve the issue of budgeting for fees related to credit card transactions. This may require legislation.
61. The TIC should evaluate the ability of the State's network infrastructure to accommodate various forms of electronic commerce, and the abilities of its contractors and suppliers to engage in it.
62. The State should identify ways of sharing GIS mapping resources with the Federal, municipal and borough governments, and explore opportunities to form partnerships with private agencies and organizations that have demonstrated strong mapping initiatives.
63. The Department of Education should develop and make accessible an information clearinghouse on standards, best practices, model requests for proposals, teacher training opportunities, etc.

**By 2000:**

64. The State should make all publications available to the public, available electronically.
65. The State should assess how telecommunications technology might be employed to help educate and train Alaskans for the changing work force requirements of the future.
66. The State should establish an Electronic Commerce education program in order to facilitate the sharing of resources and the resulting savings between the State and the business community.
67. The State should establish a single method of electronic authentication/verification of an entity that will be used by all agencies. Without this, an individual may have several IDs when communicating with multiple departments and in some cases possibly several within a single department.
68. The State should accommodate the public's need to do financial transactions in and with state offices through a communications requirements study. This would determine the network needs to provide financial transaction authorizations for credit, debit, and smart cards, and wire transfers.
69. The State should use telemedicine technologies for delivering State health services and information, to the extent that quality of and access to services and information are maintained or improved, and costs are maintained or reduced.

**Long Term:**

70. Basic 911 service should be available in all locations in the State. It is important to have the ability to dial 911 from any telephone (regular or cellular) and for the call to be routed to one of the regional dispatch centers in the State.



# Information Technology Human Resources

## SUMMARY

Training is a large part of the human resources issue in Alaska and in the telecommunications field in general Technologies change rapidly, and keeping state employees up on the latest developments takes a concerted and continuing effort. The State of Alaska has traditionally had a problem recruiting and retaining qualified people in the field of data processing. Currently, the State does not compete with private enterprise wages. As the State aggressively pursues the electronic world it needs to deal with this problem.

## GUIDING PRINCIPLES

71. The State should promote ongoing information technology training for end users and support personnel to enhance the ability to deliver services to Alaskans. Issues: Allocating or sharing scarce and expensive human resources among priority projects on a strategic information plan Keeping working environments in pace with technology and taking full advantage of the state's investment in technology Funding training necessary for skill enhancement appropriate for a profession as dynamic as information management "Outsourcing" alternatives that should be used to hire skills as needed, so as to provide an alternative to retaining a skill permanently on staff

## RECOMMENDATIONS

### By January 1998:

72. The State should review its options regarding its technical recruiting by conducting a salary and benefits survey. The survey must include the type of people we want to hire, not just a cross section of everyone who is looking for a job or who has technical people on staff. The first step in the process is to interview agency managers to learn what skills are needed and at what competency levels.
73. The State should assess the future needs of Alaskans for training in the uses of technology as part of the basic K-16 educational experience.
74. The State should emphasize training through a technical grant program or endowment that provides training and degree opportunities statewide, allowing educators to renew skills.
75. The State should allow for recruiting programs for technology positions at colleges and universities to be on-going. Incentives of one form or another need to be provided. Incentives for current, qualified employees is also a must. Also, current employees not working in the field should be provided encouragement and training if they want to make the career change.

### Long Term:

76. The State should explore developing a pool of technical resources to form its own internal "corporate university." Some of the most talented and dedicated analyst/programmers in State government started with the State in other positions, and have built upon this experience. This "university" could educate existing staff who have a fundamental understanding of the business processes and teach them the technical skills needed to support those business processes as analyst/programmers. The goal of such a program would be to provide competency in a core set of basic computing skills.

# Governance

## SUMMARY

State law vests in the Telecommunications Information Council (TIC) the authority to set policy on state government's voice, video and data systems. With that governance role, the TIC and its various subcommittees also assume responsibility for communicating with the private sector, the federal government and local governments on issues relating to development of the telecommunications infrastructure to meet the state's needs.

State law charges the TIC with responsibility to adopt this state Telecommunications and Information Technology Plan, which provides a list of recommendations for action. Many of the recommendations must be carried out by the TIC and its subcommittees. This chapter lists the guiding principles and recommendations for action to be carried out by the TIC in future years. It also includes recommendations for other agencies with missions that relate to telecommunications and information technology, such as the Alaska Public Utilities Commission , the Governor's Office and the state Department of Law.

## GUIDING PRINCIPLES

77. In order for the TIC to expand and improve its planning process, state government must define its "business vision, " which should be primarily concerned with making the internal operations of state government more efficient and more responsive to Alaskans. The business vision will define the short-term objectives of the Governor as well as longer term goals.

78. The TIC's continuing information technology planning process should incorporate the following goals:

- Chosen technologies should support the business of government.
- Alignment of information technology among executive, legislative and judicial branches.
- Appropriate information exchange and system integration.
- Sound management over the transition to distributed and public access technologies while effectively maintaining, enhancing, and replacing foundation legacy information environments.
- Effective management of state technical personnel, hardware and software resources.

79. The TIC should consider standards on an ongoing basis as part of a continuing information technology planning process. To determine where to standardize the process should consider costs and benefits. Benefits may include:

- Reduced costs of acquisition, development and maintenance.
- Faster development
- Easier sharing of data
- Easier sharing of skills
- Improved product quality
- Reduced demand for some supervisory decisions.

80. State agency capital project requests for information technology and telecommunications should conform to the goals and recommendations of the State Telecommunications and Information Technology Plan.

81. Group purchasing of hardware, software and services by state agencies should be encouraged by TIC policies.

82. The TIC and the Alaska Public Utilities Commission should take the lead in informing concerned groups about Federal Communications Commissions proceedings in the Telecommunications Act of 1996, and service in an advisory capacity as requested.

83. The TIC should lead state government wherever possible in developing partnerships for the purposes of information sharing, coordination, needs assessment, demonstration, and evaluation of statewide telemedicine activities.

84. TIC policies should encourage agencies to pursue the most cost effective and responsive means of providing services to the public; be that by internal effort, collaboration with other agencies or by

outsourcing to the private sector. Any cost/benefit analysis must include the impact of such decisions on any other state agencies and state government as a whole.

85. The TIC should maintain the infrastructure developed through the Satellite Interconnect Project.

## RECOMMENDATIONS

### By January 1998:

86. The TIC should coordinate the collection and aggregation of locally-based information, and with the involvement of the public, service providers and other interested parties, and use this information to create a more predictable view of demand for rural telecommunications services.

87. The TIC should provide a clear, open and visible telecommunications and information technology planning process. The process should include:
    - A statewide information technology profile, beginning at the agency level.
    - An inventory of the existing base of software, hardware, applications, technical support, users, local area networks, the wide area network, mainframes, etc.
    - Projected changes over the mid and long terms.
    - An organization structure at the agency and state level.
    - A reassessment of personnel issues.
    - An evaluation of standardization at the state level.
    - An evaluation of "transition issues" over the life of the plan - organizational, network, software and hardware.
    - Development of strategies for funding and timing.

88. The TIC should establish a framework of rules and standards for evaluating information technology and telecommunications capital projects requested by state agencies and a finance plan for maintenance of state government's information technology infrastructure.

89. The Governor should convene a working group or task force to define the State's "business vision" as it relates to the efficiency of internal operations and better customer service.

90. The TIC should establish a policy which acknowledges Internet e-mail as a legitimate transport for the exchange of correspondence with the public.

91. The TIC and the Department of Law should work together to assist state agencies in development of electronic commerce:
    - The Department of Law should assign at least one position in the Governmental Affairs Section of the Civil Division to develop an expertise, references, and contacts for changing state statutes to accommodate electronic commerce.
    - The TIC should seek legislative approval of minor changes to statutes that would encourage electronic commerce and revise statutes that mandate a paper product or manual process.

92. The TIC should adopt relevant technical standards for which there are no reasonable alternatives. The state should carefully consider the cost/benefit of standardization in technologies where there are many reasonable alternations and/or no clearly dominant standard exists. This considerations should be an open, visible process with broad participation, including private sector and other public sector interests that could be affected.

93. The TIC should support the broadcasting commission that provides oversight, marketing and monitoring support of the state's satellite infrastructure.

94. The TIC should review Alaska legislation that may impact the development, implementation, and use of telemedicine systems, and conduct a review of telemedicine legislation from other states.

95. The TIC should lead a review of state management and procurement policies to encourage competition among telecommunications services providers on technical service standards, prices, and development of broader band services.

96. The TIC should establish a working group to act as a clearinghouse for new proposals to implement the Alaska State Telecommunications and Information Technology Plan and the federal Telecommunications Act of 1996.

97. The TIC should establish a state educational telecommunications advisory committee.

98. The TIC should promote creation of consortia to improve telecommunications services to Alaskans. These consortia can collaborate on resources, standards, grant proposals and more. A model is the Distance Delivery Consortia in Bethel,

which brings together experts in education, health care and telecommunications.

99. The State should be actively involved in the National Governor's Association "Telecommunications Working Group" and the Western Governor's Association "Smart States" Initiatives.

100. The Alaska Public Utilities Commission should continue to take the lead in compliance with the federal Telecommunications Act of 1996, particularly with respect to universal service and long distance issues.

**By 2000:**

101. The TIC should work with the Alaska Public Broadcasting Commission to update and revise the commission's strategic plan and to build an increased accountability for the use of state funds by grantees.

102. The TIC should develop a point of focus within state government that would provide the administration, management, knowledge base, consultation, and, where appropriate, liaison with the private sector for any one technology. (An example: Electronic Data Interchange. Some agency needs to be the manager of agency working groups, the source of current state standards, a contact for private sector firms wishing to "partner" with the state, etc.)

103. The TIC should seek approval of one, or possibly two, full-time staff to assume leadership for development of Electronic Data Interchange and electronic commerce. The learning curve for EDI and electronic commerce is high.

104. The TIC should establish a formalized organization responsible for facilitating the development of telemedicine services by public and private health care providers.

105. The state Department of Health and Social Services should identify the infrastructure needs of the Alaska health care delivery system. The assessment should be used as the basis for a comprehensive, statewide, telemedicine plan.

106. The TIC should develop a long-term, statewide emergency communication plan for the State of Alaska. The plan should address issues such as access, dispatch, coordination, and medical contacts for emergency medical services.

107. The TIC should convene a forum of federal/military/state/local entities to establish joint participation on initiatives and issues related to emergency communications.

108. The Department of Commerce and Economic Development should extend its own planning framework to address ways in which telecommunications technology could be used to support economic development goals and objectives.

109. The TIC should review and revise all state policies to allow increased flexibility for educational use of technology and telecommunications.

**Long-term:**

110. The TIC should lead the way in urging that technology and telecommunications standards be met for acquisition and retention of teaching and administrative licenses.

# Funding

## SUMMARY

The cost of a telecommunication and information technology infrastructure within Alaska will require a substantial capital investment and will require an ongoing operational and equipment replacement budget. The cost of provisioning the state government's communications systems should be viewed in the context of all state resources and the desire to encourage community and private sector investment in modern telecommunications techno'ogy.

Telecommunications and Information Technology is critical to the development of Alaska. This state is faced with a very real problem of isolation from the rest of the nation and the world. That potentially wide gap can be bridged through the creative use of telecommunications. If we do not take advantage of these tools, we face the very real possibility of being left behind in the 20th century, while other states and nations progress to the 21st.

## GUIDING PRINCIPLES

111. All Alaskans must recognize that there is a State government telecommunications and information technology infrastructure vital to their well being that must be funded at a basic level each year. It is incumbent on State government to develop a plan recognizing this and funding that infrastructure's basic costs.

## RECOMMENDATIONS

### By January 1998:

112. The Alaska Rural Communications Service, or ARCS, system should develop a way for communities and individuals to contribute their support for the system.
113. The State should propose a legislative endowment similar to Alaska Science Technology or recurring legislative appropriations for the creation and upkeep of the state's telecommunications infrastructure in Alaska.
114. The State should pursue partnerships with private, community consortiums. These consortiums could contribute matching funds on community based programs.
115. The State should pursue financial options such as revenue bonds for the acquisition of information technology.
116. The State should provide incentives for a provision or building of new services to providers, communities or companies for hardware and software requirements. Incentives should not be ongoing or provided if the service was going to be provided anyway as part of their business plan.
117. The State should consider a telephone surcharge for funding Basic 911 systems and education technologies.
118. The TIC should investigate funding options, and its role and responsibilities for meeting information technology needs.
119. The State should develop a funding strategy to deploy new technology which will advance the state's investment in wide scale, cost-beneficial distribution of audio and video services, including public broadcasting signals.

# Telecommunications in Alaska

**by H.A. "Red" Boucher**

H.A. "Red" Boucher is a telecommunications consultant, former Lt. Governor and State Representative. During his six years in the State Legislature from 1985 to 1990 he chaired the House Special Committee on Telecommunications (upon which Representative Fran Ulmer also served) and authored the legislation that founded the Telecommunication Information Council. As the founder and first chair of the Council, he has a unique vantage point of the history and future of telecommunications in our state.

The history of telecommunications development in Alaska is a history of constantly pushing the edge of the technology envelope. With the advent of the Alaska Communication System through projects such as White Alice the civil authorities of the territory and the state adopted programs that piggybacked civil needs on systems that were military in design and use. Moving from military telecommunications dependence in the early 1970's Governor Egan established a controlling policy for the future. Governor Egan proclaimed that universal telephone service should be made available to all citizens of the state. From the initiatives of Governors Egan and Hammond the state in cooperation with Alascom installed small satellite earth stations in over 200 communities. For the first time hundreds of villages would have basic telephone service and a dedicated emergency and health channel. A simple system that would change the life style of rural Alaska. This was a first for Alaska; a first for the United States and a first for the world.

The state introduced low-powered television to rural Alaska in 1973. Under special licensing from the Federal Communication Commission the Alaska Educational Broadcasting Commission installed stations at Unalaska and St. Paul Island. Programming initially was provided by video tapes shipped from Anchorage; later receive-only television terminals would provide the programming. The LPTV stations were the first in Alaska and first in the world.

While the credit for these many advance can be shared by numerous persons, the beginning can be traced to two outstanding Alaskans, Governor Bill Egan and Augie Hiebert. Governor Egan had the foresight to give direction to the state's telecommunication policy and Augie Hiebert had the tenacity of effort that would lead Alaska into the satellite era. Those individuals that followed their lead did so with a purpose and a resolve of bringing the best in telecommunications to all citizens of our state.

Alaska was pioneering the way at the dawn of the Information Age in the 70's and 80's, we must again develop a plan that improves the quality of Alaskan life, empowers our people, connects all Alaskans, enhances educational opportunities for our youth and creates an economic engine that benefits all Alaskans.

The key words to the Information Age are "connectivity," "access" and "content." The technology is already there and is growing at a revolutionary rate. The state of Alaska has more computer power per capita than any state in the Union. The challenge is to use this power to connect our people, create economic opportunity and improve our quality of life. Just as the Information Highway backbone is connecting America we in the 49th state must see that the Alaska backbone connects all Alaskans, allowing them to participate more fully in the future of their state.

The next few decades will witness profound alterations not only in the way we live, work, entertain and inform ourselves, but also in the strategies of business, the dynamics of the marketplace, the competition between companies and between countries, the process of wealth creation and even the role of government. By whatever name we call it, multimedia, Internet, the Information Highway, the digital revolution is already rapidly reconstructing the world we live in a new and significantly different form.

The following statement, written by Dr. Larry Pearson of the Department of Journalism and Public Communications, UAA, and me was the conclusion of a September 1987 report to the Governor and the Legislature titled "The Telecommunications Information Council:

Legislative History and Implementation Plan."

> "The new Telecommunications Information Council has been given a mandate which empowers it to bring great changes to the state of Alaska. It can change the way people communicate. It can help the state government to organize its information resources and to use them in ways that were impossible before."
>
> "The Telecommunications Information Council can bring Alaska fully into the Information Age. It can formulate the larger policies and provide the needed direction as Alaska's information systems continue to develop."
>
> "Or ....it can choose not to accept the vision. It can take a technocratic stance that traps us in the present. We will then remain pioneers, working with the tools of pioneers... while civilization passes us by."

During the years since CSHB40 was signed into law by Governor Cowper the response to the challenge has been less than adequate. From a state that invested five million dollars in telecommunication infrastructure in 1975 and introduced "Learn Alaska" to an envious world we have drifted into the backwaters of the Information Age.

The Telecommunications Information Council offers us the promise of intelligently managing our telecommunications resources and planning their future development. However, it has yet to fulfill its mission. Recent efforts by the Knowles/ Ulmer administration hold great promise for the future.

When the young student in Akutan, Eek or Mud Bay reaches out to the digital world of knowledge with the same tools as the student at West High in Anchorage we will have built our on ramp to the Information Highway. Until this happens we will be much like we were before the advent of the satellite demonstration project, unconnected

In summary, Legislative action and regulatory reform by Alaska's Congressional delegation, the Executive and Legislative branches and the regulatory bodies, in partnership with industry, must lead the way. During the process the citizens of Alaska must have the opportunity to participate in the building of a communication system that again assumes the leadership role that Alaska once had. "Learn Alaska" is history because of a lack of vision, "Learn From Alaska" is the opportunity before us. The time is now, the choice is ours. If we fail to do this we will find Alaska trapped in the past working with the tools of pioneers.....while the information highway bypasses our 49th state.

# Comments or questions about this plan?

**Contact:**

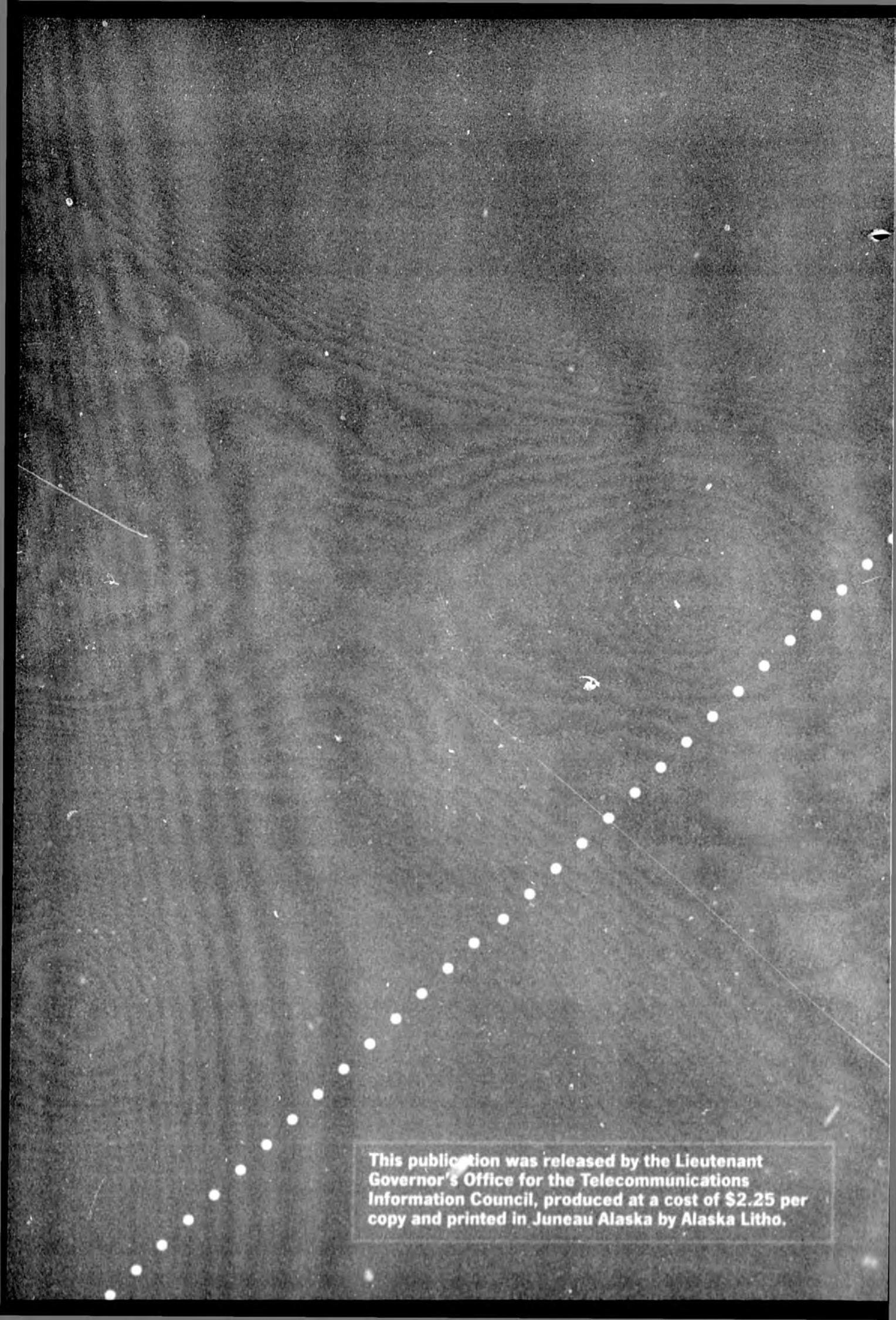
Andy Kline
Special Assistant, Telecommunications
Lieutenant Governor Fran Ulmer
P.O. Box 110015
Juneau, Alaska 99811-0015

Phone: (907) 465-3520
Fax: (907) 465-5400
andy_kline@gov.state.ak.us

Without the following people's hard work and good ideas, this plan would not have been possible:

Mark Badger
Tim Banaszak
Sharon Bandle
Lynn Bartlett
Ken Bischoff
Howard L. Bonar
Red Boucher
Mark Boyer
Tom Brady
Bennett Brooks
Susan Browne
Geron Bruce
Vicki Bukovick
John Cacy
John Cameron
Glenda Carino
Amy Carroll
Ed Christian
Bob Cole
Allen Cooper
John Corso
Lamar Cotten
Karen Crane
Tim Crawford
April Crosby
Rick Cross
Damon Cruz
Michael Cushing
Dennis Daigger
Rory Darling
Jerry DeFrancisco
Larry Dietrick
Daryl Donaldson
Jay Dulany
Patricia Dunn
Steve Eason
Tom Edrington
Susan Elliott
Deb Erickson
David Essary
Jack Fargnoli
Frank Ferrante
Neal Freid
John Fritz
Tom Garrett
Dave Germer
Susan Goodman
Rich Grayson
Bill Gregory
Dean Guaneli
Jim Harpring
Jeff Harrison
Jeff Hartman
Bob Heavilin
Bob Helm
Shawn Henderson
Ron Hensley
Alex Hill
Linda Hoff
Sue Hosford
Marcia Hubbard
Becky Hulse
Bob Jenkins
Mark Johnson
Karen Jordan
John Katz
Jack Keating
Jamie Kenworthy
Cheryl Kirk
Andy Kline
Pam LaBolle
Bill Legere
David Leone
George Lindamood
John Lindback
Marina Lindsey
Bob Lohr
Pierre A. Lonewolf
Leo Lutchansky
Della Mathis
Carol McCabe
Annalee McConnell
Rich McMahon
Bob Medinger
Barbara Miklos
John Monahan
Doug Moore
Karen Morgan
Lynn Morley
John Morrone
Rose Munafo
Peter Nakamura
Larry Nakata
Mike Noel
Jason Ohler
Fred Pearce
Gordon Peterson
Lee Peterson
Dugan Petty
Steve Politsch
Catherine Reardon
Jim Rowe
Bob Rubadeau
Virginia Rusch
Kristin Schultz
Dan Shanis
William Shechter
Veronica Slajer
Del Smith
Joe Spears
Arlene Sword
Larry Talley
Dia Taug
Donna Tollman
John Vezina
Frank Wallis
Don Wanie
Susan Warner
Frank Williams
Al Zangri

There are many others who helped with their time and attention to this project. Thanks to all of those listed and to anyone who was inadvertantly left off this list.



This publication was released by the Lieutenant Governor's Office for the Telecommunications Information Council, produced at a cost of $2.25 per copy and printed in Juneau Alaska by Alaska Litho.

HB 345

TONY KNOWLES
GOVERNOR

P.O. Box 110001
Juneau, Alaska 99811-0001
(907) 465-3500
Fax (907) 465-3532

STATE OF ALASKA
OFFICE OF THE GOVERNOR
JUNEAU

January 22, 1998

The Honorable Gail Phillips
Speaker of the House
Alaska State Legislature
State Capitol
Juneau, AK 99801-1182

Dear Speaker Phillips:

Alaska can take a positive step into the age of technology by allowing industry and government to conduct business electronically. This bill I transmit today will legalize electronic signatures in our state, providing an opportunity for state agencies to better serve the public "online" and for businesses to act with increased efficiency.

This bill has been developed under the direction of the state 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.

The bill would legalize electronic signatures between consenting parties and authorize state agencies to use electronic signatures in interactions with the public. Some notarization requirements that could hinder an agency's ability to use electronic signatures would be repealed.

This legislation updates our laws to better mesh the new technological realities of how business and government can be conducted more efficiently. I urge your prompt and favorable action on this measure.

Sincerely,

Tony Knowles
Governor

# HB 345
# 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.
5. Authorize filing electronic documents with the state archives in the Department of Education.

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:** Accomplishes the following:

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

2. Establishes that the use of electronic signatures between consenting parties is legal in Alaska. An electronic signature would have the same legal standing as a handwritten signature.

3. Specifies that the Lt. Governor's Office or other state agencies can adopt regulations for the use of electronic signatures in conducting state business or for use of electronic signatures by businesses and individuals.

4. Defines electronic signatures and records.

**Section 2:** 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 3:** Specifies that information in state records that would compromise the security of an electronic signature is an "exception" from the state public records statute.

**Sections 4 – 41:** Open the door for the state Department of Commerce and Economic Development to allow businesses and corporations to file reports electronically and verifying them with electronic signatures. These sections revise statutes in the corporations and partnership codes to remove notary requirements on various documents filed with the DCED.

**Sections 42 – 45:** Revise statutes in AS 34.45 to remove the requirement that signatures on reports or other forms filed with the state regarding unclaimed property be notarized and replace it with the requirement that signatures be made under penalty of unsworn falsification.

**Sections 46 - 49:** Revise statutes relating to the state archives system to allow the archives to accept electronic records.

**Sections 50 – 53:** Revise various statutes in AS 45.50 relating to regulation of trademarks to remove the requirement that signatures on certain forms filed with the state be notarized.

**Section 54:** Allows agencies to proceed with developing regulations necessary to implement this legislation before the effective date of the bill.

**Sections 55 – 56:** Provide effective dates.

# Electronic Signature Legislation

## States With Current Legislation (affected sectors):

| | |
|---|---|
| Arizona | (State Agencies; Secretary of State) |
| California | (Health Care; Insurance; Death Certificates; All others) |
| Colorado | (Financial; Legislative) |
| Connecticut | (Health Care) |
| Delaware | (State Agencies) |
| Florida | (Notarizations; All others) |
| Georgia | (Taxes; Motor Vehicles; All others) |
| Illinois | (State Agencies; Comptroller; All others) |
| Indiana | (All *but* Legislative and Judicial branches and Educational institutions) |
| Iowa | (Voter Registration) |
| Kansas | (All) |
| Louisiana | (Health Care; Justice System; All others) |
| Maine | (Motor Vehicles) |
| Minnesota | (Taxes; Motor Vehicles; All others) |
| Mississippi | (Secretary of State; All others) |
| Missouri | (Political Filings) |
| Nebraska | (Architecture & Engineering) |
| Nevada | (State Agencies; Justice System) |
| New Hampshire | (State Agencies) |
| North Dakota | (State Agencies; Secretary of State) |
| Ohio | (Health Care) |
| Rhode Island | (State Agencies) |
| Tennessee | (Justice System) |
| Texas | (State Agencies; Motor Vehicles) |
| Utah | (Justice System; All others) |
| Virginia | (State Agencies) |
| Washington | (All) |
| Wyoming | (Secretary of State) |

Numerous other states have legislation that sets up certification authorities for digital signatures or that creates task forces to study digital signature technology. Additionally, many states have pending legislation that deals with digital or electronic signatures.

Only Alabama, Alaska, Arkansas, Idaho, Pennsylvania, South Carolina, South Dakota, and West Virginia had not begun to address the usage of digital signatures as of 9/8/97.

**Electronic and Digital Signature Legislation**

| State | Bill Identification | Passed/ Enacted | Drafted/ Pending | Comments |
|---|---|---|---|---|
| | | | | |
| [redacted] | | | | |
| Arizona | 96 AZ H.B. 2444; 96 AZ Ses. Laws 213; AZ Rev. Stat., Sec. 41-121 | 4/18/96 | | The Secretary of State (SoS) shall "approve for use by all other state agencies, and accept digital signatures for documents filed with the office of the SoS." The SoS may adopt rules to implement this section. |
| [redacted] | | | | |
| California | CA Govt. Code Sec. 16.5 | 10/4/95 | | Draft regulations issued by SoS 5/23/97. Specifies public hearing to be held 7/15/97. Final enactment is expected 9/97. Only governs electronic signatures affixed to communications with public entities. |
| | 95 CA A.B. 1577 | YES | | Digital signatures may be used for government transactions. |
| | 97 CA S.B. 1338 | | 2/28/97 | Enacts CA Electronic Commerce Act of 1997. Creates a planning committee to direct, plan and implement a state operational plan for electronic data interchange, electronic commerce and information management for the state government. |
| | 97 CA S.B. 49 | 4/14/97 | | SoS must make reports filed to SoS available on a public computer network. SoS must develop a system for electronic transfer of data that uses public and private keys with digital signatures. PKI only. |
| | 97 CA S.B. 7 | 5/17/97 | | Similar to CA S.B. 49. |
| | 97 CA S.B. 955 | 6/9/97 | | Permits health care service plans and insurers to accept electronic signatures. |

| State | Bill Identification | Passed/ Enacted | Drafted/ Pending | Comments |
|---|---|---|---|---|
| California | **97 CA A.B. 44** | 6/24/97 | | SoS must assign a task force to study creation of a digital electoral system. Report due 4/1/99. |
| | **Digital Signature Regulations** | 5/23/97 | | Digital signatures must be created by an acceptable tech (PKI, signature dynamics, and more expected in the future). Keyholder must use "reasonable care" in maintaining security/secrecy of private key. Establishes a list of authorized Certification Authorities (CAs). |
| | **Public Hearings on 16.5** | 7/15/97 | | Final legislation to be issued in 60 days (Sept. 97). |
| | **97 CA A.B. 721** | 8/26/97 | | Electronic filing of documents such that they shall be deemed valid originals once converted into paper form as long as they include a digital signature that meets requirements of CA law. |
| | **95 CA A.B. 2755** | 9/24/96 | | Permits use of electronic signature (or other indicator of authenticity approved by state registrar) for death certificates. |
| Colorado | **97 CO S.B. 155** | 4/24/97 | | Financing statements may be filed electronically when accompanied by an electronic signature. |
| Connecticut | **Gen. Stat. CT Sec. 19a-25a; '95 Public Act 95-257** | 1995 | | Commissioner of Public Health and Addiction Services directed to adopt regulations for the use of electronic signatures for medical records maintained in hospitals, if he deems them necessary. |
| | **97 CT S.B. 1308** | | 3/19/97 | Establishes a task force to study the usage of digital signatures -- technology, creation, authentication and verification, and legality. Report due 1/1/98. |
| Delaware | **95 DE S.B. 458** | 7/12/96 | | Amends Title 29 of DE Code to permit the use of electronic signatures and the use of electronic approval for state officers in approving payment for services. |

| State | Bill Identification | Passed/ Enacted | Drafted/ Pending | Comments |
|---|---|---|---|---|
| Georgia | **97 GA S.B. 103** | 4/22/97 | | Any person may, but is not required to, accept or agree to be bound by an electronic record executed or adopted with an electronic signature. Encourages state govt. and private firms to conduct their business using electronic media. Authorizes pilot projects in all state agencies. |
| Hawaii | **HI Rev. Stat., Chap. 601; '95 HI S.B. 2401** | 6/17/96 | | Creates a task force to explore digital and electronic filing of court documents. Reports annually. |
| | **97 HI S.B. 961** | | 3/6/97 | Provides for the licensing and regulation of CAs by Dept. of Commerce and Consumer Affairs (DOCCA). CAs must: employ a notary, file a guarantee, and submit to performance audits. DOCCA will be a CA. Digital signatures will be accepted as a manual signature except in the case of negotiable instruments made payable to bearer. |
| [illegible] | | | | |
| Illinois | **97 IL 945** | | 1/13/97 | Authorizes use of digital signatures for all transactions. Mentions PKI. |
| | **97 IL H.B. 276** | | 4/18/97 | Allows for the use of digital signatures in any communication between a state agency and the Comptroller in which a signature is required or used. |
| | **97 IL S.B. 516** | 6/27/97 | | Identical to '97 IL H.B. 276. |
| | **IL Elec. Commerce Security Act** | | 9/3/97 | Digital or electronic signatures satisfy any rule of law that requires a signature. PKI mentioned. |
| Indiana | **97 IN H.B. 1945** | | 5/6/97 | Digital signatures may be filed or received by the state. Only applies to transactions within the state, outside of the judicial and legislative branches and educational institutions. Provides that the State Board of Accounts is responsible for implementing and administering authentication and allowable technology. Only PKI permitted. |

| State | Bill Identification | Passed/ Enacted | Drafted/ Pending | Comments |
|---|---|---|---|---|
| Maryland | **97 MD H.B. 1015** | | 2/3/97 | Provides for the licensing and regulation of CAs. SoS is a CA and shall adopt regulations for licensing, audits, investigations, duties, etc. of CAs. Similar to UT approach to digital signatures. Only PKI. |
| Maryland | **97 MD S.B. 822** | | 2/10/97 | Nearly identical to '97 MD H.B. 1015. |
| | **97 MD H.B. 1386** | | 2/10/97 | Establishes a task force to study the usage of digital signatures -- technology, creation, authentication and verification, security, and legality. |
| Massachusetts | **MA Electronic Records and Signature Act** | | 4/17/97 | Equates all electronic signatures (including digital signatures) with traditional signatures for evidence admissibility and weight. |
| Michigan | **97 MI S.B. 204** | | 2/19/97 | Provides for the licensing and regulation of CAs and subscribers and addresses the recognition and liability of repositories. PKI only. |
| Minnesota | **Electronic Signature Legislation** | YES | | Facsimile and digital signatures may be used in limited situations such as with the Dept. of Administration Organization, orders and papers relating to workers compensation, and electronic tax returns. |
| | **97 MN H.F. 56** | | YES | Defines digital signatures. Deals with public and private transactions. PKI only. |
| | **97 MN H.B. 871** | | 2/20/97 | Provides for the electronic conduct of state business. Authorizes the Commissioner of Administration to approve the use of electronic approvals and digital signatures for state business. PKI only. |
| | **97 MN S.B. 240** | | 4/30/97 | Nearly identical to 97 MN H.B. 871. |

| State | Bill Identification | Passed/ Enacted | Drafted/ Pending | Comments |
|---|---|---|---|---|
| Missouri | **97 MO S.B. 16** | 7/7/97 | | Provides for the acceptance of electronic signatures on electronically filed reports by candidates for public office if it becomes possible to verify the legitimacy of electronic signatures. |
| Montana | **97 MT H.B. 468** | | 2/18/97 | Authorizes the SoS to develop and implement a statewide electronic filing system. Requires the SoS to promulgate rules on access, security, and integrity of electronic filing. |
| Nebraska | **97 NB L.B. 42** | | 1/9/97 | Authorizes the use of electronic signatures in the place of manual signatures for all communications provided that it conforms to the specific regulations adopted by the SoS. |
| Nebraska | **97 NB L.B. 286** | | 1/14/97 | Authorizes the usage of digital signatures in the place of manual signatures in communications with state agencies as long as they follow specific regulations adopted by the SoS. The SoS is required to promulgate regulations before 9/1/98 on the usage of digital signatures. |
| | **97 NB L.R. 262** | | 5/22/97 | Provides for a study of the issues surrounding the enactment of digital signature legislation, including the policy issues presented by 97 NB L.B. 42 and 97 NB L.B. 286. |
| | **97 NB L.B. 622** | 6/16/97 | | Authorizes persons licensed to practice architecture or engineering to use electronic signatures with electronic seals as long as they are protected with an "electronic revision approval system." |
| Nevada | **97 NV S.B. 42** | 4/26/97 | | Provides for the usage of electronic signatures in financial transactions pertaining to the State. |

| State | Bill Identification | Passed/ Enacted | Drafted/ Pending | Comments |
|---|---|---|---|---|
| New York | **97 NY S.B. 2238; 97 NY A.B. 6813** | | 3/4/97 | Similar to UT and WA digital signature statute. Charges the SoS with adopting regulations to govern the usage of digital signatures. Authorizes the usage of PKI technology only. |
| North Carolina | **97 NC H.B. 290** | | 2/20/97 | Establishes a legislative study commission on electronic commerce to include: an evaluation of the feasibility and desirability of authorizing the use of digital signatures, the legislation of other states, and the benefits of regulating CAs. |
| North Carolina | **97 NC H.B. 925** | | 4/10/07 | Designed to protect the privacy of health information. Permits the acceptance of electronic signatures as a legally binding signature for the identification of any individual, entity, or health information associated with an individual or entity. |
| | **97 NC S.B. 1005** | | 4/21/97 | Nearly identical to '97 NC H.B. 925. |
| | **97 NC H.B. 1047** | | 4/21/97 | Establishes a legislative study commission on information technology to review the current information technology that impacts public policy. Otherwise nearly identical to '97 NC H.B. 290. |
| North Dakota | **97 ND Concurrent Res. 4024** | | | Directs the legislative council to study the development of an electronic mail and management policy for government entities. Permits official business to be conducted electronically using digital signatures. |
| North Dakota | **97 ND S.B. 2071** | YES | | Provides that the SoS shall adopt rules concerning electronic telecommunications and the use of electronic signatures for documents filed electronically with State agencies. |
| Ohio | **97 OH H.B. 243** | 1/3/97 | | Permits the use of electronic signatures on authorizations for medical records. Intended to facilitate in-hospital verifications of medical reports, diagnoses, and similar administrative signatures. |

| State | Bill Identification | Passed/ Enacted | Drafted/ Pending | Comments |
|---|---|---|---|---|
| Texas | **97 TX S.B. 748** | | 2/26/97 | Amends the Business and Commerce Code to allow digital signatures to authenticate written electronic communications sent to state agencies, subject to the rules adopted by the Comptroller, State Auditor and the Attorney General. |
| | **97 TX S.B. 787** | | 3/3/97 | Nearly identical to '97 TX S.B. 748. |
| | **97 TX H.B. 984** | 5/1/97 | | Similar to '97 TX S.B. 748 except that it is not limited to communications sent from or received by a State agency. |
| | **97 TX S.B. 370** | 5/20/97 | | Authorizes the Dept. of Transportation to accept license applications that are transmitted with a digital signature. |
| | **97 TX S.B. 645** | 5/20/97 | | Authorizes the State Comptroller to establish procedures for using a digital signature for any document or data submitted to the Comptroller and for the purpose of State agency transactions. |
| Utah | **UT Code Annotated 46-3-101 to 504** | YES | | "Utah Digital Signature Act." First legislation to authorize the commercial use of digital signatures. Governs use of public-private key encryption and CAs and was designed to comport with various national and international standards already in place. CAs are licensed by the Utah Dept. of Commerce. Protects a subscriber's private key as property. |
| | **97 UT H.B. 95** | 2/4/97 | | Provides that a notary's acknowledgement on an electronic message or document is considered complete if it has been digitally signed in the presence of a notary and if the notary signs the acknowledgement with a digital signature even without the imprint of the notary's official seal. |
| | **96 UT S.B. 73** | 3/8/96 | | Makes slight technical adjustments to Sections 46-3-103 and 46-3-301 of UT Digital Signature Act. PKI only. |

| State | Bill Identification | Passed/ Enacted | Drafted/ Pending | Comments |
|---|---|---|---|---|
| Washington | **97 WA S.B. 5308** | 4/15/97 | | Amends WA DSA to provide that the SoS is a CA. SoS also given the authority to adopt rules to govern CAs. PKI only. Effective 1/1/98. |
| [redacted] | | | | |
| Wisconsin | | | Fall 97 | Bill in the process of being drafted |
| Wyoming | **WY Statutes 9-1-306** | | | Authorizes the use of digital signatures for documents filed electronically with the SoS. Also extends civil and criminal penalties applicable to fraudulent manual or facsimile signatures to electronic signatures. Authorizes SoS to adopt regulations to govern the use of digital signatures. |
| **Federal Measures** | | | | |
| Clinton Administration | **1997 Electronic Data Security Act** | | 3/12/97 | Enables the development of a key management infrastructure for a public-key-based encryption. Authorizes the Secretary of Commerce to register CAs and key recovery agents. |
| U.S. FDA | **Regs. On Elec. Records; Elec. Sigs.** | 3/20/97 | | Sets forth criteria for the acceptance of electronic records and signatures by the FDA. |
| U.S. Judicial Conference | **Federal Rules of Civil Procedure -- Rule 5** | Oct-95 | | Courts may, by local Rule, permit the electronic filing, signing and verification of documents. |
| | **Federal Rules of App. Proc. -- Rule 25** | Oct-95 | | Courts may permit by local Rule, the filing of papers by electronic means, provided such means are consistent with any technical standards established by the Judicial Conference. |

# Georgia Electronic Records and Signatures Act

# SENATE BILL 103

**By: Senators Tysinger of the 41st, Egan of the 40th, Oliver of the 42nd and others**

# AN ACT

To amend Title 10 of the Official Code of Georgia Annotated, relating to commerce and trade, so as to enact the "Georgia Electronic Records and Signatures Act" to provide for a short title; to provide for legislative construction and definitions; to authorize the use of electronic signatures instead of written ones and provide for the legal effect of such usage; to amend Code Section 50-18-72 of the Official Code of Georgia Annotated, relating to exceptions to the disclosure of public records, so as to include certain information relating to electronic signatures in the exceptions; to amend Chapter 29 of Title 50 of the Official Code of Georgia Annotated, the "Information Technology Policy Act of 1995," so as to provide for legislative intent; to provide for authority for encouraging the conduct of governmental and private sector business using electronic media and provide for powers and duties of the Georgia Information Technology Policy Council; to provide for pilot projects; to provide for the Electronic Commerce Study Committee and its membership, allowances, duties, and powers; to provide for an effective date; to repeal conflicting laws; and for other purposes.

BE IT ENACTED BY THE GENERAL ASSFMBLY OF GEORGIA:

SECTION 1.

Title 10 of the Official Code of Georgia Annotated, relating to commerce and trade, is amended by adding at the end a new chapter to read as follows:

CHAPTER 12

10-12-1.

This chapter shall be known and may be cited as the "Georgia Electronic Records and Signatures Act."

10-12-2.

The provisions of this chapter shall be construed to promote the development of electronic government and electronic commerce.

10-12-3.

As used in this chapter the term:

(1) "Electronic signature" means an electronic or digital method executed or adopted by a party with the intent to be bound by or to authenticate a record, which is unique to the person using it, is capable of verification, is under the sole contract of the person using it, and is linked to data in such a manner that if the data are changed the electronic signature is invalidated.

(2) "Record " means information that is inscribed on a tangible medium or that is stored in an electronic or other medium or that is stored in an electronic or other medium and is retrievable in perceivable form. "Record " includes both electronic records and printed, typewritten, and tangible records.

10-12-4.

Any person or entity, including but not limited to any department or agency of the state or any of its political subdivisions, may, but shall not be required to, accept or agree to be bound by an electronic record executed or adopted with an electronic signature. Where a person or other entity accepts or agrees to be bound by an electronic record executed or adopted with an electronic signature, then:

(1) Any rule of law which requires a record of that type to be in writing shall be deemed satisfied; and

(2) Any rule of law which requires a signature shall be deemed satisfied.

SECTION 2.

Code Section 50-18-72 of the Official Code of Georgia Annotated, relating to exceptions to the disclosure of public records, is amended by striking "or" at the end of paragraph (10) of subsection (a) thereof, striking the period at the end of paragraph (11) of said subsection and inserting " or ", and adding immediately thereafter the following:

"(12) Public records containing information that would disclose or might lead to the disclosure of any component in the process used to execute or adopt an electronic signature, if such disclosure would or might cause the electronic signature to cease being under the sole control of the person using it. For purposes of this paragraph, the term "electronic signature" has the same meaning as that term is defined in Code Section 10-12-3."

SECTION 3.

Chapter 29 of Title 50 of the Official Code of Georgia Annotated, the "Information Technology Policy Act of 1195," is amended by adding at the end a new Code section to read as follows:

"50-29-12.

(a) The General Assembly desires to promote economic development and efficient delivery of government services by encouraging state governmental agencies and private sector entities to conduct their business and transactions using electronic media.

(b) All state agencies, authorities, and boards are authorized to establish pilot projects, which are to serve as models for the application of technology such as electronic signatures, through public and private partnerships with private companies providing such technology related services. Such pilot projects shall be approved by the Georgia Information Technology Policy Council. Such projects shall consider both commercial and government applications, be inclusive of major categories of electronic signature technology, and be established through a request for proposal process. The pilot projects are intended to provide a proof of concept for the application of technology, such as electronic signatures, and to serve to educate the General Assembly and the public at large as to the benefits of electronic signatures as well as the role of state government in any future regulatory capacity. One such pilot project may involve digital signatures and the use of a public key infrastructure established by a service provider. Any private partner chosen for these pilot projects may establish user fees to pay for the cost of these services so that

no state funds would be required.

(c) State agencies establishing pilot projects shall submit quarterly progress reports on such projects to the Georgia Information Technology Policy Council, and the council shall then submit such reports to the Electronic Commerce Study Committee. The council shall monitor the success of such pilot projects and provide technical assistance to the extent that resources of the council are available.

(d) There is created the Electronic Commerce Study Committee to be composed of 12 members. The committee shall study the issues relating to electronic records and signatures. The President of the Senate shall appoint five members to the committee, three of whom shall be members of the senate and two of whom shall be citizen members with recognized interest and expertise in electronic commerce. The President of the Senate and Speaker of the House of Representative shall also each designate from among their legislator appointees one cochair of the committee. The Georgia Information Technology Policy Council shall appoint one member to the committee. The Secretary of State shall appoint one member to the committee. The committee, upon the call of either cochair, is authorized to conduct meetings at such places and at such times as it considers expedient and to do all other things which are necessary or convenient to enable it to fully and adequately exercise its powers, perform its duties, and accomplish its objectives and purposes. Legislative members and citizen members shall receive the allowances authorized by law for members of interim legislative committees for their services on the committee but shall receive the same for not more than five days. Members of the committee who are state officials, other than legislative members, and state employees shall receive no compensation for their services on the committee, but they shall be reimbursed for expenses incurred by them in the performance of their duties as members of the committee. The funds necessary for the reimbursement of the expenses of state officials, other than legislative members, and state employees shall come from funds appropriated to or otherwise available to their respective departments. All other funds necessary to carry out the provisions of this subsection shall come from the funds appropriated to or otherwise available to the Senate and House of Representatives. If the committee makes a report of its findings and recommendations, with suggestions for proposed legislation, if any, such report shall be made on or before December 15, 1997. The committee shall stand abolished December 15, 1997. "

SECTION 4.

This Act shall become effective upon its approval by the Governor or upon its becoming law without such approval.

SECTION 5.

All laws and parts of laws in conflict with this Act are repealed.

Martin 47th offers the following amendment: Amend SB 103 by inserting following the word and symbol "usage;" on line 7 of page 1 the following:

"to provide for recovery by a person whose electronic signature is used in an unauthorized fashion; to provide for a definition;".

By deleting the quotation mark at the end of line 32 of page 2 and by inserting between lines 32 and 33 of page 2 the following:

"10-12-5.

A person whose electronic signature is used in an unauthorized fashion may recover or obtain any or all of the following against the person who engaged in such unauthorized use, provided that the use of such electronic signature in an unauthorized fashion was negligent, reckless, or intentional:

(1) Actual damages;

(2) Equitable relief, including, but not limited to, an injunction or restitution of money or property;

(3) Punitive damages under the circumstances set forth in Code Section 51-12-5.1;

(4) Reasonable attorneys' fees and expenses; and

(5) Any other relief which the court deems proper.

As used in this Code section the term "person" means a natural person, corporation, trust, partnership, incorporated or unincorporated association, or any other legal entity.

Adopted in House 3/20/97

Senate Agreed to House Amendment 3/24/97

# 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.

# 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

# Digital Signature Act: Examples

## Subscriber Denies Verified Digital Signature

Susan owned and operated a video movie sales and rental business. Her supplier informed her that she could place purchase orders from her Internet account for faster service, if she digitally signed the orders and obtained a certificate from a licensed certification authority.

Susan visited Cedric, a licensed certification authority, who issued her a certificate. Cedric gave Susan a printout of the certificate with its contents labeled for identification, and Susan signed a receipt containing a second printout to which was appended the following paragraph:

**Acceptance:** The undersigned has reviewed the foregoing certificate, finds it to be accurate and in accordance with representations made to the licensed certification authority issuing it, and therefore hereby accepts the foregoing certificate pursuant to the Utah Digital Signature Act.

Susan signed below the paragraph in ink and noted the current date. Cedric also took an instant photograph of Susan and attached it to her signed acceptance.

Susan connected to her supplier's WorldWide Web catalog of new offerings and ordered 500 copies of Dangerous Dreams, a movie that had just begun to show in theaters. She digitally signed the purchase order using the private key corresponding to the public key in the certificate Cedric had issued.

The next evening, she decided to take in a movie, saw Dangerous Dreams, and disliked it. The 500 copies of Dangerous Dreams arrived the next morning. Susan rejected the shipment and phoned her supplier to explain, deciding to feign ignorance of the order. She acted surprised, told the supplier that she had never ordered the 500 copies of Dangerous Dreams.

Finding itself overstocked with Dangerous Dreams inventory, the supplier sued Susan for breach of their sales contract. Susan alleged in her answer that she had never ordered DangerousDreams and that the order was within the statute of frauds of Utah Uniform Commercial Code 70A-2-201 (1994).

**Under the Utah Act:**

> Cedric, the certification authority, has little risk of liability, since the foregoing facts do not indicate that he breached a duty under the Utah Act. He also appears to have documented the issuance and acceptance process well, should evidence of them be needed in the litigation between Susan and the supplier.
>
> Susan, the subscriber, will probably be held liable for breach of a promise to purchase the 500 videotapes, assuming that the contract between Susan and the supplier requires her to accept delivery of goods shipped as ordered. Susan will probably fail to persuade the trier of fact that she had nothing to do with the purchase order, since it bears her digital signature verified by the public key in the certificate.
>
> If she challenges the certificate, Cedric has good evidence to support it. Susan will bear the burden of proof in attacking her signature pursuant to 406. Her statute of frauds claim will probably fail, because the purchase order would be considered signed under 401 of the Utah Act and written under 403.
>
> The supplier can probably recover from Susan for breach of their sales contract. If Susan succeeds in challenging the certificate, the supplier could probably recover damages from Cedric for his error, but it does not appear from the foregoing facts that Cedric erred.

The repository does not appear to be liable from the foregoing facts.

---

## Subscriber Loses Private Key, Revokes Certificate

Cedric, a licensed certification authority, duly issued a certificate to Susan, who accepted it. Cedric thereupon published the certificate in a recognized repository.

Susan, a grocer, authorized Agnes to use the private key corresponding to the public key listed in the certificate to purchase inventory as needed. Agnes failed to comply with the terms of her employment, so Susan placed her on probation.

Unable to resolve the problems with Agnes and continue intensive supervision of her performance, Susan removed purchasing from among Agnes's duties. Susan also revoked the certificate for Agnes's key pair, and Cedric published notice of the revocation in the repository that the certificate indicated as the repository in which notice of revocation would be published.

Resenting her reassignment, Agnes issues several unnecessary orders and quit her job.

Northwest Supply, Inc. received an order for 500 crates of lettuce, but did not bother to verify the digital signature on the order. Northwest shipped the 500 crates of lettuce. Since Susan already had plenty of lettuce and could find no evidence of an order of 500 crates to Northwest, Susan rejected the shipment. Northwest was able to sell only 50 crates of the lettuce at a price that did not even cover the expenses of sale. The rest of the lettuce rotted. Northwest sued Susan for the price of the lettuce.

Southwest Supply, Inc. also received an unauthorized order from Agnes. Southwest tried to verify the digital signature on the order, but found it could not be verified by any known certificate.

Southwest requested Susan to confirm the order, but Susan could find no record of it and informed Southwest that the order was apparently spurious. Southwest ignored the order.

**Under the Utah Act:**

> Susan, the subscriber, is probably not liable for breach of its sales contract with Northwest, since Northwest can produce no properly authenticated order.
>
> Revocation of the certificate gave notice to Northwest that the digital signature capability allocated to Agnes was no longer reliable. Thus, at the time of the digital signature, no reliable link between Susan and the critical key pair exists, so Northwest has clear notice that the key pair can no longer be identified as Susan's.
>
> Northwest, which relied to its detriment on an unverifiable digital signature, will very likely bear the loss due to the order it filled despite the unverifiability of the order's digital signature. The only evidence identifying the digital signature with Susan is evidence that Susan, through revocation, had indicated was unreliable. Having notice that the digital signature was unreliable, Northwest will bear the loss of relying on it, despite clear notice through revocation of the certificate.
>
> Southwest realized that the digital signature was unreliable and therefore did not rely on it. Southwest suffered no loss.
>
> Susan, the subscriber, is very likely not liable for the lettuce shipped by Northwest, since she revoked the certificate and thereby gave notice that digital signatures verifiable by the corresponding public key were unreliable.
>
> The repository appears to have performed its duty to effect publication as required. It is

accordingly not liable.

---

## Subscriber Loses Private Key, Does not Suspend or Revoke Certificate

Cedric, a licensed certification authority, duly issues a certificate to Susan, who accepts it. Cedric thereupon publishes the certificate in a recognized repository. Susan's private key, which corresponds to the public key named in the certificate, is kept on a floppy disk, which she places in her purse.

Irving steals Susan's purse, including the private key. Susan never suspends or revokes the certificate. Before the certificate expires, Irving discloses the private key to Fred, who cashes a check drawn on Susan's account payable to a numbered, anonymous account in a state having rigorous bank secrecy laws. Fred disappears immediately after cashing the check and cannot be found.

**Under the Utah Act:**

> Cedric, the certification authority, is not liable for any loss in this scenario, since Cedric issued and published the certificate in compliance with the law ("duly"). Even if he had erred in issuing the certificate, demonstrating proximate causation of the forgery loss from an error in issuance may be difficult.
>
> Susan, the subscriber, is liable if she failed to exercise reasonable care in safeguarding the private key. Thus, if the trier of fact finds her negligent in keeping the private key safe, Susan will be liable for the loss caused by the forgery.
>
> Since Susan failed to revoke the certificate, she runs a serious risk of liability for negligence in safeguarding the private key, until the certificate expires of its own accord.
>
> The repository is not liable, since it published a certificate at the request of a duly licensed certification authority and never received a notice that the certificate was revoked or suspended.
>
> Fred, the forger, is, of course, liable, but, since he "disappeared", he cannot be served with process, so a court cannot obtain jurisdiction over him to enable anyone else to recover from him.
>
> Irving, the interloper and thief, is also liable under the common law tort of conversion. However, finding Irving and collecting a judgment from him could prove problematic.

---

## Certification Authority Retains and Misuses Subscriber's Private Key

After a rather large claim was paid pursuant to a title insurance policy for an encumbrance appearing on the county recorder's records shortly after a closing, the XYZ Title Company decides to file all deeds and mortgages electronically henceforth. Cedric, an XYZ employee, obtains a license as a certification authority and buys the Certificates R Us software package containing "everything you need" to be a certification authority.

At XYZ's next closing, Susan, the grantor, appears, pen in hand, to sign her deed, but Cedric persuades Susan to sign digitally using a certificate he will issue at no additional charge other than the "usual"

closing costs.

Cedric uses the Certificates R Us software and his portable computer to generate a key pair for Susan, and issues Susan a short-term certificate, which she accepts. Cedric publishes the certificate in a recognized repository. Susan digitally signs the deed and Cedric records it. Susan also signs a request authorizing an electronic funds transfer for the benefit of XYZ Title Company to cover the closing costs.

After the closing but before the certificate expires, Cedric realizes that Susan's privatekey is still on his portable computer. He helps himself to another funds transfer from Susan's account, which he requests, authorizes, and digitally signs using her private key.

He makes the transfer for the benefit to ABC Home Electronics for a new stereo.

Susan, in reviewing a the status of her account, cannot account for some funds and discovers a funds transfer to ABC on her bank statement. After a conversation with ABC, she sues Cedric and XYZ Title Company.

**Under the Utah Act:**

> Cedric, the certification authority, is liable as a constructive trustee of the private key for Susan's benefit. Since he did not act in the interest of Susan, the beneficiary of the constructive trust, in buying himself the stereo, he could be surcharged (in other words, Susan could collect money damages from him for breach of his fiduciary duty).
>
> Alternatively, rather than surcharge the trustee and collect a money judgment, Susan could also trace the proceeds of her private key and take the stereo, since Cedric has the legal but not the equitable title to the stereo. Since Susan's loss arises, not from her reliance on the certificate but rather from Cedric's breach of a fiduciary duty, the liability limits applicable to reliance on a certificate do not apply.
>
> XYZ Title Company, the certification authority's employer, may be vicariously liable under respondeat superior principles for Cedric's breach of trust and conversion of the trust property.
>
> Certificates R Us, producer of the software used by Cedric and XYZ, could perhaps be liable under a products liability or warranty claim, if its key management functionality wrongfully failed to provide warnings and processes to the certification authority for eradicating a subscriber's private key.

---

## Certification Authority Misidentifies the Subscriber

Susan Smith, a subscriber, applies to Cedric, a licensed certification authority, for a certificate. Oddly enough, Susan prefers to pronounce her name "Suzanne" in spoken English, and she does so with Cedric. Cedric asks her several questions orally, but asks for nothing in writing and does not ask to see a driver's license or other evidence of identity.

Since Susan does not have a distinguished name, Cedric gives her one. Cedric issues a certificate bearing the name "Suzanne Smith" and publishes it in a recognized repository.

There is someone else in the community who actually bears the name "Suzanne Smith". Susan signs a contract and purchase order for a quantity of widgets from UV Wholesale, Inc. (UVW). UVW has accounts for both Susan Smith and Suzanne Smith.

After checking the certificate, they conclude that the order is from Suzanne, and ship and invoice accordingly. Suzanne is surprised to find widgets at her loading dock, so she rejects the shipment and

refuses to pay the invoice. Meanwhile, when the widgets do not arrive on time, Susan covers by buying widgets from RST.

After UVW fails to receive payment for the widgets it shipped, the signature problems are finally sorted out and the defect in the certificate is discovered. UVW then sues both Susan (who pronounces her name "Suzanne") for fraud and negligent misrepresentation, and Cedric for certification authority malpractice (misrepresentation in the certificate).

Susan cross-claims against Cedric for issuing a faulty certificate, and Cedric cross-claims against Susan for misrepresentation.

**Under the Utah Act:**

> Cedric, the certification authority, is probably liable to UVW for failure to confirm Susan's identity in accordance with Cedric's representations pursuant to 303. Proper confirmation would have pointed up the error in spelling Susan's name.
>
> Susan, the subscriber, may be required to indemnify Cedric pursuant to 304(4), and may also be liable to UVW under the common law, if a tribunal concludes that her pronunciation of her name amounts to fraud or negligent misrepresentation.
>
> The repository is not liable, since it merely executed a request for publication. Section 502(2) provides that a recognized repository is not liable for effecting publication of information provided by a certification authority.

---

## Failure to Check for Revocation of Certificate

Cedric, a licensed certification authority, has issued and published a certificate at the request of Susan, a subscriber.

Susan then loses her private key and revokes the certificate.

Cedric effects the revocation and publishes notice of it.

Later, Irving finds Susan's private key, and, rather than return it to her, he uses it to write himself a check drawn on Susan's account, on his way into oblivion. The bank accepts the check, verifies the signature in its local cache of certificates without discovering the revocation, and pays cash to Irving.

Susan eventually protests the charge against her account for an item not properly payable under Uniform Commercial Code 4-401 (1992).

Under the Utah Act:

> Cedric, the certification authority, is not liable, because no failure to comply with applicable practice requirements is indicated in the facts as given.
>
> Susan, the subscriber, is not liable for losing the private key, because she revoked the certificate before Irving signed the check, assuming that the time of signature can be established.
>
> Revoking the certificate released Susan from her duty to keep the private key secure, see Utah Act 307(6).
>
> Irving, the interloper, is liable for forging the check, if he can be found and has assets from which a judgment can be collected. More precisely, under Uniform Commercial Code 3-403

(1992), the digital signature, while ineffective as Susan's signature, is nevertheless effective as Irving's signature.

The drawee-payor bank will probably bear the loss, because it relied on erroneous information that the certificate was still outstanding. It cannot verify the signature by reference to a certificate valid at the time of signature, therefore, part 4 of the Utah Act is generally inapplicable, even though the bank's out-of-date cache contained an ostensibly valid certificate. The bank could attempt to prove a signature at common law, but the attempt would probably not succeed, because Susan could very likely demonstrate that the signature on the check was not her mark made with the requisite intent, since she had previously lost the private key, as indicated by her revocation of the certificate identifying the private key with her, and by other evidence.

---

## Lack of Any Certificate at All, Unknown Party

Adam digitally signs electronic mail, which he sends to Betty, promising to paint her living room if she will weed his garden. Betty accepts by digitally signing return electronic mail.

After Betty weeds a garden that she thinks is Adam's, she demands that the owner of the garden paint her living room. The owner refuses, claiming never to have heard of Betty, her living room, digital signatures, or electronic mail. Betty eventually tracks down the person who holds the user account to which she directed her electronic mail, but she searches in vain for a certificate anywhere that identifies the account holder as Adam.

In correspondence with the reported account holder, an unidentified person denies any knowledge of the contract Betty insists she made.

**Under the Utah Act:**

Betty, lacking a certificate linking the public key to anyone, cannot authenticate the digitally signed offer as the act of any identifiable person, even though she accepted the offer by performance. Unless Betty can somehow show that the account holder in fact holds the public key corresponding to the private key used to sign the mail, independent of any certificate, Betty cannot identify the other party to her contract. Absent such identification, the contract would be invalid for lack of a second party and of demonstrable mutual assent.

---

## Lack of Any Certificate at All, Known Party

Susan, a subscriber, and RST Wholesale did business for several years, until some time after Susan's certificate expired. Susan, ignoring invitations from her certification authority to renew the certificate, simply kept sending purchase orders and payments to RST with digital signatures verifiable only by Susan's now expired certificate.

RST did not always check and attempt to verify digital signatures on every order, so RST did not immediately notice when Susan's certificate expired. RST's bank noticed, however, and advised RST that Susan's payment of the order bore an unverifiable signature.

RST's bank refused to credit RST's account for Susan's payment for fear that the payment was not authentic or secure.

RST advised Susan that her certificate needed to be updated, and Susan promised to renew it "when I get a chance". Meanwhile, she sent another electronic order to RST, which this time, aware of its bank's

concerns, attempted to verify the signature and found it verifiable only by the public key listed in an expired certificate.

RST advised Susan that, pursuant to their sales agreement, RST needed digital signatures verifiable by a valid certificate. Susan responded angrily that she would take her business elsewhere. After several months of inability to collect for the previous order, RST sued Susan to collect the previous order bearing the digital signature verifiable only by the expired and hence invalid certificate.

Under the Utah Act:

> RST, which relied on Susan's order, may be able to collect Susan's payment, but with difficulty, if at all. If Susan paid by a negotiable instrument, RST will need to prove that she signed the instrument , see Uniform Commercial Code 3-401 (1992), without the aid of Utah Act 401 to satisfy the signature requirement, or the presumptions of Draft Amended Utah Act 406.
>
> If Susan paid by electronic funds transfer, RST will need to establish an authorized payment order pursuant to 4A-202 of the Uniform Commercial Code, which includes a requirement of a "commercially reasonable method of providing security against unauthorized payment orders".
>
> It is perhaps questionable whether reliance on an expired certificate is commercially reasonable. On the underlying sale transaction, RST may face a defense from Susan if the order was a contract for the sale of goods for a price of over $500, see Uniform Commercial Code 2-201 (1992), and 401 and 403 of the Draft Amended Utah Act will not apply in satisfaction of the signature and writing requirements.
>
> In short, the lack of a digital signature verifiable by a valid certificate leaves RST to rely on law outside the Utah Act, and RST will face much greater difficulty in establishing its rights.
>
> Susan, the subscriber, will be liable to RST as noted above, if RST can marshal evidence sufficient to persuade the tribunal that Susan authenticated the order or payment. However, RST's task is much more difficult, and Susan's defenses are much stronger, than if Susan's digital signature had been verifiable by a valid certificate.

---

## Delay in Publication

Cedric, a certification authority, revoked a certificate at the request of Susan, its subscriber, and notified Reginald & Reed Repository, Inc. (RRR), where the certificate had been published. RRR automatically queued the notice of revocation for input into the program which updates its certificate revocation list, but before the notice was processed, an errant, malevolent, or mischievous operator in RRR's employ deleted the queue and its contents, including Cedric's notice of revoking Susan's certificate.

Several days later, Irving forged a check to himself using Susan's private key, which corresponds to the public key in the certificate.

The drawee bank verified Susan's digital signature on the check by reference to the ostensibly still valid certificate, and accordingly paid the check. Later, a system administrator at RRR discovers that Cedric's original notice of revoking Susan's certificate had not been processed and completed processing of the revocation, backdating the time-stamp on publication of the notice to the date of the original request for publication.

Susan's bank debited her account for the check forged by Irving using Susan's private key. Susan protested that the item was not properly payable, because she had revoked the certificate so the check

lacked her signature, as evidenced by a return receipt from Cedric's records requesting publication of the notice of revocation.

The bank's records, however, show that the certificate was still outstanding in their routine download of certificates for operational purposes, both shortly before and after cashing the check.

Morton Monitoring and Archiving Service, which regularly archived certificates in compressed files time-stamped by Tim Trustworthy, is called upon to resolve the factual discrepancy.

Morton's files demonstrate that the certificate was outstanding for several days after Irving cashed the forged check, thereby bringing to light the failure of RRR, the repository, to effectuate the publication in a timely manner.

Under the Utah Act:

> Irving, the forger, if he can be found and can be proven to have forged the digital signature with Susan's private key, is liable because the Uniform Commercial Code 3-403 (1992) treats a forged signature as an effective signature by the forger. However, the prospect of locating Irving, let alone recovering damages from him, is ordinarily dim.
>
> As between the bank and RRR, the repository, the trier of fact would probably resolve the factual question whether the repository effectuated a timely publication based on the only independent witness, Morton, which corroborates the bank's account of the facts.
>
> Section 502 of the Draft Amended Utah Act provides that a repository is liable for failing to effect publication on time.
>
> Susan, the subscriber, is not liable because she revoked the certificate. Under 307(6) of the Utah Act, the revocation is effective in relation to Susan, regardless of publication, "one business day after the subscriber requests revocation in writing, supplies to the issuing certification authority information reasonably sufficient to confirm the request". Irving forged the check "several days" after the operator deleted the notice of revocation from the processing queue. Assuming that Susan can prove that she requested the revocation in writing and supplied information reasonably sufficient to confirm it, the revocation has taken effect with respect to her.
>
> Cedric, the certification authority, is not liable because he published notice of its revocation. Section 307(7) of the Utah Act provides that "Upon notification as required by subsection (5) of this section, a licensed certification authority is discharged of its warranties based on issuance of the revoked certificate and ceases to certify as provided in subsections 303(2) and 303(3) in relation to the revoked certificate."

---

## Unlicensed Certification Authority

Cedric, an unlicensed certification authority, issues a certificate to Susan. Susan uses the private key corresponding to the public key listed in the certificate to sign a short-term land sale contract and eventually a deed.

The recording authority refuses to accept the deed because the signature cannot be verified by reference to a valid certificate issued by a licensed certification authority, and is not acknowledged, and hence does not qualify for recordation under Utah Code Ann. 57-3-1 (1995).

Grover, the grantee, thereupon becomes suspicious, and attempts, for the first time unfortunately, to verify the signatures on the contract and the deed. After much searching, Grover finds a certificate for Susan in the Certificates R Us computer bulletin board, which publishes any certificate sent to it, no

questions asked. Grover, wishing he had been more prudent in assuring signature quality, asks Susan to sign the contract and deed again, but Susan seems surprised at the request and refuses.

Since Grover cannot record the deed he has received, he sues Susan to require her to sign a recordable deed pursuant to the contract. Susan denies that she signed either the contract or the deed. Grover must nevertheless persuade the trier of fact that Susan signed the contract.

Since Cedric is unlicensed, introducing the certificate as evidence creates no presumption that the contract is authenticated by Susan. To authenticate the contract in the face of Susan's denial, Grover must call Cedric as a witness.

Cedric did not obtain a license because he was casual about issuing certificates and found the statutory requirements too burdensome. After going through several shoeboxes full of odd-sized pieces of paper, Cedric found a brief note with Susan's name on it, her phone number, a date, the words "long brown hair", and nothing else.

Cedric could not identify Susan from a series of photographs of multiple women having long, brown hair, or from any other records.

However, Cedric is prepared to testify that his usual practice was to compare an applicant's appearance with that on a photo identification card before issuing a certificate.

Whether the contract can be introduced as evidence depends first on whether the court finds in Cedric's questionable testimony enough of a link to Susan to hold that the contract is authenticated.

Second, even if the contract is introduced as evidence, Susan can dispute its authenticity by arguing the weight of the evidence, and can also claim lack of mutual assent by denying the principal indication of her assent, her signature.

Under the Utah Act:

> Grover, the person relying on Susan's digital signature, will have much greater difficulty in establishing his legal rights than if Susan's digital signature had been verifiable by a certificate issued by a licensed certification authority.
>
> Susan, the subscriber, may be liable based on the certificate issued by the unlicensed certification authority, if Grover can sufficiently identify Susan with the material key pair.
>
> Cedric and the Certificates R Us repository are liable only in the apparently unlikely event, on these facts, that they breached a contract to Susan or committed negligent misrepresentation under the common law.
>
> If Cedric had been licensed, evidence of the certificate would satisfy the authentication requirement under section 401 of the Utah Act, and section 405 would deem the digital signature to be acknowledged, and thereby qualify it for recordation and introduction into evidence. Further, section 406 of the Draft Amended Utah Act would Grover to a presumption that the certificate identified the digital signature as Susan's.
>
> Parties relying on digital signatures therefore have an incentive to insist upon a certificate issued by a licensed certification authority. Nevertheless, signatures are not invalidated for lack of licensure, if they can be established by other means, such as an admission of signature by the purported signer or evidence linking an identifiable person to a transaction.

# Anna Eshoo

**U.S. House of Representatives**
**14th Congressional District of California**

November 12, 1997

## Eshoo Introduces Digital Signature Legislation

***Initiative Would Improve Security and Speed Up Online Government Transactions***

Related Sites

Washington, D.C.--Rep. Anna Eshoo (D-CA) and Rep. W.J. (Billy) Tauzin (R-LA) have introduced the Electronic Commerce Enhancement Act, which would instruct federal agencies to make versions of their forms available online and allow people to sign the forms using digital signatures--the online equivalent of written signatures. At present, only some government documents are available online, and most agencies accept only physical signatures to verify the authenticity of forms sent to them. Rep. Eshoo serves on the House Commerce Subcommittee on Telecommunications, Trade, and Consumer Protection, which is chaired by Rep. Tauzin.

"When I established a Virtual District Office on my Web site, I tried to provide constituents with seamless online service for casework they need me to pursue on their behalf with federal agencies," said Rep. Eshoo. "I was disappointed to learn that while constituents can electronically send me information about their problems with the government and download some federal forms, I cannot begin casework for them unless privacy release forms with their physical signatures are on file. This legislation would allow work to begin immediately on constituent casework.

"The Electronic Commerce Enhancement Act would establish Washington more firmly in cyberspace and make government agencies more user-friendly in the process. By encouraging the broader use of digital signatures, it also would encourage the development of electronic commerce and the technology associated with it."

The widespread use of online forms can improve the speed and efficiency of government service since people would no longer need to travel to government offices for forms or request forms to be sent to them through "snail mail." Further, certified digital signatures can offer greater assurance that documents are authentic and unaltered. They also can minimize the chance of forgeries or people being able to escape responsibility for documents by claiming to have had their signatures forged.

If fully implemented, the legislation could save taxpayers millions of dollars in costs associated with copying, mailing, filing, and storing government documents. For example, Hewlett Packard estimates it could save $1 million each year if digital signatures were allowed for the W-4 form alone.

Digital signatures will work much the same as signature cards kept on file by banks to prevent fraud and taken out when needed to verify authenticity. There may be several levels of secure digital signature, depending on the importance of the document. The most secure will be based on encryption technologies, but the whole document need not be encrypted to achieve a secure digital signature. Under the Act, digital signatures accepted by the government will be as reliable as appropriate for the purposes of the electronic forms submitted.

Eshoo's legislation gives the Office of Management and Budget and the National Telecommunications and Information Administration twelve months to establish a way for agencies to put all their forms online and two additional

to establish a way for agencies to put all their forms online and two additional years to finish putting them online. These forms must be able to be completed, signed, and filed with agencies electronically, along with any payments associated with them. Agencies receiving digitally signed forms must promptly issue electronic receipts to people submitting the forms. The Act allows federal agencies to permit their employees to have digital signatures for use with people outside the government. In addition, employers required by law to collect, store, or file paper forms completed by their employees can store such forms electronically if that is how the forms are submitted.

The Act provides for an open framework for private industry to create the software and certificates needed to verify that someone who digitally signs a form is, in fact, who they claim to be. People could use the same digital signatures on state forms and contracts with other citizens. Further, the legislation requires digitally signed government forms to be compatible with standards and technology for digital signatures used in the private sector.

###