Executive Summary:

Perhaps one should consider the State CP Model not a CP for public key certificates, but a policy for e-signing: identifying signers, establishing signatures, and establishing the integrity of signed objects. Surely the State CP is meant to address PKI, but it is influenced by State activities related to citizen customer relationship management; seems to be driven from a top-down perspective; and allows that other e-signing mechanisms than PKI may be used. Overall, it appears to view PKI as a tool option that technologists can use to accomplish the goals of e-gov and e-signing. It is definitely a “discussion Draft.”

The State CP Model can be understood better in the context of supporting State-wide e-signing services (accessing and receiving – “signing for” – contractual services and agreements) with more limited need for interoperation with other entities, (States or Federal government). Cross certification between State CAs (rather than mapping via a bridge mechanism) perhaps does not present an onerous burden if the potential is for few inter-State cross relationships to exist, for instance in cases of regional reciprocity. The State CP model defines a single OID for the several different certificate types (confidentiality/encryption and digital signature. Maybe that works in a preponderantly State-confined environment, where the State can manage the applications and use of the certificates “within the enterprise.”

Like HEPKI’s CP work, the State CP Model is being developed with the help of an extended community represented by NECCC (National Electronic Commerce Coordinating Council). Though NECCC is a decidedly different community than HEPKI and represents State auditors, comptrollers, procurement officers, secretaries of state, governors and chief administrators… in addition to State CIOs. The focus of the State CP model is in providing the infrastructure for State business and services for citizens and improving efficiency of government services. Unlike the higher ed community, the States do not come to CP Model development with the same basis of Internet access as a “given” and Internet2/Abilene capability as the next phase. So States have the whole issue of telecommunications infrastructure development to address. Finally, it would appear that States do not see a need for anonymous certificates, the point of certificate binding is in fact to assure that online transactions are tied explicitly to known and registered entities.

Essentially, the State CP exhibits a top-down approach to e-signing solutions. This is not necessarily a PKI CP policy where certificates per se may have various uses such as access to resources, or to be used anonymously. The state CP does have some strong areas, such as its approach to governing law, auditing mechanisms (and sources),
August 9, 2001

financial responsibility (CA bonding and signed agreements with subscribers), disaster recovery, liability and risk. There may well be opportunity for HEPKI and States if they were to combine their initiatives to some degree, at least in referencing the strengths of their approaches: HEPKI coming from a strong technology and interoperability perspective, States from legal and business perspectives.

Some further observations:

**NECCC Activities a Clue** – Looking at some of the NECCC activities over the past several years, it is clear that the overall intent is to use existing forums to discuss State e-gov issues on a national and regional scale. If the white papers and publications of NECCC provide insight, then important initiatives and focus for states include:

- **Establishing “internet-like” broadband telecommunications** – Not all states are wired. (“Internet-like” apparently does mean that some may use local solutions rather than being fully “on the net.”)

- **Addressing the digital divide** – While most of higher ed provides connectivity for its citizens, states have to contend with availability of access and connectivity to all its citizens. It is not surprising then that the fine details of PKI are not yet high on the agenda. (Though, hmmm, what about university custodial staff? Do we have hidden digital divide?)

- **Portal solutions and web services** – A NECCC white paper promotes the establishment of Statewide strategies for portals in providing access to state government services. There are significant projects underway in a number of States. Indeed, this need for improving citizen access is a driver. Defined services (access to health services, driver’s license services, housing assistance) are the point, portals are a solution, PKI is way down the list as an implementation option.

- **Justice Agencies as model for interagency sharing** – A significant initiative is underway for law enforcement agencies to share information. Since they do this already and it is an existing inter-state activity, the justice departments are developing mechanisms for secure, authenticated exchange of information. It seems that much of this is being accomplished with other mechanisms than PKI per se, such as XML documents and transmission using SSL, IPsec…

- **Privacy** – Privacy is focused on ensuring that States protect citizen’s data and information. Anonymity is not really the issue. Policy tends to mean, “what’s your privacy policy” as in “we don’t share your info…” not policy as in PKI Policy.

**Funding** – All these activities require major funding.

**Interoperability equation** – There are 50 States. There are over 4,000 U.S. institutions of higher education. Interoperability is a very different problem. The State CP model is not trying to solve as heterogeneous an interoperability problem.

**Identity issues** – State CP Model looks to certificates to bind identity of citizens so as to ensure access to specific e-signing services and that’s the problem being addressed.
(rather than “digital signing”). HEPKI is probably looking at certificates as a much more multi-purposed object, including signing, but also access to resources and services or other uses by relying parties.

Comments on Specific CP sections:
[Bolded items are my commentary]

1.1.1 Policy overview – “[commentary - This Certificate Policy may be the total policy framework for a state’s electronic signature and confidentiality/encryption uses, in that case the term “___ PKI” is sufficient. If this Certificate Policy is part of a larger policy framework for a state’s electronic signature and confidentiality/encryption uses or if there are reasons to describe particular communities or processes, then the term “ESI” (Electronic Signature Infrastructure) might be useful to describe a particular framework established for a specific community or class of applications]” That is: the use is “electronic signature.” See NECCC ref. below: Framework for Electronic Signature Reciprocity, pre-Release Version 1.0 March 29, 2001 by NGA/NECCC E-SIGN Interoperability Work Group.

1.1.1 Policy overview – “The use of confidentiality/encryption keys is appropriate for the confidentiality/encryption of designated information.

“The use of Certificate Policy Digital Signatures Medium Assurance is appropriate for all transactions with Government Entities in _______(state) that require authentication and / or a signature.

“The use of Certificate Policy Digital Signatures High Assurance is appropriate for all transactions with Government Entities in ________(state) that require authentication and /or a signature that require a high-level of assurance.

“The use of Certificate Policy Notary Digital Signatures is appropriate for all electronic notarizations in _________(state).” This CP is focused on “signatures” per se, modeling a traditional signing environment of contracts and agreements.

1.3 Community and Applicability – “CAs participating in the ___ PKI are not obligated to issue, recognize or support all of the ___ PKI policies. They are also not limited to issuing certificates only in accordance with these policies.” I read that generously* as: if a State doesn’t want to implement all features, they may do so. Such as not providing for Notary Signatures. And if they choose to issue other certificates via other CPs, they may. (In same way that HEPKI CP might be implemented in a support of a “PKI Lite” model…)

*else one might ask, “How can one rely on a CA that doesn’t follow its CP!??”

1.3.4 Subscribers – “Certificates in the ___ PKI may be issued after request or authorization for issuance from one or more Sponsors. Such certificates may be issued to employees, citizens, organizations or others with whom the Sponsor has a relationship.

A. Vandenberg
“Eligibility for a certificate is at the sole discretion of the Issuing CA. The CA may administer any number of Subscribers.” Apropos discussions in HEPKI-PAG re community, State pretty clearly defines its community. Maybe, like HEPKI, State CP should explicitly advise Relying Parties not to assume too much about holders of certificates – as holders can be designated at State’s discretion.

1.3.6 Policy applicability – “The policy applicability of each certificate is described below…

| Confidentiality/Encryption Certificate Policy | Suitable for certificate uses such as confidentiality/encryption key establishment for information exchanged with Government Entities. |
| Digital Signature Medium and High Assurance Certificate Policies | Suitable for the integrity and authentication of government transactions that are satisfied by the authentication process as defined in Section 3.1.9 and key generation as defined in Section 6.1.8.” |

Narrower definition of certificate applicability (compared to HEPKI CP: “PKCs issued by a CA MAY be used for any application.”) Maybe this narrower definition is, in a way, an approach to PKI LITE?

2.1.1.4 Time between certificate request and issuance – “There is no stipulation for the period between the receipt of an application for a Certificate and the generation of the Entity’s key material. The Issuing CA must ensure that the period for which the Entity has to complete its initialization process is no longer than _____ working days. [commentary – current practices vary, each state will need to evaluate their signing processes and define an appropriate time frame.]” Note that bracketed commentary refers to current practices of “signing processes.” Again, this CP is limited in intent.

2.1.5 Subscriber Obligations – “In all cases, the CA shall require the Subscriber to enter into an enforceable contractual commitment for the benefit of Relying Parties obligating the Subscriber to:…” i.e. State is addressing risk and liability, maybe more explicitly than HEPKI CP. Higher ed enter into contracts with its subscribers with the concept “if you accept this certificate, you’re accepting conditions” – no explicit enforceable contract?

2.2 Certification Authority Liability – [commentary – each state will need to define this section to fit their laws and the framework they intend to establish.] State probably has easier time of it than higher ed, as far as being in jurisdiction of single state entity. This enables them to be brief… legal contract law exists.

2.3 Financial Responsibility – “An Issuing CA and RA’s shall provide the following financial assurances:

• An Issuing CA shall obtain and maintain a bond from a surety, in a form and amount as required by the PMA.
• An RA shall maintain adequate financial assurance in the form of a bond, guaranty or irrevocable letter of credit, in the form and amount deemed appropriate by the issuing CA
• An Issuing CA shall maintain insurance coverage, naming the State of ____ as an additional insured, which will cover the Issuing CA, the State of _____, and their employees, officers, agents, subcontractors, designees, etc., including coverage for professional liability errors and omissions and crime coverage, in amounts as deemed appropriate by the PMA.” Better addressing of financial responsibility?

2.4.1 Governing Law – See comment in 2.2 above.

2.7.4 Topics covered by audit – State makes specific reference to “AICPA/CICA” and “FIPS 140-1” standards. Good specifics.

2.8 Confidentiality Policy – “This does not apply, however, to information appearing on certificates.” State has different view of need for anonymity, after all, the whole point is to identify entity explicitly.

3.1.1 Types of names – “The DN must be in the form of a X.501 printable String and must not be blank.” Shouldn’t be surprising since States are modeling “current signing processes.” (Though “printable” and “easily readable by a human being” are perhaps sufficiently different to require clarification of intent. After all hexadecimal is printable…)

3.1.2 Uniqueness of names – “The subject name listed in a Certificate shall be unambiguous and unique for all certificates issued by the CA. and conform to X.500 standards for name uniqueness. If necessary, additional numbers or letters may be appended to the real name to ensure the name’s uniqueness within the domain of certificates issued by the CA.” A bit more explicit (suggesting addition of uniquelyfying numbers or letters), but actually different than HEPKI CP. Yet, there is some inconsistency in referring to x.500 vs. x.501 (see 3.1.1).

4.1 Certificate Application – Note that State requires “In the case of employees [of the CA, I presume?], an acknowledgement, or in the case of other Subscribers, a signed agreement, of the applicable terms and conditions governing their use of the certificate.” Stronger than HEPKI CP? But again in the context of binding an identity for more traditional signing processes.

4.4.4 Revocation request grace period – “revocation of a certificate must be initiated immediately if the request is received during ____ State local business hours of the CA or within the following [times]” State doesn’t assume 24x7 operation. That seems to imply an acceptance of a level of risk and a different understanding of the purposes of certificates. Such operation may work well in the context of “conducting State business.” HEPKI certificate being applicable to anything – “PKCs issued by a CA MAY be used for any application” – perhaps makes 24x7 an obligation. Maybe HEPKI PKI LITE will allow easing off on the 24x7 requirement?
**4.4.5 Circumstances for suspension** – “If a CA or RA receives notification from a Subscriber or Sponsor that there is cause to revoke a certificate using the criteria stated in 4.4.1, but the authenticity of the request may not be immediately verified by the CA or RA, the CA or RA may initiate a certificate suspension.” **Interesting point – suspension based on unauthenticated request?** Perhaps justified from State perspective of liability associated with not acting promptly to safeguard welfare of citizenry… etc. etc.? Higher Education has different practice and culture – requests, especially for termination of an offered service, must be grounded in auditable facts.

**4.5 & 4.6 Security Audit Procedures & Records Archival** – Somewhat different approach than HEPKI CP, but probably reasonable. Would be helpful to cross check each section (between HEPKI CP and State CP) to look for completeness…
Selected references follow:

News Highlights from civic.com

June 8, 2001

[a.k.a I2MI has other like groups… in the same business?]

E-gov resources on the way

The Center for Technology in Government to search for e-government best practices.

“Practitioners of e-government have the promise of a road map in their quest to implement best practices.

“The Center for Technology in Government has started a yearlong research program that will examine best practices for planning, development and implementation of e-government programs.

“The E-Government: Creating Tools of the Trade program (www.ctg.albany.edu/egov) was established in response to the concerns of government managers who would like to see more definitive e-government resources, said Sharon Dawes, director of the CTG.

“ ‘Electronic government presents more than just new uses for technology,’ Dawes said. ‘This presents a whole new way to think about delivering services to consumers. We’ve found a lot of information out there on the subject, but little if any answers the question of how.’

…

“CTG chose the topics to research by surveying e-government officials at all levels nationwide. The issues raised most frequently included:

- Methods and issues of data sharing.
- An e-government knowledge repository.
- Transitioning from the static to the dynamic Web.
- Managing electronic records in e-government.
- E-government laboratories for local governments.
- Baseline measures on cost and performance of existing services.
- Guidance on building a business case for e-government.
- Case studies in collaboration.

“ ‘People who work in different sectors and levels of e-government face different issues in order to create the best system for their situation,’ Dawes said. ‘We found that people who work in administration or the design aspect, for example, were really interested in creating a business proposal for e-government. People at the local level were really eager
to create e-government labs in which to experiment as to how to create their own systems.’

“To get a broad cross-section of participants, CTG research will be conducted with help from national organizations such as the National Association of Chief Information Officers, the National Association of Counties and the National Science Foundation. The CTG also will tap subscribers to its free news service (www.ctg.albany.edu/ctgwebnews.html) as well as local government officials in Albany, where the center is located.”

The CTG is an applied research center at the University at Albany, State University of New York that works with governments to develop information strategies that foster innovation and enhance the quality of public services.
Creating Citizen-Centric Digital Government (January 2001)
This document is a statement of NASCIO's long-term vision to support the states, as laboratories of democracy, in the evolution of digital government. Focusing on four key elements in digital government implementation (Convenience and Accessibility; Trust; Efficiency and Accountability; and Innovative Investment), Creating Citizen-Centric Digital Government reflects the growing importance of the state CIO in guiding the development of this exciting government service.

My Comments:
Focus on CRM, convenience. Identity is a fact, not anonymous.
High-level paper.
Digital Government = “myGov” portal
Security = privacy statement
Technology = broadband & digital divide]

Telecommunications: Closing the Digital Divide with Broadband Internet Access (October 2000)
Developed in collaboration with the National Association of State Telecommunications Directors, this report highlights the importance of broadband connectivity for economic development, describes the key concepts and technologies involved, summarizes problem areas, and provide examples and alternatives for addressing the associated challenges. Includes case studies from Illinois, North Carolina, Puerto Rico, and South Dakota.

My Comments:
Focus on providing “the internet” or “internet-like” infrastructure.
Higher Education is way past this level, I2/Abilene…

Based on the results of a recent NASCIO survey of state chief information officers, this report examines the status of government web portals in the states. States reported on such topics as CIO authority over portals, access for citizens with technology and disability concerns, and other barriers to implementing digital government.

My Comments:
Portals and funding models focus.
“Barriers” mentioned by State CIOs include:
money, cost, skill, culture, silo mentality, legal issues, privacy,
digital divide, business processes, trust & reliability (from perspective of customer relationships, cf. “do you trust your gov’t to protect your privacy?”)
“Action Items” State CIOs thought NASIRE could do to help them implement digital government. Some responses

- “Best practices; lessons learned; reusable software modules with generic functionality; broker a common functional description of government that can be used in state after state.
- Continue to have state information executives network and discuss use of technology.
- Providing researched-based recommendations on state-of-the-art technologies; cost-effective services; fee structures; and security policy.
- More focused, timely identification of best practices; e-government issue / solution focused forums, potential e-government exchange site, in conjunction with other associations, research organizations, private sector; potential issue briefs or model approaches (e.g. e-legislation) on e-government related concerns; broker or clearinghouse for potential public/private partnerships; and develop public education, information and marketing approaches and materials suitable for use by states.
- Work with the federal government to ensure that funding to the states does not dictate a digital government direction that is inconsistent with that of the state CIO. 2) Create a national repository of components developed by other states that would be available for less fortunate states to take advantage of. 3) Raise Governor's level of awareness regarding the heavy lifting that comes with a digital government effort. 4) Feasibility of a national PKI?”

Additional Comment:

Significant that only one mention of PKI in two pages of “Action Items.”

NASCIO Justice Report - Toward National Sharing of Governmental Information (February 2000)

“In 1998, NASIRE, which represents the Chief Information Officers of the States, and the U.S. Department of Justice’s (DOJ) Office of Justice Programs (OJP) began a cooperative, grant-funded effort to facilitate governmental information sharing via a national information architecture. This project is part of OJ’s larger, ongoing Integration Initiative. It was supported by a one-year grant from the Bureau of Justice Assistance (BJA) to NASIRE. Additional information on this project can be found at NASIRE’s web site.”

My Comments:

- Focus on Justice agencies since they are highly interoperating already (in respect to needing to share information.
- Technology solutions “may require” digital signature, but document transmission and exchange more the initial focus.
- PKI not in the glossary.
- Technical standards related to document sharing: TCP/IP, http, XML, XAL, LDAP (directories, passwords, permissions), MIME email attachments,
- IPsec secure transmission.)
August 9, 2001

NECCC – National Electronic Commerce Coordinating Council
http://ec3.org/

An Alliance of
NASACT - National Association of State Auditors, Comptrollers and Treasurers
NASCIO - National Association of State Chief Information Officers
NASPO - National Association of State Procurement Officials
NASS - National Association of Secretaries of State

In Conjunction with
NGA - National Governors Association
NASCA - National Association of State Chief Administrators
ITAA - Information Technology Association of America
NACHA - National Automated Clearing House Association

NECCC selected publications –

Critical Business Issues In the Transformation to Electronic Government –12/2000

“Security
As citizens and businesses submit more information to governments over the Internet, the risk of it being stolen or misused increases. A serious concern is the theft of a citizen’s identity, which can result in financial loss to the citizen. Governments should also understand and lessen the risk of inappropriate disclosure of proprietary business information that they collect from companies. User IDs, passwords, credit card numbers, bank account numbers, and other such data are transmitted over the Internet and stored electronically in e-government applications. Should theft occur, the government entity holding the information could be subject to litigation as well as embarrassment.

Therefore, an effective security system — one designed to protect data where it is stored and during transmission from citizen or business to government — is essential to e-government. It protects the citizens, businesses and the government by:

• Safeguarding assets and sensitive information from loss, misuse, inaccuracies, or alteration.
• Preventing interruptions in service delivery.
• Validating the identities of the parties involved in any transaction or data exchange.

These objectives are largely accomplished through the use of security technology, such as digital signatures, encryption, and firewalls. However, due to rapid changes in technology, these security measures must be reviewed, monitored, and tested regularly. In addition, citizens must be educated about the necessity of security measures, such as private passwords, for their own protection.”

My Comments:
Technology is the tool to accomplish objectives.
Technology as magic bullet – “through the use of security technology, such as digital signatures, encryption, and firewalls”
August 9, 2001

“Technology

As computer systems become more and more interconnected, controlled planning, design, development, and implementation are key factors in creating systems that work with other systems. Standards to monitor development and to ensure compatible communications are essential. The hardware and software that build and connect these systems must accommodate rapid growth and provide for continued interoperability.

Systems must be designed to provide a user-friendly, single point of entry that an average citizen can access. Service levels must be adequate to attract users and demonstrate benefits of use. Regardless of the technology used, sufficient testing of system interfaces is crucial to effective operability. System design must also address policies for data retention so that any discrepancies or customer complaints can be resolved.

Given the vast amount of technology available, governments should be mindful of standard platforms and tools that have been proven reliable. Technical requirements for creating effective networks, Internet and Intranet connectivity, must be carefully planned.

Technology will continue to advance rapidly and governments must face the challenges of e-government to thrive in the 21st century. With this in mind, systems should be developed with the flexibility to accommodate changes in technology and provide a continued ability to communicate in the modern world.”

My Comments:
Very high-level view of technology.
No details (let technologists figure it out?)

Legal Readiness

An effective legal framework ensures that governments have the opportunity to keep pace with the new era of global communication and efficiently provide citizens with valuable services. This framework should identify and address legal obstacles to e-government. Legal obstacles may include the differences that exist between traditional data collection requirements (that is, sharing of information collected by and provided to various government agencies) and the ease of electronically collecting and sharing data.

Legislative revisions may be required, as current laws, rules, and regulations may not recognize the legality of electronic documents and processes. For example, legislation should ensure that electronic authorizations, contracts and signatures have the same legal effect as those done on paper. (However, due to the nature of technology, giving them the same legal effect may change or even eliminate the traditional ways these items are completed, such as the notarizing of a document.) Additionally, governments may consider the required quorum at meetings to be met through the electronic participation of officials rather than by the officials’ physical presence.

Ideally, a legal framework that allows for the implementation of e-government processes and services will:

- Preserve basic public policy goals, such as privacy and security, retention, and public access to information.
August 9, 2001

- Provide the statutory basis of, authority for, and regulations related to the government processes and services that may be supplied electronically.
- Assign responsibility for and ownership rights to the data provided and accumulated electronically.
- Address the sharing of data collected by one government agency with other government agencies that require the same information.
- Clearly define jurisdictional responsibilities related to intergovernmental transactions and business to government transactions.
- Provide a mechanism by which legal requirements are recognized and enforced.
- Provide a basis for the establishment of fees related to electronic processes and services.
- Identify the records that should be maintained, the period of retention, and the required storage media.
- Not be technology-specific or favor one form of service delivery (traditional or electronic).
- Minimize costs and the potential for litigation.

To adapt to the electronic environment, governments need to establish a legal framework that treats electronic processes and traditional processes equally.”

My Comments:
- Legal issues focused on how traditional processes move to online.
- Privacy and security policy are about citizen data protection and protection of an online environment (not PKI technology per se)

E-Government Strategic Planning – A White Paper
Released December 13, 2000
NECCC Annual Conference
Las Vegas, Nevada

“DUAL ROLE OF GOVERNMENT
Our economy is transforming from an industrial base to a knowledge and information base. In this transition, government must protect the economic well-being of its citizens as well as transform its functions and services. Government is becoming both service provider and policy-maker, watching out for the interests of all citizens and promoting social and economic values espoused by its citizens. As policy-maker, government should consider planning for a digital society as a whole; electronic government is only a part of this role. To fully understand the importance of an e-government strategic plan, it is first necessary to understand the broader requirements of the digital society.
- Economic development – The attraction, retention, incubation and support of new knowledge-based industries, while still supporting the existing economic base, through government policy, legislation and incentives.
• **Telecommunications policy** – The government articulates the need for, and encourages the access to high-speed telecommunications throughout its jurisdiction.

• **Education** – Ensuring all citizens are ready and capable of capitalizing on the new technologies.

• **Government Services** – The government must be a role model in the use of e-commerce and a catalyst in bringing the digital society to its citizens.

The remainder of this paper will address the government services area. [Emphasis added]

…

**LEGAL**

In most jurisdictions laws and regulations need to be adapted to support e-government and e-commerce in general, and without executive leadership and support this can be a difficult task. Any government’s elected officials must understand the strategic nature of e-transformation, and be willing to support enabling legislation that will remove statutory and regulatory barriers that undermine the rapid adoption of e-government. For example, state legislatures should permit the use of digital signatures in various forms in lieu of handwritten and recorded signatures. …

“The NECCC has established several E-SIGN working groups to address the legal, security, policy and interoperability issues related to E-SIGN legislation and other initiatives…”

**TECHNOLOGY**

…Information Architecture is typically divided into three domains:

• Application Architecture
• Data Architecture
• Infrastructure Architecture

**Application architecture** might include standard components for pieces of programming code that can be reused. It may also include a common "look and feel" for all of enterprise’s web pages.

In **data architecture**, format standards can be instrumental in moving inter-governmental data exchange forward. An emerging and very probable e-government-oriented format standard for data exchange is eXtensible Markup Language (XML), an internationally accepted, Internet-oriented data formatting language for self-defined data structures. *(For more information on XML, see: An Introduction to XML’s Potential Use Within Government; NECCC; December 2000)*
**Infrastructure** refers to the "plumbing” of e-government, namely the telecom protocols and the physical backbone, security practices, hardware standards and other standards across the enterprise. Its architecture provides a roadmap to developers of e-government. Because it is applied enterprise-wide, economies of scale will accrue. The standards mean less diverse training, thus more depth on technical skills.

An enterprise architecture that is designed to support rapid growth is called “scalable” and is designed to anticipate a rapid growth curve and frequent changes. By building a scalable infrastructure for the enterprise, complexity can be reduced and points of failure limited, thus improving security.”

**My Comments:**

- Strategic planning document, not tactical (though higher ed might argue, as does The Burton Group for instance, that PKI should be strategic.)
- Overall focus is on providing improved government services.
- Technology viewpoint is high level.
- E-signatures is more about legal aspects of accepting such signatures.
- PKI isn’t mentioned until the “E-Gov Readiness Quiz” where it’s part of Legal quiz questions:

| 1. Our organization can identify (through use of Public Key Infrastructure and/or biometric identification) parties to an electronic transaction such that they cannot repudiate the transaction. |

---

**Framework for Electronic Signature Reciprocity, pre-Release Version 1.0**

March 29, 2001
NGA/NECCC E-SIGN Interoperability Work Group

“It is recognized that there are many signing processes to form electronically signed electronic documents. Different signing processes provide varying levels of certainty and flexibility when identifying a person, attributing a signature to them and assuring signed document integrity. These variations suggest a need for defined levels of trust to establish the extent to which a state government or other entity can assume that an electronically signed electronic record (e-record) received from another state has authenticity, integrity, and reliability. … A state or other entity must understand trust in an objective way for effective electronic signature and e-record decision making and processing. This framework provides objective criteria for determining levels of trust in electronic signatures and e-records.

“…The three general factors used to determine the overall risk of such a dispute and the level of care to be taken in the signing process are: risk of monetary loss, reputation risk, and productivity risk.

“…This policy will identify appropriate implementations for basic, medium, and high trust levels as far as how the:
August 9, 2001

- Signer is identified.
- Signer is linked to the signature.
- Signature is linked to the integrity of the record.”

My Comments:

Yet it is possible to accomplish the above (providing basic, medium, and high level of assurances that identify, sign, and link signature to record) without using any PKI. For instance, for High level signature one can provide: “A shared secret and a cryptographic key or biometric stored on a hardware token where the key or biometric cannot be accessed without the shared secret and the shared secret is only known by the signed and the hardware token” or “A biometric where the signer needs to be present to sign.”

This is essentially a document about forms of electronic signature, which addresses cryptographic keys and public key certificates as among other choices.