

Digital Signature Working Group

September 12, 2000

Meeting Notes

Meeting Chair: Phil Sibert

philip.sibert@hq.doe.gov

(202) 586-2541

PARTICIPANTS

DOE - Headquarters

Germantown

Carol Blackston

Forrestal

Phil Sibert

Mabel Harding

Maria Simms

Connie German

Argonne National Laboratory

Barry Finkel

Doug Engert

Janet M. Anderson

Miriam Bretscher

Laurie Tyzenhaus

Lawrence Livermore National Laboratory

Nick Mitschkowetz

Frank Ploof

OSTI

Lowell Langford

Savannah River Operations Office

Barry Hudson

Rick Endler

WIPP

Meg Milligan

The ground rules were given.

II. ADMINISTRATIVE ISSUES (Phil Sibert)

Phil Sibert started the meeting. Phil said he has been on detail to the National Nuclear Security Administration. He is not sure if he will be able to continue as chair of the Working Group. The group needs to think about finding a new chair. He asked for the group to send him any nominees.

Phil said the DOE CIO, John Gilligan will be leaving DOE at the end of this week. The acting CIO is Nancy Tomford. There is some reorganization going on in the CIO organization. Phil met with Mr. Gilligan about the Digital Signature Considerations document. Mr. Gilligan recommended that Phil give copies to Tom Rowlett, Director, Policy Organization, and John Pryszyka, who is the Acting Deputy Associate CIO for Cyber Security. Then let them decide how to publish the document, which is final. Once the web page is working, a PDF version of it will be posted.

III. CRITIQUE OF THE NEW ELECTRONIC SIGNATURE LAW (Barry Hudson)

Barry Hudson said the Millennium Digital Commerce Act (S.761) was signed on June 6, 2000, by President Clinton. The purpose of the Act is to regulate interstate commerce by electronic means, and encourage continued expansion of electronic commerce in the operations of free market forces..

Barry said his perception of the bottom line is if the Federal government has decided that market-driven, technology neutral non-regulatory approaches to electronic signature vs. digital signature are good enough for interstate commerce and work between agreeable parties, then why isn't it good enough for Federal agencies.

The act promotes use of electronic signatures and records, provides a consistent legal foundation so interstate commerce can happen, is good for the economy, and lets it be driven by market forces rather than be regulated by the Federal government.

The act will promote confidence for use of this technology for commerce and also for online government. There is only one mention of government use of electronic commerce in the Act. Then there is discussion about developing a consistent National legal infrastructure.

In the definition section of the Act, a signature is a symbol, sound, or process used to authenticate a transaction; an electronic signature would be a signature in an electronic (digitized) form attached or logically associated to the transaction. That is all that defines any kind of rigor for conducting electronic commerce electronic signature.

Commercial Code. Whatever the parties involved in the transaction agree to is good enough for an electronic signature. Parties should be permitted to use whatever they want until contested in court. Then they would have the opportunity to prove in court their approaches are valid. Barry said this was a weakness in the Act. Unless electronic signatures method align with industry-recognized mechanisms, it would be hard to prove the validity of that in court.

In escape clauses, it provides for the Security and Exchange Commission to prescribe regulations for standard formats for storage of electronic records and signatures. Notwithstanding laws that specify the required technology, the parties may decide on method. Barry said that he interpreted it to mean if a law was passed that requires a particular technology, then all bets are off. Phil said he agreed with that. Barry said it sounds like the door is open until someone decides on the required technology, which is not likely to happen for a while.

It outlines the actions of the various Federal agencies have to undertake in order to make this law is implemented, managed, and proven to be sound. The Secretary of Commerce is chartered to evaluate commercial packages for electronic records against U.S. Postal Services operations. Identify and adopt the appropriate products and services (standardization of commercial best practices and products). Sounds like the reverse if we don't let the market drive the standards, then they will adopt the standards. The Secretary of Commerce is also charged with identifying impediments to commerce and promote the acceptance and use.

Action Item - Need to determine whether DOE has prepared a response to OMB (what kind of responses OMB is receiving). Agencies have to report to OMB within 6 months of enactment of this Act any regulations or laws within an agency that are barriers to the enforcement of the Act. The implication is that FIPS and digital signature are only recognized electronic commerce within DOE that could or could not be reported as a barrier to the Act. The Act allows use of electronic signatures rather than digital signatures. Within 1 year after reporting to OMB, have to report to Congress actions for removing the barriers. Phil said he was not sure that digital signature or PKI were regulations that could be considered a barrier to use of other kinds of technology. Barry Hudson said that the sites were working under the assumption that any type of electronic signature implemented has to be FIPS compliant. The gray area is the distinction between electronic and digital signatures. Phil said he thought that a digital signature was a type of electronic signature, which is a generic term for all kinds of identification. Carol Blackston said no (FIPS) standards were specified in the law. It just mentioned adoption of products and services. There is no clear guidance available with standards specific to digital signature or electronic signature, but it is needed. Nick asked if the CIO information architecture would mandate what is going to be used, would this be a legal problem.

Barry said that H.R. 1572, which would have mandated that all Federal agencies implement a PKI, was introduced the same time as the Millennium Digital Commerce Act and has not gone anywhere. Given a choice of electronic commerce without any specific technology being dictated

market is doing or implementing something that is strong, reliable, and can validate like PKI. If DOE goes the electronic rather than digital route, then need to determine what barriers exist in current policies and regulations, document them, and send them to OMB.

Phil said he was not aware of any court cases related to the use of electronic signatures. Phil said one of the things mentioned about the law's purpose is the development of consistent National legal infrastructure. He said he did not see how this could happen. Nick Mitschkowetz said if looking at the Act and the X.12 EDI transactions (legacy electronic commerce implementations), they are basically the same. Act is looking for an electronic process (any process that two individuals can agree upon) that will be legal. EDI is basically the same, just more formal. Could use it as a role model and just add signatures. The transaction relies on the underlying process that is being used. The Act is looking for a process rather than a specific technology.

Phil talked about the Secretary of Commerce's responsibilities to adopt appropriate products and services. He said the Commerce Department is not creating any non-security FIPS. Phil said he understood the Act to mean that the Secretary of Commerce would take products and evaluate them, stating that a product does in fact do what the vendor says it does, but would not go beyond that. Carol Blackston said NIST is basically out of general standards generation, but still creating security-related standards. They may endorse products, perform conformance testing or have labs do it. The language is vague. Carol felt the Act pertained more to the private sector than the Federal government. She questioned if there would be another law that would pertain to the Federal government. DOE does not have that many services that directly support the public.

Carol said there is a Federal E-Gov initiative and the DOE contact is Ethan Weiner. He would have the Federal viewpoint on this. Phil asked about Andy Yocke. Carol said he is involved, too. Barry said he wondered who at DOE is preparing a response to OMB. He felt that assurance and repudiation were ignored in the Act. PKI would provide inherent, validatable trust.

Action Item - Phil will talk with Ethan Weiner about making an E-Gov presentation at the next DISIWG meeting. He will also talk with Ethan and Andy Yocke about the E-Gov position. He will also talk with legal about whether anyone has done an analysis of the applicability of the Act to DOE.

Frank Ploof said he agreed with Barry. Frank said it probably was a good law in that it allows multiple technologies to be used. The issue is picking the right technology for the job. It probably would not be appropriate to do PKI digital signatures on every transaction. As DISIWG transitions into the next phase, one of the things it could provide for DOE is an assessment of the different technologies and their appropriate use. GAO said that if digital signatures are used for transactions, they have to be robust. One issue would be what kind of infrastructure and technology will be required, what will it cost, etc. Phil said having multiple technologies on more than one infrastructure is costly. However, DOE tries to avoid having just one vendor for a

Phil said that everyone needs to look at a business case to make a decision whether or not security is an issue that needs to be addressed. The security aspect will drive the technology used. If there must be non-repudiation and authentication, the technology needs to be robust. Financial transactions will have oversight from OMB and GSA.

Nick said the law allows a range of solutions. What is an issue is risk. People need to look at the applications they service and then at the risk to decide. May need to put in place the most robust and secure system possible that will provide enough protection for the maximum risk. Frank said he saw this as an opportunity to quickly move into the e-business world. Barry said that for smaller transactions it is setting a fairly low bar for using PKI. These transactions would need something less than PKI.

Action Item - Frank said an action item for DISIWG would be to look at the law, look at the technologies, see what makes sense for where, and then issue guidance for what to use where. Phil said that was mentioned in the Considerations document, but not in detail. Tried to cover what people would need to consider when looking at using digital signatures, which are a type of electronic signature. An assessment of different technologies would be an enormous task that would take too long. It may not be possible to get meaningful information disseminated before a new technology evolved. Frank said he saw that NIST or GSA were working on that. Maybe DISIWG could tie into their efforts. Phil said the NIST organization is responsible for providing that kind of guidance. Their independent laboratory testing process has provided a number of products that have been evaluated/validated for use in Federal applications.

Action Item - Phil said need to ask Commerce where they are headed in relation to the law. Barry said legitimizing electronic records issue was not included. NARA shall be consulted concerning matters involving authenticity of records, their storage retention, and usability for legal purposes. Nick said a large part of the issue for LLNL is how to apply this technology to actually freeze a record (held as authentic and unaltered). From a records perspective, would apply a very high-end secure implementation of a digital signature process like a robust PKI infrastructure to that particular application. The same technology or infrastructure built for the record would also be applicable to other DOE transactions; e.g., clearances. Need to focus on what would be necessary to implement a high-end process. Meg Milligan said on the question of electronic records, have to ask what type of record, what is the retention period, how robust is the system. What is the definition of robust. Need something that will be malleable, migratable, and transferable and have a quality assurance product included. Nick said that what is important is defining standards. The infrastructure put in place has to be able to generate the kind of documents that can be managed long term. Frank said this is all related to process, policy, and procedure issues; it not a technology issue. An archivist or notary gets records ready for "n" years retrieval and verification. It is time to take care of out-year verification documents.

Barry Finkel said to make sure that everyone is looking at the final version of S.761. In the

Action Item - Phil asked for volunteers for a technology assessment group.

Barry Hudson asked if the technology used internal DOE would be different from that used with external DOE. Phil said this would be driven by the business case and risk. Could use different technology for interfacing with the public depending upon the risk or security requirements. For interoperability and a PKI, using certificates for digital signatures, a framework has been established to do that. There are no rigid requirements for a particular product. If PKI is considered as a technology, then it is a narrow determination of what will be used. It is driven by the fact that certain things need to be protected and authenticated. PKI and digital signature are one way to do that. Need to determine level necessary and then provide guidance.

The Considerations document will be submitted through the channels in the CIO organization and then will be issued. Nick asked how to get someone from the policy group to attend DISIWG meetings.

Action Item - Phil said he would ask a representative from the policy group to attend the next meeting and give the group some insight on policy or guidance to be issued for use of digital or electronic signatures.

Carol Blackston said there is a security committee of the Federal CIO Council. She wondered if they were discussing PKI and digital signatures in the Federal community. Phil said there are three co-chairs on the Security, Privacy, and Critical Infrastructure Committee. Mr. Gilligan is Security; Mr. Roger Baker (Commerce) is Privacy; and Mr. Fernando Burbano (State) is Critical Infrastructure.

Action Item - Check with the CIO Committee to see the status of PKI and digital signature.

Carol said the Federal CIO Council Interoperability Committee recently approved the charter of an XML Working Group looking at XML applications Federal-wide, especially with regard to records management (standard forms, electronic records management). She said the Working Group is looking for participants. If anyone is interested, just forward her your e-mail address. Her address is carol.blackston@hq.doe.gov.

IV. USING PKI FOR AUTHENTICATION IN A GRID ENVIRONMENT (Doug Engert)

Doug Engert covered the following topics. (A copy of his presentation will be posted in ppt.)

–GRID Environment

A grid environment is where there are many computers across multiple sites; users have accounts

–Security issues for the GRID Environment

Multiple organizations do not always have a memorandum of understanding in place with various organizations, but have issued accounts to individual users. The authentication mechanism cannot support this. Process-to-process communication is where a user starts up a job or process and needs to have other processes contact him so they can communicate. There are firewall and authentication issues involved.

–It's more than Client-Server

Need to have local control of resources so can authenticate using PKI, but authorization is still performed locally.

–Globus GSI

Globus is a DOE research project that is funded by NASA, DARPA, and others. The web site address is www.globus.org. There are a number of components, including toolkits (Kerberos, etc.). The security component is called GRID Security Infrastructure, which supports single-sign-on.

–Globus Security Infrastructure (GSI) Features

Using X.509 public key certificates; can support multiple certificate authorities, including commercial using the SSL protocol. Can create delegation certificates; e.g., short term certificates; has U.S. export exemption since not really using encryption, using public key certifications, but not encrypting data; have GSSAPI implementation to interface with a number of applications.

Can use any vendor's CA; can use Entrust, Netscape CA; can use DOE PKI as an application. Globus is running at DOE labs and sites around the world (installations on five continents); CA in operation since 1998; 25K certificates issued.

–GSI Applications

Can work with various security applications; has modifications to SSH to use a public key for SSH authentication; commercial SSH for Windows (SecureCRT); modifications to FTP/FTPD; expect to use with CORBA and SASL.

–Delegation using Proxy Certificates

The server, after authenticating the client, creates a key pair and certificate request, sends request

–Local site authorization

Client authenticates a local site for access. Server uses grid-map file to map certificate subject name to local userid. It is up to the site to grant access to a user.

–Interface with local site security infrastructures

Can interface with Kerberos, DCE, AFS, Secure-ID, and smart cards (uses same code as Netscape on Win32); generate proxy certificate with Entrust. Work with smart cards from a vendor and get it to work on PC to get to applications. Password goes only to smart card, not over the network.

–Conclusions

GSI is becoming widely accepted; uses well-established security protocols (SSL); can use production CAs (Netscape, Entrust); can interface to current site security; can delegate; can do process-to-process application; allows local site to perform authorization and accounting; and single sign-on.

Frank Ploof asked if DOE was able to issue certifications, what would be done with the 25K they have issued. Doug said each of the Globus processes could be running for trust multiple CAs. Phil said the CA would be interchangeable through the PKI Federal bridge. Frank asked if they had looked at the different assurance levels—how is the system rated in terms of assurance. Doug said the Globus CA would probably be the lowest level; the CA is there to get Globus up and running; more of a research CA.

Frank asked if the vision was to have DOE issue certificates for sites and contractors that could be used by Globus users. Would this negate the need for a Globus CA. Doug said it is up to each site which CAs and users they trust.

Nick asked that once a Globus user is authenticated and logs onto a site and the user is logged onto everything, is there no need-to-know partitioning. Doug said it was up to the local site.

Action Item—Phil asked Doug to work on a presentation for the 2001 Computer Security Conference. Frank said he could probably do the same thing at the PKI workshop in August 2001.

Nick M. said he was interested in the fact that the CIO wanted a strategy for implementing PKI at DOE. Keep talking about an ubiquitous application for use by sites. Would CIO champion since it is a cross-cutting application. Wants real-time access to certain data bases (clearance data base). Could expand data base to include badges and certificates with a need-to-know engine.

Frank Ploof said a group was meeting in October at LLNL to discuss adding smart cards to badges. The group is called Access Systems Quality Panel headed by Darryl Toms.

Action Item—Phil said he would get in touch with Mr. Toms.

Barry Finkel said there is conference on PKI Interoperability in December in Atlanta, GA. The address is www.misti.com.

Phil thanked Barry Finkel for the legislative update.

V. GENERAL DISCUSSION

PKI Workshop Update (Frank Ploof)

Frank said this was the first time the DOE PKI Workshop was separate from a conference. There is a growing emphasis on PKI and making people aware of it. There were 80 attendees at the Workshop, which was intended for people who had an interest in PKI, but not a lot of knowledge.

Day 1

Entrust gave a generic overview of PKI.

Day 2

Focused on the Federal aspect; John Pryszka gave Mr. Gilligan's presentation; Mr. Gilligan is an ardent supporter of PKI. Looking for funds to establish a DOE PKI.

Sharon Shank gave a presentation on DOE PKI strategy and historical information over the last several years. Sharon Shank, with the assistance of the Policy Management Authority (consists of the sites who have PKI CAs), put together the strategy that was presented to Mr. Gilligan.

Rich Guida, the security champion for establishing the Federal PKI bridge CA, gave a presentation. He outlined the history of his efforts. There is a bridge CA. It alleviates the need for multiple PKIs and cross certifications. He has developed a plan for agency participation.

NSA gave a presentation on their initiatives. NIST also gave a presentation. They are critical in the standards arena; they have a pilot to determine what works and what does not. Overall Federal activity is divided into three groups: Business, Legal, and Technical (NIST has been the lead in this arena for the last 5 years). Sites look to NIST for the technical standards and follow on FIPS.

Federal agencies are seeding that effort.

Day 3

There were vendors and PKI was presented in greater detail.

Microsoft, with Windows 2000, has built-in CA capabilities; only have to check a box during install to get the CA. MS is focused on its underlying technology and their new architecture. The current version is not as robust as users would like it to be, so most are going to wait until the next release in the next 6-9 months. MS will be a serious contender in the marketplace. The server cost is basically free; hard to compare other with other CAs.

LUNA gave a presentation on level 3 hardware encryption. If a high assurance CA is needed, need to move the CA activities to a separate piece of hardware.

DBSign gave a presentation. They do digital signatures for relational data base applications.

Entrust had a Q and A session from questions generated from the first day of the Workshop.

There was a lessons-learned session. Talked about collaboration over the years; more details on what a PKI really is; Frank gave a presentation on PKI application level services used for digital signatures, secure mail, etc. Then there was a presentation on training and deployment—how to get the information to the end users, what kind of training is required, is training required, have users sign forms once training is completed or a visual ID issued.

Day 4

More presentations on CAs focused on high assurance, what assurance levels are, what is a high assurance level CA—how is it different from a medium assurance level CA; what is different in DOE. It was suggested that each site have a medium assurance or even a low assurance. If there is a high assurance, there should only be one and that would be at Headquarters. Sites would get their high assurance from Headquarters rather than having their own.

Registration authority pilot was discussed—what is a registration authority, what do they do, what kind of security is necessary, what kind of identification, what are risks involved, is it needed at DOE, need to establish procedures for registration authorities and training requirements.

Discussed an example of secure web services. Honeywell, Albuquerque, has a 100-user system using Entrust direct, which provides for client to site authentication to a secure data base.

Then there was a biometric presentation. Frank said there continues to be new technology, but it

VII. NEXT STEPS – no discussion

Next televideo conference meeting is **Wednesday, October 18, 2000 at 1:30 - 3:30 EDT.**