

## **Digital Signature Working Group - March 21, 2001 Meeting Notes**

### **Meeting Chair: Phil Sibert**

philip.sibert@nnsa.doe.gov

202-586-2541

## **PARTICIPANTS**

### **DOE - Headquarters**

#### **Germantown**

Jay Blewett

Carol Blackston

George Seweryniak

Connie German

#### **Forrestal**

Phil Sibert

Paul Lewis

Mable Harding

### **Argonne National Laboratory**

Barry Finkel

Miriam Bretscher

### **Chicago Ops Office**

Laurie Tyzenhaus

### **Kansas City**

Lauren Wood

### **Lawrence Livermore National Laboratory**

David Ganyon

Larry Medina

Nick Mitschkowetz

### **Nevada Office**

Fred Walden

Carol Perry

### **Oak Ridge Ops Office**

Sharon Adams

**OSTI**

Lowell Langford  
Madelyn Wilson

**SPRO**

Brian Sandoval

**Savannah River**

Roger Campbell  
Gary Monroe

**WIPP**

Gail Ellet

**I. GROUND RULES (CONNIE GERMAN)**

The ground rules were given.

**II. ADMINISTRATIVE ISSUES (PHIL SIBERT)**

Phil talked about people who said they would attend these sessions, but don't. We are burning up some precious resources by reserving conference facilities and not using them.

**Digital Signature Considerations Document**

Phil said the Group talked last month about providing some input on the rewrite of the digital signature Considerations document. Technology keeps moving along and rules and regulations keep changing. We need to keep the document as current as possible. Phil did receive some input concerning the records management section from Fred Walden. Phil asked Fred to go over his comments/changes.

Fred said he brought up at the last meeting that NARA had issued a new guideline, *Records Management Guidance for Agencies Implementing Electronic Signature Technologies*. It is a good document and maybe we should do something about either referencing it in our Considerations document or incorporating parts of it in there. Rather than lifting pieces out of it, Fred put a paragraph in the section entitled National Archives and Records Administration Issues a paragraph referencing the NARA document. The only other changes he made to the document were some minor corrections to the retention schedule.

The Digital Signature Working Group Considerations document latest version is dated September 20<sup>th</sup>. Should be on the web site (<http://CIO.DOE.GOV/UCSP/CONSID.HTM>).

## Legislative Update

Phil asked Paul Lewis to give an update on legislation. Paul said not a whole lot had come up in terms of new bills in this new administration. There are a couple of bills to amend the paperwork reduction act. One of them is HR-541. This amendment is suppose to minimize the burden on federal paperwork demands on small businesses, educational non-profit institutions, federal contractors, state and local governments, and other persons through the sponsorship and use of alternative information technologies. Paul felt that it may be something of interest to the Group.

HR-721 is suppose to ensure the business of the federal government is conducted in the public interest and in a manner that provides for public accountability, efficient delivery of services, and reasonable cost savings, and prevents unwanted government expenses.

Phil asked Gail Ellet from West Valley to look at the Records Management section in the Considerations document. She said she would try to take a look at the document before the April meeting.

## Standards Update

Phil asked Carol Blackston how things were with NIST. Did she have any updates. Carol said that NIST does not seem to be doing a whole lot lately. They are restructuring. She has not noticed anything new. Phil said NIST has just restructured their information technology laboratory and have added a couple of new divisions. One activity they are working on is the outreach activity.

## GENERAL DISCUSSION

Phil said that NIST has a web site dealing with cryptography that covers topics of interest to DISIWG members. The web site address is <http://csrc.nist.gov/encryption/tkdigsigs.html>.

***ACTION ITEM:*** Phil said there was an article in the newspaper not too long ago about a flaw in the secure hash for digital signatures. He will make a note and see if he can find something for the next meeting on that.

Fred Walden asked if there is an electronic web link for the NARA guidance report? Phil said it is on the DISIWG web site. The NARA web site address is [nara.gov/records/policy/gpea.html](http://nara.gov/records/policy/gpea.html). This should be available from the DOE Information Technologies Standards web site.

Lowell Langford asked about the minutes from previous meetings. Phil said they need to be posted.

Phil said he talked to Sharon Shank this week about a transition of the DISIWG to her group. We can continue working the way we are until the transition plan is in place. There are some things going on in Headquarters that would take cryptography, PKI, etc., out of SO and place them in NNSA, but not sure if that is going to happen or not.

## **Site Updates**

Lowell Langford, OSTI, said his replacement on the DISIWG is Madelyn Wilson. She was in attendance at the meeting. They have no significant digital signature work in progress.

Brian Sandoval at SPRO said they are looking into PKI. They are suppose to have a teleconference with Nelson Barry tomorrow to work out some of the details with their technical people.

Phil asked Fred Walden, Nevada, if they were working on anything with digital signatures? Fred said they are trying to implement the form program for what we call phase three of the electronic forms project. Carol Perry has come on-board to push that forward.

Savannah River attendees (Roger Campbell and Gary Monroe) said that Nelson Barry came out in February and set them up with a registration authority and a server. They are trying to produce as many certificates as possible; probably about 100 per month until they get to about 500. Not sure how many people they are going to have with the capacity and the maintenance right now. Just developing the program from the PKI stand point. Phil asked if they had their own certificate authority there. They said they had a registration server off the Headquarters server. Phil - Are cross certified with all the other sites that are connected to Headquarters. Yes.

Phil - Are you doing this for more than just the federal force? Are you doing it for contractors as well? They are supporting the main M&O contractor at this time per Sharon Shank's approval; she approves each certificate. They are funding the whole program. Phil - Did they indicate how long they would continue that funding? They hope it is quite a while, but have established funding for the next fiscal year. Phil - Did Headquarters provide the server or did you? They purchased the server. Phil - are you providing the manpower? Yes. Are you expected to use this as more than just an e-mail application? It would be, as you know, the big driver is the UCNI regulation and the upcoming OUO material primarily for that type of encryption.

Phil asked Gail Ellet, WIPP, if anything was happening at WIPP. She said not that she was aware of.

Lowell Langford, OSTI, said that David Bellis has requested from Headquarters "X" number of certificates.

Phil asked George Seweryniak what was happening in the ESNet area. George said they have a lot of proposals that they are handling right now, mostly SIDAC. One of the SIDAC proposals is of interest. It is a 3-year proposal for PKI deployment across ESNet. Total value is about \$3M. It will be evaluated next month. That's the only thing really happening. ESNet is moving to a new carrier. Phil said that sensitive information is unclassified data that needs to be protected during transfer.

Lowell Langford said he heard that the SF-52, one of the personnel forms, was going to be made available electronically and that there would be some type of electronic signature used in association with that electronic form. Did not have any details just yet. Phil asked where Lowell heard this. He said the Headquarters Human Resource person. SF-52 is one of the forms filled out when an employee is going to retire. Phil asked if there are any other applications that people are aware of using electronic signatures. Mable Harding, MA-3.3, said she attended the meeting to see what is going on. They are not implementing PKI or digital signature yet. Need to get more information before making a decision.

What is the process that people go through to request certificates from DOE Headquarters? Phil said to call Sharon Shank and ask her.

***ACTION ITEM:*** Phil said he would will check with Sharon Shank to see if we can't get that added to the minutes for this meeting so everyone will know what the process is.

### **Electronic Government Update (Ethan Weiner)**

Ethan Weiner said he worked with electronic government. Primary, what they are doing here in the department is looking at the kinds of technologies that we can employ to do business or to serve the public, but also to work with the business community through technology transfers. He is also working with other government agencies. There seems to be different elements in the Department developing transitional capabilities for distinct services to distinct groups. A good example is EM has a digital photo archive which DOE elements and the public can use, with each having distinctly different levels of access. There is development of in-house capabilities in laboratories where employees have central administrative functions to smooth out the administrative processes they perform. Also starting to see where the front end is being designed to simplify access to information as opposed to being a promotional tool. DOE strength lies with information and products created for very distinct communities. Most of these communities are in education or in business, be it with science technology or with other government agencies, but it is still an extension of what we do in the course of our day-to-day business.

We are taking traditional working processes and putting them into the digital world. The processing of paper can become electronic. I think it will happen within the next decade. DOE is not a typical Federal agency in its relationships and interfaces with the public and being

going to be around for sometime. We as employees will start doing business with our traditional administrative side of the house electronically as opposed to dealing with people. Right now a lot of our grants are still being submitted on paper. However, the Office of Science has developed an electronic grant process that has been ongoing for a couple of years, but we are still using a lot of paper. Phil asked if digital signatures were being used in the grants process for authorization purposes. George said he was not involved in that part of it, so could not comment on it, unfortunately. George said Dick Yockman could give an the update on who is handling that now.

Phil asked SR if, when someone retires, a process is in place at Savannah River to get that certificate revoked the day it happens? SR said there is a process, at the time they lose their access badge, at the exit interview. Phil asked him to explain that process. When a person leaves, SR reports the certificate back to Headquarters, Nelson Barry's group thru the RA server. We report that the person has left and to revoke the certificate. Is there a process in place for seeing that the certificate is revoked the minute they walk out the door? Yes, SR has a working relationship with personnel. When someone leaves, they notify us. In the future, we see the access badges and certificates being a dual capability. The new employee gets half of a certificate number and later on we will have the other half and work it with the ID badge.

Lowell Langford, OSTI, said they have just gone through the process of commenting on the request from NARA for snapshots of web sites and such. Do you think that they would want to expand this to our E-Commerce records at some point in time? I think that this committee needs to be aware that this could happen. It will cost a fortune if the draft schedule is ever approved. It is estimated that there are more than 27 million web sites available to the public. Can you imagine the cost of that and doing snapshots annually?

Ethan Weiner said there have been difficult discussions with NARA based on what they think we should do. Most of his counterparts in other agencies think that NARA is not looking at this realistically and the impact it will have on agencies. There is not enough storage space made to keep current copies of all the records that go out electronically.

Fred Walden, NV, said he saw an article in the paper where the United States Postal Service was going to be offering certificate authorities and would be working with government agencies when they first roll this out. Phil said no one at DOE has been looking at using this postal service. It is competition with a GSA program.

Lauren Wood, Kansas City, said he would like to argue that the postal service is not a very good example of a way to deal with this. They do not have time stamps that you can depend on. It is only a date stamp, with a chance of them not having it right. A great many post offices are private-contractor operated; government employees are not running them. A good many of them cannot even read their own postal regulations. Many post offices do not have the ability to do

Phil asked Lauren how he would do it if the United States Postal Service is not the right way to go? Lauren said for the general public, the commercial supplier is the best idea. Like a bank, or something? Yes. Do we need federal regulations on which they would operate? Yes, there should be some. Some states already have regulations.

Phil asked Paul Lewis if he had any thoughts on the American Bar Association and their activities lately regarding digital signatures? Paul said they had a committee that was very active several years ago. They provided some substantial input to the states by way of a model code for digital signatures. The states had taken some diverse conclusions to the whole idea of digital signatures and the process both conceptually and philologically. There may be more than one major approach to the whole idea of digital signatures and how they are to work at the state level.

**ACTION ITEM:** Phil said we will have an agenda item for next meeting to update the American Bar Association activity in the digital signature arena. Connie German was asked to research their web site. Paul said he could probably find some time to look into it.

A question was asked of Lauren Wood, at Kansas City, about going commercial with a certificate authority and what regulations would be required. What happens if Verisign goes bankrupt? Lauren said he did not have an answer for that. There is a certain guarantee having a certificate authority for the public in a place like the United States Postal Service facilities. You are pretty much guaranteed they are not going to go bankrupt. There would be a smooth transition from one postmaster to the next. Utah has financial responsibility requirements that pretty much forced the signature authorities to be somebody like a bank, which had some real assurance of longevity.

Phil asked Chicago if they had any updates. They responded that currently there is training going on. They have personnel in CH from Headquarters doing the Entrust training overview. Hopefully, some folks will get up and running pretty quickly. Do not know of any applications being developed.

Phil asked Savannah River if they had anything else to add. They had a question concerning the crypto modules. FIPS 140-1 is followed for PKI, and we have to have complainant software with FIPS requirements. Is that the same as with the digital signatures? Phil said yes.

The next meeting is scheduled for April 18<sup>th</sup>. We would appreciate any comments or ideas for the agenda. We would also like volunteers for presentations.

Phil said he wanted to keep the meeting monthly for the present. There may be a time when DISIWG would only need to meet bi-monthly. This can be decided later. Phil thanked all those who participated.