Technical Issues in Phase 1[1]

Web-based Submission of the Discharge Monitoring Report[2]

EPA Contract #68-W5-0030[3]

Delivery Order #0004

Revised August 31, 1999

1 Scope 3

2 Phase 1 Technical Issues Identified 3

2.1 Technical Issues Related to the Receiving Web Site 3

2.1.1 Time out for General Electric 3

2.1.2 Accessed Denied when IP Address Switching was Detected 3

2.1.3 Comments, Signing Official and Date Fields Not Stored 4

2.1.4 DMR Parameter Lines Not Sorted as Participants Expected 4

2.1.5 Tab Order was Top to Bottom rather than Left to Right 4

2.2 Accessing the Certificate Authority Through Firewalls 4

[1] Deliverable 6.3, Information Dynamics, Inc.

[2] A field test in the State of New York of the digital signing and submission of the Discharge Monitoring Report using an Adobe Acrobat Exchange plug-in to a Web browser as the electronic form environment which is connected interactively across the Internet to a receiving Web site. Cryptographic and handwritten biometric digital signatures are evaluated in this pilot.

[3] Submission of Environmental Data Under the Taiwan-USEPA Technical Cooperation Agreement

2.3 Problems Related to SSL 4

2.3.1 Loading Long Adobe Forms with SSL Enabled 4

2.3.2 Verifying Signatures with SSL Enabled 5

2.4 Problems Related to Applying the Digital Signature 5

2.4.1 CAPI Error when Attempting to Sign 5

2.5 Problems Related to Using the Smart Card 5

2.5.1 Smart Card Disabled after Incorrect PIN was Entered 5

2.5.2 Smart Card Must be Inserted before Web browser is Launched 6

2.6 Hardware and Software Installation Issues 6

2.6.1 CDs Could Not be Read 6

2.6.2 Graphics Acceleration and Screen Scrolling Speed Needed to be Changed after Smart Card Installation 6

2.6.3 Smart Card Drivers needed update to prevent blue screen on shutdown 6

2.6.4 Wrong Version of CTL3D32.DLL 6

3 E-mail Messages Related to Phase 1 Technical Issues 8

3.1 Saving Comment Pages and Signature Name & Date Fields 8

3.2 Blank Form when Adobe Acrobat Exchange is Opened for the First Time 9

3.3 Server Timeouts 11

3.4 Alternate Registration Procedure using a Web Browser 13

3.5 Use of Smart Cards for LRA Access Control and Signing 18

3.6 Problem Loading Form Data with SSL Enabled 21

3.7 Signature Verification Problem with SSL Enabled 23

3.8 Microsoft Smart Card Library Update for Shutdown Problem . 27

3.9 Wrong Version of CTL3D32.DLL 29

1 Scope

This document lists the technical issues identified in Phase 1 of a pilot test of the Web-based submission of the New York State Discharge Monitoring Report (DMR) conducted in the State of New York June – November, 1999, beginning with the installation of the pilot hardware and software components on the pilot participant's computers in June of 1999 and ending with the conclusion of Phase 1 in August of 1999. Technical issues identified prior to the involvement of the pilot participants in Phase 1 are discussed in the document, "In-house Test Results".

2 Phase 1 Technical Issues Identified

Technical issues identified in Phase 1 subsequent to the in-house testing period are described in the sections below. E-mail correspondence related to these technical issues is found in Appendix A.

2.1 Technical Issues Related to the Receiving Web Site

The following issues are related to the receiving Web site established for the DMR pilot.

2.1.1 Time out for General Electric

One of the pilot participants, General Electric, reported receiving time out errors when accessing the receiving Web site. Both the application server time out and the database server time out were increased.

2.1.2 Accessed Denied when IP Address Switching was Detected

One of the pilot participants, General Electric, reported being denied access to the Web site due to a security violation. A check of the Web site's application server log revealed that the IP address of the General Electric participant's computer appeared to be switching between two different IP addresses, which was detected as a security violation by the Web site's HAHTsite application

server. This behavior was speculated to occur because General Electric was using a load balancing router to divide outgoing network traffic among two or more firewalls. As a workaround to this problem, the HAHTsite application server was configured not to check for session hijacking.

2.1.3 Comments, Signing Official and Date Fields Not Stored

The comments, signing official and date fields were being stored for all pilot participants. This was traced to a programming error which only manifested itself when a DMR permit contained more than one discharge number, or when a form contained more than one page. This error was corrected in the customized application server code.

2.1.4 DMR Parameter Lines Not Sorted as Participants Expected

Some pilot participants reported that the order of the parameter lines within the DMR form deviated from what they had seen in the paper DMR forms. The order of the lines in the electronic DMR was determined by their order in the data set received from the New York State Department of Environmental Conservation which was used to pre-populate the forms.

2.1.5 Tab Order was Top to Bottom rather than Left to Right

Pilot participants preferred a tab order which progressed left to right across a parameter row rather than the default tab order within the Adobe Acrobat Exchange form. The tab order was reconfigured.

2.2 Accessing the Certificate Authority Through Firewalls

Three of the pilot participants (General Electric, Allied Signal and IBM) employed firewalls which blocked network access to the certificate authority server from the E-Lock certificate registration program installed on the pilot participant's computer. E-Lock Technologies provided an alternative registration process which uses an Internet Explorer 4.01 Web browser, since browsers can usually be configured to access external sites through firewalls.

2.3 Problems Related to SSL

The following issues are related to the use of Secure Sockets Layer (SSL) to encrypt network traffic between the Web browser and the Web server.

2.3.1 Loading Long Adobe Forms with SSL Enabled

When Secure Sockets Layer (SSL) was enabled between the pilot participant's Netscape Navigator 4.51 Web browser and the receiving Web site, DMR forms greater than one or two pages failed to load with pre-populated data received from the application server. This effect was not seen with Internet Explorer 4.01. To allow the longer DMR forms to load pre-populated data from the application server in the pilot, SSL was turned off after the pilot participants had successfully passed their login ID and password to the receiving Web site. The reduction in the number of DMR pages which could be loaded when SSL was used with Netscape Navigator may be related to the way in which Netscape Navigator handles the memory overhead required by SSL.

2.3.2 Verifying Signatures with SSL Enabled

The verification of digital signatures initially failed once SSL was enabled. An update of the digital signature verification component at the receiving Web site was required to verify digital signatures when the data transmissions between the Web browser and the Web server were encrypted with SSL.

2.4 Problems Related to Applying the Digital Signature

The following problem was observed by one pilot participant when attempting to digitally sign a completed DMR form.

2.4.1 CAPI Error when Attempting to Sign

The Village of Champlain reported an internal CAPI error when attempting to apply a cryptographic digital signature using the E-Lock digital signature plug-in. An attempt to re-register a new certificate in an attempt to reset the operating system's cryptographic service also failed. The pilot participant from the Village of Champlain did not feel that he had the time to continue to troubleshoot this problem.

2.5 Problems Related to Using the Smart Card

The following issues are related to the use of the smart cards by the pilot participants.

2.5.1 Smart Card Disabled after Incorrect PIN was Entered

One pilot participant from IBM established a four-digit PIN number to enable the use of his smart card, and then went on vacation. When he returned, he had forgotten the PIN. In attempting to guess the PIN, he disabled the smart card,

which only allows three incorrect PIN numbers. He was sent a new smart card via postal mail.

2.5.2 Smart Card Must be Inserted before Web browser is Launched

The client computer was observed to crash or lock up if the smart card is inserted after the Web browser is launched. Normal behavior of the smart card was observed if the smart card is always inserted before starting the Web browser.

2.6 Hardware and Software Installation Issues

The following issues are related to the installation of the hardware and software components by the pilot participants.

2.6.1 CDs Could Not be Read

Two pilot participants (Montgomery County Sanitation District No. 1 and Indeck Energy Systems) had difficulty reading the CDs required for installing the pilot software. Montgomery County had difficulty reading the read-write CDs which were not mass produced. Another computer on the network could read these CDs, however, and the required files were copied over the network. In the case of Indeck Energy Systems, it appeared that there was an intermittent problem with the CD drive on the computer. Retries ultimately allowed the installation to proceed to completion.

2.6.2 Graphics Acceleration and Screen Scrolling Speed Needed to be Changed after Smart Card Installation

In one case (the Village of Champlain) the pilot participant needed to reset the graphics card acceleration setting and screen scrolling speed to prevent lockups of the user interface when using a Web browser. This change was needed after installing the software for the smart card.

2.6.3 Smart Card Drivers Needed Update to Prevent Blue Screen on Shutdown

One pilot participant (General Electric) experienced a blue screen error upon shut down of the computer when the smart card reader was attached to the serial port of the computer. Updating the Microsoft smart card library solved this problem. This update was then applied for the other pilot participants.

2.6.4 Wrong Version of CTL3D32.DLL

One pilot participant (Allied Signal) experienced a warning message that the wrong version of the CTL3D32.DLL file existed on an NT computer after completing the DMR pilot installation of software components. Allied Signal was provided with an NT version of the CTL3D32.DLL to replace the Windows 95 version which was detected on the computer after the installation. It is not clear whether the Windows 95 version was installed by one of the DMR software components, or whether the incorrect version pre-existed on the computer.

Appendix A

3 E-mail Messages Related to Phase 1 Technical Issues

The following E-mail messages are related to technical issues which were identified in the Phase 1 of the DMR pilot and provide a sense of how these issues were experienced in the context of the pilot. These E-mail messages are not intended to be a comprehensive discussion of each issue from origin to resolution.

3.1 Saving Comment Pages and Signature Name & Date Fields

```
-----Original Message-----
From: Lewis, Todd
Sent: Wednesday, August 18, 1999 10:37 AM
To: 'Steve Vogler'
Cc: 'Meredith Streeter'; 'Chuck Haugh'; Liu, WeiShing; Yang,
AnPing
Subject: FW: DMR on the web


Steve, we checked on this problem after the telecon, but our
initial tests showed that comments could be saved.  With
this report from Rosendale, we created a duplicate of the
database for all of the pilot participants and were able to
find a problem which affected Rosendale, but not all pilot
participants.  When comments are submitted, programming at
the receiving Web site tries to identify the monitoring time
period which should be applied to the submitted comment.  To
do this, the start dates for all of the discharge numbers
(within the permit number and the selected stop date) are
scanned to determine the earliest start date.  When only one
discharge number is present in the permit (Rosendale's
case), the discharge number remained in a global variable,
and the submitted comment was processed as a discharge
report rather than as a comment.  The attempt to store the
comment as a discharge report was not accepted by the
database, which is why the Rosendale comments were not
stored.  This has been corrected for Rosendale and any other
pilot participants who may have been affected, and this
correction is now in production.
```

In the process, we were also able to discover why some participants reported that the signature name and date were not being saved. These data fields are saved in a separate table compared to other DMR data, and there was a problem storing signature name and date on DMR forms longer than one page. This problem has been corrected, and the correction is now in production. [In any case, the signature name and date can only be entered on the last DMR page, which explains why some pilot participants reported that these fields on DMR pages other than the last were not yellow in color.]

Thank you,

Todd
TLewis@idinc.com

-----Original Message-----
From: patricia marsh [mailto:h2oopr@cwixmail.com]
Sent: Friday, August 13, 1999 7:46 AM
To: mustreet@gw.dec.state.ny.us
Cc: sevogler@gw.dec.state.ny.us
Subject: DMR on the web

I have gone back and filled in the name and date information and resigned the forms. I then submitted them. I did this for most of the monitoring periods. Let me know if they came through.

I tried several times to submit comments. Each time, I lost all of the information. I tried saving it. I got a note saying the data had been saved, but it was not. I could not retrieve any of it. Since I do not type well, this became very frustrating.

Pat Marsh

Rosendale WWTF

3.2 Blank Form when Adobe Acrobat Exchange is Opened for the First Time

-----Original Message-----
From: Lewis, Todd

Sent: Wednesday, June 23, 1999 1:28 PM
To: 'Steve Vogler'
Cc: cshaugh@gw.dec.state.ny.us; Liu, WeiShing; Yang, AnPing; 'IDI-EPA
Distribution'
Subject: RE: Village of Champlain

Steve, this appears to be a memory management issue controlled by the operating system (e.g., Windows 95, 98 or NT) of the client (e.g., pilot participant's) computer. If the Adobe plug-in cannot allocate sufficient memory to process the display of the DMR form completely, then it will only display the form template (the blank DMR). We haven't determined whether this is because the Adobe Exchange plug-in is not sufficiently aggressive in attempting to obtain this required memory from the operating system, or whether the operating system is not doing a "garbage collect" frequently enough to release memory which may have been previously used by other applications. We have seen this behavior only occasionally on some computers.

The workaround is to use the back button on the browser to return to the page where the DMR forms are selected, close Adobe Acrobat Exchange (by clicking on the X in the upper right-hand corner of the Adobe Exchange window), and then select the DMR form again from the Web page. When the Adobe Exchange plug-in opens for the second time (since the last restart of the client computer or use of a memory-intensive application), it appears that the operating system will have detected the previous attempt to allocate memory and will have automatically performed a memory clean-up operation which will allow the Adobe Exchange plug-in to allocate sufficient memory the second time it is opened. Then the entire DMR (template + data) should be visible.

This problem should only occur the very first time the Adobe Exchange plug-in is opened, and should go away on the second and subsequent uses until the computer is restarted (or a major application is run on the client computer while the Adobe Exchange plug-in is closed).

Please see if this holds true for Champlain.

Thank you,

Todd

TLewis@idinc.com

-----Original Message-----
From: Steve Vogler [mailto:sevogler@gw.dec.state.ny.us]
Sent: Wednesday, June 23, 1999 12:53 PM
To: TLewis@idinc.com
Cc: cshaugh@gw.dec.state.ny.us
Subject: Village of Champlain

Hi Todd; I got a call from Bob Jewell and he claims that when he pulls up a DMR to fill out there is no pre-populated information on the form (just a blank DMR). I tried to walk him thru the steps and he seems to be doing everything correctly. I logged in using Champlain's ID and everything looked O.K. to me (all the information was pre-populated) Is this possible?

Thanks
Steve

3.3 Server Timeouts

-----Original Message-----

From:	Lewis, Todd
Sent:	Wednesday, June 23, 1999 1:12 PM
To:	'Steve Vogler'
Cc:	'Chuck Haugh'; Liu, WeiShing; Yang, AnPing
Subject:	FW: Time out.

Steve, our server log indicates that, yes, more than one hour had passed between the time Glenn logged in (11:36:54) and the time the application server timed out (12:38:49). Evidently the one-hour timeout is still too short. It will be increased to three hours sometime today once we see that the current active users have logged off or have timed out. However, with this longer timeout there is the danger that all 25 connections to the application server will be used up if you, Nick, Meredith, Chuck and the pilot participants don't use the logout tab to log out of the site after finishing a session.

Thank you,

Todd
TLewis@idinc.com

-----Original Message-----
From: Liu, WeiShing
Sent: Wednesday, June 23, 1999 12:58 PM
To: Lewis, Todd
Cc: Yang, AnPing
Subject: Time out.

Todd,

23 Jun 1999 11:36:54 Info: A new instance of \Current\Current.htx is being started with StateId TgYkX6Lskj6nbHHM04s8esYsIz.

23 Jun 1999 12:38:49 Info: The application with StateId TgYkX6Lskj6nbHHM04s8esYsIz timed out due to inactivity: Elapsed Time: 3715 Run Time: 0.200 CPU Time: 0.050 Pages: 1

It's over one hour of time limit between two pages.

Weishing Liu

-----Original Message-----
From: Lewis, Todd
Sent: Wednesday, June 23, 1999 1:01 PM
To: 'Steve Vogler'
Cc: cshaugh@gw.dec.state.ny.us
Subject: RE: Internet Security and Form Submission Prototype

Steve, I'm glad the alternative registration process worked. Yes, the message Glenn received is an error message from the application server which processes the submission request. Glenn had this timeout problem when we were all at General Electric to help him with the first install. We increased the timeout setting to one-hour and haven't noticed any further problem with the other participants until now, although it is possible that this timeout is still too short once the participants begin to spend time filling out their DMRs completely. It is necessary to set a timeout to handle the possibility that the pilot participants forget to log out of the site (with the logout tab), and the application server used for the pilot has a license for only 25 simultaneous connections. The server needs to know to disconnect them after a reasonable time. The application server measures this time starting from the log in (when the user ID and password is entered). Is it possible that more than an hour passed between the time Glenn initially login in and the time he submitted the completed DMR? [If so, then we can try increasing the timeout to 2 hours. If not, then we need to look elsewhere for an explanation.]

Thank you,

Todd

TLewis@idinc.com

-----Original Message-----
From: Steve Vogler [**mailto:sevogler@gw.dec.state.ny.us**]
Sent: Wednesday, June 23, 1999 12:42 PM
To: TLewis@idinc.com
Cc: cshaugh@gw.dec.state.ny.us
Subject: Internet Security and Form Submission Prototype

Hi Todd; I have been working with Glenn Swalm (GE) this morning using the Alternative Certificate Registration Process. He was able to register and successfully create the key. The problem he had was when he filled out a DMR, signed it and tried to submit it he got the following error messages.

Error message:
HAHTsite 3.1 webapps Server reports the following:

The requested application has timed out. Please restart the application by browsing to its hor

HAHTsite 3.1 webapps Server reports the following Error:

The application page HS_JScript_Header for StateId TgYkX6Lskj6nbHHM04s8esYsIz could no be run: The StateId is not authorized for this client address.

Is this a problem with the server ?

Thanks
Steve

3.4 Alternate Registration Procedure using a Web Browser

```
-----Original Message-----
From: Lewis, Todd
Sent: Tuesday, June 22, 1999 11:41 AM
To: 'Jayant Sane'
Cc: 'IDI-EPA Distribution'
Subject: FW: Alternative Certificate Registration Process
for Allied Signal and General Electric


Jayant, here is a copy of the announcement from the New York
State Department of Environmental Conservation which was
sent to Allied Signal and General Electric.
```

Thank you,

Todd
TLewis@idinc.com

-----Original Message-----
From: Steve Vogler [mailto:sevogler@gw.dec.state.ny.us]
Sent: Tuesday, June 22, 1999 9:07 AM
To: charles.divine@alliedsignal.com; glenn.swalm@ps.ge.com
Cc: cshaugh@gw.dec.state.ny.us; TLewis@idinc.com
Subject: Alternative Certificate Registration Process for Allied Signal and General Electric

Good morning; E-LOCK has provided a way through the firewall to complete the enrollment and also to register. The url to enroll is https://epa-ca.e-lock.com/Enroll/ and the url to register is https://epa-ca.e-lock.com/elock/ELockEnroll1/ . Please let me know when you are going to try the enrollment so that E-LOCK can monitor the server for any problems.

My phone number is 457-0828.
Thanks
Steve

-----Original Message-----
From: Lewis, Todd
Sent: Monday, June 21, 1999 2:19 PM
To: 'Steve Vogler'
Cc: 'Chuck Haugh'
Subject: FW: Alternative Certificate Registration Process for Allied
Signal and General Electric

Steve, E-Lock has provided a way through the firewall for Allied Signal, General Electric, and possibly also IBM (which has a socks-based firewall) in order to complete their registrations. Has anyone tried it yet? If not, do you know when they will (because E-Lock would like a heads up so that they can monitor the server for any problems during this time).

Thank you,

Todd

TLewis@idinc.com

-----Original Message-----
From: Jayant Sane [mailto:jayant@eLock.com]
Sent: Friday, June 18, 1999 6:58 PM
To: Lewis, Todd
Cc: 'IDI-EPA Distribution'; 'Steve Vogler'; 'Chuck Haugh'
Subject: RE: Alternative Certificate Registration Process for Allied Signal and General Electric

Just being curious. Did anybody get to try this alternate registration mechanism?

When you (whoever) plans to use it, pl let us know in advance. So in case of any problems or unforseen eventualities we will know if it is our problem or anything else.

Regards,
-Jayant

-----Original Message-----
From: Jayant Sane [mailto:jayant@eLock.com]
Sent: Thursday, June 17, 1999 5:17 PM
To: Lewis, Todd; 'Ray Langford'
Cc: 'IDI-EPA Distribution'; 'Steve Vogler'; 'Chuck Haugh'
Subject: RE: Alternative Certificate Registration Process for Allied Signal and General Electric

Hi Todd,

We have completed the browser based method for registering certificates. Participants desiring to register using this method can connect to the following url (using IE browser): http://epa-ca.e-Lock.com/eLock/ELockEnroll1

The page expects the one-time access code supplied during user enrollment. Ensure that the smart card do not have any keys/certificates before proceeding.

Notes:
1. As mentioned earlier, this method currently is available only thru IE 4.0 or higher browser.

2. The page currently expects access code for creating signature key/certificate. So should not be used to obtain exchange keys/certificates (administrators should continue to use "Register with PkiServer" application).

Regards,
-Jayant

-----Original Message-----
From: Lewis, Todd
Sent: Thursday, June 10, 1999 4:46 PM
To: 'Jayant Sane'; 'Ray Langford'
Cc: 'IDI-EPA Distribution'; 'Dr. Prakash Ambegaonkar'; 'Chris O'Connor';
'Steve Vogler'; 'Chuck Haugh'
Subject: RE: Alternative Certificate Registration Process for Allied Signal and General Electric

Jayant, this approach seems promising to me, since browsers at both Allied Signal and General Electric were already configured (or alternatively the firewalls were configured) to allow the browsers to access external Web sites at URLs beginning with https:\\. Since IE 4.01 SP2 is required for the pilot anyway to install the necessary cryptographic component updates to Windows 95 and Windows NT, then all the pilot participants would have access to IE 4.01 SP2 for the purpose of completing a registration. [For general production, I would hope you could eventually find a way to also use Netscape Navigator 4.5x and above for this purpose, but, in order to get through the registration step for people who are currently blocked by a firewall, IE 4.01 SP2 would be sufficient for the pilot.]

Thank you,

Todd
TLewis@idinc.com

-----Original Message-----
From: Jayant Sane [mailto:jayant@eLock.com]
Sent: Thursday, June 10, 1999 2:45 PM
To: Lewis, Todd; 'Ray Langford'
Cc: 'IDI-EPA Distribution'; 'Dr. Prakash Ambegaonkar'; 'Chris O'Connor';
'Steve Vogler'; 'Chuck Haugh'

Subject: RE: Alternative Certificate Registration Process for Allied Signal and General Electric

Todd,

Given our understanding that the browsers, the way they are configured, in GE and/or Allied Signal are able to pass thru their respective firewalls, even with SSL traffic, we feel there is a potential for doing the certificate requisition/registration using web browser -- the process of getting the certificate after having obtained the access-code (instead of PkiClient/Register with PkiServer application).

However, the registration process would be limited/restricted to IE 4.0 onwards browser only. Also since this was not part of the original specs/functionality we have not tested it yet though think to be a viable option.

Pl let me know your thoughts about it.

-Jayant

-----Original Message-----
From: Lewis, Todd [mailto:TLewis@idinc.com]
Sent: Thursday, June 10, 1999 12:24 PM
To: 'Jayant Sane'; 'Ray Langford'
Cc: 'IDI-EPA Distribution'; 'Dr. Prakash Ambegaonkar'; 'Chris O'Connor';
'Steve Vogler'; 'Chuck Haugh'
Subject: Alternative Certificate Registration Process for Allied Signal and General Electric

Jayant & Ray, I don't have an update from the New York State Department of Environmental Conservation concerning any progress made by the DMR pilot participants located at either Allied Signal or General Electric on reaching the E-Lock CA server through their respective corporate firewalls for the purpose of completing their key registration and certificate creation. This probably means that the people in these two companies who are participating in the pilot have not yet received a response from their internal IT departments to their requests to obtain access to the CA server.

Suppose that this situation remains unresolved well into next week. This implies to me that, in a production environment, a design which requires the E-Lock registration (PKI Client) application to make a connection to the E-Lock CA server to add the public key to the identity information in the certificate template (and therefore create a complete certificate), won't be easily implemented by individual departments and programs within a large company that has a firewall and also has a strict, deny-based security policy with respect to new client-server dialogs, even if these dialogs are based on a high-level HTTP or HTTPS protocol. [Obviously this would be a less important consideration if the whole company (e.g., all of General Electric or Allied Signal) were to make a strategic, comprehensive decision to deploy this PKI technology throughout the company. In this case, the IT department would be responding to planned, high priority requirements from top management rather than an isolated, ad hoc request of an individual or department within the company. In the real world, however, the introduction of new technology often begins with an individual or small internal group experimenting with a new idea, achieving a level of success and then expanding the implementation incrementally within their organization. The fact that the E-Lock registration process is blocked by firewalls in two out of the seven companies participating in the DMR pilot is, in my opinion, a warning that finding a flexible way to accommodate these firewall restrictions may play a significant role in the ability to introduce this type of PKI implementation "from the ground up" within larger companies.]

For the purposes of the pilot, to accommodate these two companies (Allied Signal and General Electric), would it be possible to conceive of an alternative method of forming the completed certificate (i.e., an alternative registration process) which may have different PKI security policy implications but which would nevertheless allow the DMR pilot participants located within Allied Signal and General Electric to make it through the registration process and go on to the remainder of the pilot activities?

Thank you,

Todd
TLewis@idinc.com

3.5 Use of Smart Cards for LRA Access Control and Signing

-----Original Message-----
From: Lewis, Todd
Sent: Tuesday, June 22, 1999 11:26 AM
To: 'Nick Onderdonk-Milne'
Cc: 'Steve Vogler'
Subject: RE: Gemsafe

Nick, please read the E-mail I sent to Steve (which I have copied into the body of this message below). You will need to use a separate smart card (available in Chuck Haugh's office) to authenticate your browser to the certificate authority Web server for the purpose of accessing the Local Registration Authority administrative console, and be sure that the smart card you are attempting to register doesn't already have a pre-existing key pair. You will receive an error like the one you report if the smart card already has a key pair before you begin the registration process. The access code supplied in the E-mail to Steve (below) is for registering the smart card you will use to access the LRA administrative console. The smart card in the box I gave you can be used for signing DMRs after being registered with the access code you receive as a result of the enrollment process.

It is possible that the registration procedure will fail occasionally if a connection to the certificate authority server cannot be established at exactly the time you attempt the registration. If this occurs, you will need to reinitialize, and then release, the smart card using the GemSAFE Card Details Tool before attempting the registration process again. (Steve knows how to do this.)

Thank you,

Todd
TLewis@idinc.com

-----Original Message-----
From: Lewis, Todd
Sent: Thursday, June 17, 1999 3:56 PM
To: 'Steve Vogler'

Cc: cshaugh@gw.dec.state.ny.us; 'IDI-EPA Distribution'; Liu, WeiShing;
Yang, AnPing
Subject: RE: E-LOCK Administrators

Steve, since Nick presumably was successful in completing the install of all of the dependent components (e.g., browser updates, Adobe, GemSAFE, smartcard, and E-Lock client) he has all that he needs right now to do the Admin function. The Admin install won't add anything more that is necessary to accomplish this. The Admin program, if used, will place an icon under the "e-Lock ATS for EPA" folder which is just a shortcut to a URL on whatever browser is set as the default. Since Netscape is probably the default browser, and IE should be used for the Admin function (because IE will display all the LRA administrative console screens correctly), installing the Admin program really doesn't help in this case.

In order to access the Local Registration Authority administrative console to perform the Admin function, Nick will need to register as a Local Registration Authority administrator. To do this, he will need to use two smart cards -- one which will allow him to access the LRA administrative console, and another which will allow him to sign DMR forms. If Nick has already gone through the enrollment and registration process for signing DMRs, then you need to take a pencil and mark the smart card which has been used for this purpose "sign". [If Nick hasn't enrolled and registered his smart card, then mark this smart card, "sign" anyway to reserve it for this future use.] Chuck Haugh has two extra smart cards in his office. Take one of the extra smart cards and mark this smart card "admin".

Place the "admin" smart card in Nick's smart card reader. Use the low-level GemSAFE card details tools utility to verify that this smart card does not contain an existing key (it shouldn't unless it has been used already). Be sure to release the smart card. Then start the "Register with PKI Server" application in the "e-Lock ATS for EPA" folder. For the one-time PIN use: 001B3FFEBC7225B11D38731004033260

The above one-time PIN (access code) is valid until you successfully complete the registration process. After the registration process is complete, this one-time PIN (access code) has no further meaning or use.

After you have achieved a successful registration of the "admin" smart card (and with the "admin" smart card still inserted in the smart card reader), open the Internet Explorer 4.01 browser on Nick's computer and go to the following URL:

https://epa-ca.e-Lock.com/eLock/EpaLra

Nick's IE browser should then produce a window asking if the certificate shown should be presented to the server (using wording which expresses this intent). Do what it takes to say the equivalent of "yes" (e.g., OK, Next, Finish, Yes, or some other synonym). Then Nick should be able to see the LRA administrative console on his computer and be able to do what June is doing as an LRA administrator.

Remember to ask Nick to use Internet Explorer when doing LRA admin functions, and be sure to place the "admin" smart card in the smart card reader. When Nick is signing DMRs, he should use the Netscape browser and place the "sign" smart card in the smart card reader. [Note: If Nick completes the registration of the "admin" smart card before he completes the registration of the "sign" smart card, be sure that he places the "sign" smart card in his smart card reader when registering to sign DMRs.]

If Nick uses the GemSAFE Card Details Tool utility to change the user PIN on one or both of this smart cards, remind him that the PIN number is specific to the smart card he is using (e.g., don't use the PIN for the "admin" smart card on the "sign" smart card and vice versa.

Todd
TLewis@idinc.com

-----Original Message-----
From: Nick Onderdonk-Milne
[mailto:nlonderd@gw.dec.state.ny.us]
Sent: Tuesday, June 22, 1999 10:45 AM
To: TLEWIS@IDINC.Com
Subject: Gemsafe

I am having trouble registering the admin card. Please call me @ 518-485-8781 or send me your number so I could call you. The error I get is Error unknown (code 80090023)

3.6 Problem Loading Form Data with SSL Enabled

-----Original Message-----

From: Lewis, Todd
Sent: Tuesday, June 08, 1999 4:09 PM
To: 'Steve Vogler'
Cc: 'Chuck Haugh'; 'IDI-EPA Distribution'; 'Kimberly Nelson'; 'Kimberly Nelson (Yahoo)'; Liu, WeiShing; Yang, AnPing
Subject: FW: Champlain Install (Viewing DMRs)

Steve, as of Tuesday afternoon, June 8, we are able to load, sign and submit one- two- and three-page DMR forms using Netscape Navigator 4.51. Please use the User IDs and passwords for the various pilot participants to test the loading of the DMR forms from your computer to confirm this result in your own experience. The following changes were made in the pilot configuration to achieve this result:

1) Secure Socket Layer was turned off when loading the DMR forms. [There was an unexpected interaction between Secure Socket Layer, Netscape Navigator and the Adobe Exchange Form which reduced the amount of pre-populated data which could be received by the browser and/or form from the server. This interaction was not seen with Internet Explorer (but Internet Explorer introduces the problem of creating multiple open windows when used with Adobe Exchange 3.01 and HAHTsite, so Netscape Navigator is still the preferred browser for this reason).]

2) A "public space" memory setting in the HAHTsite application server was increased to 12MB. [This improved the size of DMR form which could be resubmitted a second, third and subsequent time.]

[An unrelated problem signing the DMR which was observed in the test on Chuck Haugh's laptop at NYS DEC on June 4 was traced to the need to update the E-Lock signature verification application on the server to verify signatures if a Secure Socket Layer (SSL) connection was used. This signature verification program was updated to allow signature verification in the presence of SSL. Signatures then did verify properly. However, because of the effect of SSL upon the ability of DMR forms to load when the Netscape browser is used, SSL was turned off when DMR forms are loaded from the server.]

As a result of the above configuration changes made at the receiving Web site (https://discovery.idinc.com/current/), Allied Signal, the Montgomery County Sanitary District 1, Champlain, and Rosendale (all of which have DMRs with two or three pages) should now be able to load their DMR forms. [General Electric and Indeck Energy Systems have exclusively one-page DMR forms and therefore were unaffected by this problem.] The 3-page DMR in the NYSDEC test data set should also load. [General Electric and Allied Signal will not be able to complete their certificate registration process until they are able to grant access to the

certificate authority server through their firewall and/or border routers. Is there any update from either General Electric or Allied Signal related to the status of the requests the pilot participants have made to their IT support to allow this access?]

Thank you,

Todd
TLewis@idinc.com

-----Original Message-----

From: Lewis, Todd
Sent: Friday, June 04, 1999 5:24 PM
To: 'Steve Vogler'
Cc: 'Chuck Haugh'; 'IDI-EPA Distribution'
Subject: Champlain Install (Viewing DMRs)

Steve, the current (June 4) status of viewing DMRs is that DMRs greater than one page won't complete their load into the Netscape browser for subsequent display by the Adobe Exchange plug-in. Champlain has a 3-page DMR and Rosendale has a 2-page DMR, so a problem similar to what occurred at Montgomery County Sanitary District 1 will occur in Champlain and Rosendale on your next install if nothing changes between now (Friday, June 4) and when you go to the site next week.

This problem is Netscape-specific. Internet Explorer 4.01 will load and display the forms correctly. The downside of using Internet Explorer with Adobe Exchange 3.01 is that each new Web page and Exchange form opens in a new window, and these new windows don't work properly after their first use. The workaround is to be sure to close all but the original Internet Explorer window as well as the Adobe Exchange window before doing anything for a second time. To switch from Netscape to Internet Explorer you will need to change the Adobe Exchange Weblink setting (File->Preferences->Weblink) to the location of the Internet Explorer executable and add a Content_Type (MIME) setting of application/vnd.fdf for the File Type=Adobe Acrobat Forms Document in Windows Explorer->Tools->Options->File Types. We had done this together during the May 5-7 installs, but please let me know if you need more detailed instructions.

This issue is being worked aggressively and there may be another status update before you go out to Champlain and Rosendale next week.

Thank you,

Todd
TLewis@idinc.com

3.7 Signature Verification Problem with SSL Enabled

-----Original Message-----
From: Ray Langford [mailto:ray@elock.com]
Sent: Wednesday, June 09, 1999 11:20 AM
To: Lewis, Todd; 'Manisha'
Cc: IDI-EPA Distribution; Liu, WeiShing; Yang, AnPing
Subject: Re: Digital Signatures and SSL (FIXED)

----- Original Message -----
From: Lewis, Todd <TLewis@idinc.com>
To: 'Manisha' <manisha@fcpl.co.in>; Ray Langford <Ray@elock.com>
Cc: IDI-EPA Distribution <idi-epa@elock.com>; Liu, WeiShing <WLiu@idinc.com>; Yang, AnPing <AYang@idinc.com>
Sent: Tuesday, June 08, 1999 6:08 PM
Subject: RE: Digital Signatures and SSL (FIXED)

Manisha, thank you for updating the server verification DLL to handle https. [Why does changing the transport impact the way the signature is verified?]

Manisha & Ray, in my original E-mail on this subject (below), I noticed that an additional window from Gemplus opens asking for a PIN number a second time when the submit button on the form is pressed. This appears to be related to a setting within Netscape Navigator (Communicator->Tools->Security Info->Cryptographic Modules->GemSAFE->View/Edit->Disable). If the GemSAFE cryptographic module is disabled within Netscape, then the PIN window does not appear when the submit button is pressed.

→ Todd,
The GemPlus install may have detected Communicator and installed a driver for it when it installed. When the submit button is pressed, Communicator may be getting some indication that the GemPlus card is active which may cause it to query the card causing the second PIN request dialog. To prevent this, as you pointed out, this driver should be disabled in Communicator so that it doesn't use or know about the presence of the GemPlus Smartcard.

There also appears to be a strong and unexpected relationship between the presence of SSL and the ability of Netscape 4.51 (or 4.6) and Adobe Exchange 3.01 to complete the loading of the FDF datastream and display the DMR form. Fewer pages can be displayed when SSL is enabled in Netscape. Increasing the public space within the HAHTsite application server appears to increase the number of pages which can be displayed, especially when a DMR form is selected to be resubmitted to the server. Do you have any idea why SSL would

play a role in how many pages of the DMR form can be displayed? Does SSL generate a large memory overhead for the Netscape browser?

→ I would expect pages and forms secured in an SSL channel to incur additional overhead for the cryptographic operations and for the browser to special case the page/form data. The browser will perform a number of steps in an attempt to keep the data from an SSL connection separate from non-secured pages. This may include handling the page cache differently, maintaining info about and monitoring URLs to warn when moving from secured to non-secured pages, etc. When E-Lock Technologies (actually Frontier Technologies) developed our own browser with SSL support a number of years ago, there was additional overhead required to support an SSL connection. How large this overhead would be in Internet Explorer or Communicator, I suspect only the browser developers at Microsoft or Netscape would know.
Thank you.
-- Ray

Thank you,

Todd
TLewis@idinc.com

-----Original Message-----
From: Manisha [**mailto:manisha@fcpl.co.in**]
Sent: Monday, June 07, 1999 10:40 AM
To: Lewis, Todd; Ray Langford
Cc: IDI-EPA Distribution; Liu, WeiShing; Yang, AnPing
Subject: Re: Digital Signatures and SSL (FIXED)

Hi Todd,
Looks Like you haven't got my mail to Weishing couple of hours back .. Here it is again.
There was a problem On the server end in ETIPDFVERF.DLL . It wasn't designed to handle https. Attached is the fixed ETIPDFVERF.DLL.

Hi Weishing,

1. I have reproduced the problem with the https as you have mentioned below:

2. https - failed. "The form was not Signed before submitting!!" message from client naxdmr_ETI_VerifySignature.

On the serverside in the ETIPDFVERF.DLL we were parsing the URL only for

http and not for https. We have fixed this problem. I am attaching the ETIPDFVERF.DLL . Please replace the current ETIPDFVERF.DLL on discovery with this one. Make sure you are replacing the file in correct place i.e from where it is registered.

Attached is the Fixed ETIPDFVERF.DLL.

2. I have moved my testing server Caeser to have SSL enabled. But for some URL's (dynamic pages) I am still getting the URL as http://...
Please send me a step by step procedure for making my
http://caeser.fcpl.co.in/epadmr/ site SSL enabled.
Then you can also test with Caeser once I make it SSL enabled.

Let me know the status of testing with discovery with https.

With regards
Manisha

-----Original Message-----
From: Lewis, Todd
Sent: Saturday, June 05, 1999 11:07 AM
To: Ray Langford; Manisha Tidke
Cc: IDI-EPA Distribution; Liu, WeiShing; Yang, AnPing
Subject: Digital Signatures and SSL

Ray & Manisha, on Friday (June 4) WeiShing collected some evidence that digital signatures work when the client is connecting to an http:// site without SSL, but produce an error (informing the signer that the form was submitted without being signed) if the form is submitted while connected to an https:// site with SSL. It is too early to confirm whether SSL is the critical variable, but, if it is, then this result surprised me. I would have thought that SSL would be a lower-level transport process which would not interact with the functionality of creating and verifying signatures.

However, in a test which I did on Friday afternoon using a Windows 95 laptop connected to the Internet via a 28 Kb/sec dial-up line before I left the New York State Department of Environmental Conservation (NYS DEC), I did see evidence of either corruption of the client environment or an attempt by the browser (Netscape Navigator 4.51) to access the smart card when sending the FDF data stream to the server when the Submit button on the form was pressed.

I selected a one-page DMR form (a one page Adobe Exchange form representing a Discharge Monitoring Report with pre-populated data) while connected to the https://discovery.idinc.com/current/ site using SSL. I did not enter any new

data into the DMR form. I pressed the E-Lock signature icon on the form, selected a certificate in the resulting dialog box, and pressed the OK button. The Gemplus software then displayed a window asking for the PIN number of the smart card. When I entered the PIN number of the smart card, the Gemplus and E-Lock windows closed and a check mark appeared on the E-Lock signature icon on the form. I then pressed the Submit button on the form. Before the browser sent the FDF data stream to the server, the Gemplus software displayed a window asking for the PIN number (an unexpected event). I typed in the PIN number for the smart card for the second time in this scenario. Then the Gemplus window closed and the browser sent the FDF data stream to the server. Then an HTML page appeared notifying me that I had submitted the form without signing it.

I received the same error (the form was submitted without being signed) on the same machine and DMR form using Internet Explorer 4.01 SP2, but I would have to go through this sequence again to confirm whether the PIN number window appeared a second time using IE 4.01 SP2.

Does this result mean that the browser is confusing the purpose of the smart card when SSL is used (e.g., attempting to use the smart card for SSL cryptography rather than for signing)? Or is SSL creating memory overhead which is corrupting the environment needed by the E-Lock plug-in to complete the signature? Or is something else happening?

Thank you,

Todd
TLewis@idinc.com

3.8 Microsoft Smart Card Library Update for Shutdown Problem

```
-----Original Message-----
From: Lewis, Todd
Sent: Wednesday, June 02, 1999 5:27 PM
To: 'Steve Vogler'
Cc: 'IDI-EPA Distribution'
Subject: FW: GemSAFE/Todd Lewis/GemSAFE-PC/SC Issues/ID Inc.


Steve, Gemplus has provided a utility (see attachment) which
they have asked us to run to help fix the reported shutdown
problem when the smart card reader is attached.  Would you
```

please run this utility on your computer and reply with the results?

Thank you,

Todd
TLewis@idinc.com

-----Original Message-----
From: Mark.Weaver@gemplus.com
[mailto:Mark.Weaver@gemplus.com]
Sent: Wednesday, June 02, 1999 8:50 AM
To: tlewis@idinc.com
Subject: GemSAFE/Todd Lewis/GemSAFE-PC/SC Issues/ID Inc.

Hello Todd,

I received your request from Market Support and I just wanted to follow up on this. I have made a request to the GemSAFE Product Team that I am a part of and I will provide you with further information when I receive it.

This from what I understand looks like a possible PC/SC issue. Attached you will find smclimb.exe which is a executable tool that may fix some of the issues that you are facing. Please run this program and advise me on the status of your inquiry.

If you have any other questions please advise and I will assist you.

Regards,

Mark T. Weaver
Product Support Engineering
(Hotline-NORAM)

INFORMATION AUTOMATIC VIRUS CHECK (GEMPLUS) No virus known.

-----Original Message-----
From: Lewis, Todd

Sent: Wednesday, June 02, 1999 7:05 AM
To: 'Gemplus Technical Support'
Subject: Shutdown and Dial-up Problems When Using GemSAFE 1.0 Domestic

Dear Friends, we are supporting the U. S. Environmental Protection Agency's pilot on submitting environmental compliance reports over the Internet from companies in the State of New York. On one computer, we experience an unexpected shutdown problem (a blue screen). All computers in the pilot have IE 4.0, Netscape 4.51, Adobe Acrobat Exchange 3.01, GemSAFE 1.0 Domestic, and E-Lock Assured Transactions (ATS 2.1) installed. The Gemplus smart card reader included in the GemSAFE 1.0 Domestic kit is attached to an available serial port and to the keyboard port of the computer. Another device (e.g., modem, label printer, graphics tablet, etc.) may be connected to another available serial port on the computer.

The computer which shuts down with a blue screen is a recent model Dell desktop and has the Gemplus smart card reader installed on COM2 and a label printer installed on COM1. We have been able to show that the blue screen which appears at shut down only appears when the Gemplus smart card reader is physically attached, and will always appear upon shut down if the computer has been booted up with the Gemplus smart card reader attached. This will occur even if the smart card reader is not used in any way, and if no other software applications are used between start up and shut down.

On other computers, we have seen the message "Netscape Navigator has performed an illegal operation" upon shutdown when the Gemplus smart card reader is attached. On an IBM ThinkPad 770, we have seen that the Windows 95 dialup feature doesn't work normally with the Gemplus smart card reader attached. In these latter cases, we have not yet done all the tests needed to isolate the Gemplus smart card reader as the only factor. I am including these observations because they may be related to the blue screen on shutdown which was conclusively isolated to the presence of the Gemplus smart card reader. All current tests were done under Windows 95, release B.

Are you aware of the occurrence of a behavior which is the same or similar to what we have experienced when the Gemplus smart card is physically attached to a computer where GemSAFE 1.0 Domestic software is used? Do we need to upgrade the Gemplus software or drivers?

Thank you,

Todd Lewis
TLewis@idinc.com

3.9 Wrong Version of CTL3D32.DLL

-----Original Message-----
From: Lewis, Todd
Sent: Wednesday, June 09, 1999 2:56 PM
To: 'Steve Vogler'
Cc: cshaugh@gw.dec.state.ny.us; Liu, WeiShing; Yang, AnPing; 'IDI-EPA
Distribution'; 'Allen Klumpp'
Subject: RE: Allied Signal problems (CTL3D32.DLL)

Steve, the file about which Windows NT is complaining is a Windows 3D control and is used to give a 3D chiseled effect, typically to background screens within applications. If this is the first time that this error has appeared on the Allied Signal NT computer, then one of the installs (I don't know which one) probably overwrote the original NT version of this Windows 3D control with a Windows 95 version of this control. [It is possible that the question, "Setup has found a version of CTL3D32.DLL on your computer. Do you want to overwrite CTL3D32.DLL?" appeared during the installation process at Allied Signal, but I didn't notice this message myself. I have, however, seen similar questions appear from time to time during the install process, but not on all computers, because not all computers would have a version of this DLL which is different from the one which would be installed by one of the setup programs.] The fix is to replace the Windows 95 version of CTL3D32.DLL with the NT version of CTL3D32.DLL. The following URL explains how to do this and gives some background on this problem: http://www.ticnet.com/chuckw/ctl3d.htm This site primarily addresses the reverse problem (a Windows NT CTL3D32.DLL installed on a Windows 95 computer) but the Web page does contain a small note for NT users:

NT users: If you're having a similar problem, try this file.
Some background info on the problem and its solution
Read a sampling of mail from visitors

After receiving "this file" from the hyperlink on the Web page, you may need to rename it to CTL3D32.DLL before placing it in the %root drive%:\winnt\system32 directory.

Note: Allied Signal should be able to see their DMR now, given the changes which were made yesterday afternoon (June 8). Is this not the case? Can you see the Allied Signal DMR from your computer?

Thank you,

Todd
TLewis@idinc.com

-----Original Message-----
From: Steve Vogler [mailto:sevogler@gw.dec.state.ny.us]
Sent: Wednesday, June 09, 1999 1:43 PM
To: TLewis@idinc.com
Cc: cshaugh@gw.dec.state.ny.us
Subject: Allied Signal problems

Hi Todd; Allied is still getting the following error message when they tried to look at a blank DMR form

" This application uses CTL3D32.DLL, which is not the correct version. This version of CTL3D32.DLL is designed only for Win32s or Windows 95 systems." They are using Windows NT. Do you think the smclib.exe file fix would correct this ?

Thanks
Steve